

A Complete Guide For Information Gathering by Maltego

By Berat TUNA

What is Maltego?

Maltego is software that used for open-source intelligence and forensics, developed by Paterva from Pretoria, South Africa. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining. As of 2019, the team of Maltego Technologies headquartered in Munich, Germany has taken responsibility for all global customer-facing operations.

Maltego permits creating custom entities, allowing it to represent any type of information in addition to the basic entity types which are part of the software. The basic focus of the application is analyzing real-world relationships (Social Networks, OSINT APIs, Self-hosted Private Data and Computer Networks Nodes) between people, groups, Webpages, domains, networks, internet infrastructure, and social media affiliations. Maltego extends its data reach with integrations from various data partners. Among its data sources are DNS records, whois records, search engines, social networking services, various APIs and various meta data.



Creators of Maltego(Left to Right): Andrew MacPherson, Chris Bohme, Andy Farrel

Where is maltego used?

Basically, maltego is used for **OSINT**, OSINT is (Open Source Intelligence) means every piece of information that can legally be gathered from any free or public sources about an individual or organization.

In Cybersecurity fields, Hacker or attacker collects every information about the target before attacking it. Information like IP addresses, Phone numbers, Names of employees, every little information is important for the attacker. He collects every information of the target system which is available for free and open-source on the internet and then creates a plan about attacking the system.

Maltego fits into the the exciting new realm of Big Data and Data Science. This is the field that enables us to find and make connections from all the data that is now available on the Internet and social networking sites. These include Twitter, Facebook, LinkedIn, Instagram and many others. If we can gather that info and make sense of it, it will enable us to know more about our target making exploits and social engineering more likely to be successful!

Besides hackers and information security engineers, Maltego and tools similar to Maltego, are used by the NSA and other governmental entities. In this way, they can track potential terrorists and other threats. For instance, if NSA finds a phone call from a person in the U.S. to a known terrorist in another country, they can then use Maltego or other tools to find that individual's many connections on the web. This can then lead to targeted surveillance of potential threats.

How to Use Maltego?

Most cyber security guards are using Kali linux and its derivatives (parrots etc ...)

They use maltego, which is easily found in offensive linux derivatives. But you can download it to ios, Windows, other linuxes too.

You can install maltego as any general software after installing it you have to create an account on maltego to login into application.

Maltego has 3 different packs-

1-community

2-Professionals

3-Enterprises

Community version is free to use and others are paid with more features.

Configure Maltego

STEPS

1. License Agreement

2. Login

3. Login Result

4. Install Transforms

5. Help Improve Maltego

6. Web Browser Options

7. Privacy Mode Options

8. Ready

LICENSE AGREEMENT: Please read and accept the following License Agreement.

General Terms and Conditions
for Software License Agreements of Paterva
(Effective 1 September 2020)


These General Terms and Conditions apply to all licenses (hereinafter referred to as "Software Licenses") of Software Products (hereinafter referred to as "Software") which are issued by Paterva (Pty) Ltd. (incorporated in South Africa under registration number 2008/005705/07), (hereinafter referred to as "Licensor") to its customers (hereinafter referred to as "Licensee") (Licensor and Licensee also referred to as "Party" and collectively the "Parties"). Software subject to these General Terms and Conditions is the intellectual property of the Licensor and/or Maltego Technologies GmbH, registered in the district court Munich, Germany under no. HRB 236523 ("Maltego"). To the extent that Software is owned by Maltego, the Licensor has sufficient rights to license same to the Licensee.

1. Contractual Object

1.1. These General Terms and Conditions govern the Software Licenses issued to the Licensee by the Licensor by way of a **Software License Agreement**. Sec. 3 specifies the scope of each Software License subscribed regarding the specific Software being licensed as well as the content, location, time and extent of the user rights.

1.2. The number of subscribed Software Licenses and the software components to which these Licenses refer are specified in the Electronic Delivery Document (sec. 2.2.) issued by the Licensor to the Licensee.

☐ Accept

 Please accept the License Agreement to continue

< Back

Next >

Finish

Cancel

Classic Login processes

Enter your details below to log in to the Maltego Community Server

Or if you have not done so yet, [register here](#)


Login

* Email Address

@gmail.com

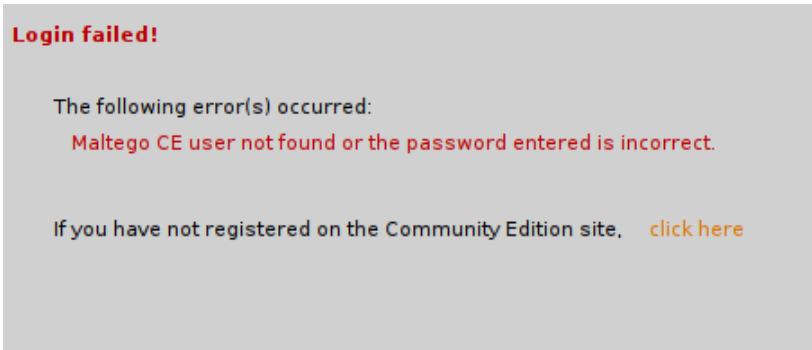
Password

.....

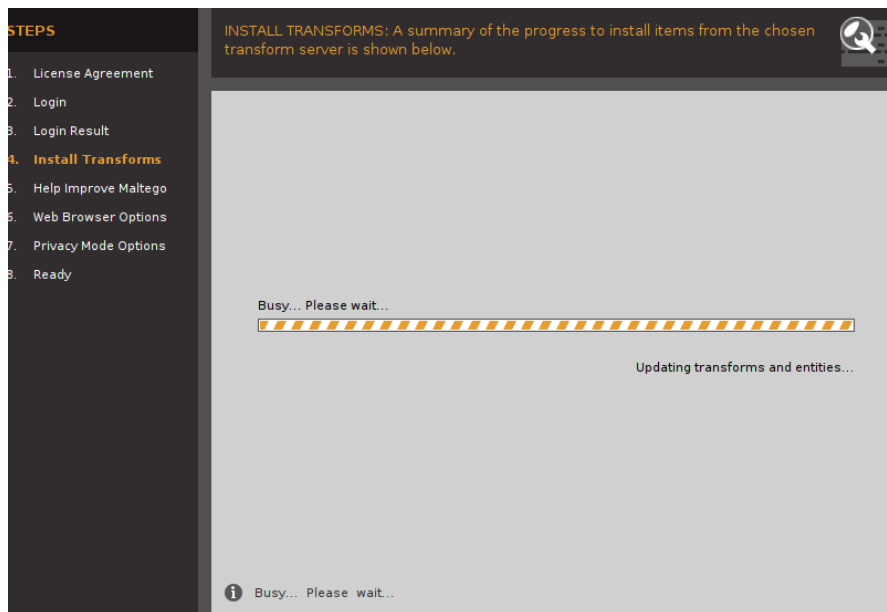


* Solve captcha

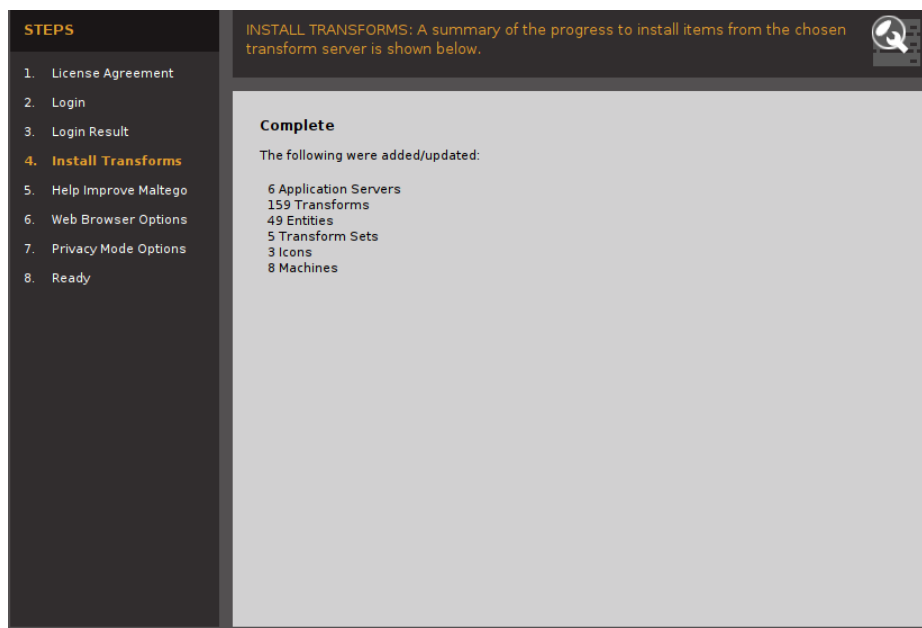
7820

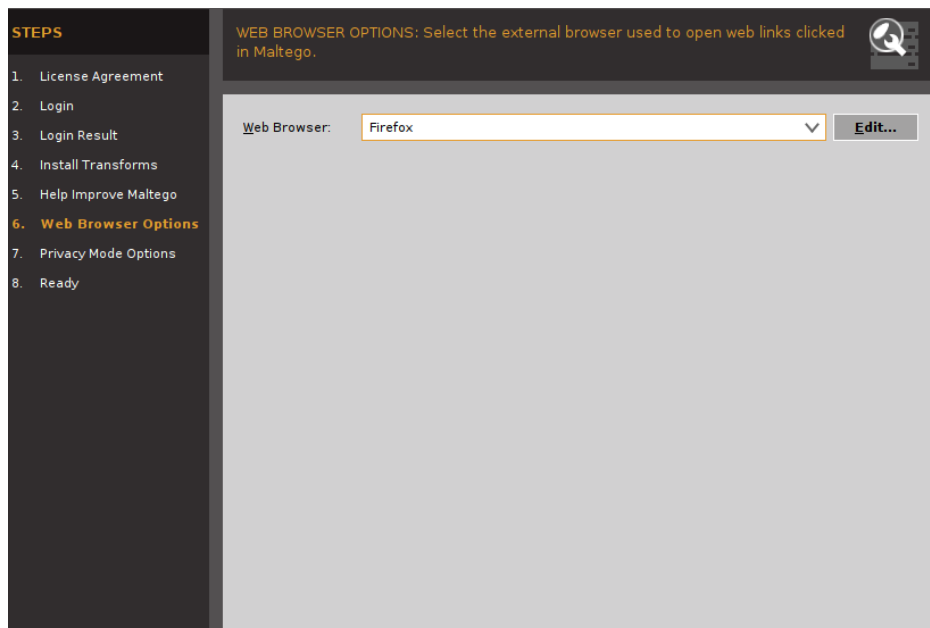


If you did not sing up click [here](#) and open a account.

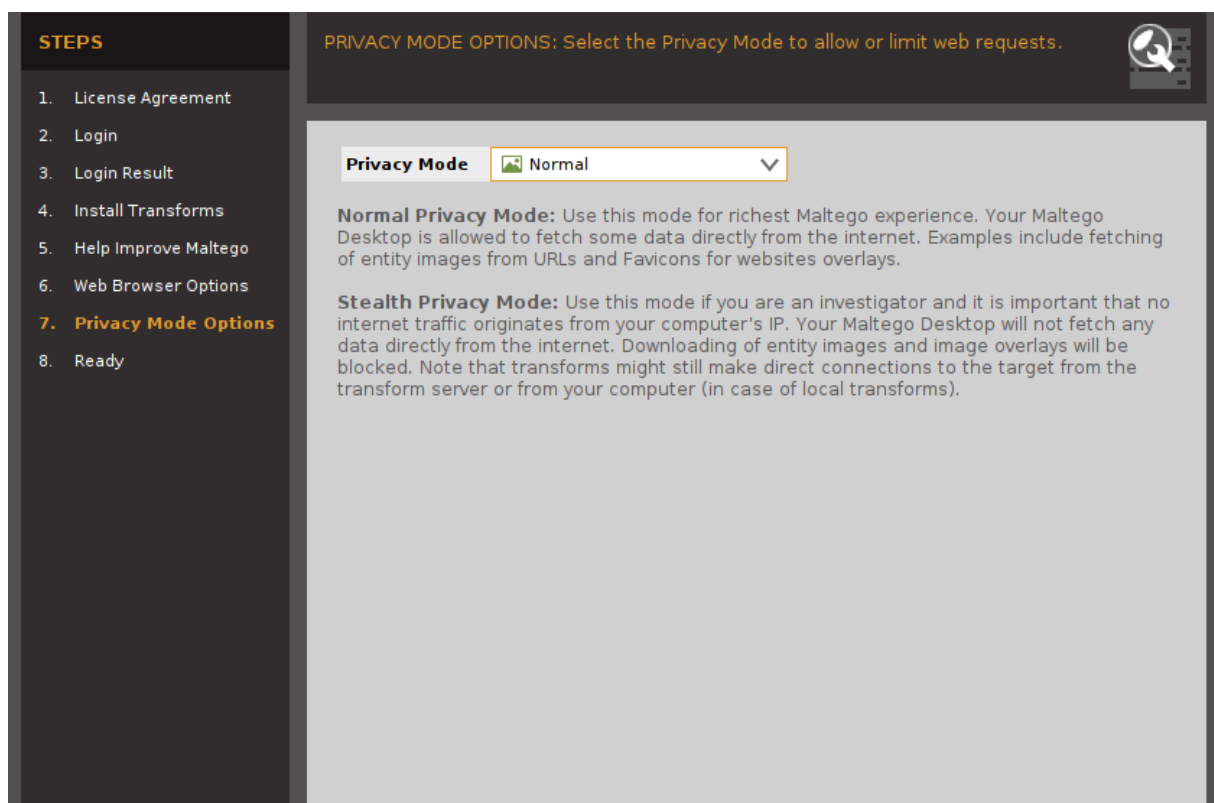


Installing tools for easier use

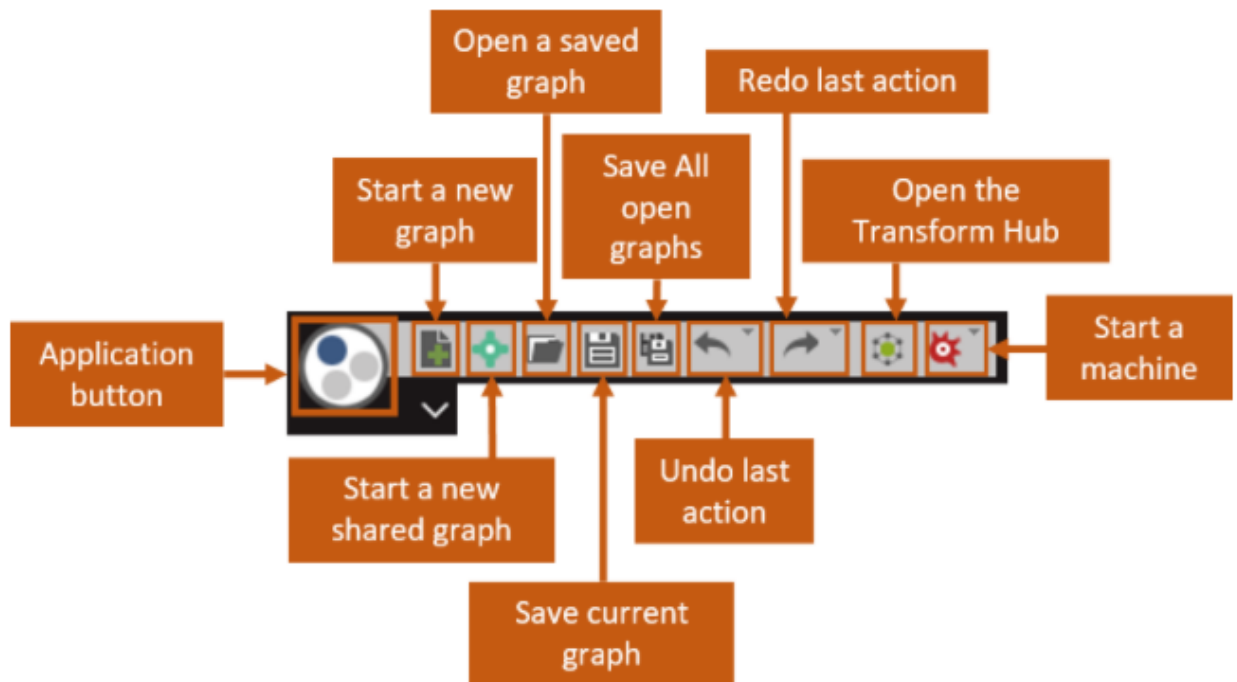


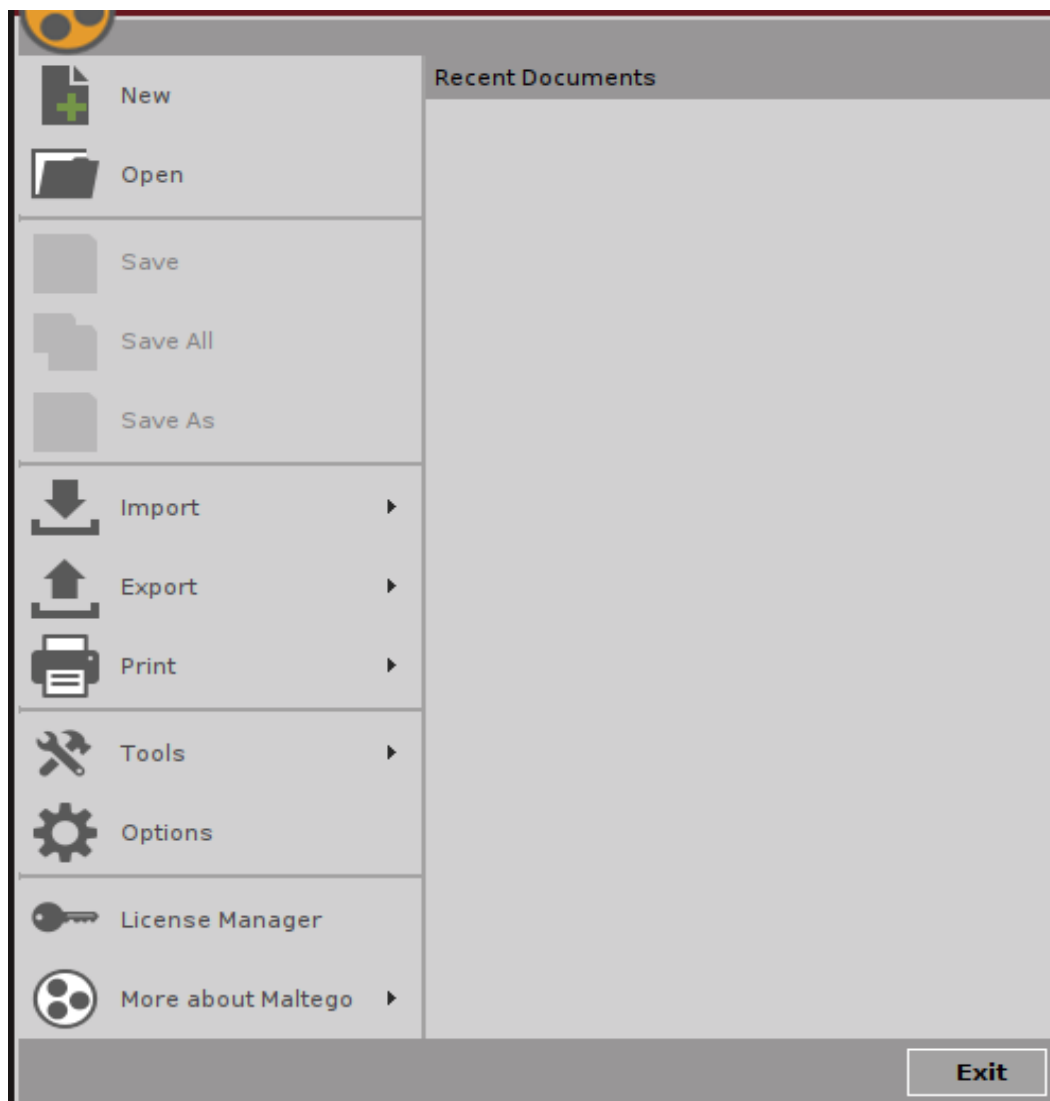


Choosing our browser: I choose Firefox because it comes default with KaliLinux you can change it if you use different Web Browser



When you open Maltego, you will find some keys in the upper left corner, let's see what these keys are for.





Click on New



This is how a Graph in Maltego looks like. Once you have created a new graph you will get a fresh page within a new tab, surrounded by a range of control windows.

Now just select the entity you want to perform OSINT on like some domain name or DNS system.

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 and a lot more...

Basically, you can gather information about all the things mentioned above. Just select an entity.

In this tutorial I will work on Domain

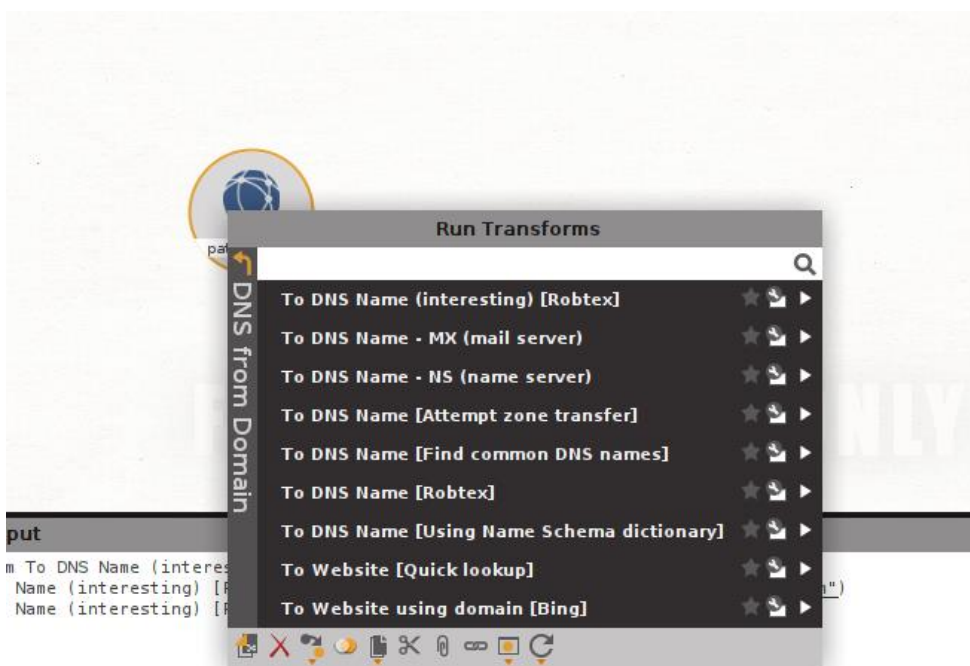


Drag the domain text and bring it to the blank paper

The part that written paterva is the place that we will work. enter the domain of the target site



After entering domain right click to domain logo then you will see a table like this.



All links has a purpose in their own way

Interesting robtex: Detailed Whois information and DNS records can be viewed on Robtex. It can provide a list of web pages running on an ip address. Whois information can be accessed on Ripe and Arin, two institutions that distribute real IP addresses.



Mx: This Transform determines if an MX record exists for the given Domain. The MX record is the mail exchanger record and is returned as an MX Record Entity. The IP address of this record gives a good indication of the network location of the target as most organizations keep their mail close to their network. This is normally used in the infrastructure foot printing of an organization. The IP Address of this record gives a good indication of the network location of the target as most organisations keep their mail close to their network. This is normally used in the infrastructure foot printing of an organisation.

.lenovo's mail has been stolen in 2015 by getting mx record dns and brute force.

<https://www.tripwire.com/state-of-security/security-data-protection/how-hackers-can-hijack-your-website-and-read-your-email-without-hacking-your-company/>

After using it



Ns: This transform determines if an NS record exists for the given Domain . The NS record is the name server record and is returned as a NS Record .This is normally used in the infrastructure footprinting of an organisation. A note of caution - it is not uncommon for organisations to unsource their name servers to their ISP or to the registrar of their domain. Thus - in terms of finding the network (e.g. resolving this to an IP address) of the target this has limited value - human inspection is advised.



Attempt zone Transfer: Turning off dns transfer does not mean that your subdomains of the domain name cannot be detected, the subdomain is detected with applications such as severe, dntalk, theharvester, but the method that will be 100% successful is the information to be obtained by dns transfer.

Find Common Dns Names: This Transform attempts to find the DNS Name on the specified Domain . This is done by testing a list of DNS Names and seeing if they exists. The list of names that are tested for can be configured inside the Transform. The default list contains the following names:

`www,mail,mx,ns,ftp,webmail,web,gateway,secure,intranet,extranet,smtp,pop` The specified domain is appended to the name and tested. If it exists it is returned as a DNS Name.



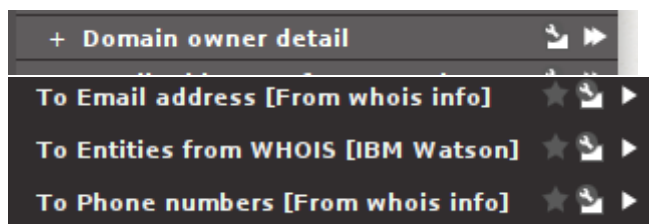
Classic Robtex: Looks for all dns's in database server



Using name schema dictionary: The Transform will try several word lists (think Lord of the Rings names, planet names, colours, TLDs etc.) as DNS names. If it finds a match in a specific word list it will try the entire word list. In this way it will try to determine the naming schema for the domain. Note that the transform can take a while to complete - especially when it finds a match in a long word list. The test depth per word list can be set in the transform. In the screen shot below we see how different TLDs exists inside the domain.



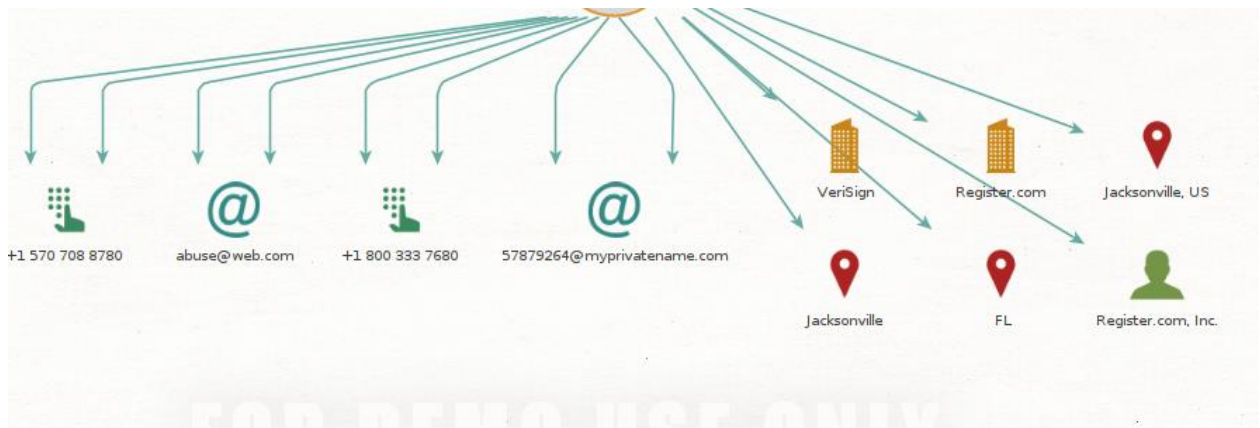
Let's take a look at Domain **Owner Details**: It is the favorite part of most cyber security professionals and social engineering phizards because it is the easiest part to manipulate people by using the numbers, information etc ... fake content. (Like the 2014 hollywood hack incident, only one man deceived celebrities by pretending to be an ios employee in that incident)



From whois info: This Transform performs a whois query on the supplied domain and parses the output for email addresses. The idea with the Transform is to provide the email address of the owner of the domain. The whois information itself is stored as a property of the domain (DomainWhois). You should always manually inspect this data to give context to results - or see if the parsing of the email address failed.

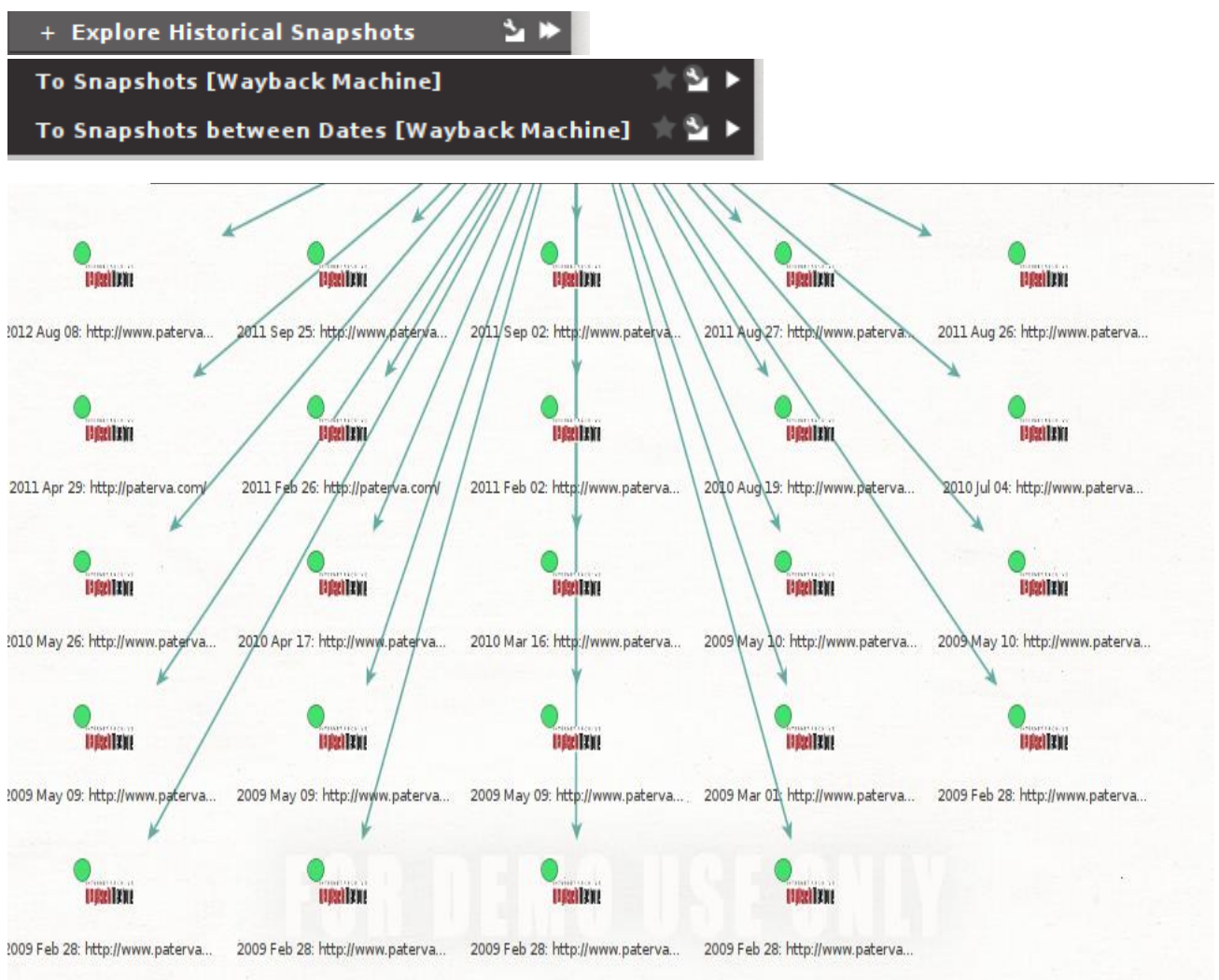
To Entities from WHOIS: This Transform obtains whois information of the domain then parses it for Entities using NER

To Phone numbers: This Transform will connect to the website where the URL (web page) is hosted, download the particular page / URL and parse it for phone numbers. Results are returned as phone number Entities. The Transform is useful when you are looking for results on a specific page, not an entire site.



As you can see a lot of detail and information for social engineering and phishing.

Explore Historical Snapshots: Shows the instant or over time status of the server, data sharing.



I searched for 2009-2015 you can change it viable options for you

One of the topics of 2009:

https://web.archive.org/web/20090228102537if_/http://www.paterva.com:80/forum/index.php?topic=115.msg250.

Domain To Files (Office)

This Transform will search for the locations of interesting documents (think Office[tm]) hosted on web sites inside the domain.

Domain To Files (Interesting)

This Transform will search for the locations of interesting files hosted on web sites inside the domain.

There are couple of Transforms that use search engines - all of them very similar. The basic recipe for these Transforms are as follows:

Expand the question. The question is the input from the GUI - be that a persons name, a domain or an phone number. When looking at a persons name for instance the name Kosie Kramer will be expanded to searches like Kosie Kramer, K Kramer, Kramer Kosie etc. In the case of a telephone number the search will be expanded to include most telephone notations used.

Assign confidence levels. Because a search for Kosie Kramer is more likely to return better results - rather than a search for KramerK, the confidence level for the first search would be higher. The confidence levels are also used to assign preference to certain file types when doing searches on documents (these are configurable in the Transform). In the same way a XLS file containing the word is likely more interesting than a PDF file.

Perform each search. The searches are performed and the snippets are obtained. It is important to note that only snippets are parsed. For parsing the entire page you need to dump to URL and process the URLs separately. Various search engines have various snippet lengths.

Parse for output Entities. Depending on what output is required the snippets are parsed for Entities - in some cases the web sites name is all that is required.

Calculate weight. The weigh is calculated from various factors - the confidence of the search, the frequency of the result, the importance of the web site where the result came from, and in some cases a correlation to the input.

Normalise. The weights are now normalised using a fairly interesting algorithm that involves the mean and standard deviation of the spread of weights. It is important to understand that a search result with a equal spread of weights are mostly useless.

Both are them suggested for Domain to

Single Image Analysis Using Reverse Image Search with TinEye in Maltego

What can u search by tinyeye?

Profiles, hastags, forums and communities

When it was posted

How it was altered

How social media audiences reacted

Why most of the cyber securists are using tinyeye technology over Google image search.

Essentials before begin

- Images must be accessible via URL
 - Local images are not currently supported

Sensitive images may be hosted on your own server and imported securely using a direct connection

Memetic Propagation Analysis

Maps the spread of an image through online communities

Ingredient Assets

Images and screenshots sourced from the Internet and assembled into memetic content

Ingredient Asset Retrieval

Involves finding original, unedited based images

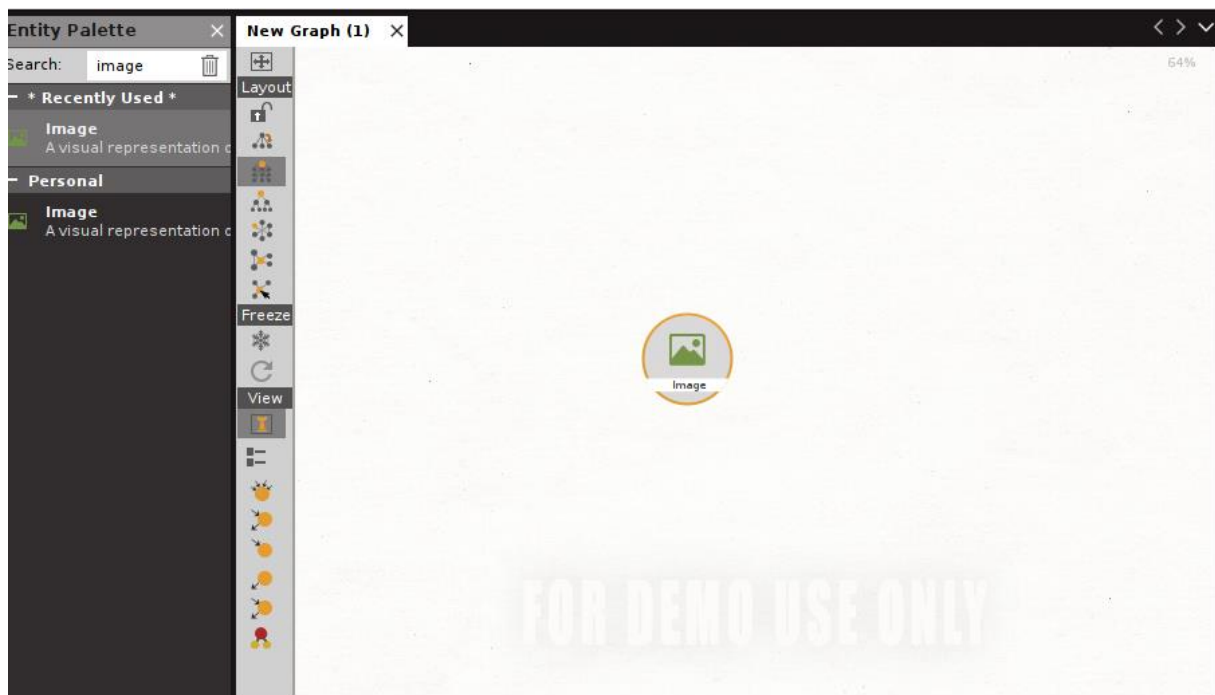
Source Retrieval

Involves finding the URL, article, or social media post where the ingredient asset was sourced from

Community Analysis

Contextualizes the hashtags, comment threads, social media groups, etc. where an image has been posted

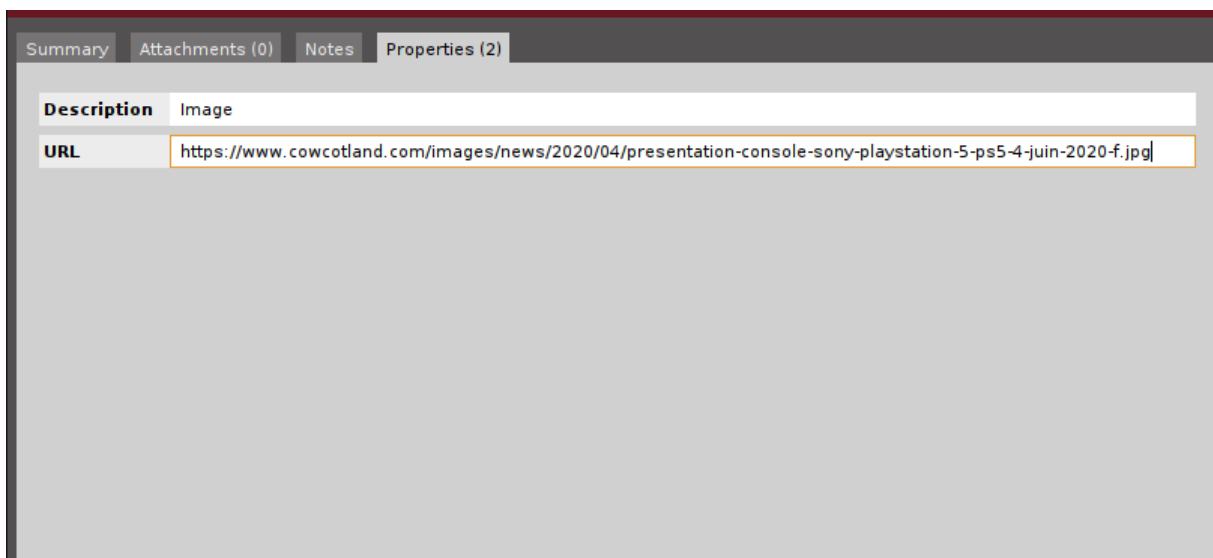
For our tutorial, copy the direct image URL attached to this training module, and paste it into the URL property field.



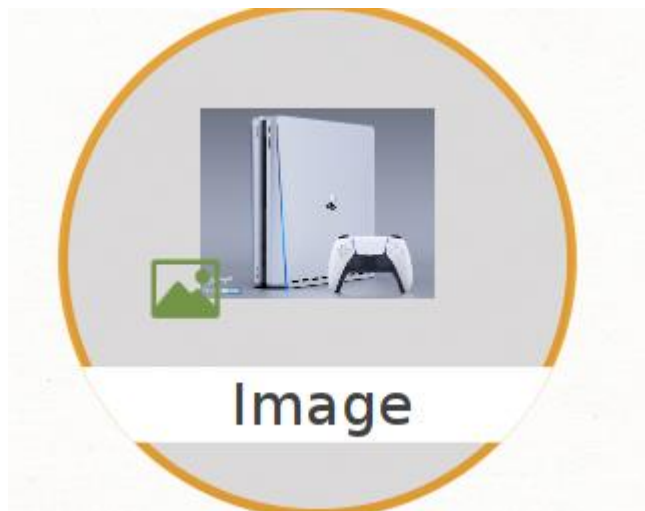
Double click to image



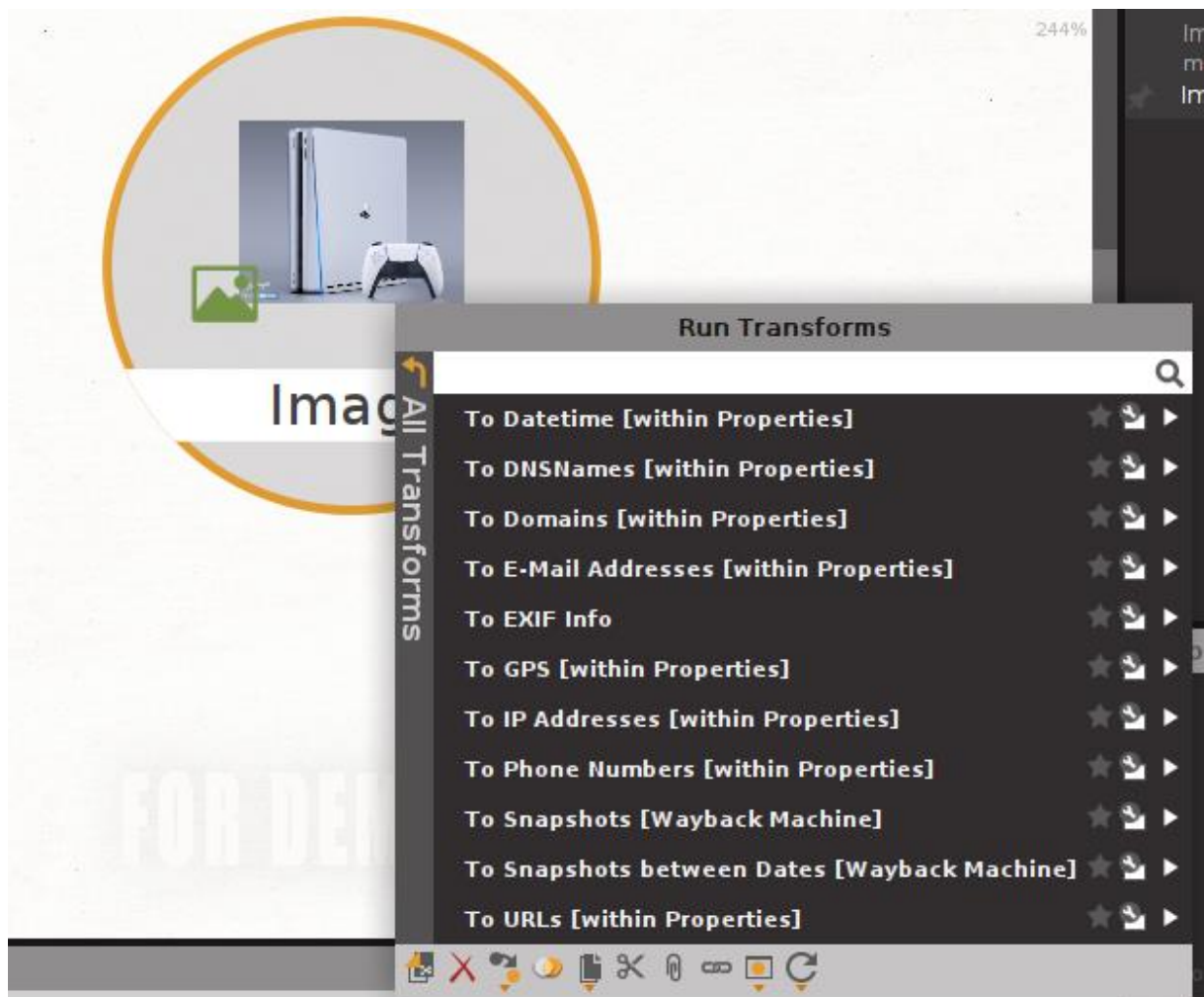
Copy its url than print it to properties-URL



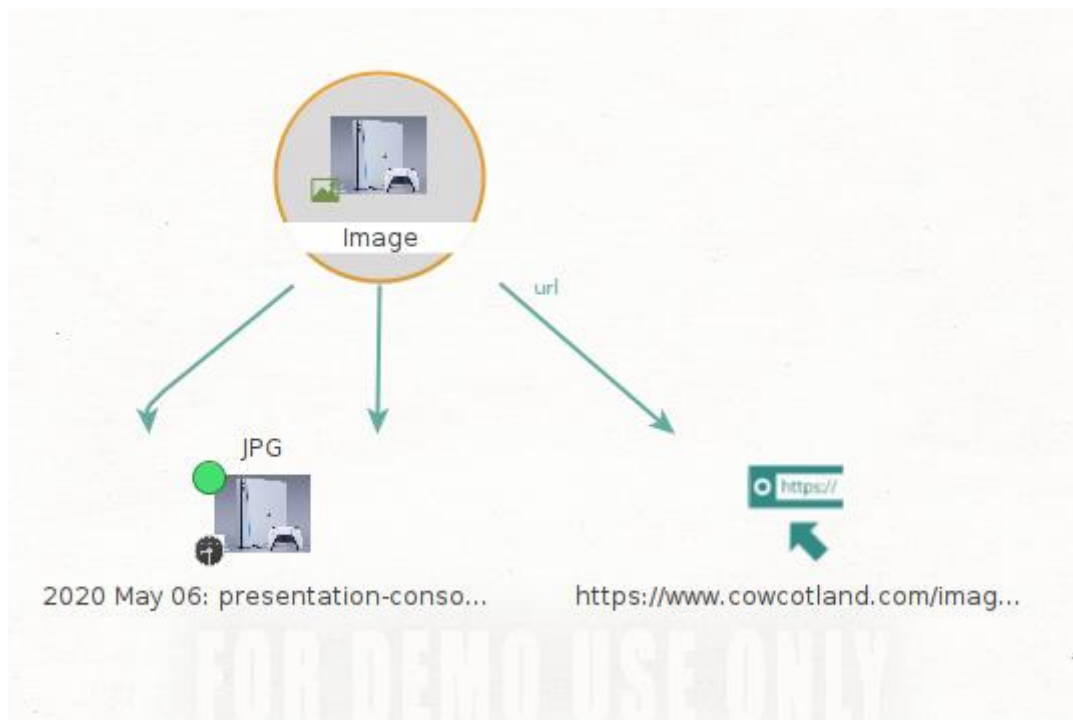
After implemmentation you will get this



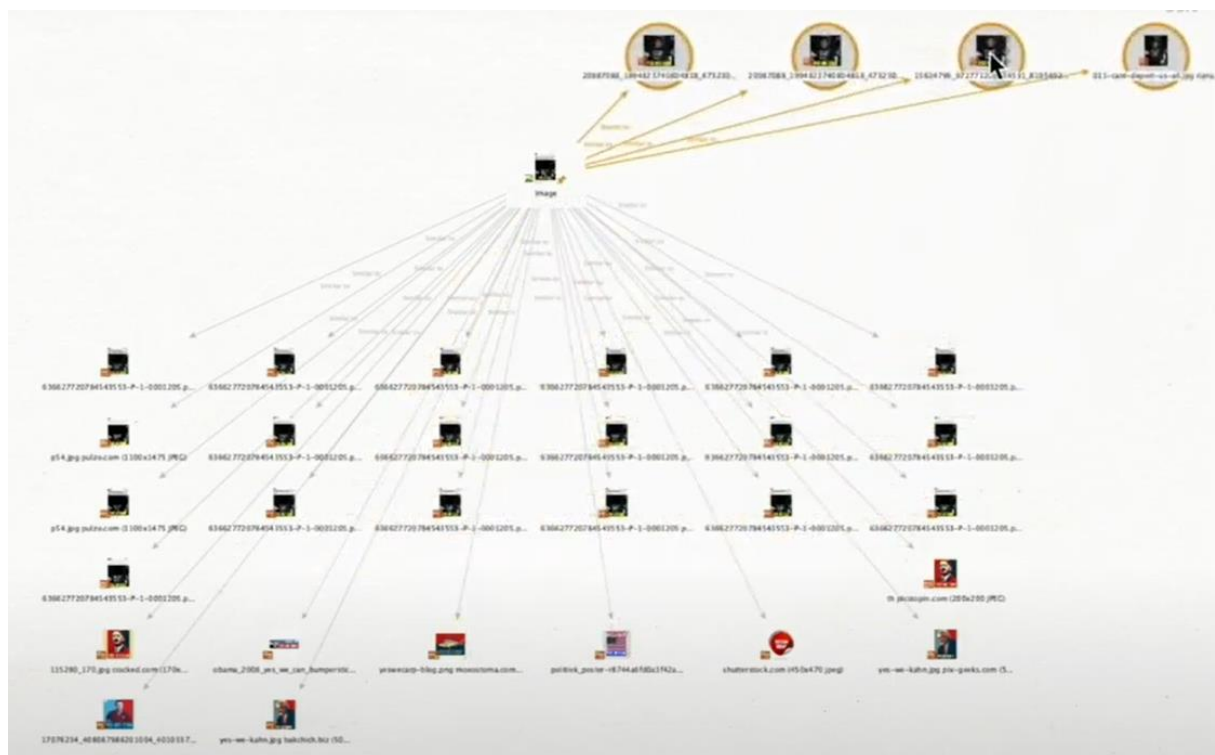
When you right click you will get the options like this:



After run all of them you will see similiar pictures, mail of sharer of content, how much time it is shared etc. In my work it was basically a playstation but some pictures lets you got more datas.



My data



An another user's data

Searching Someone's e-mail In Maltego

And we are at the last part of our work searching someone most of the phisers are uses that method for making social engineering but how they got our mails lets see

Example 1 – A phishing email Although it appears to be from O2, closer inspection, by right clicking or hovering over the name, shows the email address has been spoofed. For example, 'user123@o2-mail.com'. An official O2 email would come from '@o2.co.uk'.

This message was sent with High importance.

From: O2Billing
To: user123@o2-mail.com
Cc: user123@o2-mail.com
Subject: Your O2 bill is ready #1035346

The subject title is O2 (zero-two) not O2

Dear Customer

It is addressed generically, not to the customer by name

Your O2 bill for 28/05/14 is now ready. You can [look at your bill here](#).

In total, your bill for this month comes to £372,85. We'll request this amount from your chosen account on, or just after, the date in your bill.

To see your bill, you'll need the username and password you were given when you joined O2. If you've forgotten them, we can give you a [reminder](#).

Is your bill more than you were expecting?
If so, here's a few reasons why this might be:

- You could have gone over the minutes, texts or data that's in your allowance.
- You could have called or sent texts to numbers that can't be taken from your allowance such as International, 0800, 0845 numbers or directory enquiries.
- You have used your phone for calls, text or data whilst abroad.

Hovering over the link here will show that it will not take the user to O2's website, but to a completely unrelated website

To view any charges outside your allowance [click here](#)

A comma is used instead of a decimal point

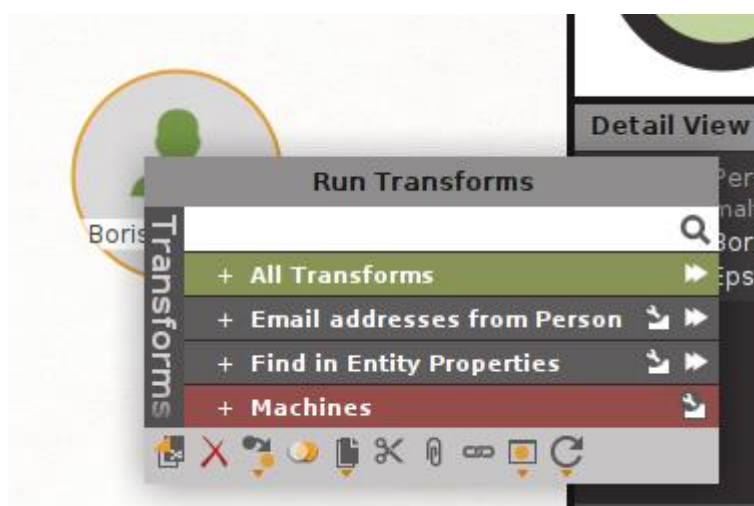
If you have any questions, just [ask Lucy](#). See our online virtual agent. You can also find out more about what's included in your bill with an [online demonstration](#).

By the time this email was sent, O2 has discontinued their 'Lucy' virtual assistant

Best regards
O2

This email is sent from Telefónica UK Limited. Registered office:
260 Bath Road, Slough, Berkshire, SL1 4DX. Registered number: 7270332.
Please do not reply.

My target will be Boris Epsheyn my first target was Ahmet Çakar a football commente but I could not find anything.



Click on email adresses from person

WARNING! DO NOT FORGET ADDING A SPACE FOR SEARCH!!!!!!

Required inputs ✕

The following transforms require inputs:

– To EmailAddress [Bing]


Domain/TLD (space=none)

Additional term (space=none)

☐ Remember

Run! **Cancel**

Than run it

 **Select email addresses**
Select relevant addresses you wish to continue with.

☐ ☒

The following results were returned	Type
<input type="checkbox"/> @info@boriserceg.com	Email Address
<input type="checkbox"/> @info@borisepshteyn.com	Email Address
<input type="checkbox"/> @info@boriserazo.com	Email Address
<input type="checkbox"/> @ceo@borisepsteindo.ca	Email Address
<input type="checkbox"/> @ceo@boriserceg.ca	Email Address
<input type="checkbox"/> @ceo@borisepshteyn.ca	Email Address
<input type="checkbox"/> @ceo@boriserufus.ca	Email Address
<input type="checkbox"/> @ceo@boriserazo.ca	Email Address
<input type="checkbox"/> @ceo@borisetc.ca	Email Address

All mails that includes directly him

Then our final form is

