PATERVA

Maltego Version 3 User Guide

Using the GUI

RT/AM/AvW

2011/01

Table of Contents

1 Introduction

Access to timely and accurate information has always played a big role in information systems security. This information is crucial to attack or defend a possible target. A large part of information gathering is making sure that you collect the right information. To attack a target you must know where the target is. A full frontal attack is not always the best idea; a better plan is to attack where security is at its weakest. To find a possible weak spot we need to know as much as possible about the target and anybody around the target with a trust relationship. We do this with proper reconnaissance and determining the Internet “footprint” of the target.

The problem that we have today is the vast amounts of information that is available. It is difficult for the human brain to see obscure links between seemingly unrelated data. It is however easy to see commonalities between pieces of information when displayed graphically. The solution is therefore a tool that can graphically display the links between pieces of data.

Maltego is an open source intelligence and forensics application. It offers you an amazing mining and gathering of information capability as well as the representation of this information in an easy to understand format. It can be used to map information regarding networks, organizations, people etcetera. Coupled with its graphing libraries, Maltego allows you to identify key relationships between information and identify previously unknown relationships between them. For example, it allows you to easily identify common infrastructure between Domain Naming System (DNS) names based on the resolution of addresses.

Maltego takes various bits of information (referred to as Entities within the application), and converts these (via code known as transforms) to other Entities. An example of this would be if you were to put a website Entity on a graph within Maltego with the value of ‘www.paterva.com’ and run the ‘To IP Address [DNS]’ transform. You would then notice that a new Entity, namely an IP Address with the value of 74.207.243.85 has been generated as a child of the original website Entity.

1.1 The concepts behind Maltego

Maltego uses a client/server architecture for the purposes of the data collection to determine the relationships and real world links between pieces of data especially Internet infrastructures such as:

- 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 can be linked using open source intelligence (when using the standard transforms). Maltego provides you with a graphical interface that makes seeing these relationships, instant and accurate and even making it possible to see hidden connections. 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, where Maltego can be adapted to your own, unique requirements.

The mapping of a network and understanding how everything fits together is an important step in getting to know a target. The process can be labour intensive and only some aspects can be automated successfully. Maltego tries to consolidate some of the required functions easily and accurately. Maltego provides accurate results that will also have been obtained when utilising other available tools and commands manually. Assuming a certain level of knowledge and experience, Maltego is easy to understand and utilise.

1.2 Client Requirements

1.2.1 Operating system

Maltego has been tested on Windows XP/Vista/7 and Linux (various distributions) as well as OSX. As Maltego is purely Java based it should work on almost any operating system. Because operating systems differ care has been taken to use an Install Shield for Windows and Linux (RPM,DEB,ZIP), a package(.dmg) for OSX and that takes of differences between these systems.

Bottom line: Maltego can be installed on all platforms.

1.2.2 Software requirements

Maltego uses Java version 6 (1.6 - at least update 10) which is available for most popular operating systems. Maltego will not function correctly with version 5 (1.5). The Maltego installer will not install or upgrade your system to Java 1.6, but this should be a painless procedure. The latest release of Java can be downloaded for your operating system at http://www.java.com/en/download/manual.jsp. This page also includes instructions for installing the software. As of version 3.0 of Maltego packages that includes the JVM can be downloaded.

Bottom line: You need Java 1.6 and you need to install it yourself unless you download a installer that already includes a JVM.

1.2.3 Hardware requirements

Maltego loves memory and raw CPU power. Rendering views take a lot of computing power and the slower your computer, the longer it will take. If your computer is under-powered this can become frustrating. If you plan to work on large graphs you'll also need some memory. Maltego version 3 is configured to use 1024MB (1GB) of RAM, but if that is all you have your OS and other apps will have nothing left to work with. We thus recommend at least 2GB of RAM, but the more the merrier. You also need a link to the Internet if you want to use the Paterva TAS (and for registration).

Almost all the data collection and processing happens on the server but the results still need to get to your computer. A fast Internet link makes Maltego work faster. Lastly, if you ever needed a reason to get a big screen you now have it. Maltego also loves big displays. Running it in 1024×768 just wouldn't feel right – but you can do it if you really have to.

Bottom line: Minimum (yuk): 2GB RAM, 2GHz, 64Kb Internet access, 1024×768 display.

Recommended (yummy): 8GB RAM, Intel I7, 1Mb+ Internet access, 1920×1080 display.

1.3 Server Requirements

1.3.1 Operating System

Maltego server is delivered as a VMWare image allowing you to run your Maltego server on practically anything that supports VMWare or a virtual machine system that can 'play' VMWare images. As such any operating system capable of running a virtual machine system can be used.

1.3.2 Software

As specified above the only software needed to run the Maltego VMWare images is a virtual machine 'player', we recommend VMWare workstation or server.

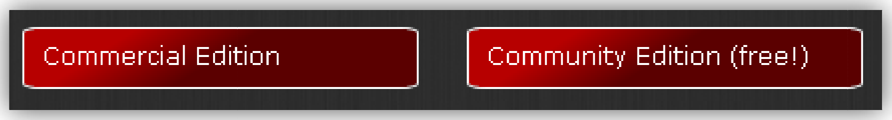
1.3.3 Hardware

- Miminum: 2GB RAM, 2GHz CPU, 1Mb Internet access
- Recommended: 4GB RAM, Intel I7, >4Mb Internet access

2 Installing the Maltego 3 Client

2.1 Download installation files

The first thing that you need to do is to decide which edition of Maltego 3 you need, the commercial edition or the community edition (CE).



2.2 The commercial edition vs. the community edition

The community edition has the following limitations set on the client:

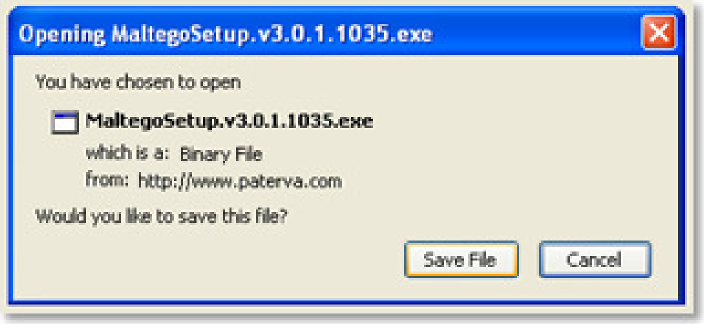
- Not for commercial use!
- Maximum of 12 results per transform
- You need to register on our website to use the client
- API keys expire every couple of days and have to be activated again
- Runs on a (slower) server that is shared with all community users
- Communication between client as server is not encrypted or compressed
- Not updated until the next major version (and we know there are some bugs)
- No end user support – you are on your own..
- No updates of transforms on server side
- Can only discover from online Paterva servers
- Paterva goes hungry...

The commercial version also has these benefits:

- Can be used for commercial use
- No limit on number of returned entities per transform
- Communication between client and server runs over SSL and is compressed
- Runs on a much more powerful server (eg. faster)
- Server is only shared by other commercial users
- Amazing end user support (love, care, tenderness and solutions)
- Updates as they happen – both on client and server
- Can be used with any Maltego server

Download the relevant files from www.paterva .com. Maltego 3 can run on Windows, Linux and soon on Apple as well.

There is a difference between the files downloaded for the commercial edition and the CE edition as can be seen in the graphic below. The bottom image is the CE windows installation executable.



Opening MaltegoSetup.v3.0.1.1035.exe

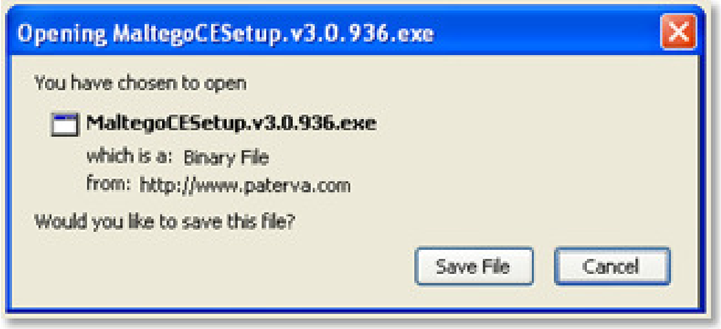
You have chosen to open

MaltegoSetup.v3.0.1.1035.exe

which is a: Binary File

from: http://www.paterva.com

Would you like to save this file?



Opening MaltegoCESetup.v3.0.936.exe

You have chosen to open

MaltegoCESetup.v3.0.936.exe

which is a: Binary File

from: http://www.paterva.com

Would you like to save this file?

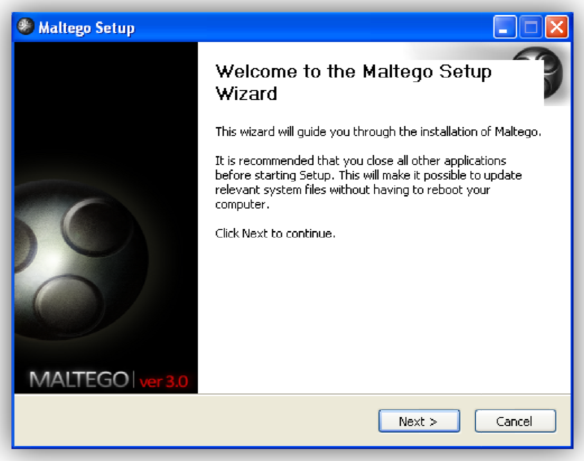
Downloading either the commercial edition or the CE edition

2.3 Installation

2.3.1 Windows

After downloading the MaltegoInstaller.exe file, double click on it to start the installation process. Follow the next few screens that will prompt you for information to complete the installation process.

The screens that you will see are as follows:



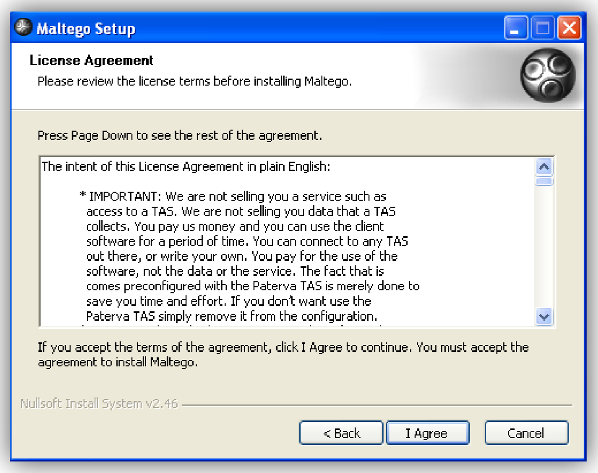
Welcome to the Maltego Setup Wizard

This wizard will guide you through the installation of Maltego.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

The Maltego 3 setup welcome screen



License Agreement

Please review the license terms before installing Maltego.

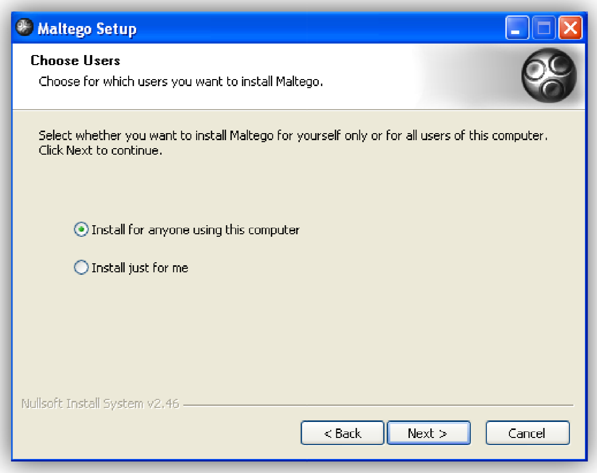
Press Page Down to see the rest of the agreement.

The intent of this License Agreement in plain English:

* IMPORTANT: We are not selling you a service such as access to a TAS. We are not selling you data that a TAS collects. You pay us money and you can use the client software for a period of time. You can connect to any TAS out there, or write your own. You pay for the use of the software, not the data or the service. The fact that is comes preconfigured with the Paterva TAS is merely done to save you time and effort. If you don't want use the Paterva TAS simply remove it from the configuration.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Maltego.

The licence agreement screen



Choose Users

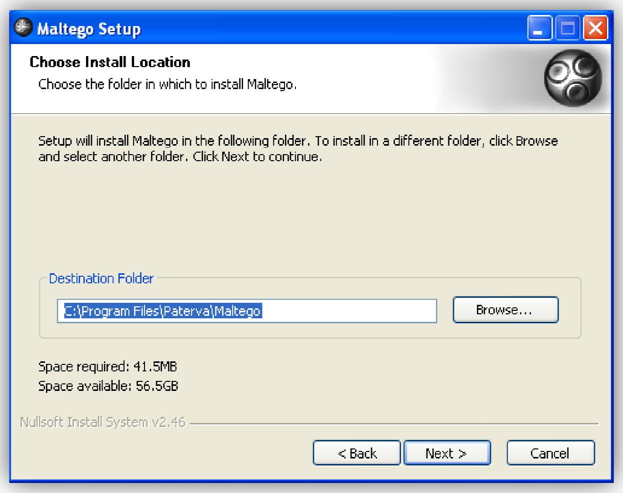
Choose for which users you want to install Maltego.

Select whether you want to install Maltego for yourself only or for all users of this computer. Click Next to continue.

● Install for anyone using this computer

○ Install just for me

Select users that will use Maltego 3



Maltego Setup

Choose Install Location

Choose the folder in which to install Maltego.

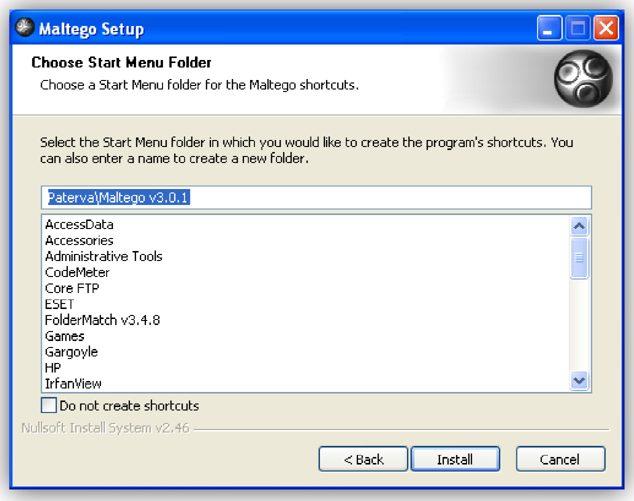
Setup will install Maltego in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files\Paterva\Maltego

Space required: 41.5MB

Space available: 56.5GB

Installation location and disk storage requirements



Maltego Setup

Choose Start Menu Folder

Choose a Start Menu folder for the Maltego shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

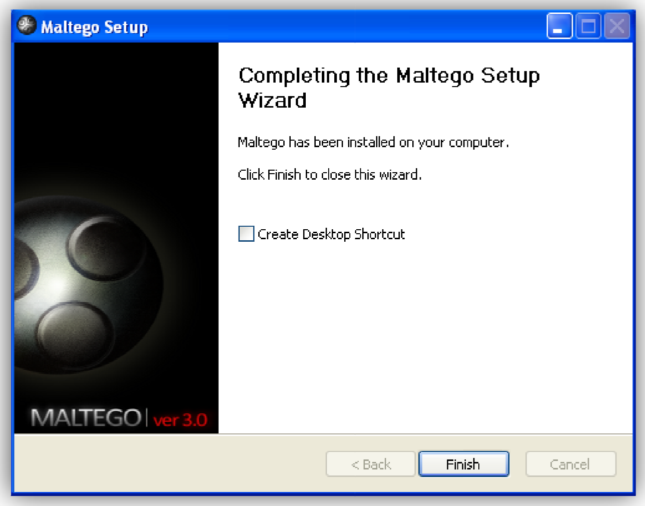
Paterva\Maltego v3.0.1

- AccessData
- Accessories
- Administrative Tools
- CodeMeter
- Core FTP
- ESET
- FolderMatch v3.4.8
- Games
- Gargoyle
- HP
- IrfanView

□ Do not create shortcuts

Start Menu setup

You might want to add icons to your desktop on the last screen:



Maltego Setup

Completing the Maltego Setup Wizard

Maltego has been installed on your computer.

Click Finish to close this wizard.

□ Create Desktop Shortcut

Adding an icon to the desktop

After installation you should see an icon on the desktop and see it in the start menu under Paterva -> Maltego.

2.3.2 Linux

You will need to have a windows (X11) system – Maltego is a graphical application. Maltego is available as a .DEB package (ideal for debian based operating systems) as well as an .RPM package (ideal for systems that can use the RPM Package Manager) and a .zip archive. After you have downloaded the package you can install it as follows:

.deb (debian package)

The Debian packages can be installed by either double clicking on the file within your window manager (such as KDE) or allowing the window managers installer to install the package. Alternatively you can also install it from command line as follows:

> *cd downloads/Maltego* (assuming that you've downloaded it here)
> *dpkg –i <maltegofile>.deb*

.rpm

The RPM file can be installed as above via your window manager by double clicking on the file or via command line as follows:

> *cd downloads/Maltego* (assuming that you've downloaded it here)
> rpm *–i <maltegofile>.rpm*

.zip

The zip archive is the entire extracted Maltego installation, essentially you can simply extract this to wherever you want Maltego installed and then run 'maltego' from the *bin* directory.

Note 1: Maltego requires the sun-java JDK and it is important that you install this version rather than the openjdk that comes with a lot of the operating systems. To do this simply following the instructions on the sun website (http://www.java.com/en/download/manual.jsp#lin)

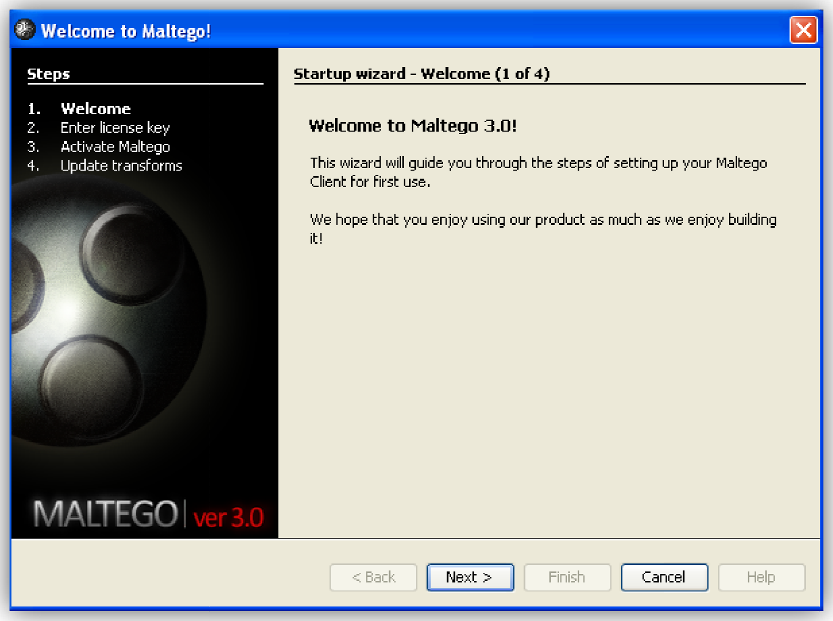
Note 2: Make 100% sure that you can read and write in the directory where you've installed the application - for instance - when you've installed the application as root and you run it under a normal user you might find that reading and writing your configuration files fails. This might cause problems.

Note 3: If you have different versions of Java on your machine you need to make sure that you are using Version 1.6 for Maltego. The best way to force Maltego to use the new Java is to run it from the command line as such:

> [MaltegoInstallDirectory]/bin/*maltego --jdkhome /path/to/your/java/install/*

2.4 Running the first time & registering

When you run Maltego for the very first time you should see a start up screen as follows:



Welcome to Maltego!

Steps

1. Welcome
2. Enter license key
3. Activate Maltego
4. Update transforms

Startup wizard - Welcome (1 of 4)

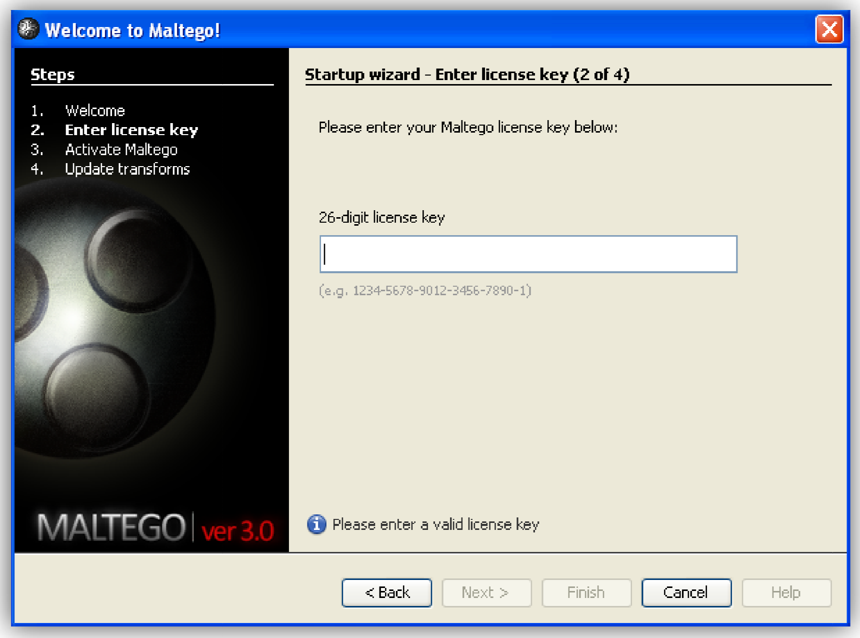
Welcome to Maltego 3.0!

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!

Running for the first time welcome Screen

Select next to continue. Maltego 3 is a commercial product and a license key is used to activate the product. The license key is valid for one year and is computer specific. Without a valid license key you can only use Maltego 3 Community Edition (CE) which is a different installation file.



Welcome to Maltego!

Steps

1. Welcome
2. **Enter license key**
3. Activate Maltego
4. Update transforms

Startup wizard - Enter license key (2 of 4)

Please enter your Maltego license key below:

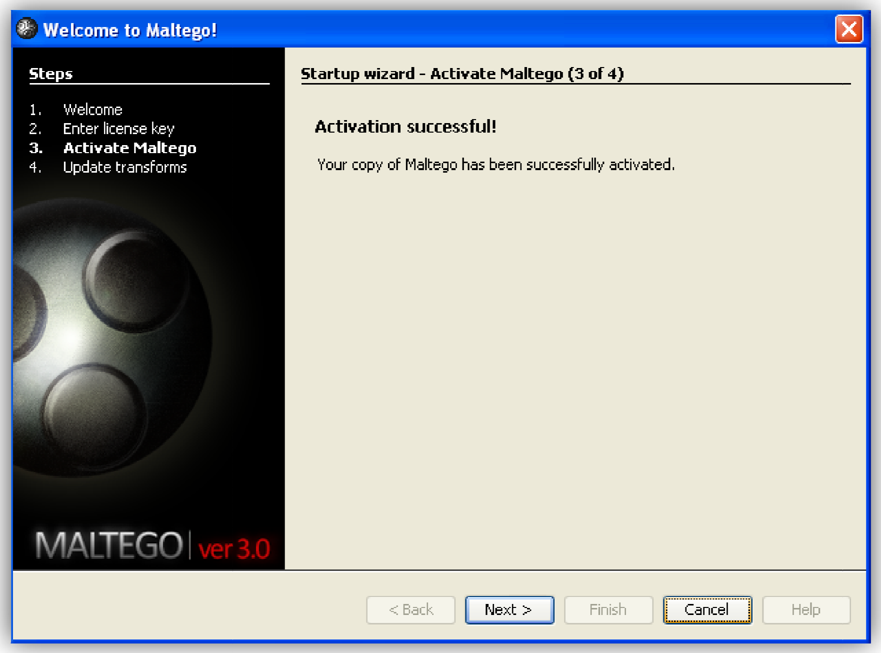
26-digit license key

(e.g. 1234-5678-9012-3456-7890-1)

Please enter a valid license key

Entering licence key

Enter your license key – is should be provided to you via email. The license key has a checksum digit (the last digit) to check that you have not made a typo. When the license key is in the correct format you will see a green check mark appear. The application will now check if the license is still valid. Note that you can use a license only once. If the license is valid the product is now activated.



Welcome to Maltego!

Steps

1. Welcome
2. Enter license key
3. **Activate Maltego**
4. Update transforms

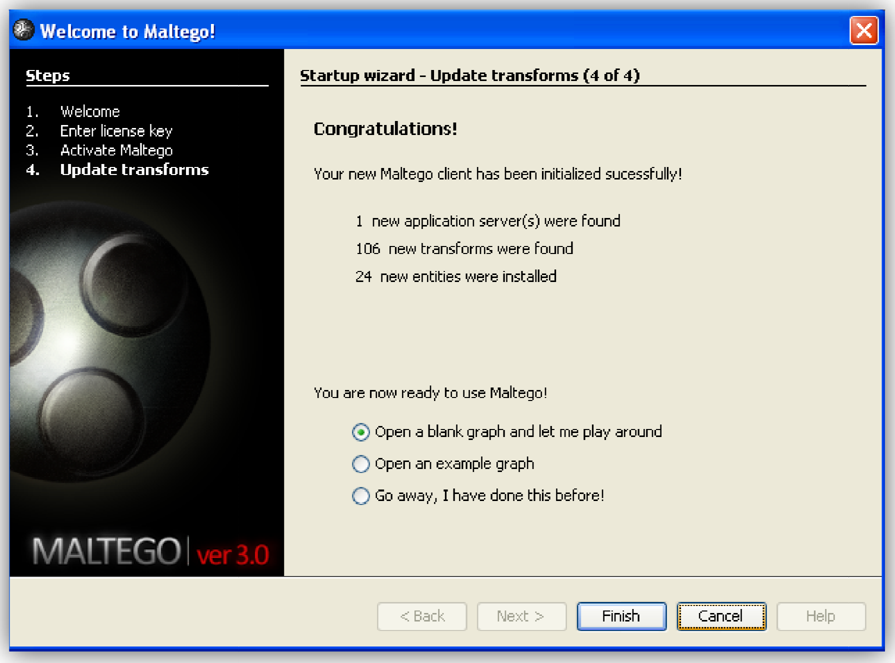
Startup wizard - Activate Maltego (3 of 4)

Activation successful!

Your copy of Maltego has been successfully activated.

Activation successful

Select next to continue and the setup wizard will update your available entities and transforms.



Welcome to Maltego!

Steps

1. Welcome
2. Enter license key
3. Activate Maltego
4. **Update transforms**

Startup wizard - Update transforms (4 of 4)

Congratulations!

Your new Maltego client has been initialized sucessfully!

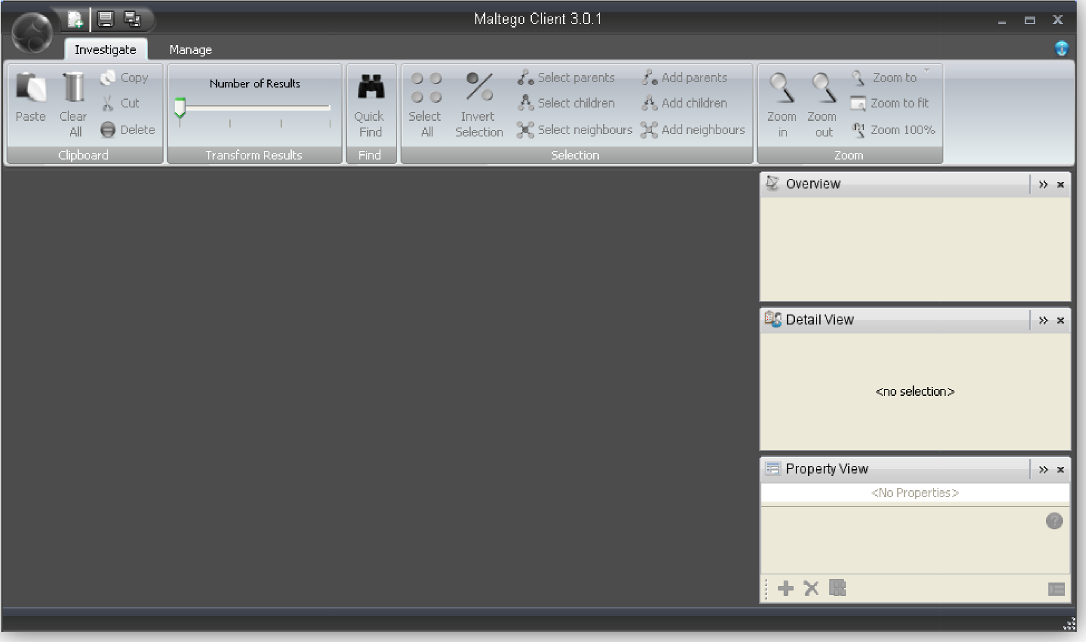
1 new application server(s) were found
106 new transforms were found
24 new entities were installed

You are now ready to use Maltego!

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

Update transforms and complete start-up wizard

Next you will get your first look at Maltego 3 and you should get an empty graph which looks like this:



A blank Maltego 3

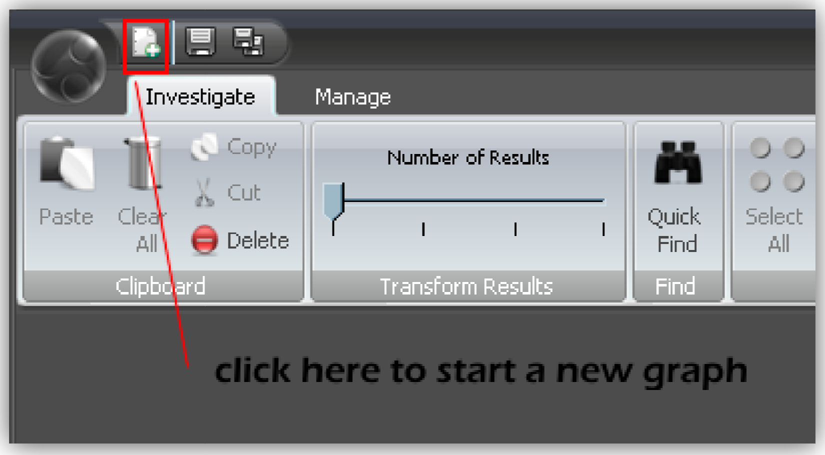
You have just successfully installed Maltego 3!

3 Getting started with Maltego 3

3.1 Your first graph

To create a new graph press *Control T* or click on the (+) button next to the application icon.

Ctrl T

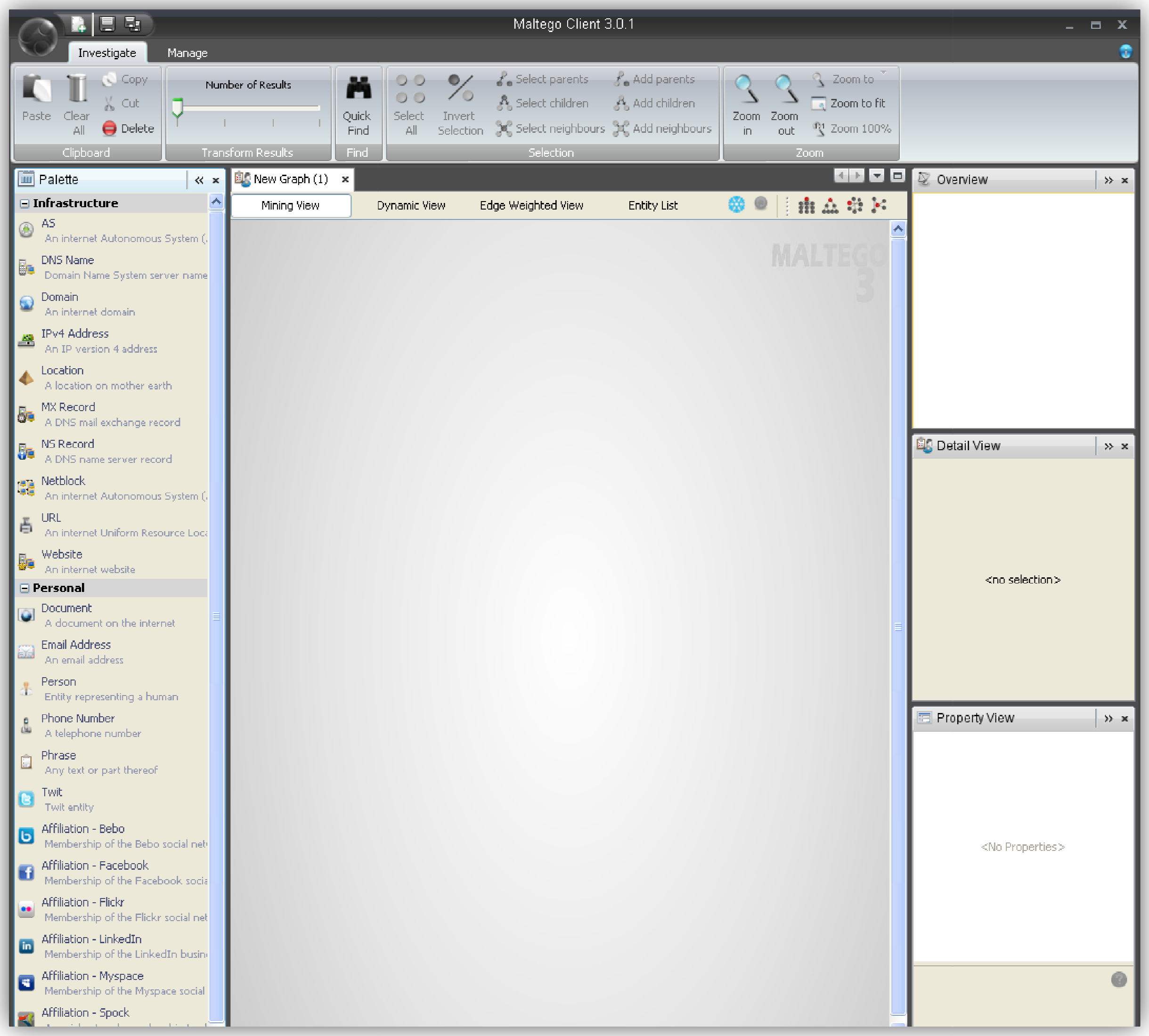


click here to start a new graph

Open new graph / tab button

You can create new graph at any time by clicking on this button. The keyboard shortcut for creating a new graph is Control T (new tab). Once you open your first graph it becomes available to add entities and to run transforms to change those entities to new entities. The palette will also become available which contains a default collection of entities.

Take Note. The term entity and nodes on a graph are used interchangeably in the document.

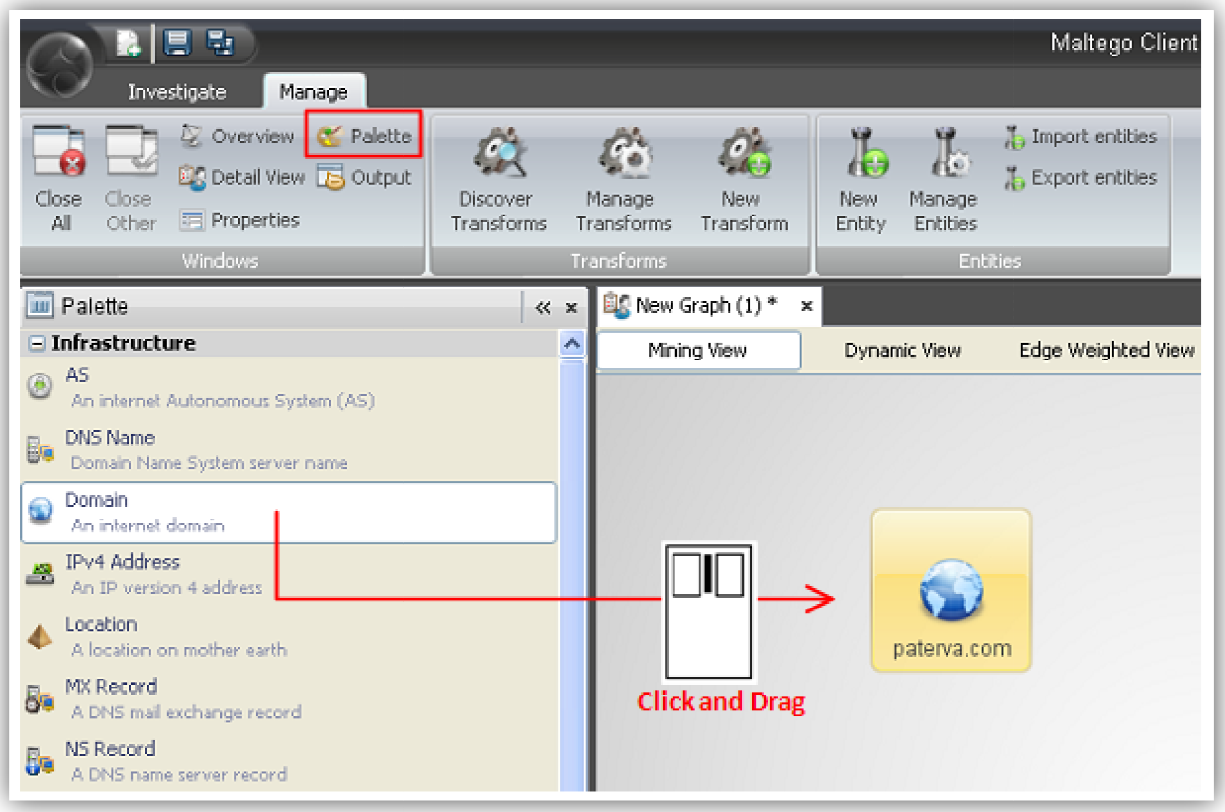


Maltego 3 with an empty graph

More than one graph can be opened. New graphs are added as tabs at the top of the graph screen.

3.1.1 Dragging an entity onto the graph

The entities available in your Maltego 3 will be displayed on your palette. The palette can also be selected from the manage tab. Click on the desired entity and drag it onto the graph area as depicted below.



Dragging entities onto the graph

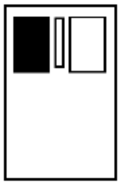
Once an entity has been dragged onto a graph it becomes one of the nodes on the graph.

3.1.2 Editing the value of a node

Double click on the text on the node or double click on the node itself to edit the value.

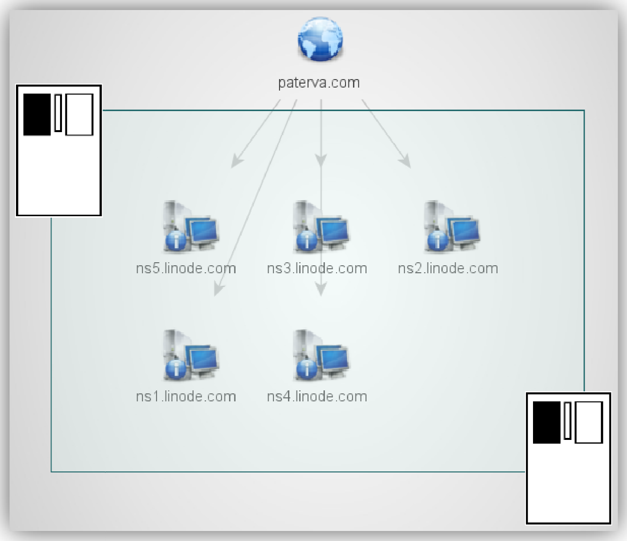
3.1.3 Selecting a node

Left click on the node you want to select. You should see the selection rectangle appear around it.



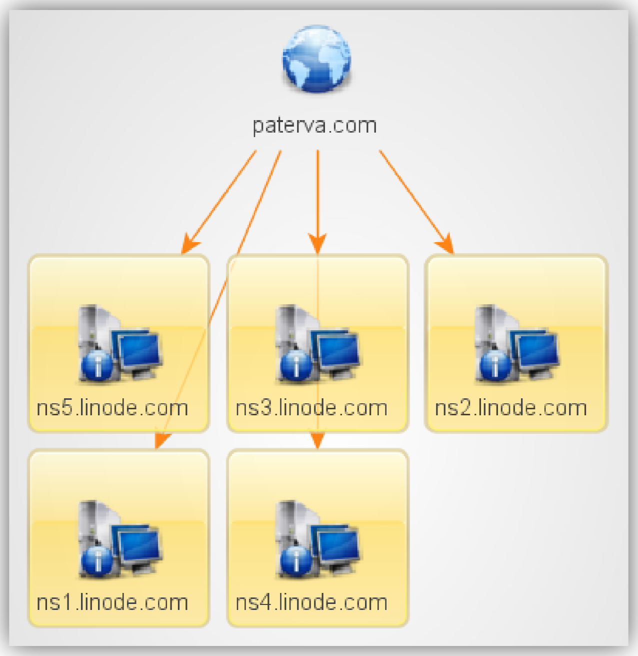
3.1.4 Selecting multiple nodes

Drag a block with mouse around the entities you want to select – while keeping the left click button in.



Selecting multiple nodes

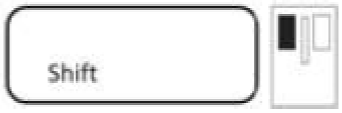
Once selected, the nodes will be highlighted as in the picture below.

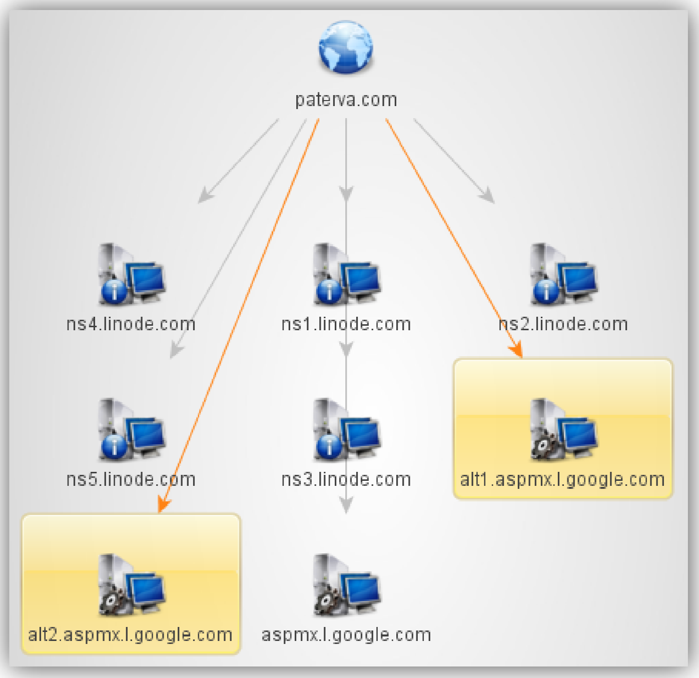


Highlighted nodes

3.1.5 Selecting single nodes at a time

When faced with multiple nodes but you only want to select specific nodes, use shift + left click. Shift + left click on each node you want to select and they will be added to the selection.



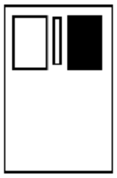


Selecting single nodes

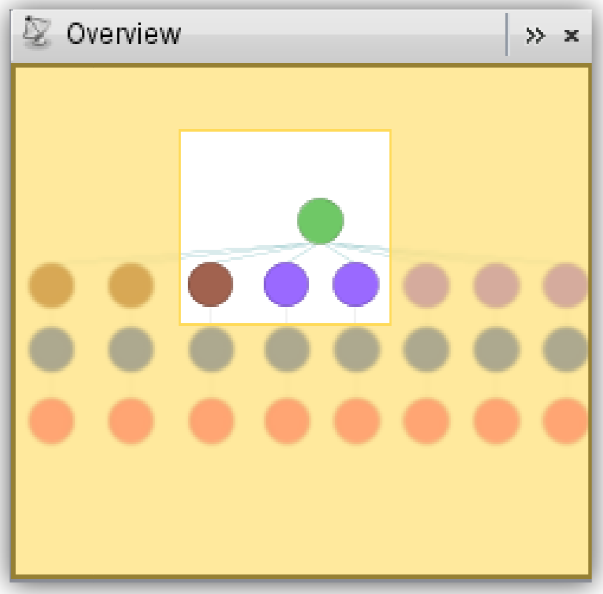
3.2 Using your mouse

3.2.1 Panning and Zoom

To pan, right click and hold while moving the mouse in the desired direction. You can also use the arrow keys to jump to the next entity in the graph. This is useful when navigating large graphs and is a lot faster than using the scroll bars.



You can move the visible frame (white box) around on the Overview view (top right) using the mouse (right click, drag) – the main graph window will update in real time. Depending on the zoom level the visible frame becomes larger (zoomed out) or smaller (zoomed in).

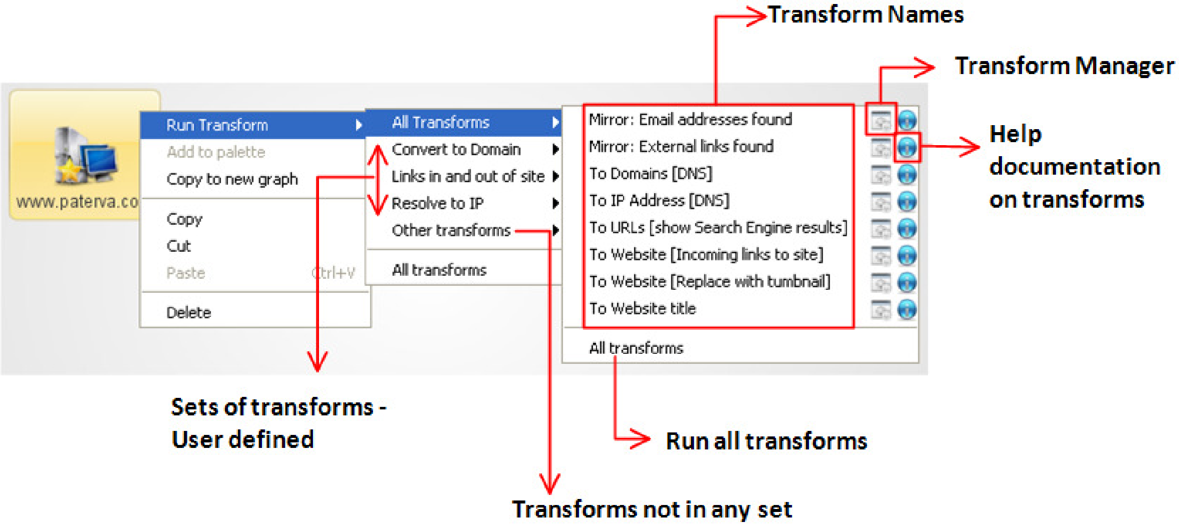


Using the Overview view to navigate a large graph

You can also use the mouse wheel to zoom in and out on the graph but more on this later.

3.3 Running a transform

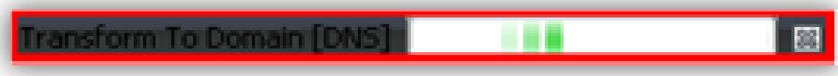
When you right click on a node a context menu is displayed. If you click on ”Run Transform” an additional context menu is displayed. If you select “All Transforms” you will see a list of transforms available for the specific entity.



All the transforms can be displayed and a selection made by clicking on a transform name. Transforms can also be grouped logically by the user into sets.

A transform quick help tag will be displayed if the pointer is held over a specific transform for a while. This quick help is tag aims to provide cryptic information about the specific transform. For detail help select the blue help bubble (blue I) which will take you to the Maltego 3 wiki page for more information about the transform and its application.

In the bottom right hand corner we can see the transform status bar indicating that we are running one transform on one entity.

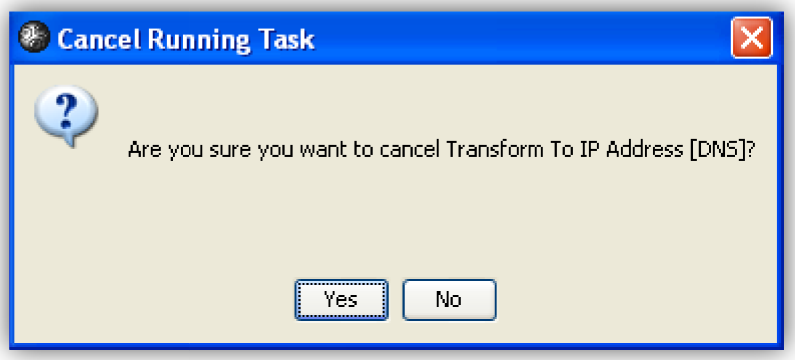


Transform progress bar

When running multiple transforms on multiple entities the progress bar will give an indication of the overall progress of all transforms. When running a single transform on a single entity the progress just shows activity of this transform.

When running a transform you will notice the progress bar at the bottom right of the screen move as it waits for the transform to complete. The [X] (far right of the status bar) allows you to easily cancel a transform (for example – if you have selected the incorrect transform and don't want the results to distort your graph with irrelevant entities).

To cancel a running transform, simply select the [X] at the bottom of the screen. You will then be given a confirmation dialog that looks as follows:


Cancel Running Task

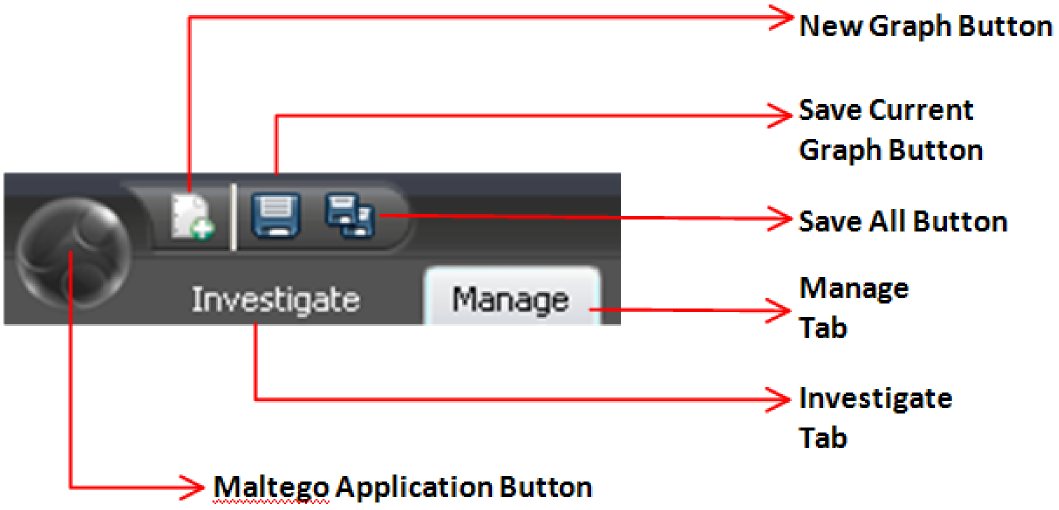
Are you sure you want to cancel Transform To IP Address [DNS]?

Cancel Transform conversation dialog

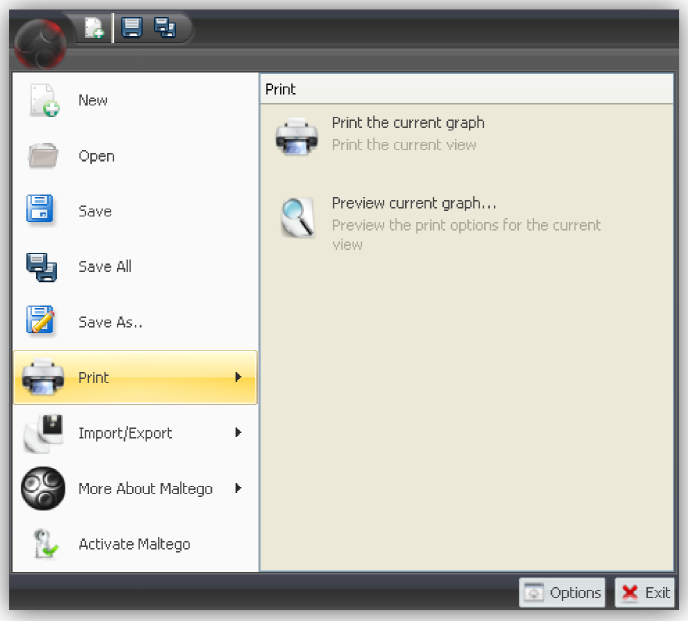
By simply selecting 'Yes' you can cancel the running transforms. Selecting 'No' will allow the transforms to complete as usual. When running multiple transforms you can simply click on the transform progress.

When running multiple transforms, selected the [x] will cancel only the most current transform being run. Should you wish to select specific transforms within the batch, first click on the Transform progress bar (bottom right), which will extend to show all of the currently running transforms, you can then follow the steps above to cancel the transforms.

3.4 Maltego Application Button

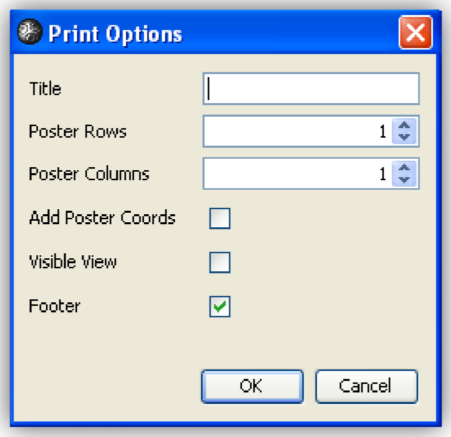


The Maltego Application Button provides access to additional functionality and resources. It firstly affords an additional way to open a new tab or graph. It further provides the normal functionality expected of a Windows application in the form of Open, Save, Save All and save a graph as. Maltego can easily load and save graphs that are saved with an .mtgx extension. The application button menu also gives the user the option to Print or preview the current graph.



Maltego Application Button Options

Maltego can also send the current graph (in whatever view or layout is it) to a printer. You can print to a single page or to multiple pages. With multiple pages you need to specify how many rows and how many columns of pages should be printed.



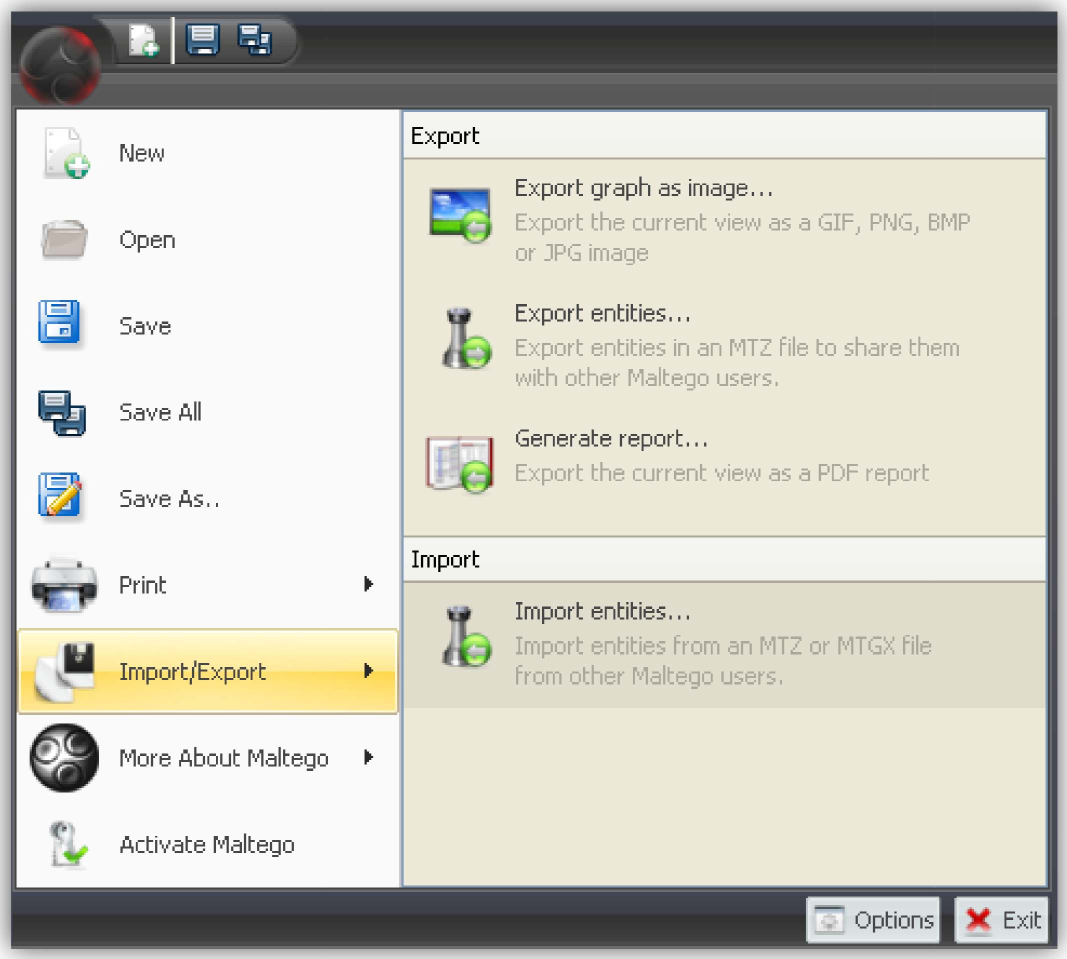
Title
Poster Rows 1
Poster Columns 1
Add Poster Coords □
Visible View □
Footer ☑

Print Options

The Import/Export option of the Maltego Application Button allows the following:

- **Exporting a graph as an image**. This allows the user to export a graph as *a* Graphics Interchange Format (GIF), Portable Network Graphics (PNG), Bitmap (BMP) or Joint Photographic Experts Group (JPEG) image.
- **Export entities**. This allows the user to export entities in an MTZ file (Maltego Archive) to share them with other Maltego users.

- **Generate report**. This will export the current view as a PDF report.
- **Import entities**. This allows the user to import entities from an "*.mtz" or "*.mtgx" file from other Maltego users.



Export

Export graph as image...
Export the current view as a GIF, PNG, BMP or JPG image

Export entities...
Export entities in an MTZ file to share them with other Maltego users.

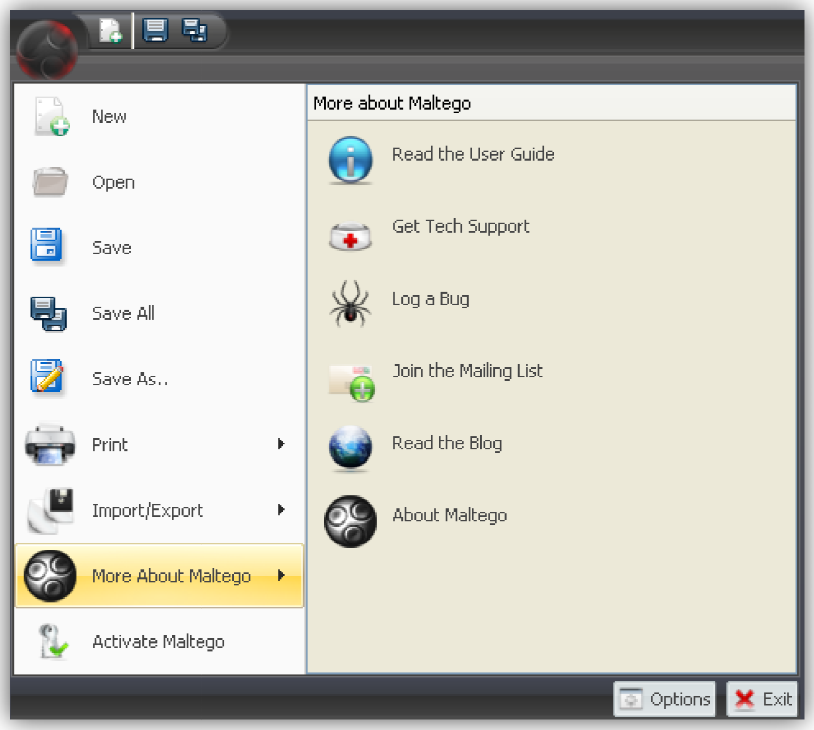
Generate report...
Export the current view as a PDF report

Import

Import entities...
Import entities from an MTZ or MTGX file from other Maltego users.

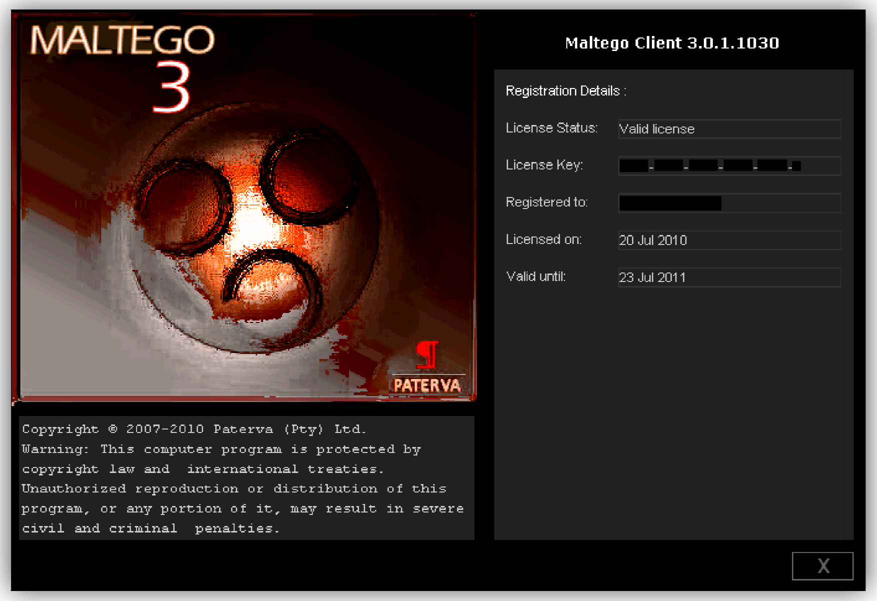
Import / Export functionality of the Maltego Application Button

The "More About Maltego" option of the Maltego Application Button provides the user with additional support options as can be seen in the graphic below:



More About Maltego

When selecting "More About Maltego" > "About Maltego" or the "Activate Maltego" options the user can view their license key information.



Maltego Client 3.0.1.1030

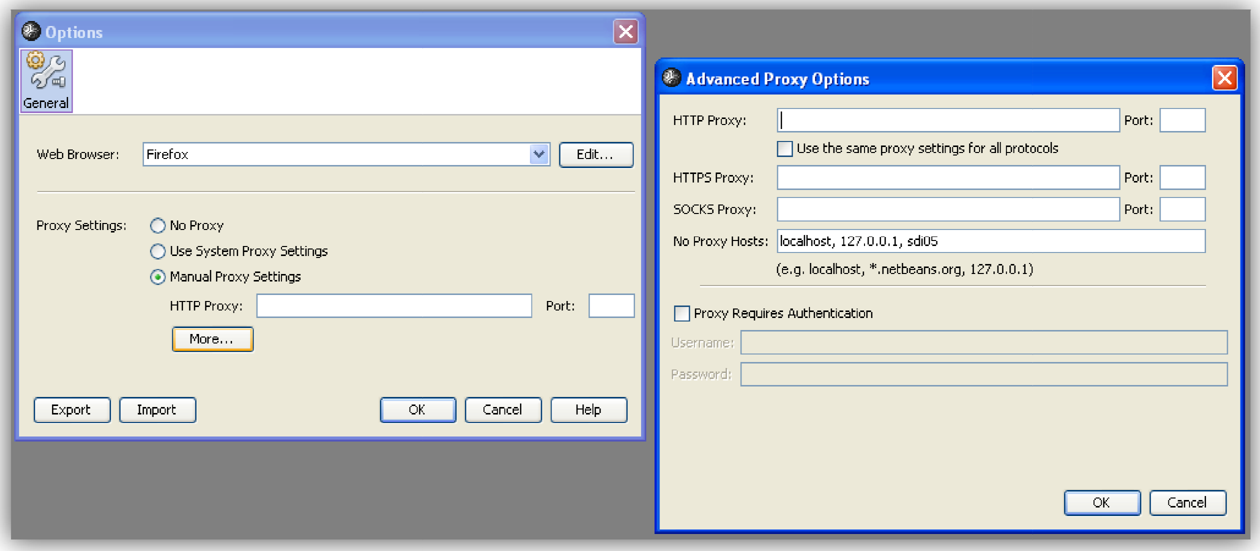
Registration Details :

License Status:	Valid license
License Key:	[redacted]
Registered to:	[redacted]
Licensed on:	20 Jul 2010
Valid until:	23 Jul 2011

```
Copyright © 2007-2010 Paterva (Pty) Ltd.
Warning: This computer program is protected by
copyright law and  international treaties.
Unauthorized reproduction or distribution of this
program, or any portion of it, may result in severe
civil and criminal  penalties.
```

Licence key information

Selecting the Options button at the bottom right corner of the Maltego Application Button menu will give the user the option to choose the default browser and to setup a proxy.



Web Browser: Firefox

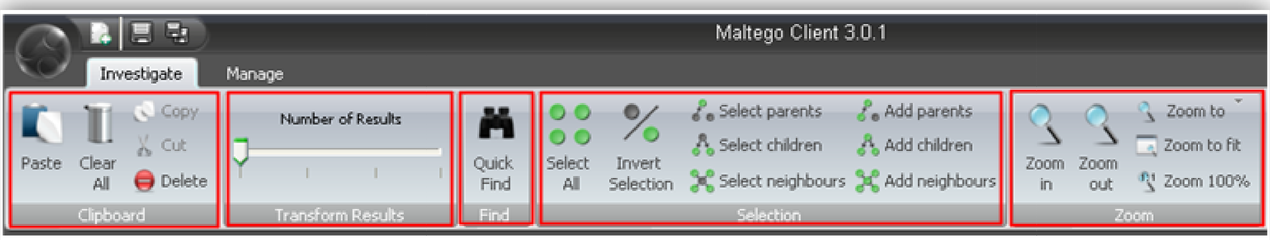
Proxy Settings:
○ No Proxy
○ Use System Proxy Settings
● Manual Proxy Settings
HTTP Proxy: Port:

HTTP Proxy: Port:
□ Use the same proxy settings for all protocols
HTTPS Proxy: Port:
SOCKS Proxy: Port:
No Proxy Hosts: localhost, 127.0.0.1, sdi05
(e.g. localhost, *.netbeans.org, 127.0.0.1)
□ Proxy Requires Authentication
Username:
Password:

Option Button to setup proxy

Proxies are often used within corporate networks as methods of controlling how clients within the network get out to the internet. Maltego requires an internet connection and if you do need to use it within your corporate network please use this option to set it up.

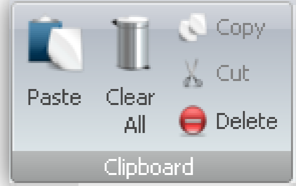
4 The investigate tab



The investigate tab of Maltego 3.0

The investigate tab is open by default when starting Maltego 3. It provides the user with numerous options to manipulate and navigate a graph. The options available are grouped in logical groups.

4.1 Clipboard



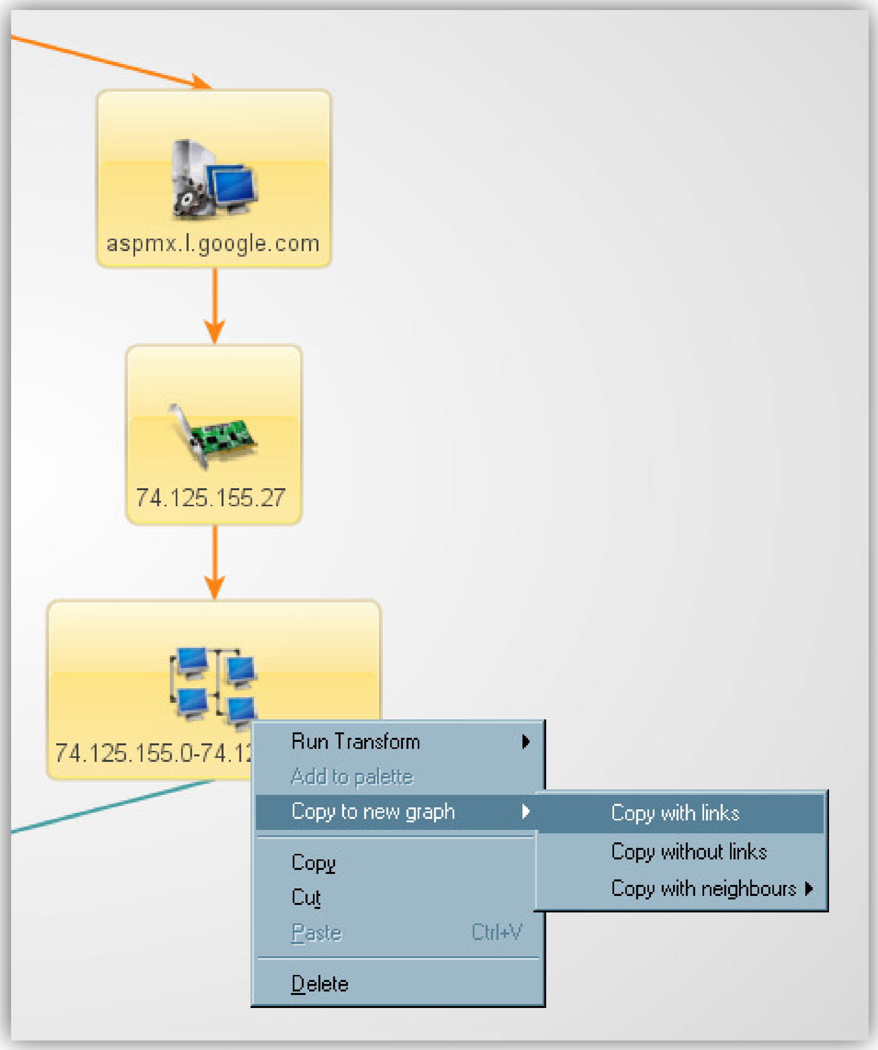
Clipboard tools on the investigate tab

The clipboard tool provides the following intuitive functionality:

- **Paste**. To paste nodes that have been cut or copied.
- **Clear All**. Clear the entire contents of the graph.
- **Copy**. To copy selected nodes.
- **Cut**. Cut selected nodes.
- **Delete**. Delete selected nodes.

4.1.1 Copy and paste between graphs

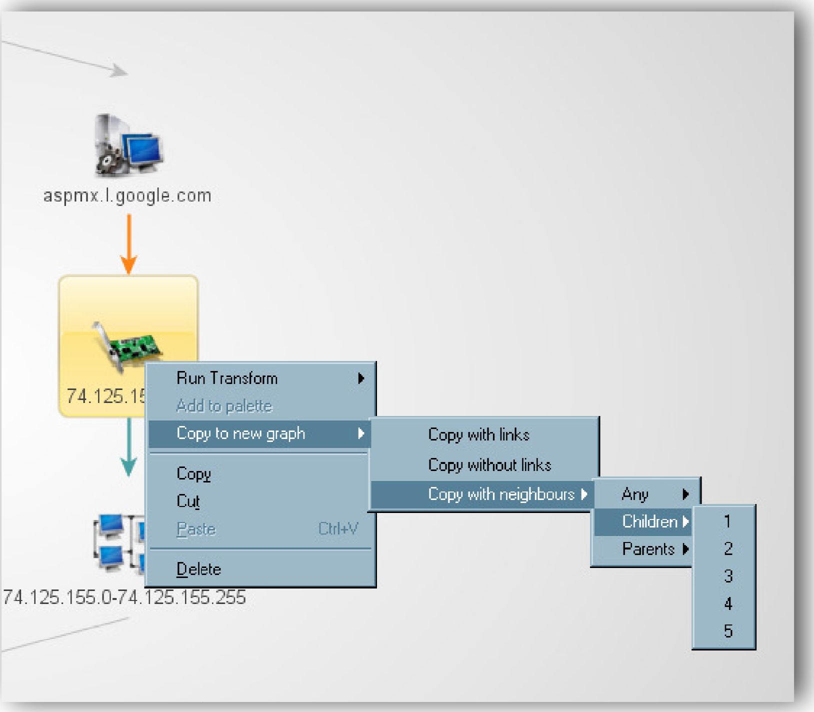
Copy and paste was a bit of an ordeal prior to version 3.0.2 but all of this has been fixed. In version 3.0.2 and later when you right click on selected entities a context menu is displayed:



Copy to new graph

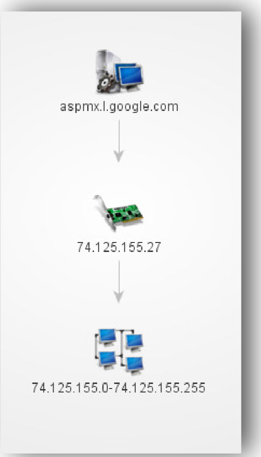
You can decide if you want the sub graph or just the entities that are selected ('Copy with links' vs. 'Copy without links').

Another new feature is 'Copy with neighbours'. This allows you to easily focus on the part of the graph that is interesting – by isolating nodes around the node of interest. There are three sub categories:



Copy with neighbours

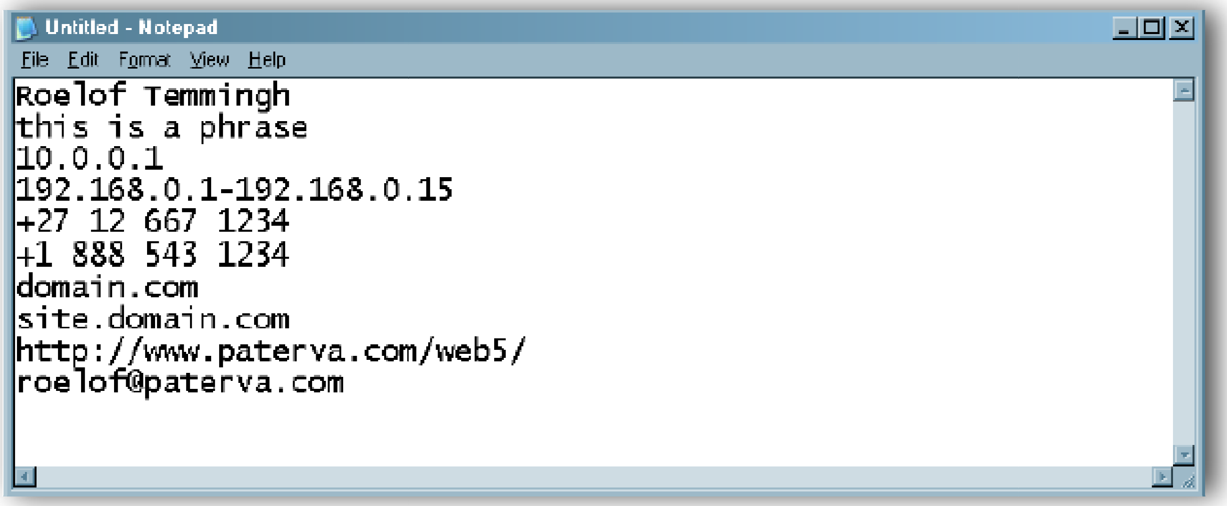
'Any' will select, copy and paste child and parent nodes to a new graph, 'Children' will only select child nodes and 'Parents' will only select parent nodes. The numeric field indicated how many level should be selected. Let's assume we want all the parents and children of the IP number selected in the example above. We'll use 'Any' and the number '1'. This will result in a new graph that looks as follows:



Result of copy

4.1.2 Copy from text

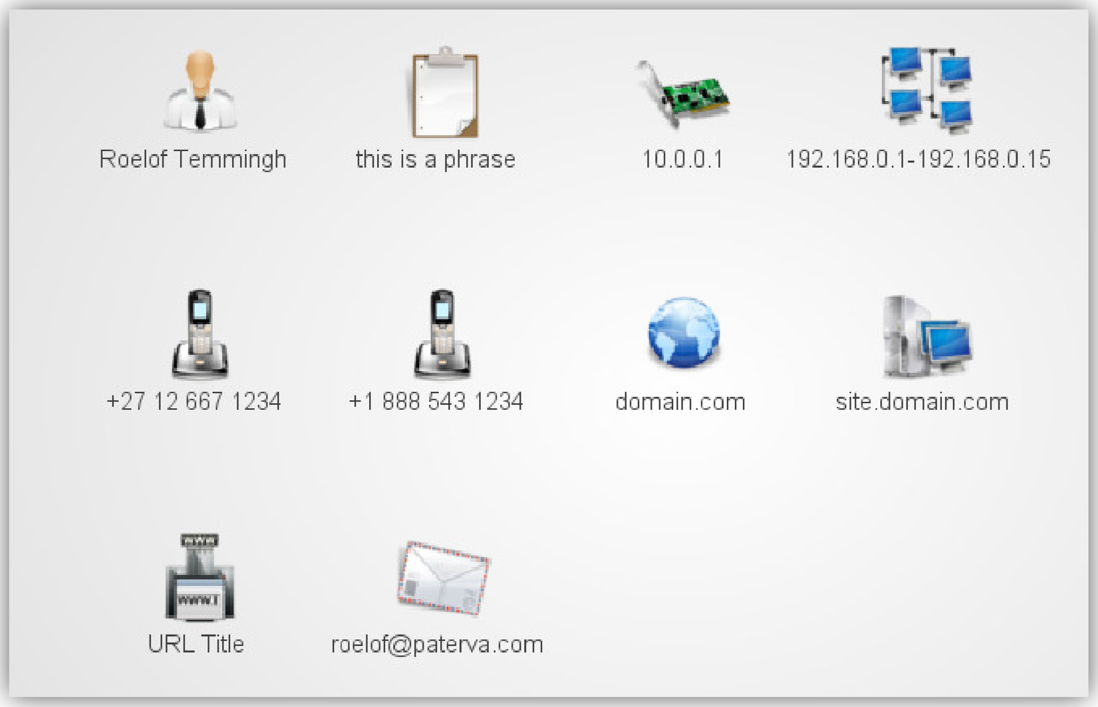
As in version 2, Maltego version 3.0.2 tries to identify the type of entity that is pasted from text. Consider the following example:



```
Roelof Temmingh
this is a phrase
10.0.0.1
192.168.0.1-192.168.0.15
+27 12 667 1234
+1 888 543 1234
domain.com
site.domain.com
http://www.paterva.com/web5/
roelof@paterva.com
```

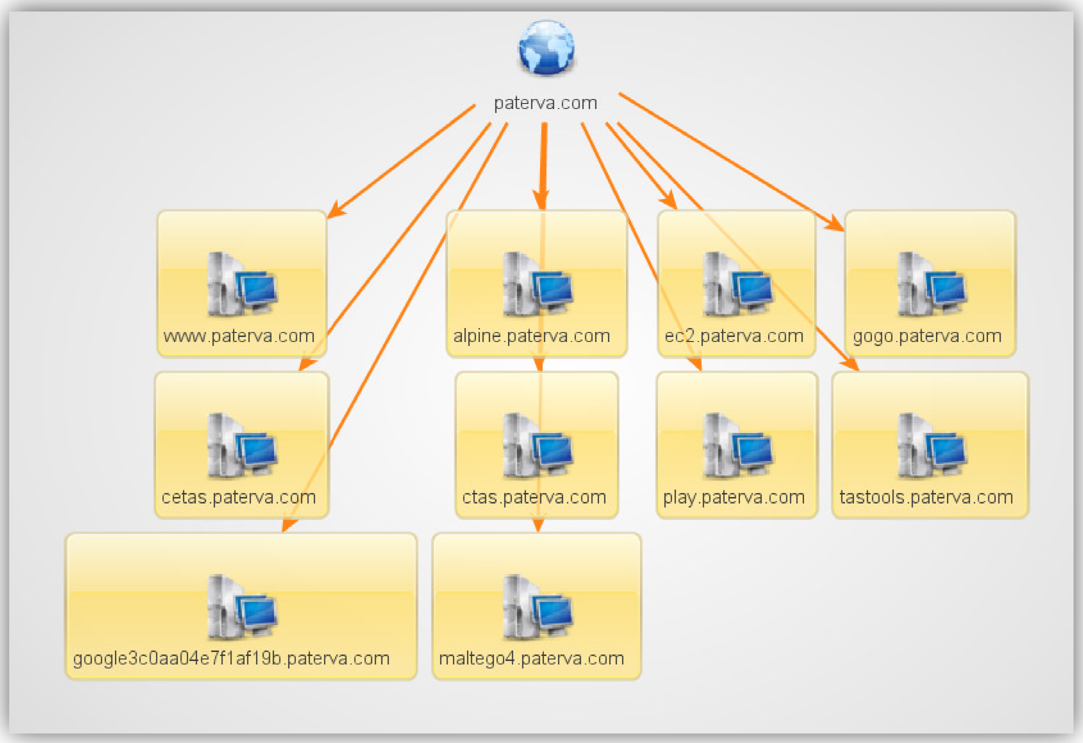
Text to be copied

Copying and pasting all of the above text into Maltego leads to:

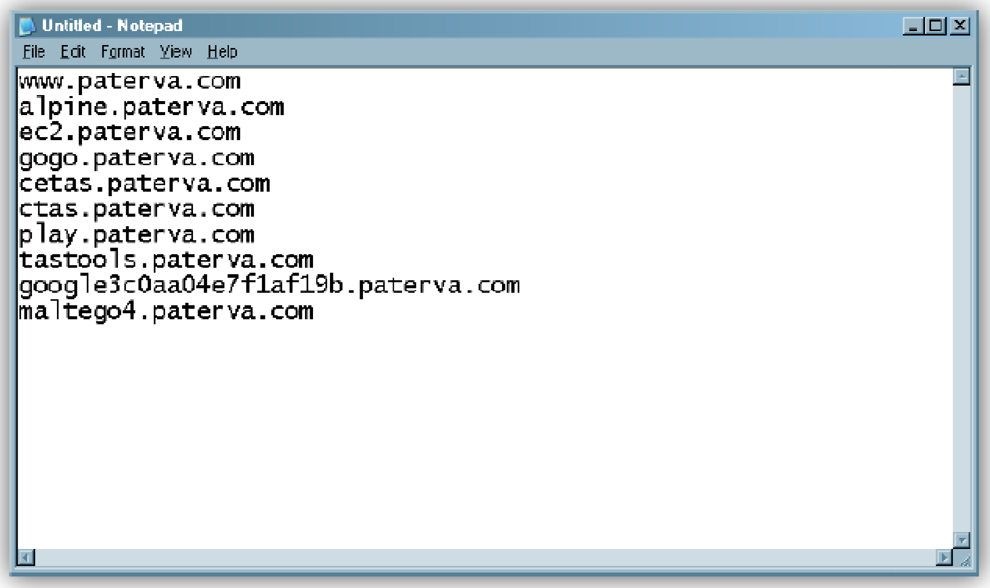


Result of copy from text

Note that the URL entity type displays the title of the URL – when pasted from text this is not displayed (but the entity will work as expected). You can also paste back from Maltego to text. Consider the following:

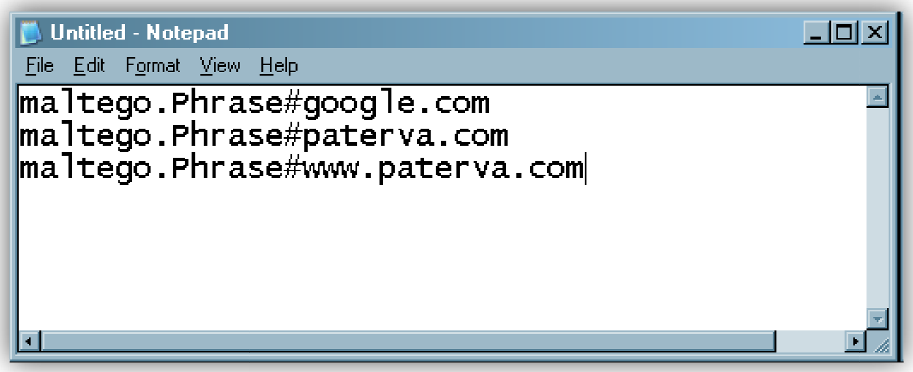


After the nodes has been selected and copied (Control C, or via the GUI buttons), pasting into a text editor renders the following:



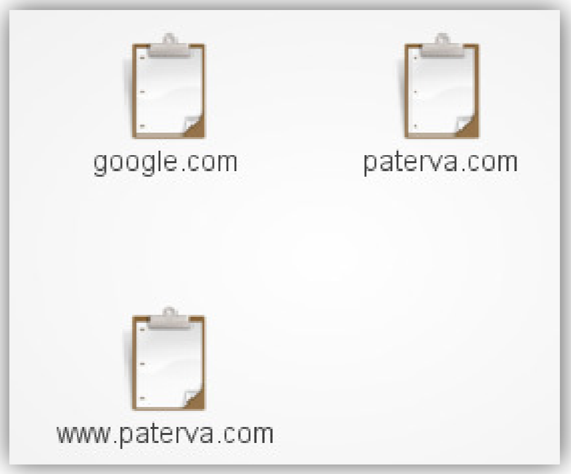
```
www.paterva.com
alpine.paterva.com
ec2.paterva.com
gogo.paterva.com
cetas.paterva.com
ctas.paterva.com
play.paterva.com
tastools.paterva.com
google3c0aa04e7f1af19b.paterva.com
maltego4.paterva.com
```

Keep in mind that Maltego will fail at recognition of complex entities in some cases (think phone numbers!) In these cases my might want to tell Maltego what the entity type is. This can be done by appending the entity value with the entity type. Consider the following text:

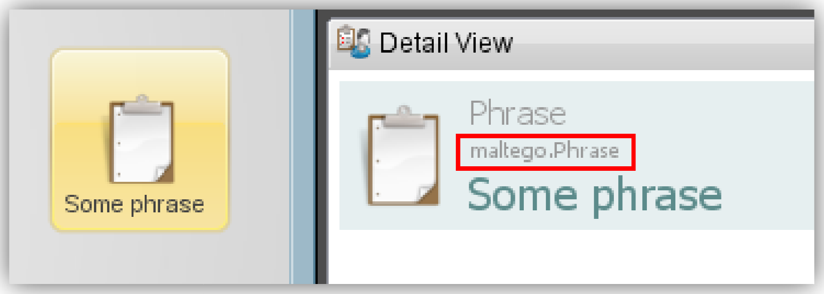


```
maltego.Phrase#google.com
maltego.Phrase#paterva.com
maltego.Phrase#www.paterva.com
```

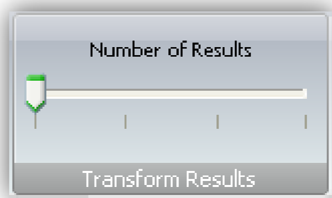
When this is selected and pasted it results in the following graph:



Entity names (e.g. what's inserted before the #) can be obtained by dragging an entity to the graph and looking in the detail view at the entity type description (highlighted in red below)



4.2 Number of transform Results – the slider



Selecting the number of transform results 12, 50, 255, unlimited (10,000)

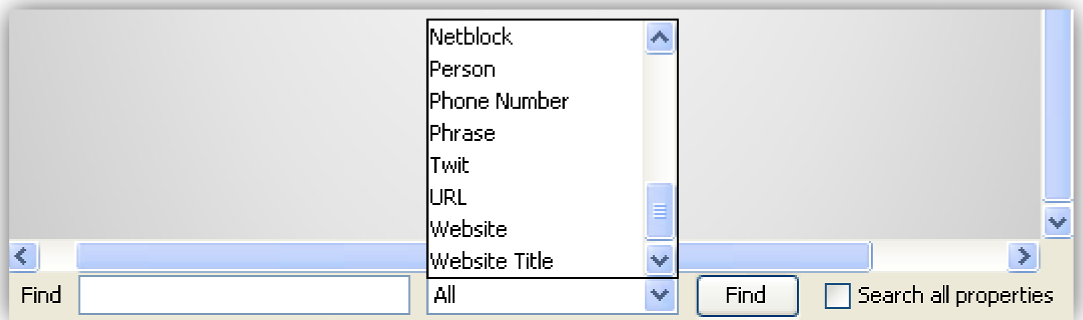
Transform results is a slider to set the number of results returned by Maltego 3. When set to the very left Maltego will only show the top 12 results, based on weight. The next setting corresponds to 50 results, then 255 and the very right to unlimited results (10 000). One needs to understand the implications of these settings. Many transforms has no concept of weight. In fact, only search engine transforms uses weight as an indication of relevance. Think about the reverse DNS results for a class C network – it can potentially return 255 results – each of them with a value of 100 (the default value), as no one DNS entry is more important than the other. Setting the slider to 12 results will only show the first 12 results – useful for simply getting an idea of what in the network, but useless for enumerating ALL the reverse DNS information of the block. In the same way setting the slider to 255 results for a search engine transform (e.g. looking for someone specific but who has a very common name) is not clever as you will be flooded with results. You have to be careful to understand how the slider works and spend time experimenting with it.

Take Note. When you do not see the amount of results that you expected to see, make sure how many results the transform result selector is set to return.

4.3 Find

The find tool on the investigate tab

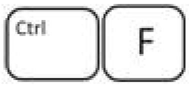
The quick find option on the investigate tab is a very handy tool to find something specific in a very large graph. Once you select "Find" the following toolbar will open at the bottom of your graph:



The Find Toolbar at the bottom of a graph

You can now enter a search term, select the specific node type or specify "All" (the whole graph) and you have the option to search all the properties (listed in the Property View). Once you select find the relevant nodes will be highlighted in the graph and the search hits will be listed in the Detail View.

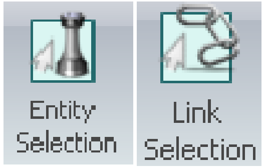
To enable searching you can also press Control + F.



Hint. It's often easier to select all nodes/entities of a specific type by not specifying a search term and picking only the type and hitting find.

4.4 Link vs. Entity mode

Maltego 3.0.2 can operate in two different modes – link selection mode, or entity selection mode. The default mode is entity selection mode. To switch between modes you can press control M or click on the mode selection icon at the top (this icon indicates the current mode):

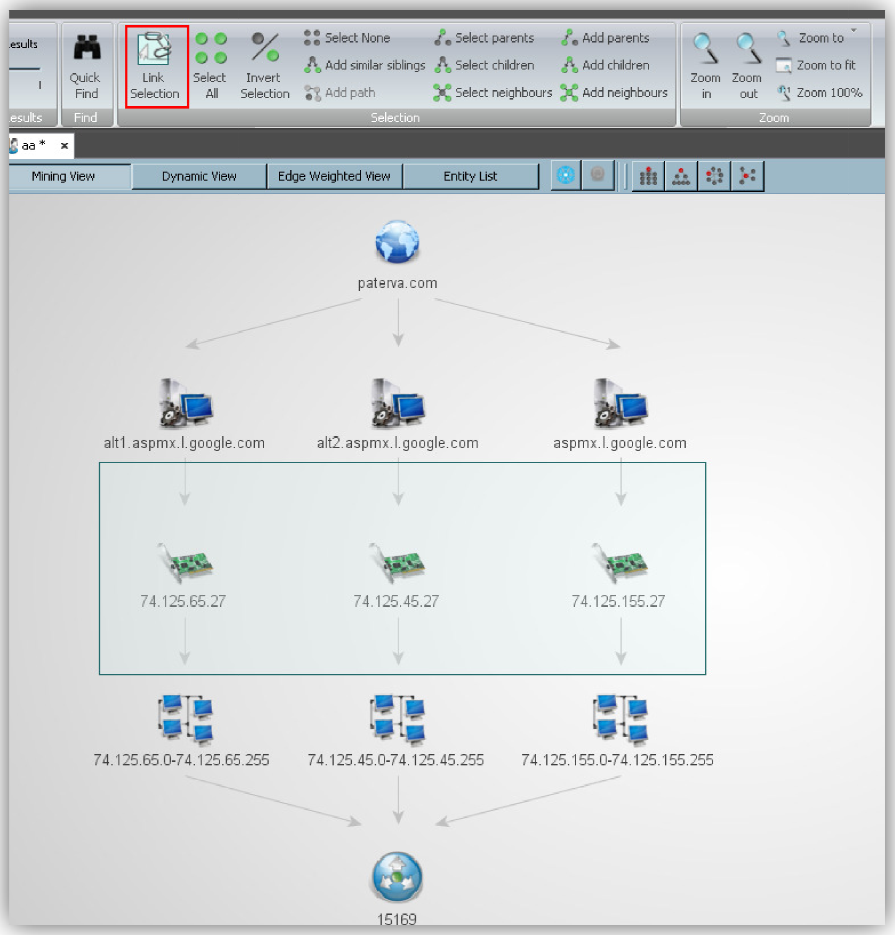


Selecting either entities or links

To quickly switch you can also press and hold the Control key while dragging or selecting.

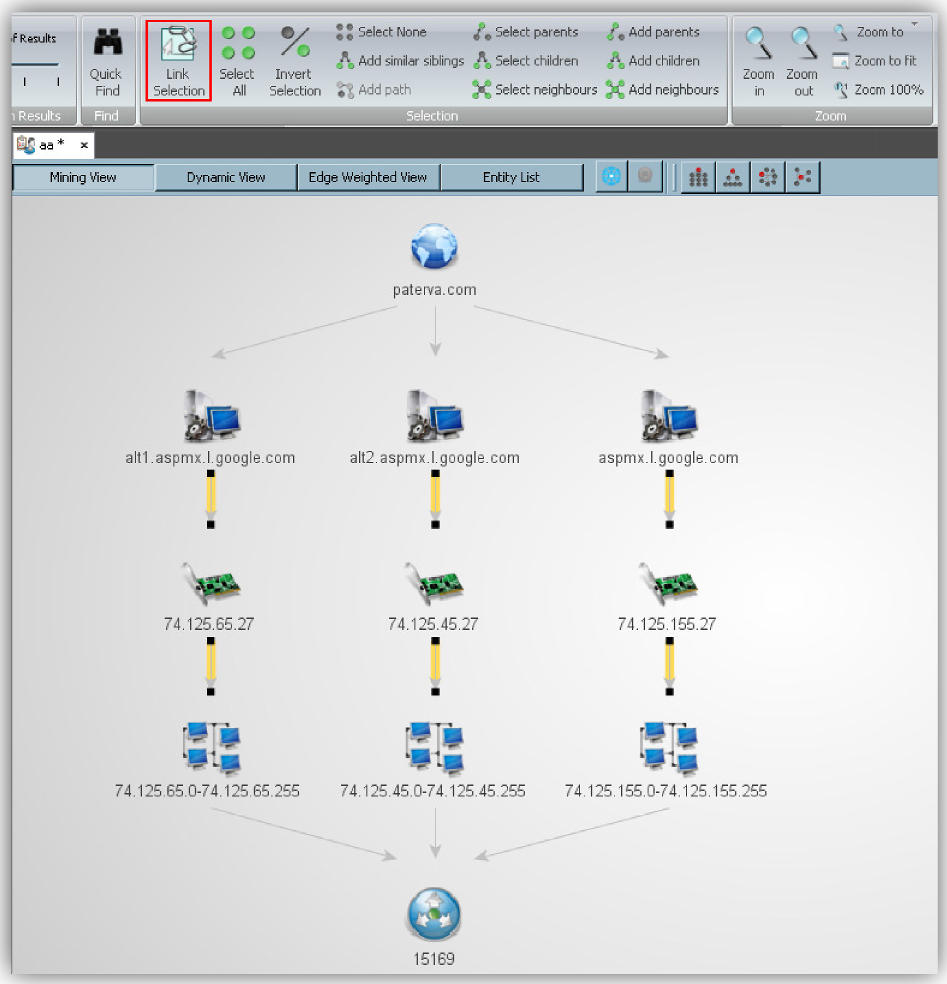
4.4.1 Link mode – selecting links

In link selection mode you will be selecting links. Dragging a box around links will select multiple links:



Selecting Links

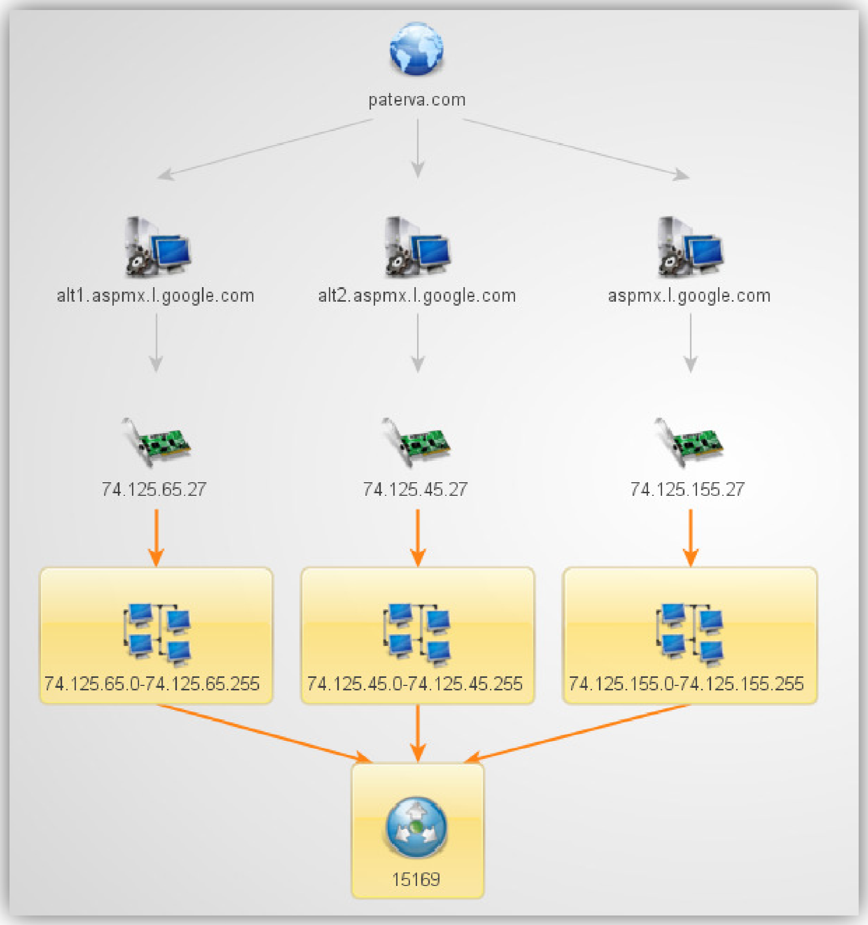
Will result in the following selection:



Links selected

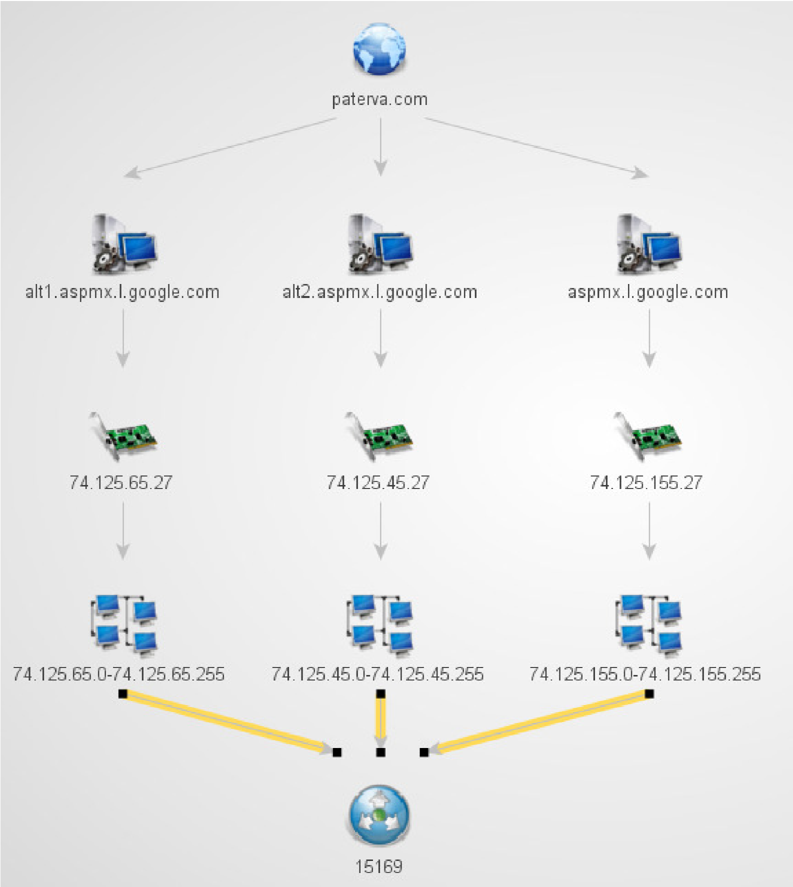
Note that link selection mode is enabled. Links can also be selected by selecting nodes (in entity selection mode) and then switching to link selection mode. This is super useful to select for instance all incoming links to an entity. Let's assume that we want to select all links coming into the AS 15169 in the graph above.

We select the AS node and then press Control Up Arrow (or click on the 'Add parents' button) to add the parents of this node. The graph ends up to looks like this:



Adding parents

Switching to Link Selection mode from here the incoming links are selected:



Selecting Links

The 'select parent', 'select child' etc. functions also works for link selection.

4.4.2 Setting up manual links

Manual links can be established in two ways:

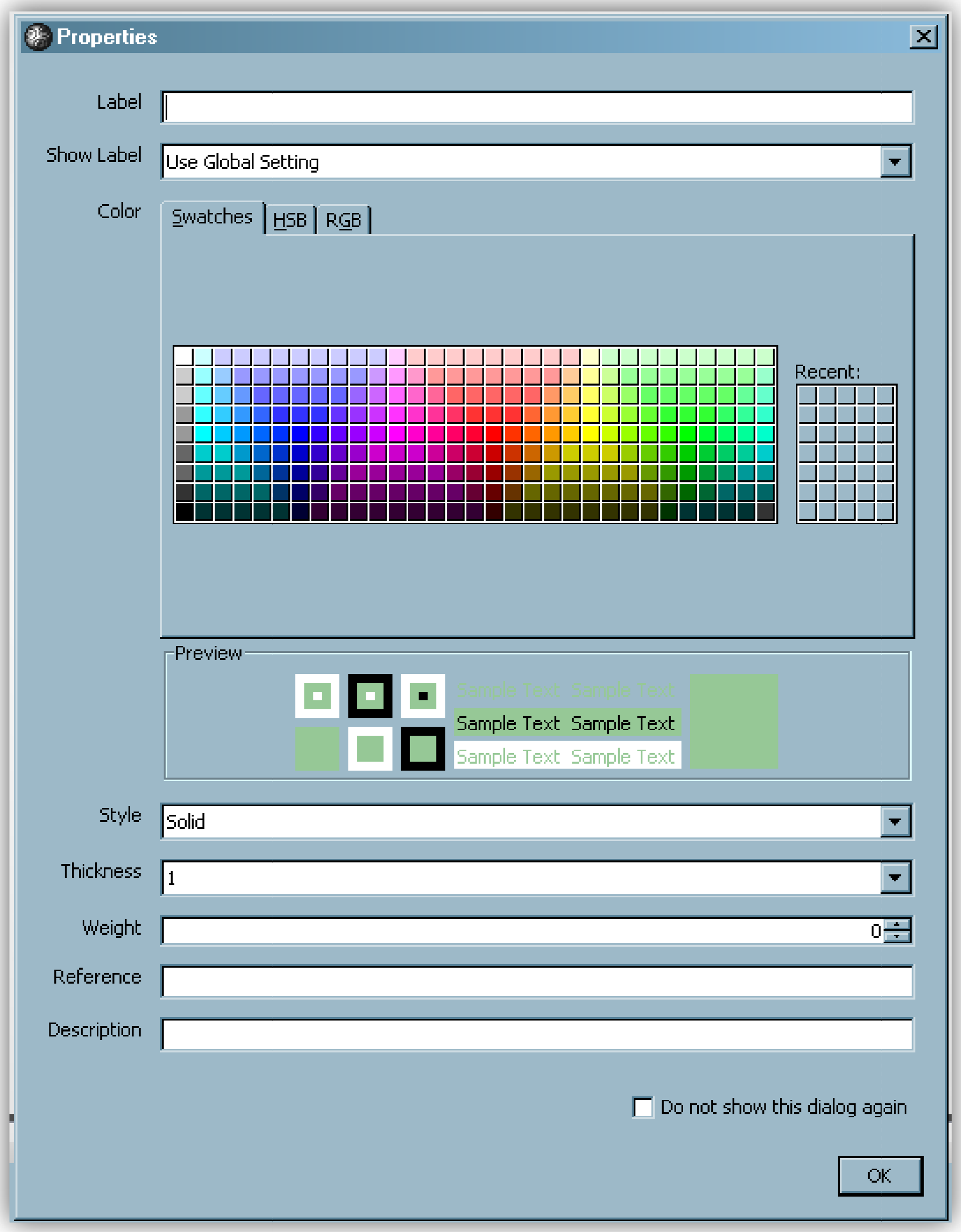
- Left click and hold on an unselected source entity, then drag link to target entity.
- In link selection mode simply connect the two entities

4.4.3 Setting link properties

Link properties can be set in three ways:

1. When a manual link is created the link property dialog pops up per default
2. By double clicking on a single link (when in Link selection mode, or holding down Control key)
3. By setting the fields in the property view (multiple links)

The link property dialog is displayed in option 1 and 2 and looks as follows:



Properties

Label:

Show Label: Use Global Setting

Color: Swatches | HSB | RGB

Style: Solid

Thickness: 1

Weight: 0

Reference:

Description:

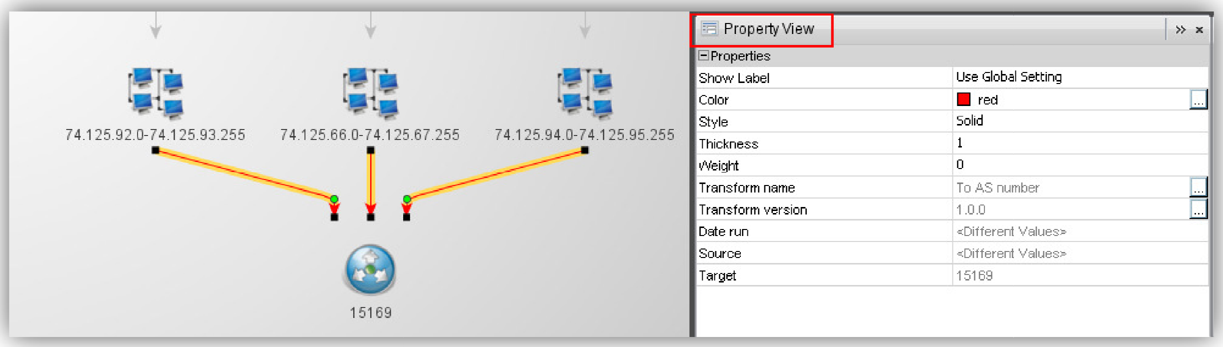
□ Do not show this dialog again

Link property dialog

From here the user can select the label (the text that will be rendered on the link), set the colour, style, thickness etc.

To set the properties of multiple links do the following:

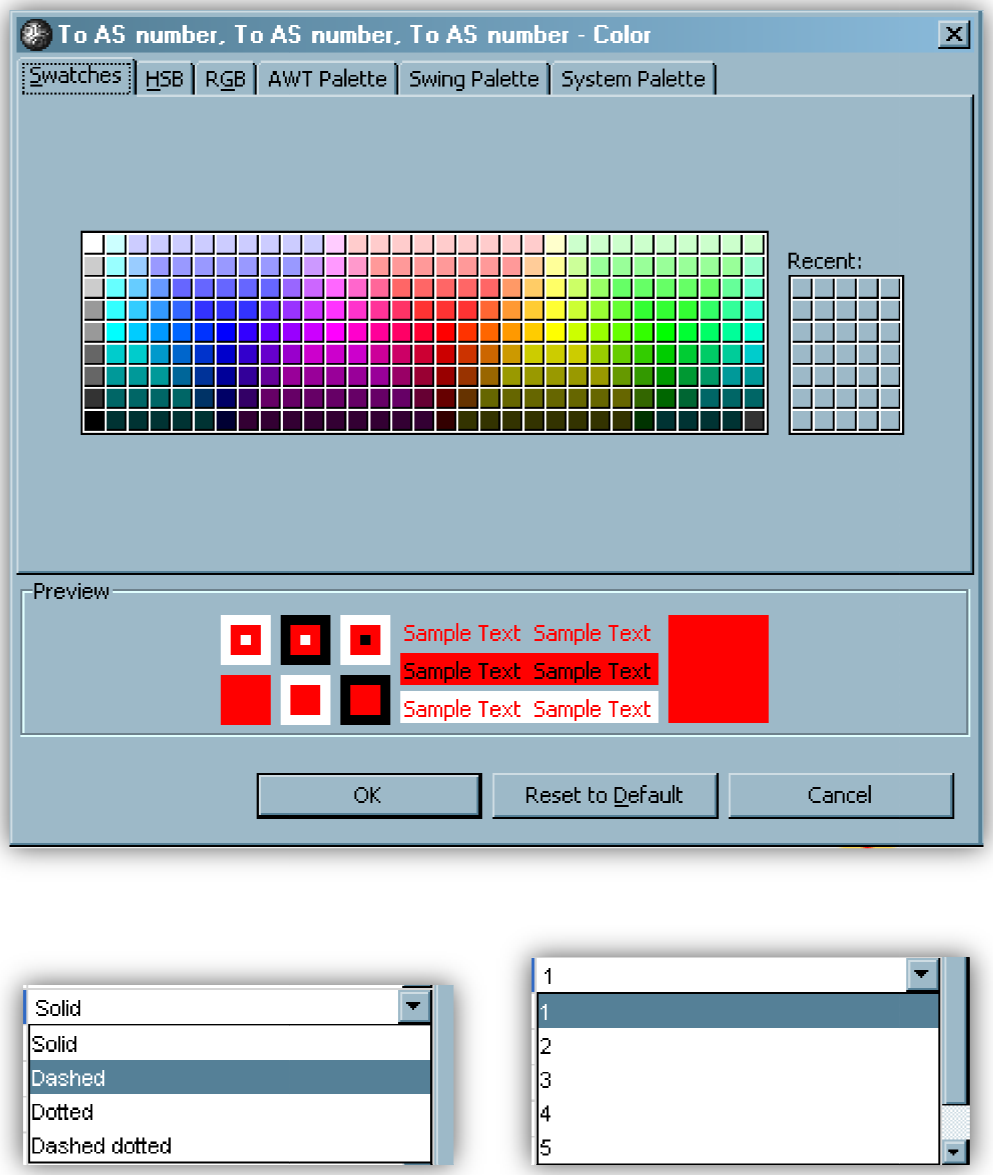
- Select the links (using any of the methods described)
- Set the properties of the links in the property view (highlighted in the screenshot below):



Show Label	Use Global Setting
Color	🟥 red
Style	Solid
Thickness	1
Weight	0
Transform name	To AS number
Transform version	1.0.0
Date run	<Different Values>
Source	<Different Values>
Target	15169

Setting properties of the links

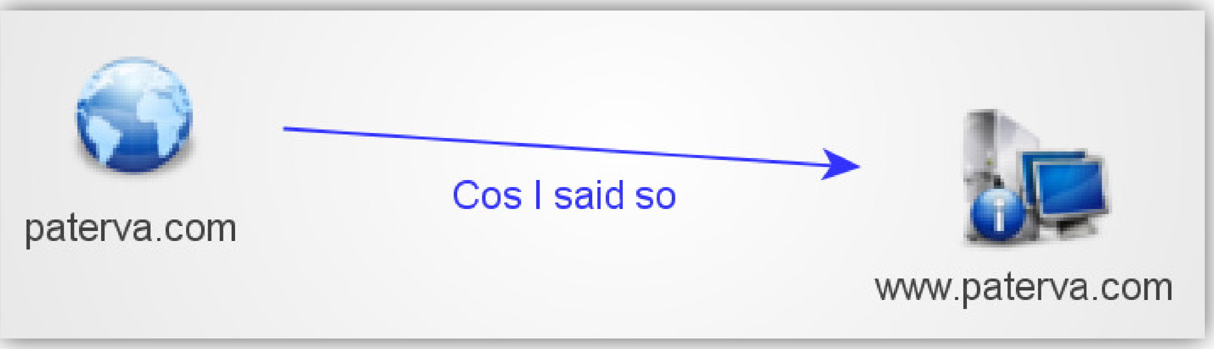
From the property view the style, thickness and colour can also be configured:



Configuring the style, thickness and colour of links

4.4.4 Link labels

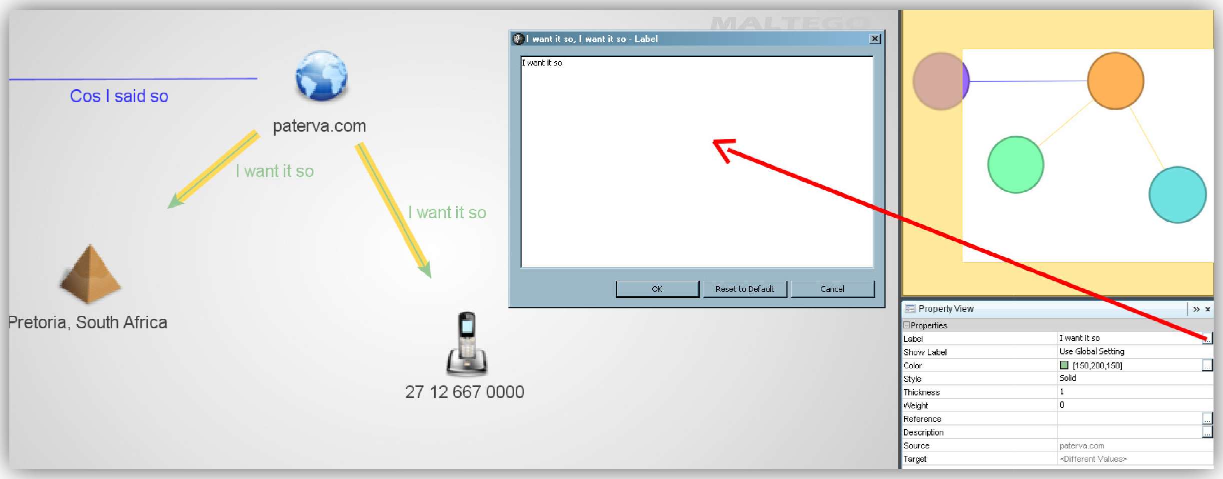
A link label is the text that is displayed on the link:



There are two types of labels:

- Those generated by transforms
- Those set up by the user

Labels generated by transforms cannot be edited by the user. Manual links can be edited by double clicking on the link (holding down Control, or when Link selection mode), and multiple links can be edited all at once by selecting them and editing in the Property view:

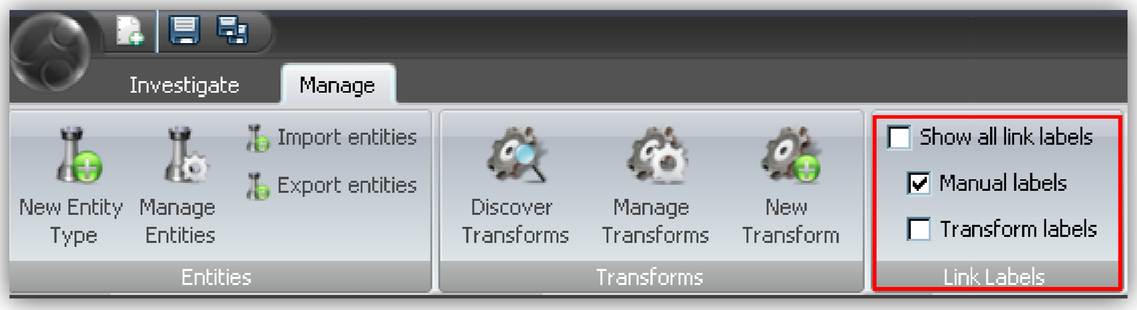


I want it so

Label	I want it so
Show Label	Use Global Setting
Color	🟩 [150,200,150]
Style	Solid
Thickness	1
Weight	0
Reference	
Description	
Source	paterva.com
Target	<Different Values>

Creating link labels

Link labels (both types) can be set to be visible or invisible. When working with a large graph you might not want to show all the transform link labels, as things get confusing real quick. By default transform link labels are set to be invisible in global settings (highlighted section).



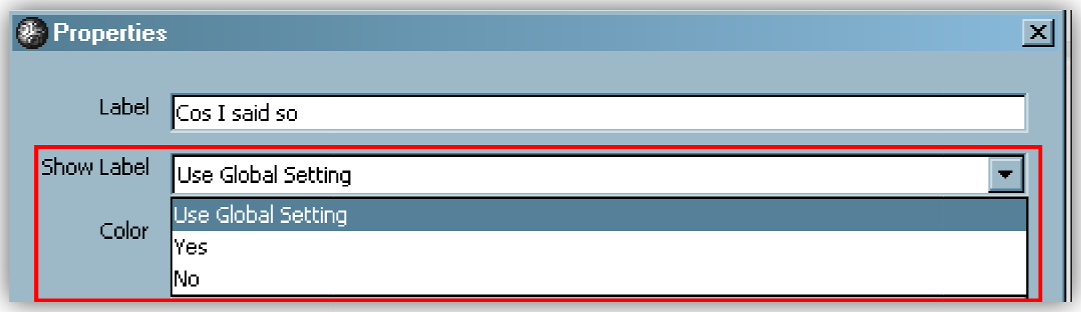
□ Show all link labels

☑ Manual labels

□ Transform labels

Labels can be hidden or displayed

Individual link labels can be set to be visible or not – independent of the global settings. This is done by selecting the link and double clicking on it (single link) or in the property view (multiple links):



Label: Cos I said so

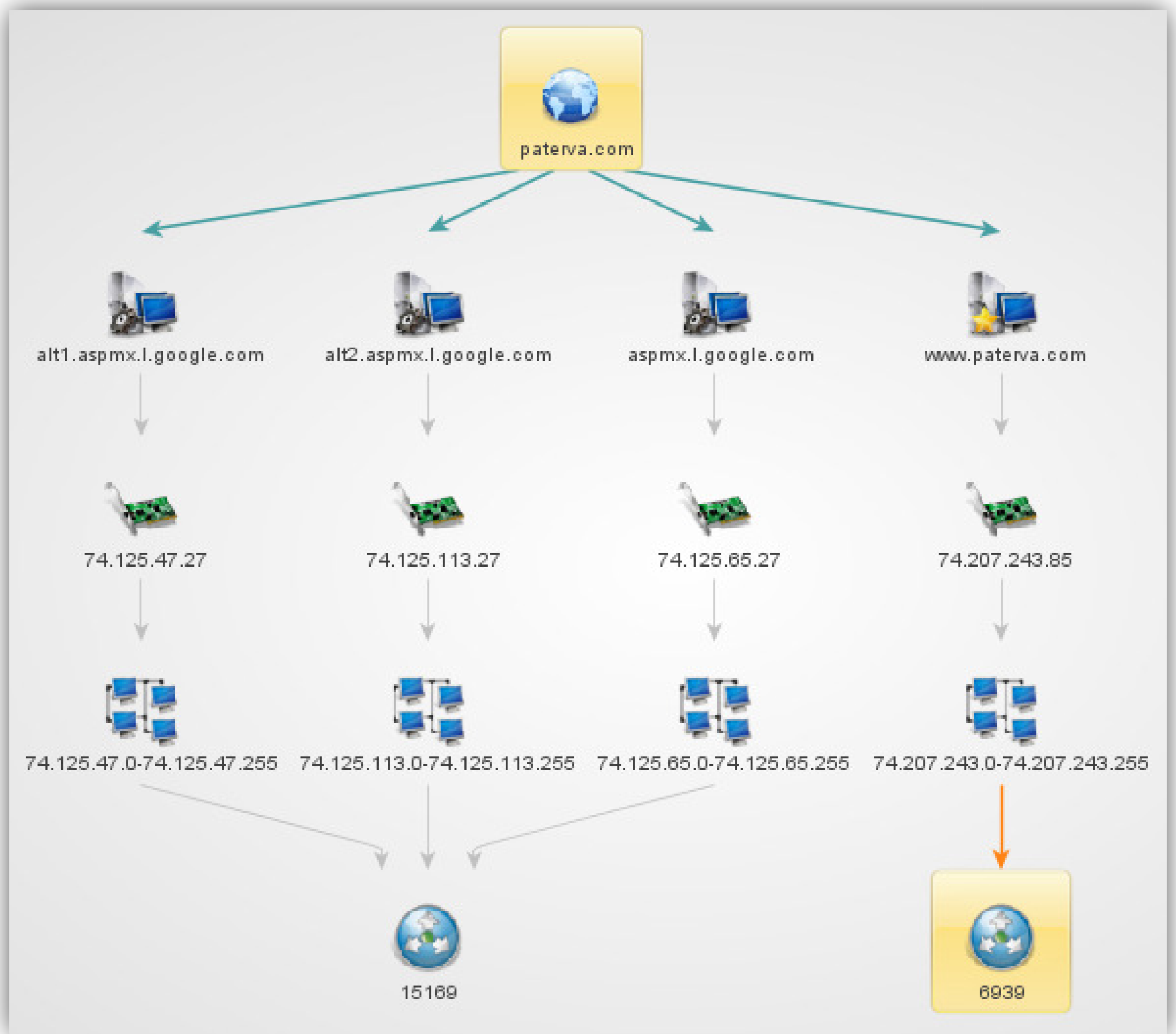
Show Label: Use Global Setting

Setting link labels to be visible or not

You can override the global setting per link by setting the 'Show label' to 'Yes' or 'No'. This applies to transform generated link labels as well as manual links.

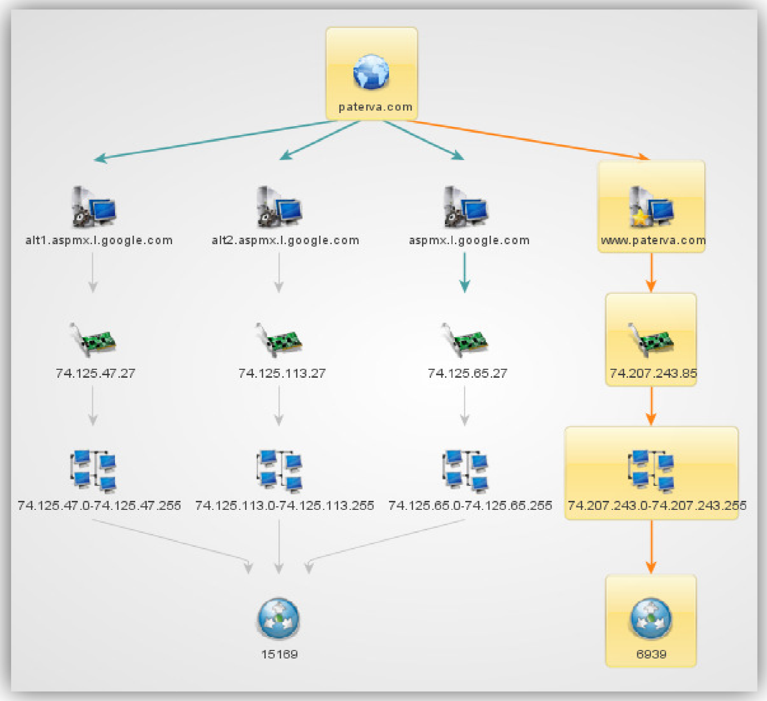
4.4.5 Add path

The 'add path' selection shortcut is most useful. It selects the nodes in the path between multiple nodes and there is disabled unless multiple nodes are selected. This is best shown with an example. Let's assume the following nodes are selected:



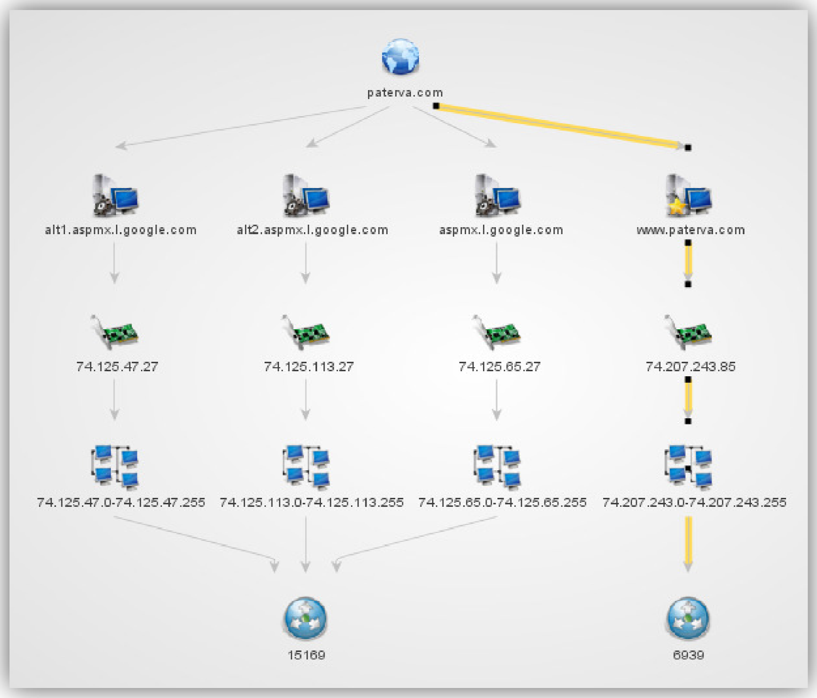
Selection to add path

When these nodes are selected and the 'Add path' button is clicked the following nodes will be selected (those along the path):



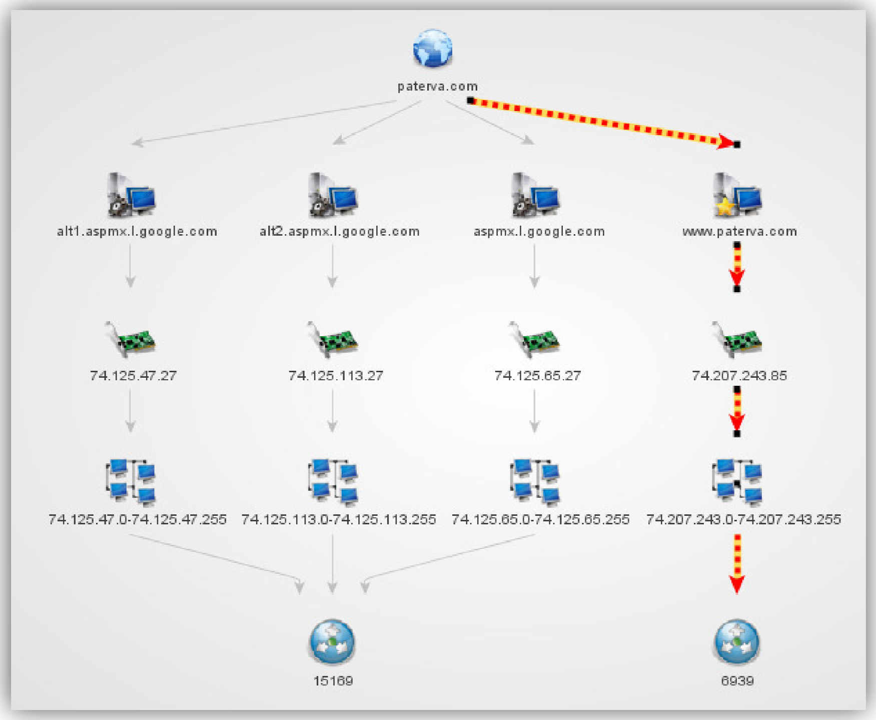
Path selected

This is very useful when combined with the Link/Entity selection mode. If the above graph is switched to Link selection mode, the links between the highlighted entities are selected:



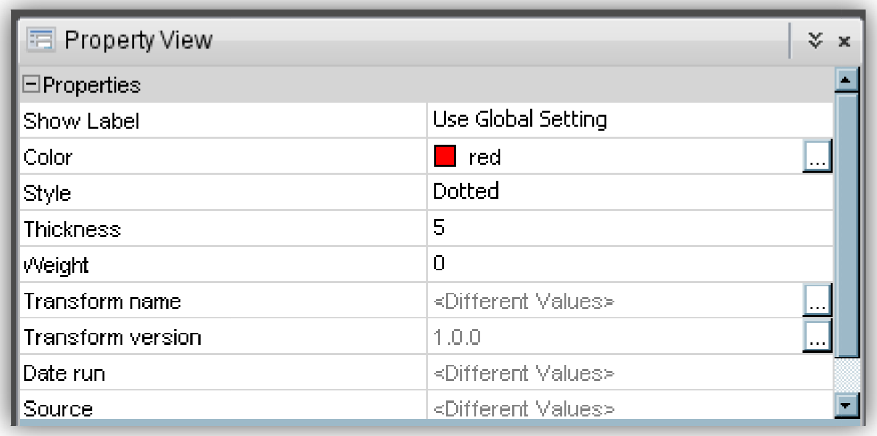
Links of path selected

They can now be edited. Let's assume we want to mark the path between the entities with a thick, dotted red line:



Properties of path links changed

The Property View for these settings ends up looking like this:

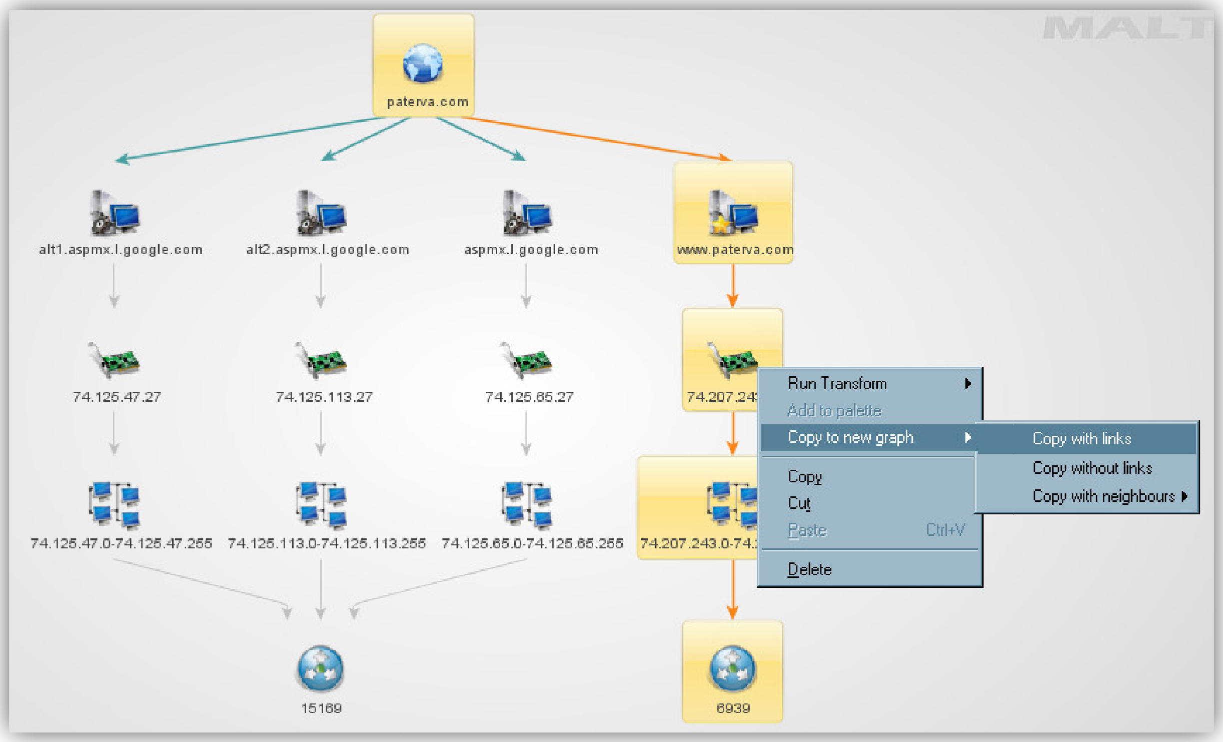


Property View

⊟Properties	
Show Label	Use Global Setting
Color	🟥 red
Style	Dotted
Thickness	5
Weight	0
Transform name	<Different Values>
Transform version	1.0.0
Date run	<Different Values>
Source	<Different Values>

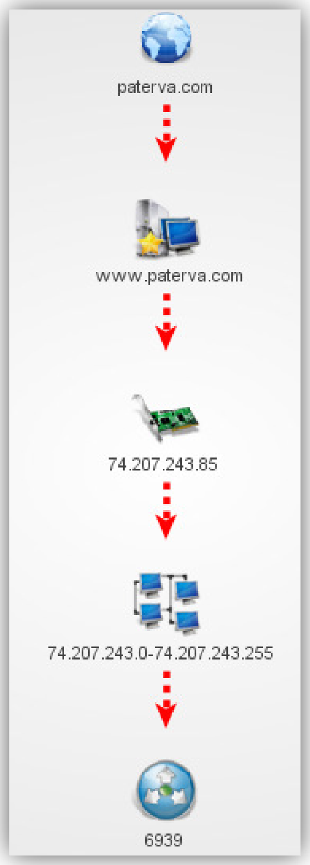
Link property view

We can also easily copy the selected path into a new graph. Switch back to entity selection mode and right click on any node – select Copy to new graph->Copy with links:



Selecting a path to be copied

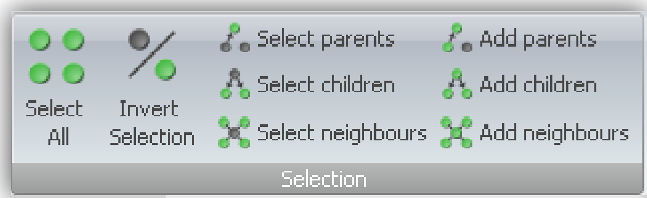
This results in a new graph with the path only:



New graph with copied path

The link parameters such as colour, style and thickness is preserved in the new graph.

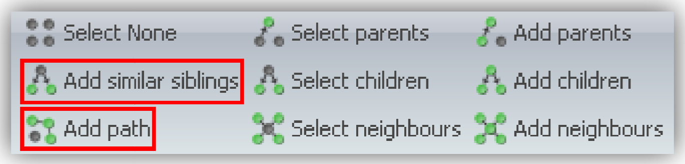
4.5 Selecting nodes



Selection Tools on the investigate tab in Maltego 3.0

4.5.1 New selection shortcuts

Two new selection shortcuts have been introduced since Maltego 3.0.2:



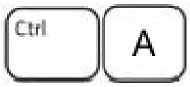
New selection options in Maltego 3.0.2

There are a few way of selecting entities.

- Simply click on the entity.
- You can select more than one entity by left click dragging a box around them.
- You can select entities one by one by click on them while holding in shift.
- Use the selection icons on the investigate tab.
- Use keyboard shortcuts.

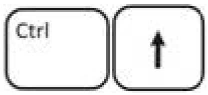
The selection options on the investigate tab are as follows:

- **Select All**. Well, select all the nodes. You can also press Control + A.

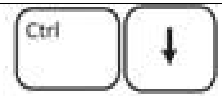


- **Invert Selection**. Invert Selection allows you to invert the selected nodes. Everything except what is currently selected will be selected.

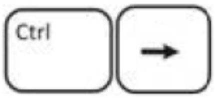
- **Select Parent**. You can select a parent of a node (e.g. the source of the selected node). This is useful to get to the original source of a child node. You can also select the node and pressing Control + Up Arrow.



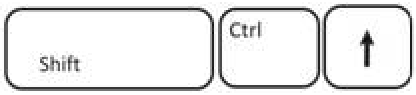
- **Select Children**. It is very useful to be able to select the children of a node (e.g. all the nodes that were created from the node). You can also do this by selecting the parent and pressing Control + Down Arrow.



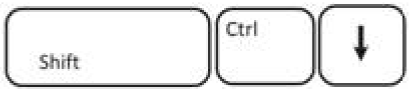
- **Select Neighbours**. Select the nodes directly adjacent to the present node.



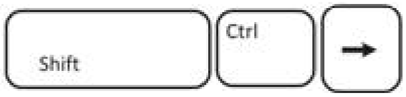
- **Add Parents**. You can select a child node and press Control + Shift + Up Arrow to select the parent while keeping the children. This is useful for selecting a "family tree", but from a child node's perspective.



- **Add Children**. Select child nodes while keeping parents selected.

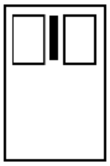


- **Add Neighbours**. Keep the present node and select the nodes directly adjacent to the present node as well.

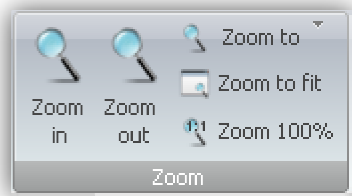


4.6 Zooming in and out

Use the scroll wheel of the mouse to zoom in and out of the graph.



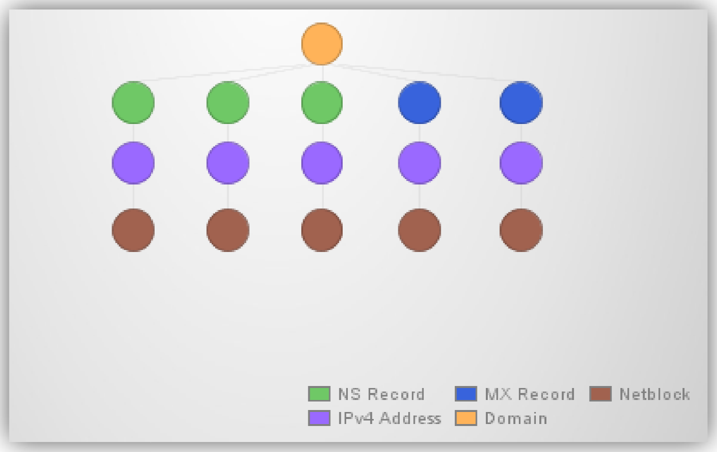
If you are using a notebook you can use the buttons on the investigate tab of the GUI:



Zoom Tools on the investigate tab

The ‘Zoom to fit’ button is very handy to quickly centre graphs (control Q on the keyboard). When zooming out on a graph you will see that it changes from detailed view to overview at a certain level. This is when it becomes impossible to read the entity’s value on the node. It therefore does not make any sense to show this detail.

When it overview mode different entities appear as different colours, with a small legend for mapping colours to entity types in the right hand bottom corner of the graph:

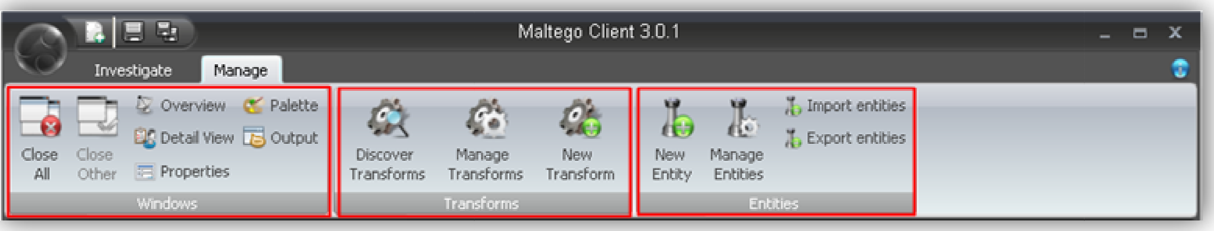


Note that the colours are not always the same – e.g. the IP address entity will not always be dark blue. This happens because Maltego can be used with custom entities, and the number of entities used is not known to the program. When zooming with the mouse scroll wheel the zoom to pointer method will be used. For example, if your mouse pointer was at the far left of a particular graph zooming in would mean that the graph would be slowly moved to the left until the central point was where the mouse pointer was rather than the central point being that of the centre of the graph.

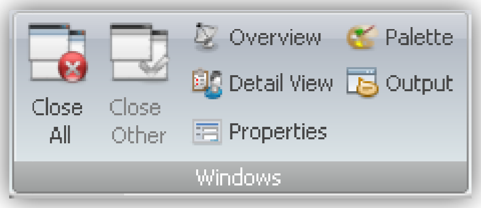
4.6.1 Zoom to selection

‘Zoom to selection’ was introduced in Maltego 3.0.3. This allows the user to select a portion of the graph using normal selection techniques and then quickly zoom to the area. This can be done by clicking on the ‘Zoom to selection’ button, or by pressing Control W.

5 Manage tab



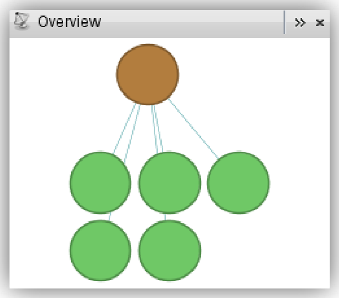
5.1 Maltego windows



Maltego 3 Windows options

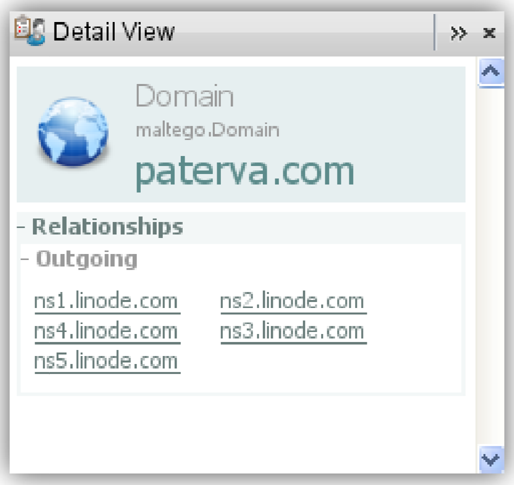
The Windows group of options under the manage tab allows the following actions:

- **Close All**. This will close all the graphs that are open at the moment. Maltego will first ask if you want to save the graphs first.
- **Close Other**. This option will close all the other graphs that are open except for the one that is currently being viewed. Maltego will first ask if you want to save any of the other graphs first.
- **Overview**. Will open the overview window on the right hand side of the screen if it is not open or it will simply change the focus to this window. The overview window provides an overview of the graph and allows for the easy navigation of very large graphs.



Overview window

- **Detail View**. This will open the detail view window on the right hand side of the screen if it is not open or it will simply change the focus to this window. Each entity has a number of properties and may have a detailed view. Most of the properties of an entity can be set while the detailed view is read-only. Detailed view information is not passed to the transform.



Domain

maltego.Domain

paterva.com

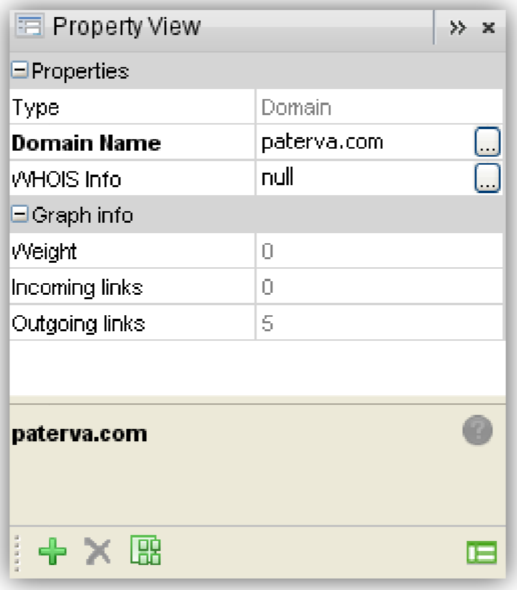
- Relationships

- Outgoing

ns1.linode.com ns2.linode.com
ns4.linode.com ns3.linode.com
ns5.linode.com

Detail View window

- **Entity Properties**. This will open the detail view window on the right hand side of the screen if it is not open or it will simply change the focus to this window. Each entity has a number of properties. Entity properties are shown and can be edited in the Entity property window. The properties of an entity are used by transforms and are passed along with the entity's value to the transform. More later.

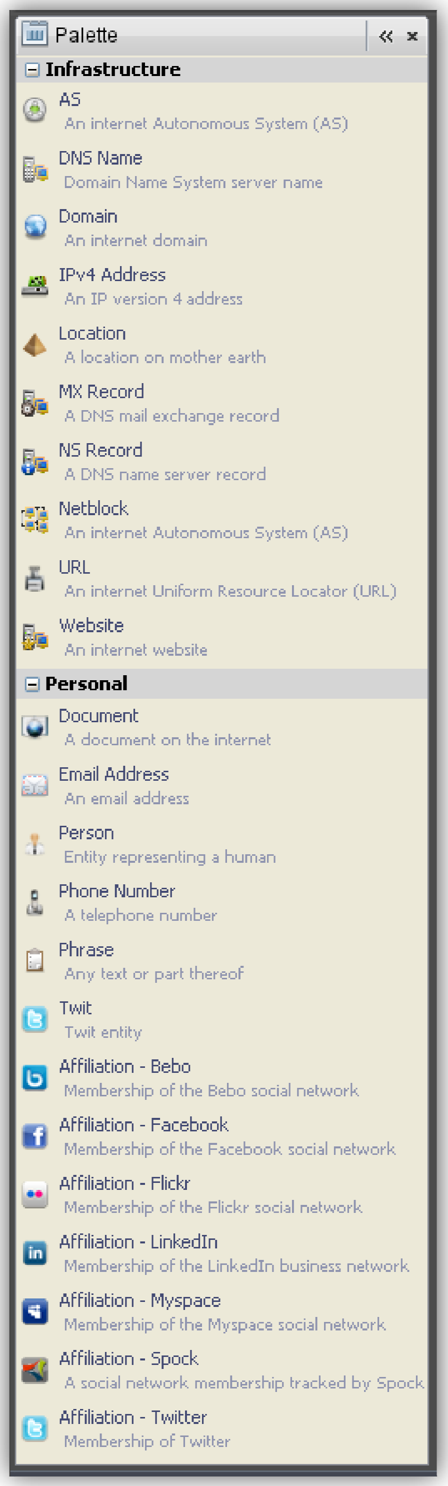


⊟ Properties	
Type	Domain
Domain Name	paterva.com
WHOIS Info	null
⊟ Graph info	
Weight	0
Incoming links	0
Outgoing links	5

paterva.com

Property View window

- **Palette**. This will open the Maltego Palette window on the left hand side of the screen if it is not open or it will simply change the focus to this window. The Maltego Palette provides a list of available entities divided into categories. By default there are two categories, namely, Infrastructure and Personal.



Infrastructure

AS
An internet Autonomous System (AS)

DNS Name
Domain Name System server name

Domain
An internet domain

IPv4 Address
An IP version 4 address

Location
A location on mother earth

MX Record
A DNS mail exchange record

NS Record
A DNS name server record

Netblock
An internet Autonomous System (AS)

URL
An internet Uniform Resource Locator (URL)

Website
An internet website

Personal

Document
A document on the internet

Email Address
An email address

Person
Entity representing a human

Phone Number
A telephone number

Phrase
Any text or part thereof

Twit
Twit entity

Affiliation - Bebo
Membership of the Bebo social network

Affiliation - Facebook
Membership of the Facebook social network

Affiliation - Flickr
Membership of the Flickr social network

Affiliation - LinkedIn
Membership of the LinkedIn business network

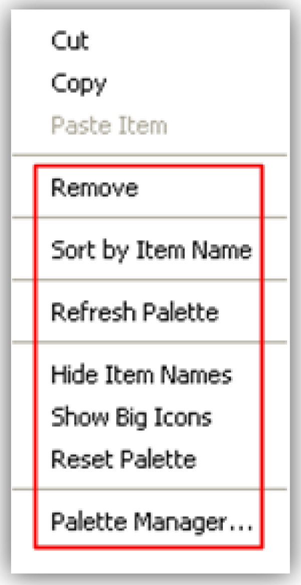
Affiliation - Myspace
Membership of the Myspace social network

Affiliation - Spock
A social network membership tracked by Spock

Affiliation - Twitter
Membership of Twitter

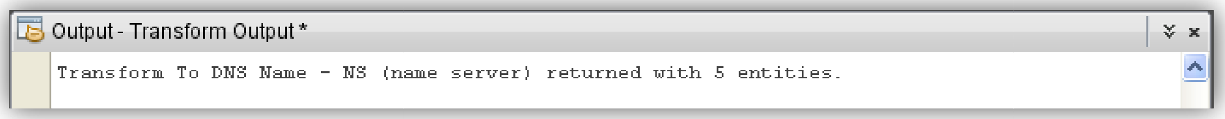
Palette Window

When you right-click on the palette you get some options to customise the display as shown below:



Options to customise palette

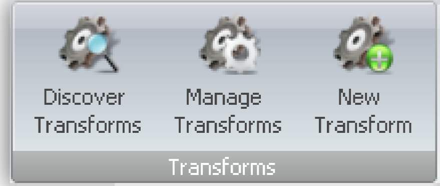
- **Output**. This will open the Output window at the bottom of the screen if it is not open or it will simply change the focus to this window. The Output window shows the output of transforms that are run. When in doubt as to what happened after a transform was run, remember to look here to see the output.



```
Transform To DNS Name - NS (name server) returned with 5 entities.
```

Output Window

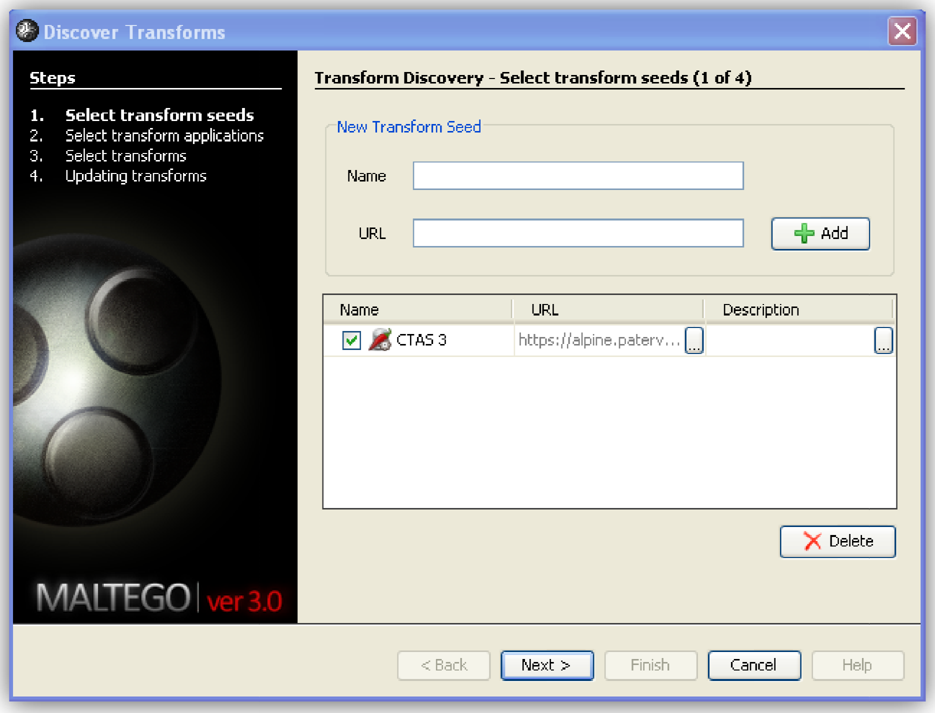
5.2 Managing transforms



Transform management

5.2.1 Discovering Transforms

The discovery process is one whereby you can discover various seeds containing Maltego transforms. This is often used when discovering new servers or determining if there are new transforms available on the servers you currently use.



Discover Transforms

Steps

1. Select transform seeds
2. Select transform applications
3. Select transforms
4. Updating transforms

Transform Discovery - Select transform seeds (1 of 4)

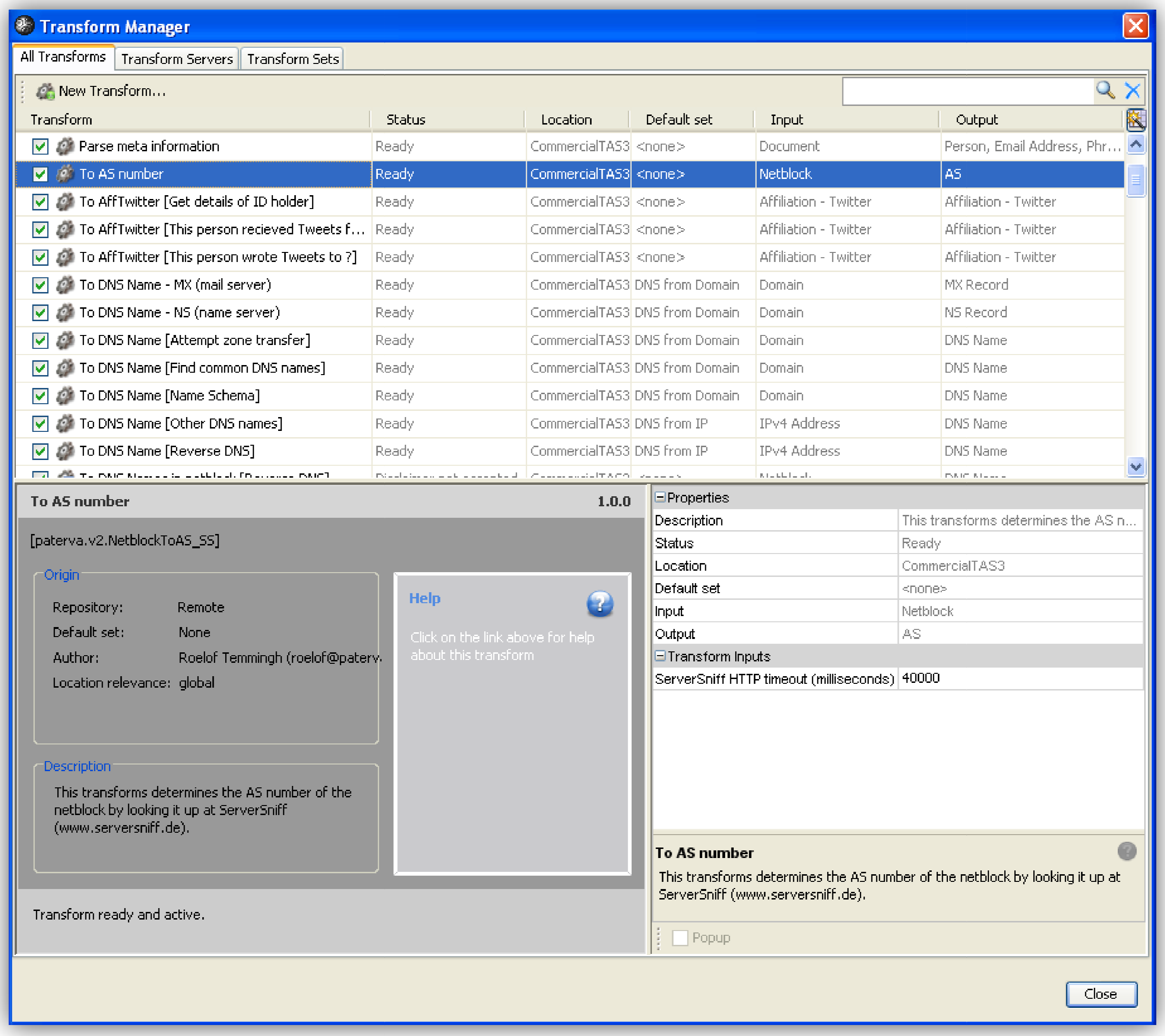
New Transform Seed

Name	URL	Description
☑ CTAS 3	https://alpine.paterv…	

Discover transforms

5.2.2 Manage Transforms

Transform Manager is a tool located within Maltego to help with the addition of transform application servers (TAS) as well as the configuration of transforms from those servers and Sets (groupings of transforms).



Transform Manager

All Transforms | Transform Servers | Transform Sets

New Transform...

Transform	Status	Location	Default set	Input	Output
☑ Parse meta information	Ready	CommercialTAS3	<none>	Document	Person, Email Address, Phr...
☑ To AS number	Ready	CommercialTAS3	<none>	Netblock	AS
☑ To AffTwitter [Get details of ID holder]	Ready	CommercialTAS3	<none>	Affiliation - Twitter	Affiliation - Twitter
☑ To AffTwitter [This person recieved Tweets f...	Ready	CommercialTAS3	<none>	Affiliation - Twitter	Affiliation - Twitter
☑ To AffTwitter [This person wrote Tweets to ?]	Ready	CommercialTAS3	<none>	Affiliation - Twitter	Affiliation - Twitter
☑ To DNS Name - MX (mail server)	Ready	CommercialTAS3	DNS from Domain	Domain	MX Record
☑ To DNS Name - NS (name server)	Ready	CommercialTAS3	DNS from Domain	Domain	NS Record
☑ To DNS Name [Attempt zone transfer]	Ready	CommercialTAS3	DNS from Domain	Domain	DNS Name
☑ To DNS Name [Find common DNS names]	Ready	CommercialTAS3	DNS from Domain	Domain	DNS Name
☑ To DNS Name [Name Schema]	Ready	CommercialTAS3	DNS from Domain	Domain	DNS Name
☑ To DNS Name [Other DNS names]	Ready	CommercialTAS3	DNS from IP	IPv4 Address	DNS Name
☑ To DNS Name [Reverse DNS]	Ready	CommercialTAS3	DNS from IP	IPv4 Address	DNS Name
☑ To DNS Names in netblock [Reverse DNS]	Disclaimer not accepted	CommercialTAS3	<none>	Netblock	DNS Name

To AS number 1.0.0

[paterva.v2.NetblockToAS_SS]

Origin

Repository: Remote
Default set: None
Author: Roelof Temmingh (roelof@paterv.
Location relevance: global

Description

This transforms determines the AS number of the netblock by looking it up at ServerSniff (www.serversniff.de).

Help

Click on the link above for help about this transform

Transform ready and active.

⊟ Properties

Description	This transforms determines the AS n...
Status	Ready
Location	CommercialTAS3
Default set	<none>
Input	Netblock
Output	AS

⊟ Transform Inputs

ServerSniff HTTP timeout (milliseconds)	40000

To AS number

This transforms determines the AS number of the netblock by looking it up at ServerSniff (www.serversniff.de).

□ Popup

Transform Manager: All Transforms

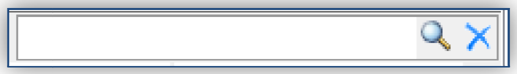
5.2.3 Editing Transforms

Transforms can be edited from the default Transform manager window (see above). From this window you can sort transforms by:

- Transform – The name of the transform.
- Status – Whether the transform is 'ready' or has requirements such as a disclaimer or input that needs to be set.
- Location – The Transform Application Servers (TAS) that this transform is found on.
- Default Set – The default set this transform can be found in.
- Input – The input entity type (what you click on to run this transform).

- Output – The output entity type(s) (What is returned after running this transform).

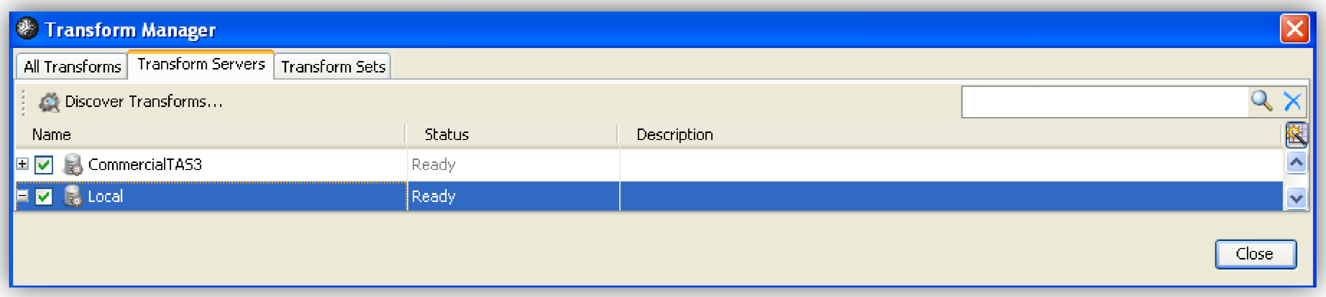
This window can also be searched via the control at the top right which will search the transform names column:



Search bar within the Transform Manager

With the default layout of the transform manager the following sections are also available:

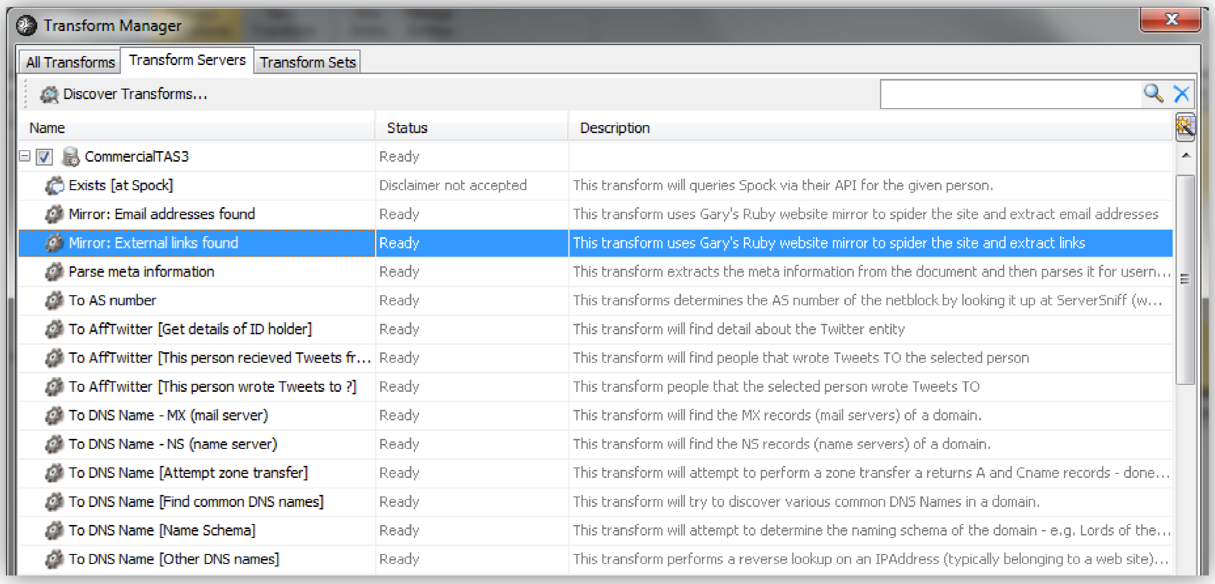
- Transform Information (Bottom left) - This section describes the transform, gives additional transform information such as transform author and informs of any user action needed, such as accepting disclaimers or if additional settings are needed.
- Transform Settings (Bottom Right) - This section allows the modification of transform specific settings such as API keys, timeouts, setting fields to popup and so on.
- Set Manager (Top Tab) - This button allows you to access the Set Manager where sets (groups of transforms) can be added, deleted and modified.
- Transform Servers (Top Tab) - This button allows you to access the Transform Servers tab whereby you can specify which transform servers are to be used and which not by turning checkboxes on and off. You can also view which transforms are available on each server.



Name	Status	Description
☑ CommercialTAS3	Ready	
☑ Local	Ready	

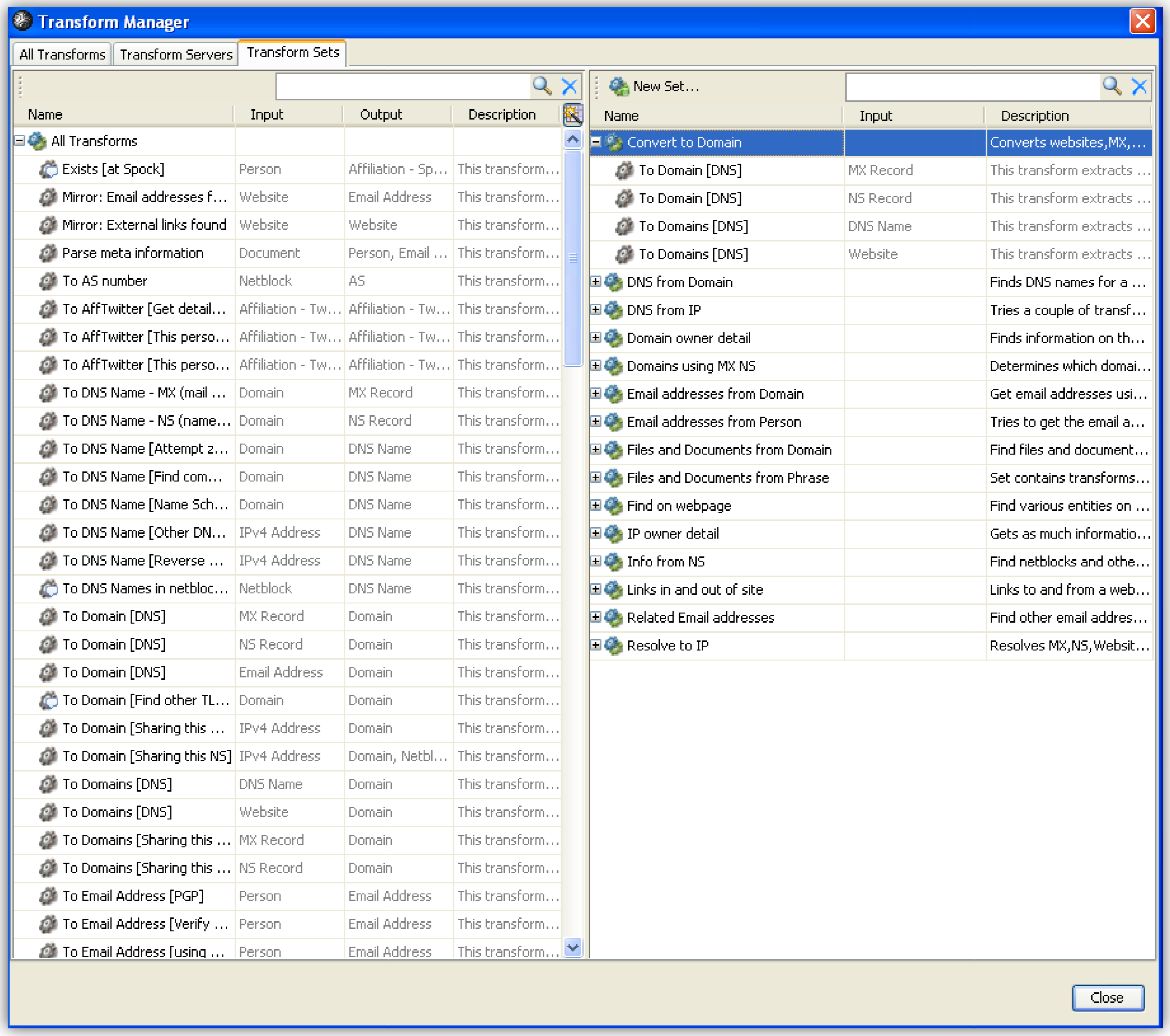
Transform Manager: Transform Servers

The Transform Servers tab displays the servers that are available to you which you can easily turn on and off to set if they are used. This is useful when you have multiple servers and would prefer not to specify every time you run a transform which server it should be run on. You can also view transforms on specific servers by expanding each server with the + icon, as seen below:



Name	Status	Description
☑ CommercialTAS3	Ready	
Exists [at Spock]	Disclaimer not accepted	This transform will queries Spock via their API for the given person.
Mirror: Email addresses found	Ready	This transform uses Gary's Ruby website mirror to spider the site and extract email addresses
Mirror: External links found	Ready	This transform uses Gary's Ruby website mirror to spider the site and extract links
Parse meta information	Ready	This transform extracts the meta information from the document and then parses it for usern…
To AS number	Ready	This transforms determines the AS number of the netblock by looking it up at ServerSniff (w…
To AffTwitter [Get details of ID holder]	Ready	This transform will find detail about the Twitter entity
To AffTwitter [This person recieved Tweets fr…	Ready	This transform will find people that wrote Tweets TO the selected person
To AffTwitter [This person wrote Tweets to ?]	Ready	This transform people that the selected person wrote Tweets TO
To DNS Name - MX (mail server)	Ready	This transform will find the MX records (mail servers) of a domain.
To DNS Name - NS (name server)	Ready	This transform will find the NS records (name servers) of a domain.
To DNS Name [Attempt zone transfer]	Ready	This transform will attempt to perform a zone transfer a returns A and Cname records - done…
To DNS Name [Find common DNS names]	Ready	This transform will try to discover various common DNS Names in a domain.
To DNS Name [Name Schema]	Ready	This transform will attempt to determine the naming schema of the domain - e.g. Lords of the…
To DNS Name [Other DNS names]	Ready	This transform performs a reverse lookup on an IPAddress (typically belonging to a web site)…

Transform Manager: Transform Servers



Name	Input	Output	Description
All Transforms			
Exists [at Spock]	Person	Affiliation - Sp…	This transform…
Mirror: Email addresses f…	Website	Email Address	This transform…
Mirror: External links found	Website	Website	This transform…
Parse meta information	Document	Person, Email …	This transform…
To AS number	Netblock	AS	This transform…
To AffTwitter [Get detail…	Affiliation - Tw…	Affiliation - Tw…	This transform…
To AffTwitter [This perso…	Affiliation - Tw…	Affiliation - Tw…	This transform…
To AffTwitter [This perso…	Affiliation - Tw…	Affiliation - Tw…	This transform…
To DNS Name - MX (mail …	Domain	MX Record	This transform…
To DNS Name - NS (name…	Domain	NS Record	This transform…
To DNS Name [Attempt z…	Domain	DNS Name	This transform…
To DNS Name [Find com…	Domain	DNS Name	This transform…
To DNS Name [Name Sch…	Domain	DNS Name	This transform…
To DNS Name [Other DN…	IPv4 Address	DNS Name	This transform…
To DNS Name [Reverse …	IPv4 Address	DNS Name	This transform…
To DNS Names in netbloc…	Netblock	DNS Name	This transform…
To Domain [DNS]	MX Record	Domain	This transform…
To Domain [DNS]	NS Record	Domain	This transform…
To Domain [DNS]	Email Address	Domain	This transform…
To Domain [Find other TL…	Domain	Domain	This transform…
To Domain [Sharing this …	IPv4 Address	Domain	This transform…
To Domain [Sharing this NS]	IPv4 Address	Domain, Netbl…	This transform…
To Domains [DNS]	DNS Name	Domain	This transform…
To Domains [DNS]	Website	Domain	This transform…
To Domains [Sharing this …	MX Record	Domain	This transform…
To Domains [Sharing this …	NS Record	Domain	This transform…
To Email Address [PGP]	Person	Email Address	This transform…
To Email Address [Verify …	Person	Email Address	This transform…
To Email Address [using …	Person	Email Address	This transform…

Name	Input	Description
Convert to Domain		Converts websites,MX,…
To Domain [DNS]	MX Record	This transform extracts …
To Domain [DNS]	NS Record	This transform extracts …
To Domains [DNS]	DNS Name	This transform extracts …
To Domains [DNS]	Website	This transform extracts …
DNS from Domain		Finds DNS names for a …
DNS from IP		Tries a couple of transf…
Domain owner detail		Finds information on th…
Domains using MX NS		Determines which domai…
Email addresses from Domain		Get email addresses usi…
Email addresses from Person		Tries to get the email a…
Files and Documents from Domain		Find files and document…
Files and Documents from Phrase		Set contains transforms…
Find on webpage		Find various entities on …
IP owner detail		Gets as much informatio…
Info from NS		Find netblocks and othe…
Links in and out of site		Links to and from a web…
Related Email addresses		Find other email addres…
Resolve to IP		Resolves MX,NS,Websit…

Transform Manager: Transforms Sets

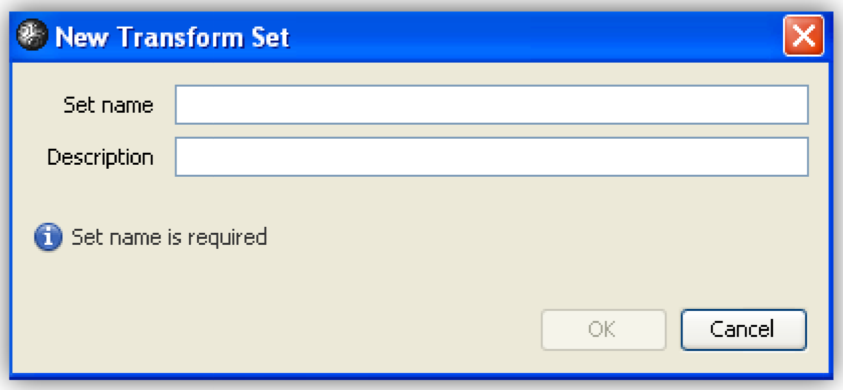
Note that there is a list of transforms and that most of them have a green icon on the left (which means they are ready to be used).

5.3 Sets

Sets are a way of grouping transforms that are commonly run together, with the default installation of Maltego you will notice various sets have been preconfigured for you, such as the "Resolve to IP" set which groups the transforms that convert DNSName, MX Record, NS Record and Website Entities to IP addresses. This has been done so that instead of having to select each individual entity type you can run a "set" of transforms on them.

To create your own sets click the Set Manager tab located within the Transform Manager (Top Right). The set manager is relatively straight forward with a basic interface to manage which transforms are within each set.

5.3.1 Creating new sets



Set name is required

To create a new set simply select the "New Set..." button within the Set Manager and fill in the Set Name and a description for the set (optional).

5.3.2 Adding/Removing Transforms from Sets

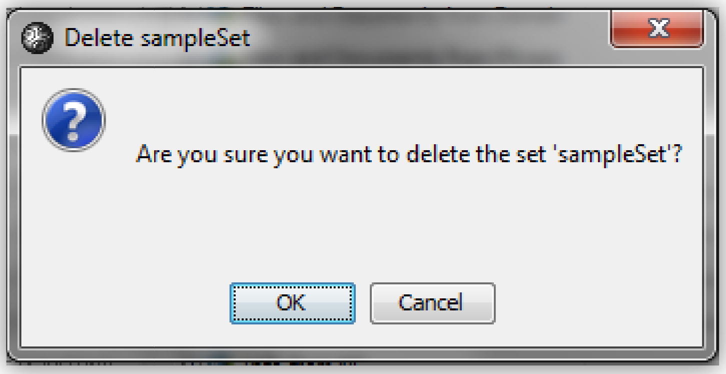
To add or remove transforms from a set start by selecting the set you wish to modify from the list of available sets within the right hand pane and then drag the transform from the left hand pane over it.

To add more than one transform to the set simply select multiple transforms by using either the shift or control modifiers and then drag the selection onto the set. Alternatively you can simply select the transforms you wish to add, right click on them and use the “Add to Set->” context menu and select the set you wish to use.

To remove specific transforms to a set select the transforms that you wish to remove within the selected set, right click and select ‘Remove from set’.

5.3.3 Deleting Sets

To permanently delete a set select the set from the right hand pane, right click on it and on 'Delete...'. You will then be given a dialog to confirm that you wish to delete the set:



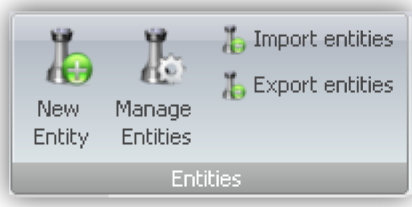
Delete sampleSet

Are you sure you want to delete the set 'sampleSet'?

Deleting Set Confirmation

Selecting OK on this dialog will delete the set permanently.

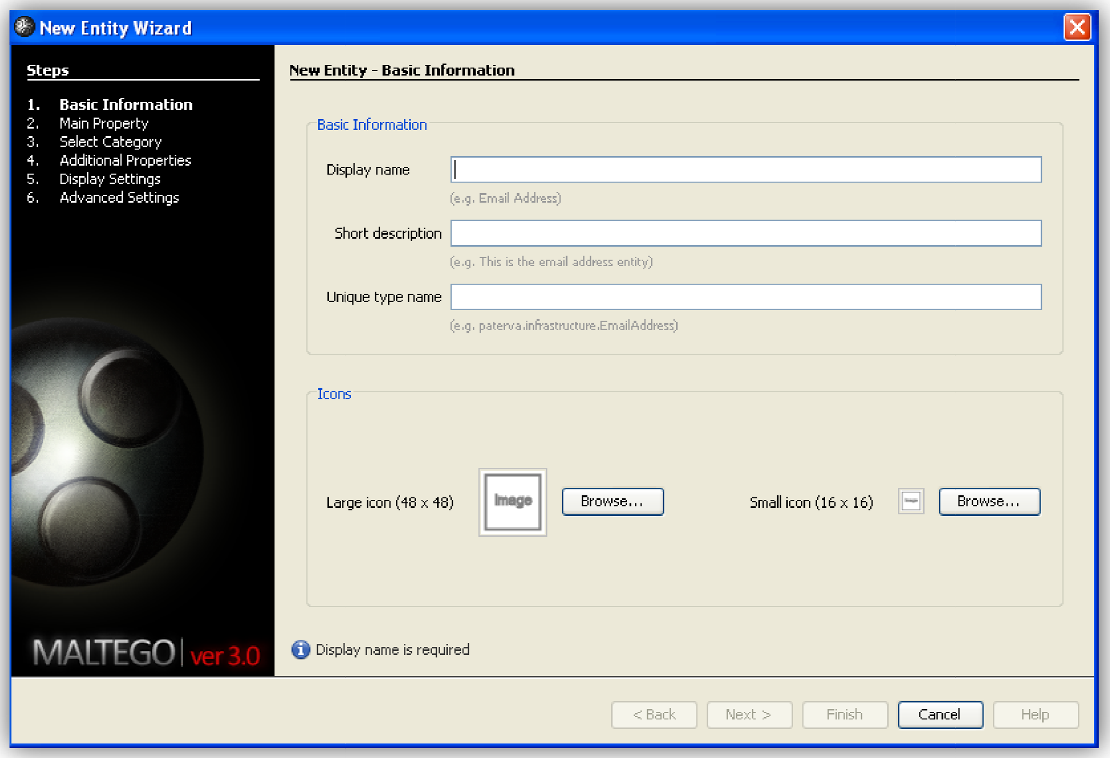
5.4 Managing entities



Entity management

The Entities section of the management tab allows the following:

- **New Entity**. Allows for the creation of custom entities. This selection opens a wizard that will guide you through the process of creating a new custom entity. The process of creating a custom entity is discussed in detail in the Entities section.



New Entity Wizard

Steps

1. Basic Information
2. Main Property
3. Select Category
4. Additional Properties
5. Display Settings
6. Advanced Settings

New Entity - Basic Information

Basic Information

Display name: (e.g. Email Address)

Short description: (e.g. This is the email address entity)

Unique type name: (e.g. paterva.infrastructure.EmailAddress)

Icons

Large icon (48 x 48)

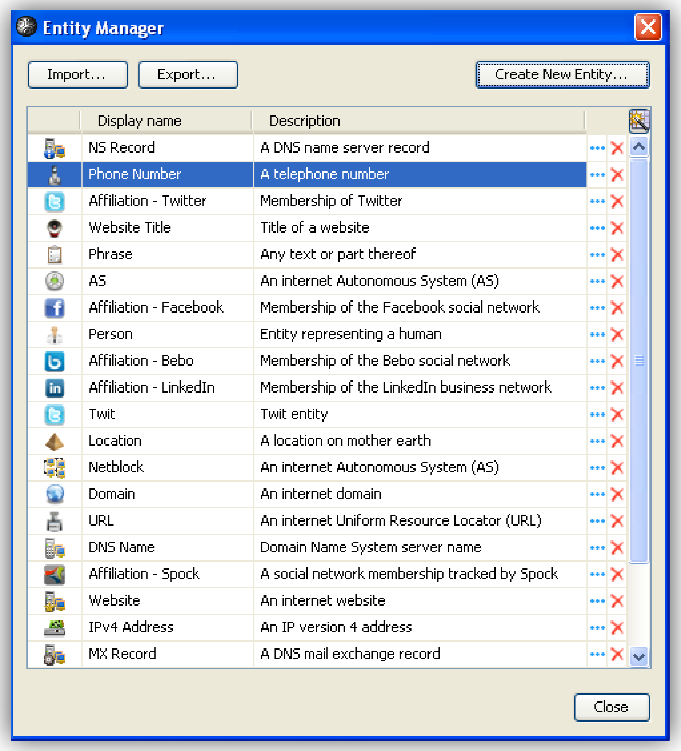
Small icon (16 x 16)

Display name is required

New Entity Wizard

Going through this wizard will allow you to create new entities with all their relevant settings as well as icons.

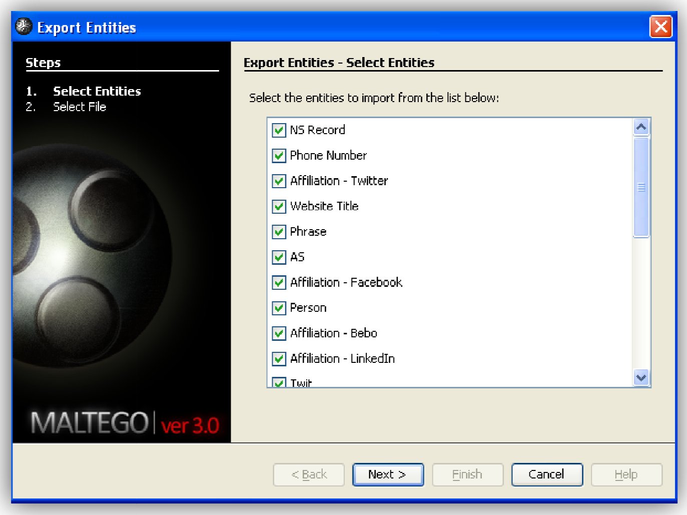
- **Manage Entities**. This option allows the user to change the properties of an entity, to delete it completely, initiate the creation of a new entity as well as the import and export of entities. More on this in the Entities section.



Display name	Description
NS Record	A DNS name server record
Phone Number	A telephone number
Affiliation - Twitter	Membership of Twitter
Website Title	Title of a website
Phrase	Any text or part thereof
AS	An internet Autonomous System (AS)
Affiliation - Facebook	Membership of the Facebook social network
Person	Entity representing a human
Affiliation - Bebo	Membership of the Bebo social network
Affiliation - LinkedIn	Membership of the LinkedIn business network
Twit	Twit entity
Location	A location on mother earth
Netblock	An internet Autonomous System (AS)
Domain	An internet domain
URL	An internet Uniform Resource Locator (URL)
DNS Name	Domain Name System server name
Affiliation - Spock	A social network membership tracked by Spock
Website	An internet website
IPv4 Address	An IP version 4 address
MX Record	A DNS mail exchange record

Entity Manager

- **The Import and Export of Entities.** Entities can be imported and exported. Entities can be Imported as part of Maltego Archives or Maltego graphs (*.mtz or *.mtgx) and Exported as a *.mtz file.



Steps

1. **Select Entities**
2. Select File

Export Entities - Select Entities

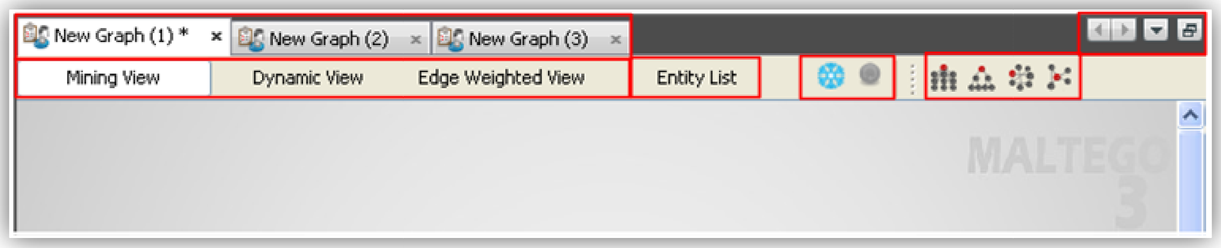
Select the entities to import from the list below:

☑ NS Record
☑ Phone Number
☑ Affiliation - Twitter
☑ Website Title
☑ Phrase
☑ AS
☑ Affiliation - Facebook
☑ Person
☑ Affiliation - Bebo
☑ Affiliation - LinkedIn
☑ Twit

Exporting Entities

6 Graph options

Screen real estate is very valuable and there is a lot of information that needs to be displayed by Maltego. Depending on the size of your screen you will need to move things around, display the differently and sometimes hide them to be able to see what you want to see. This section is all about getting the most out of your GUI.



6.1 Graph tabs

The graph tabs will display a list of all the graphs that are open. Graphs that have not been saved yet will be displayed as “New Graph (number)”. Once a graph is saved the display name on the name tag will change to the name under which it was saved. The * behind a graph indicates that it contains data and the current view will be light in colour.

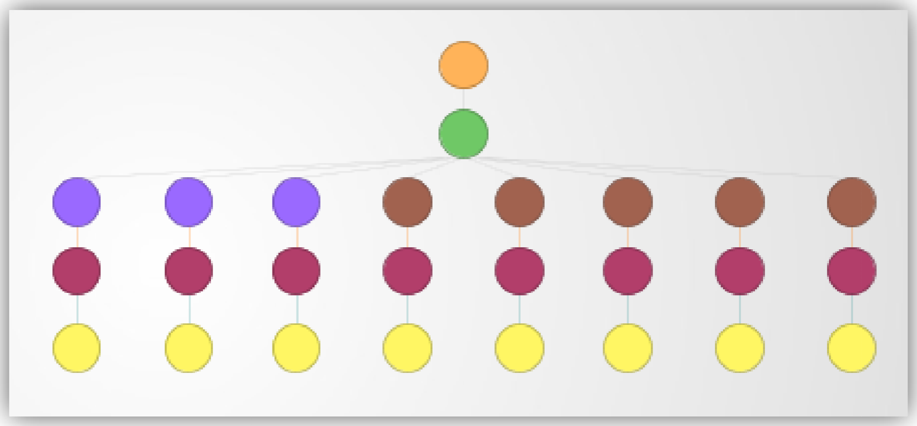
6.2 Views

Views are used to extract non-obvious information from large graphs – where the analyst cannot see clear relationships by manual inspection of data. Other than the Mining View, Maltego supports three other views:

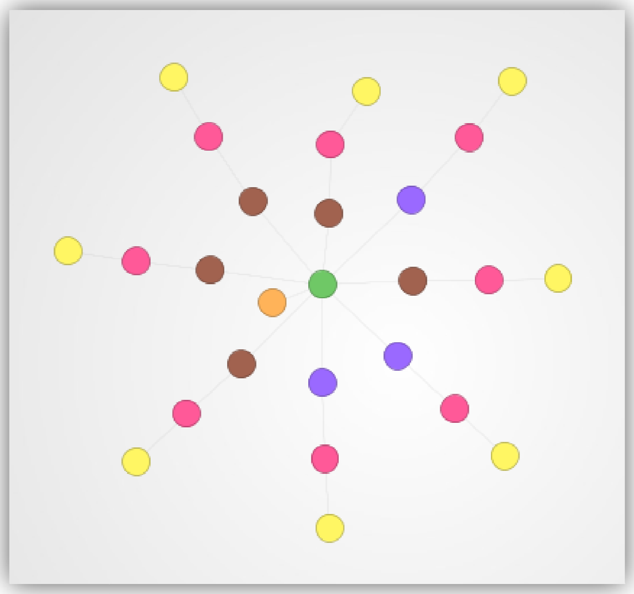
1. Dynamic view. Nodes that are calculated to be most central to the graph are given larger nodes.
2. Edge weighted view. Node sizes are based on number of incoming links. This view allows to view which nodes within your network are most linked to.
3. Entity List. Entity list is simply a listing of nodes in text format allowing you to easily sort through them and manage them based on Type, Value, Incoming and Outgoing links as well as the weight of the entities.

As with the default Mining view transforms can be run on all entities within each view.

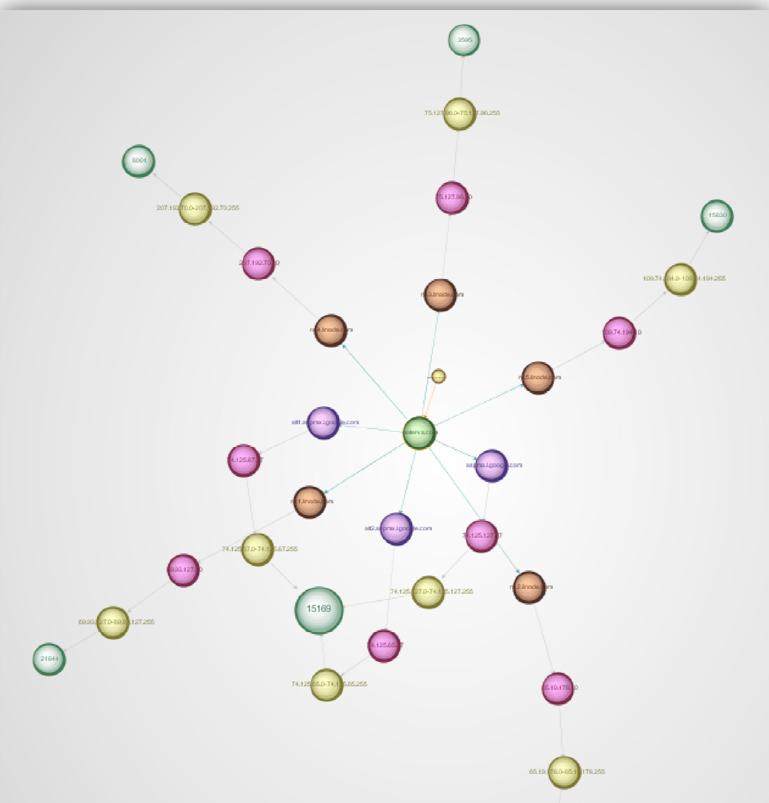
Mining view



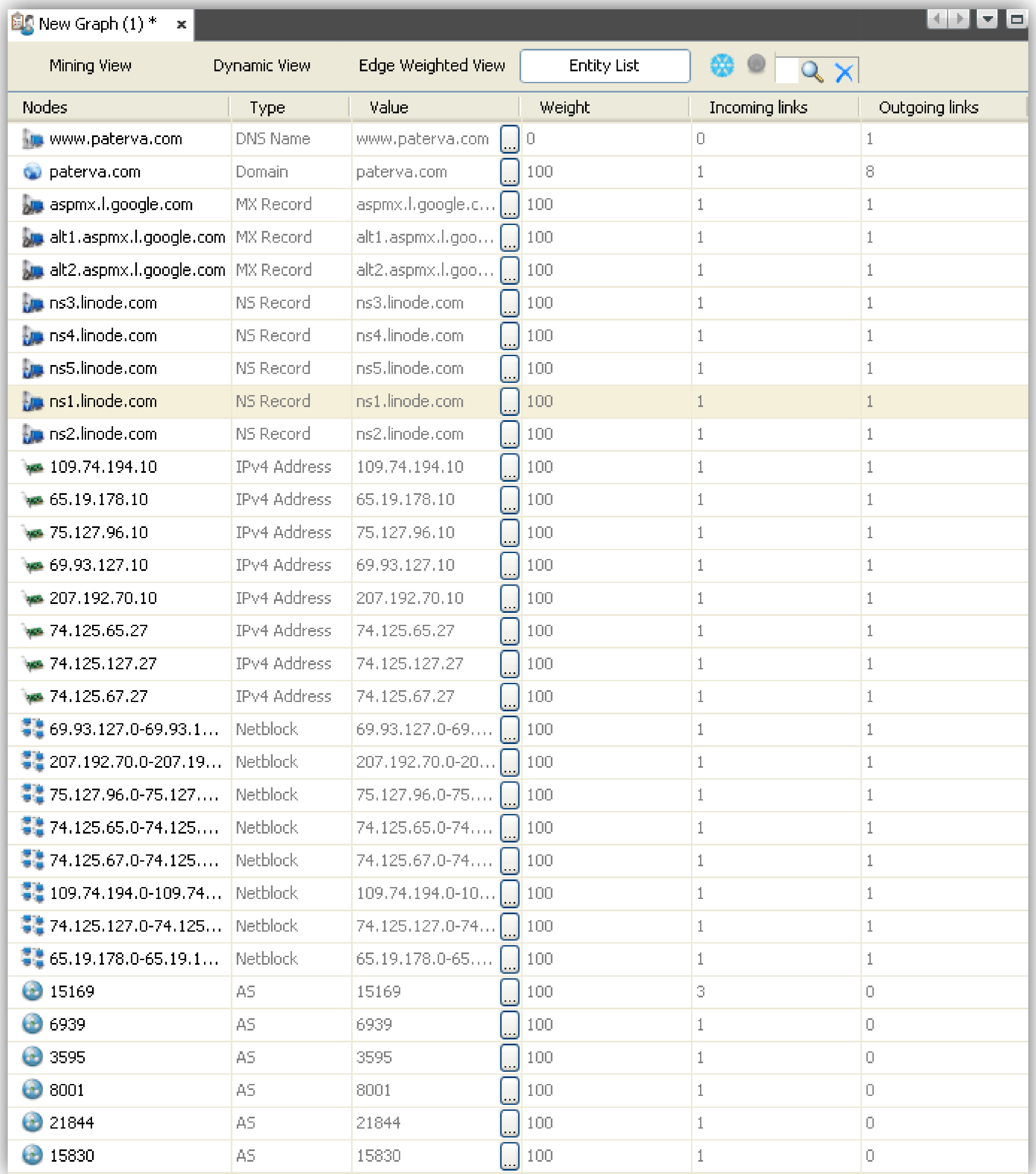
Dynamic view



Edge weighted view

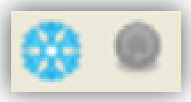

3595
6001
15830
15169
21844

6.3 Entity List

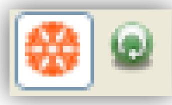


Nodes	Type	Value	Weight	Incoming links	Outgoing links
www.paterva.com	DNS Name	www.paterva.com	0	0	1
paterva.com	Domain	paterva.com	100	1	8
aspmx.l.google.com	MX Record	aspmx.l.google.c...	100	1	1
alt1.aspmx.l.google.com	MX Record	alt1.aspmx.l.goo...	100	1	1
alt2.aspmx.l.google.com	MX Record	alt2.aspmx.l.goo...	100	1	1
ns3.linode.com	NS Record	ns3.linode.com	100	1	1
ns4.linode.com	NS Record	ns4.linode.com	100	1	1
ns5.linode.com	NS Record	ns5.linode.com	100	1	1
ns1.linode.com	NS Record	ns1.linode.com	100	1	1
ns2.linode.com	NS Record	ns2.linode.com	100	1	1
109.74.194.10	IPv4 Address	109.74.194.10	100	1	1
65.19.178.10	IPv4 Address	65.19.178.10	100	1	1
75.127.96.10	IPv4 Address	75.127.96.10	100	1	1
69.93.127.10	IPv4 Address	69.93.127.10	100	1	1
207.192.70.10	IPv4 Address	207.192.70.10	100	1	1
74.125.65.27	IPv4 Address	74.125.65.27	100	1	1
74.125.127.27	IPv4 Address	74.125.127.27	100	1	1
74.125.67.27	IPv4 Address	74.125.67.27	100	1	1
69.93.127.0-69.93.1...	Netblock	69.93.127.0-69....	100	1	1
207.192.70.0-207.19...	Netblock	207.192.70.0-20...	100	1	1
75.127.96.0-75.127....	Netblock	75.127.96.0-75....	100	1	1
74.125.65.0-74.125....	Netblock	74.125.65.0-74....	100	1	1
74.125.67.0-74.125....	Netblock	74.125.67.0-74....	100	1	1
109.74.194.0-109.74...	Netblock	109.74.194.0-10...	100	1	1
74.125.127.0-74.125...	Netblock	74.125.127.0-74...	100	1	1
65.19.178.0-65.19.1...	Netblock	65.19.178.0-65....	100	1	1
15169	AS	15169	100	3	0
6939	AS	6939	100	1	0
3595	AS	3595	100	1	0
8001	AS	8001	100	1	0
21844	AS	21844	100	1	0
15830	AS	15830	100	1	0

6.4 Delay display



Default delay display



Delay display activated

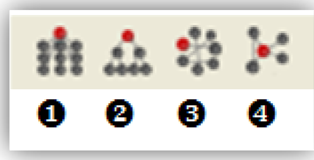
The delay display buttons are used when you have a large number of nodes that are coming into the graph (e.g. running a lot of transforms on many nodes) and don't wish for the layout to be constantly updating. By delaying the layout the application can process transforms faster as it does not need to update the display after every transform.

To freeze the graph layout simply press the blue freeze button, this button will then turn red whilst the graph is frozen. To unfreeze the graph simply press the same button (which will be red now) and the graph will resume as normal.

If, while your graph is frozen new entities have come back from a transform you will notice that the update icon located next to the freeze icon becomes enabled (green), pressing this while the graph is frozen will update it to the latest entities.

6.5 Layout

Maltego supports 4 types of layout algorithms:



Layout Options

1. **Block layout**. This is the default layout and is also used during mining. This layout is discussed in more depth later.
2. **Hierarchical layout**. Think of this a tree based layout – like a file manager.
3. **Centrality layout**. Nodes that are most central to the graph (e.g. most incoming links) appear in the middle

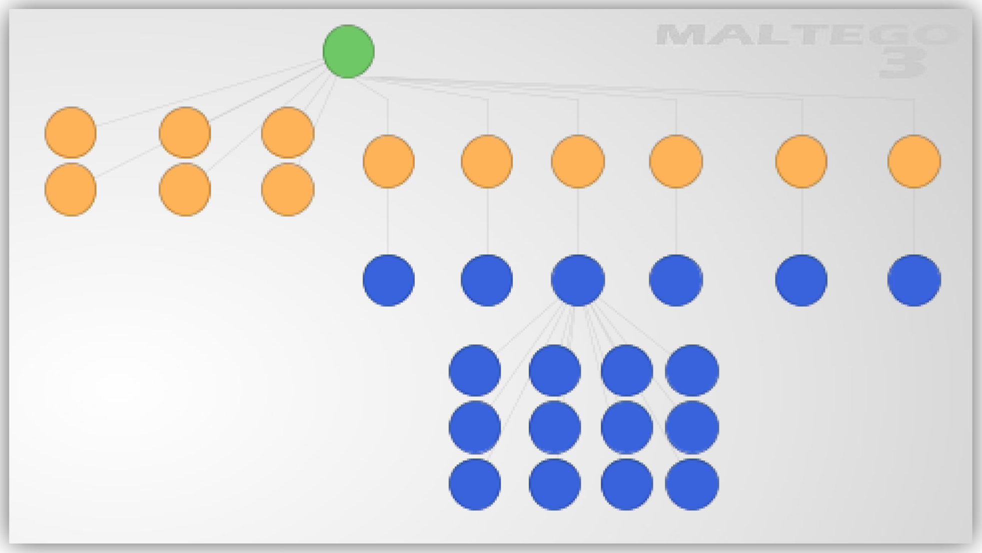
with the other nodes scattered around it.

4. **Organic layout**. Nodes are packed tight together in such a way that the distance between each node and all the other nodes are minimized.

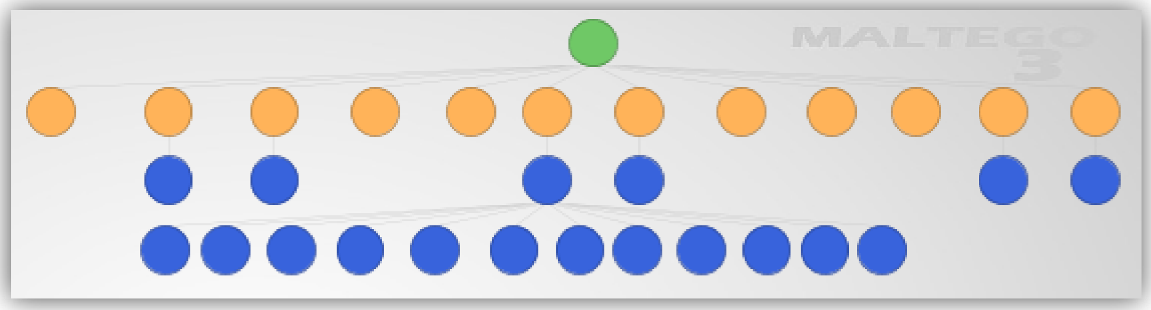
You can switch between views at any time by clicking on the relevant icon (located at the top of graph window). Selection of nodes will be preserved between layouts. The block layout is used during mining and the application will always switch to this view when new results are obtained. In this layout nodes are shown using the following rules:

1. In a block of nodes
2. Sorted by entity type
3. Sorted by entity weight

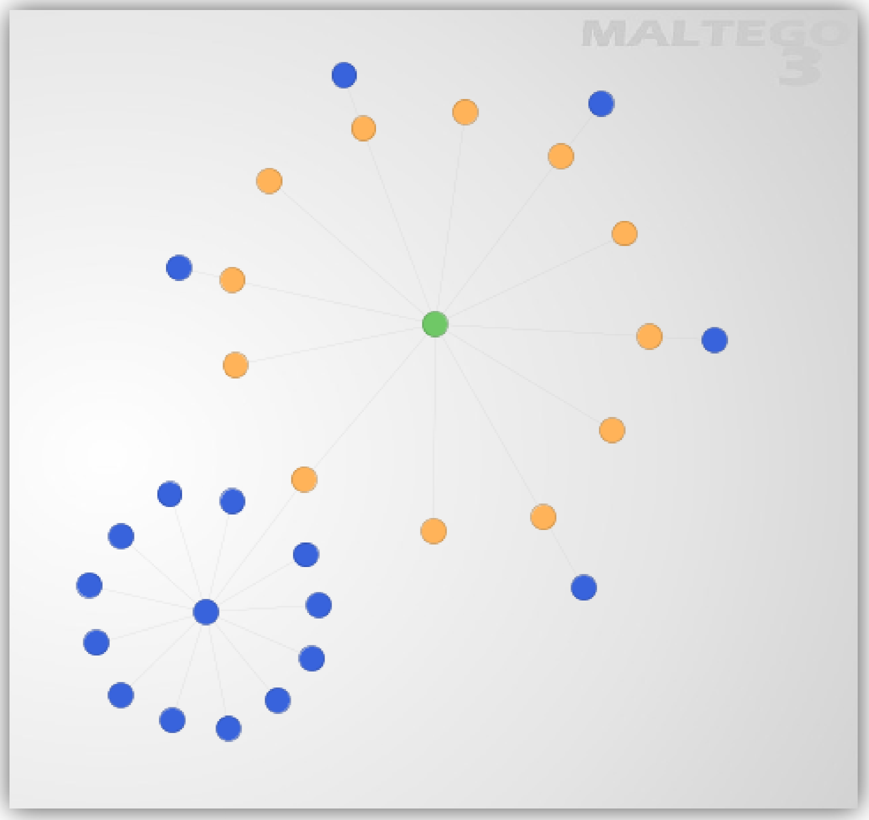
Examples of these layouts are as follows:



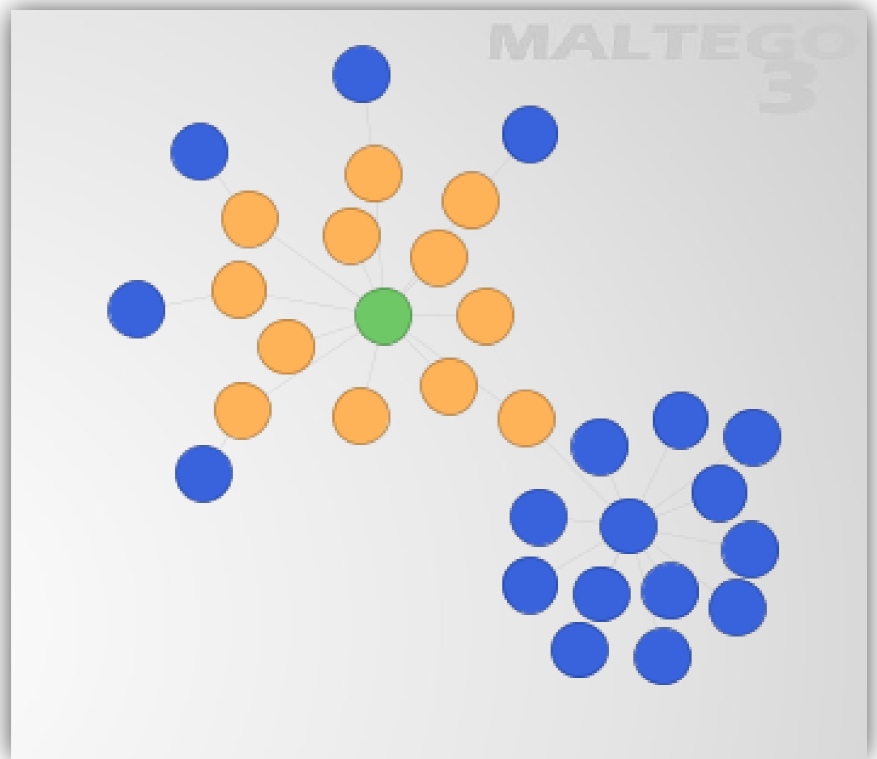
Block layout



Hierarchical layout



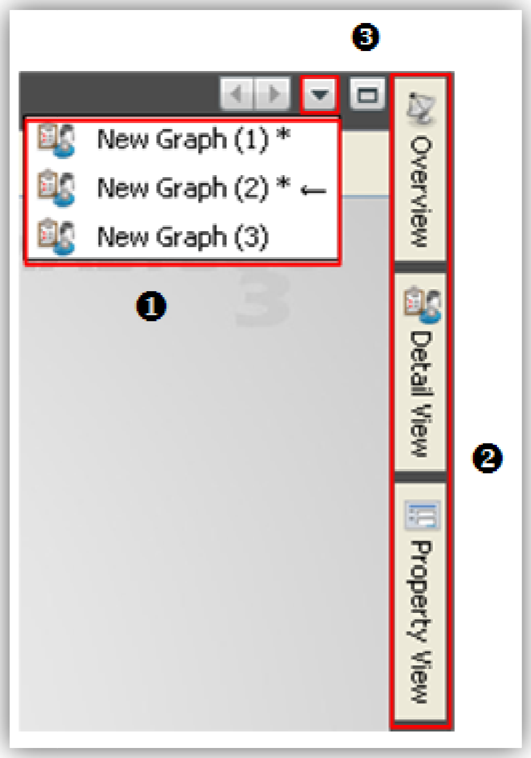
Centrality layout



Organic layout

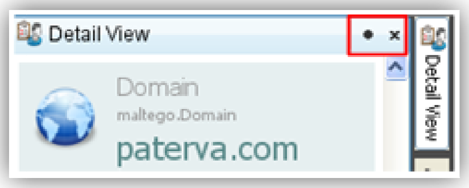
6.6 Display button

Navigating the display is always an issue of being able to see only what you want to see. For this reason the GUI has been made very versatile and adaptable. As discussed previously graphs are maintained in tabs which can be flipped through. The next section details some of the options available display information windows. On the top right hand side of the graph the following options are available:



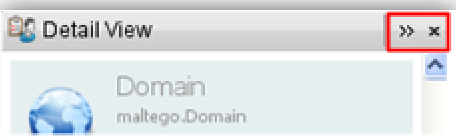
Graphs and Windows

1. **Show Opened Documents List**. The show opened documents list button will display a list of all the graphs that are open. Graphs that have not been saved yet will be displayed as "New Graph (number)". Once a graph is saved the display name on the name tag will change to the name under which it was saved. In the documents list view the * behind a graph indicates that it contains data and the arrow points to the current view.
2. **Overview, Detail View and Property View tabs**. Once these windows have been minimised they remain available as tabs at the side of the GUI. If you click on one of the tabs the window will open as seen below:



Snap in place or close Window

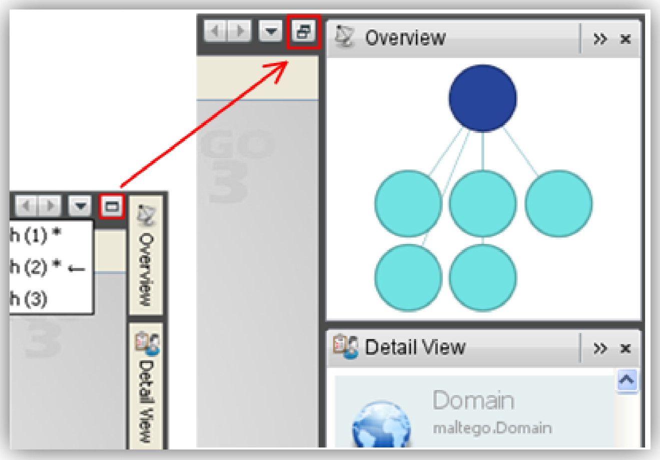
The user now has the option to let the window snap in place on the righthand side of the screen (•) or to close it completely (**x**). Once the window is in place the icons will change as seen in the graphic below:



Minimise or Close Window

The options available are now to minimise the window (**>>**) again or to close it completely (**x**). It can be opened again from the Manage tab. The windows can also be ragged around to snap into place in different configurations. It is all up to the user how he/she wants to setup their working environment and of course the amount of screen real estate available.

3. **The Minimise/Maximise button**. This button allows the user to setup two views to swop between, for example, a view with only the graph and a view with all the additional information windows (Overview, Detail View, Property View and the Output Window).



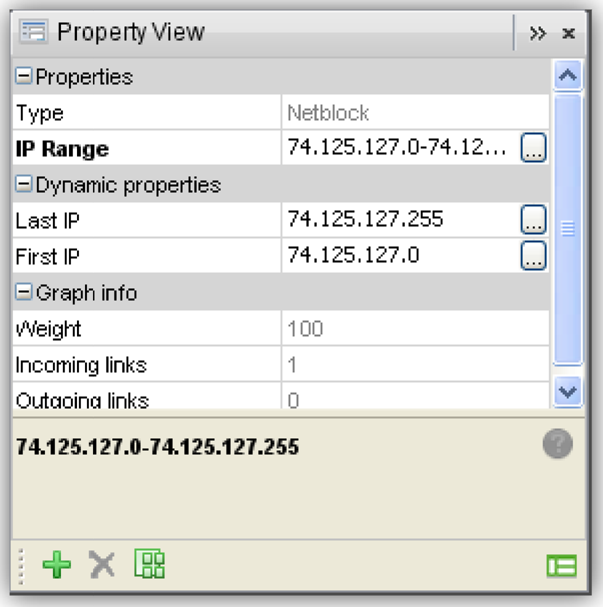
Maximise / Minimise Graph

7 Entity Properties and Detailed View

Each entity has a number of properties and may have a detailed view. Most of the properties of an entity can be set while the detailed view is read-only. The properties of an entity are used by transforms and are passed along with the entity's value to the transform. Detailed view information is not passed to the transform.

7.1 Entity properties

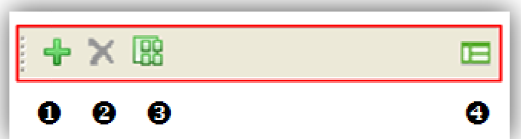
Entity properties are shown and can be edited in the Entity property window. Hereby the entity property of a netblock:



Property View

⊟Properties	
Type	Netblock
IP Range	74.125.127.0-74.12...
⊟Dynamic properties	
Last IP	74.125.127.255
First IP	74.125.127.0
⊟Graph info	
Weight	100
Incoming links	1
Outgoing links	0

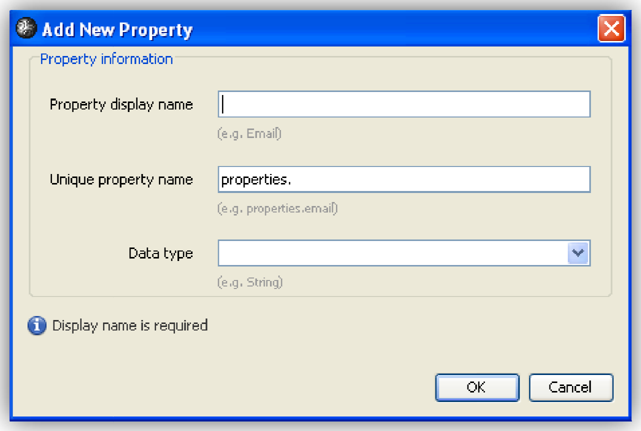
74.125.127.0-74.125.127.255



Bottom of the Property View

1. **Add new property**. Add a new property to the property view. This will add a Dynamic property that only applies to the selected entity. To add properties globally to an entity eg "Person" this has to be done via the Manage Entities option on the Manage tab.
2. **Delete new property**. Once a new property has been added it can be deleted.
3. **Edit Property Mapping**. This will allow you to set the value that is edited, displayed within the graph and what is used as an icon.

4. **Entity Properties**. Change the entity properties.



Add New Property

Property information

Property display name

(e.g. Email)

Unique property name: properties.

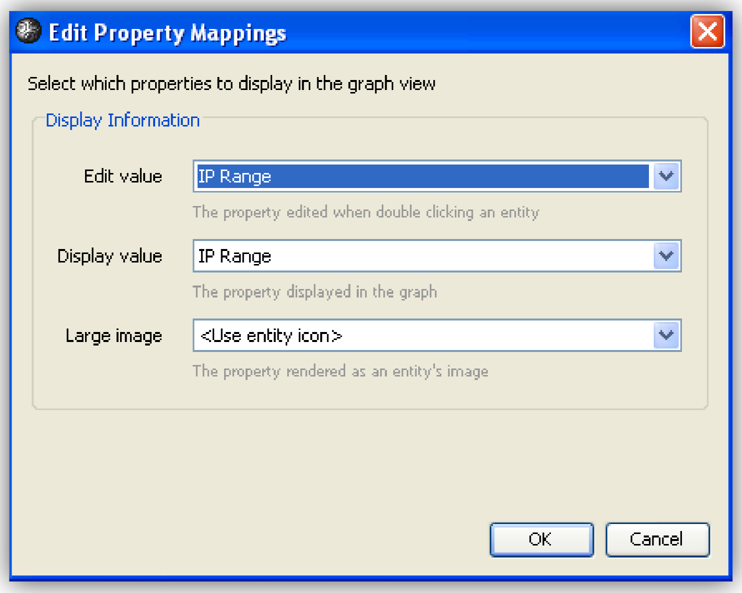
(e.g. properties.email)

Data type

(e.g. String)

Display name is required

Add new property



Edit Property Mappings

Select which properties to display in the graph view

Display Information

Edit value: IP Range

The property edited when double clicking an entity

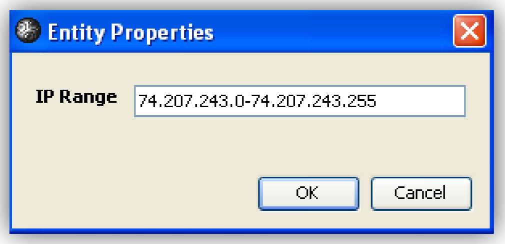
Display value: IP Range

The property displayed in the graph

Large image: <Use entity icon>

The property rendered as an entity's image

Edit Property Mapping



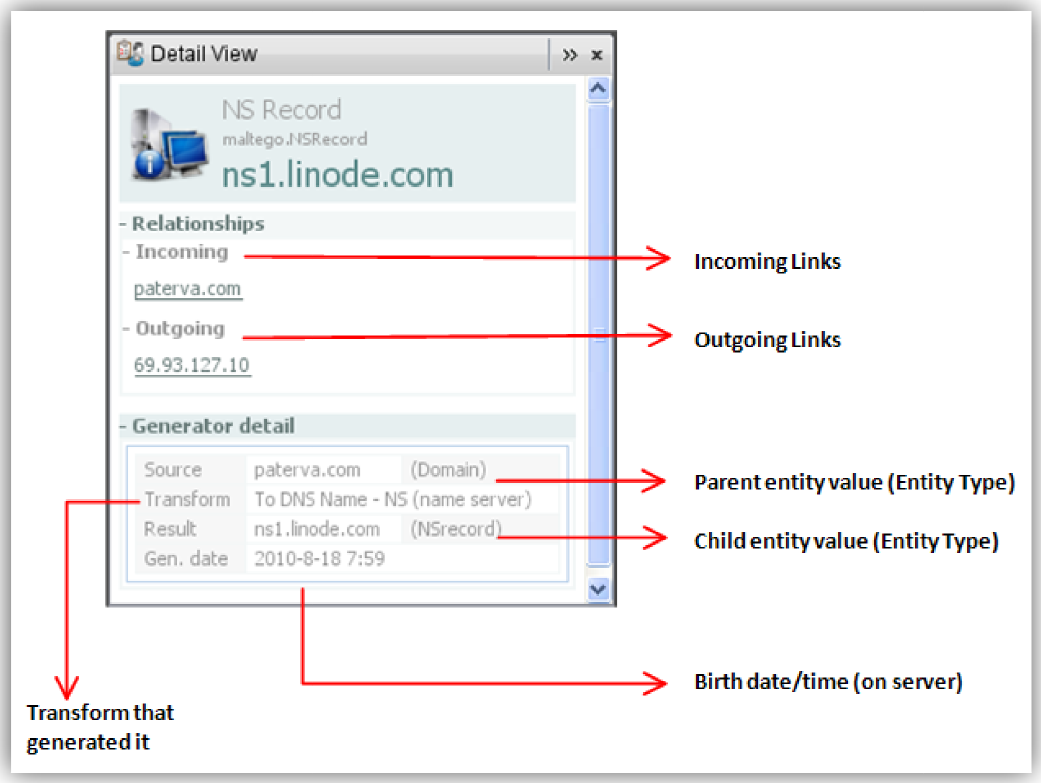
Entity Properties

IP Range: 74.207.243.0-74.207.243.255

Entity Properties

7.2 Detailed View

The detail view contains information about the entity that cannot be displayed in the main graph window. These are things that the transform author wants you to see about the entity. As the mouse is moved over entities both the entity properties and detail view is updated. The detail view of entity that is returned from the Paterva Commercial Transform Application Server (CTAS) will always contain the following fields:



NS Record
maltego.NSRecord
ns1.linode.com

- Relationships
- Incoming
paterva.com
- Outgoing
69.93.127.10

- Generator detail

Source	paterva.com	(Domain)
Transform	To DNS Name - NS (name server)	
Result	ns1.linode.com	(NSrecord)
Gen. date	2010-8-18 7:59	

Incoming Links

Outgoing Links

Parent entity value (Entity Type)

Child entity value (Entity Type)

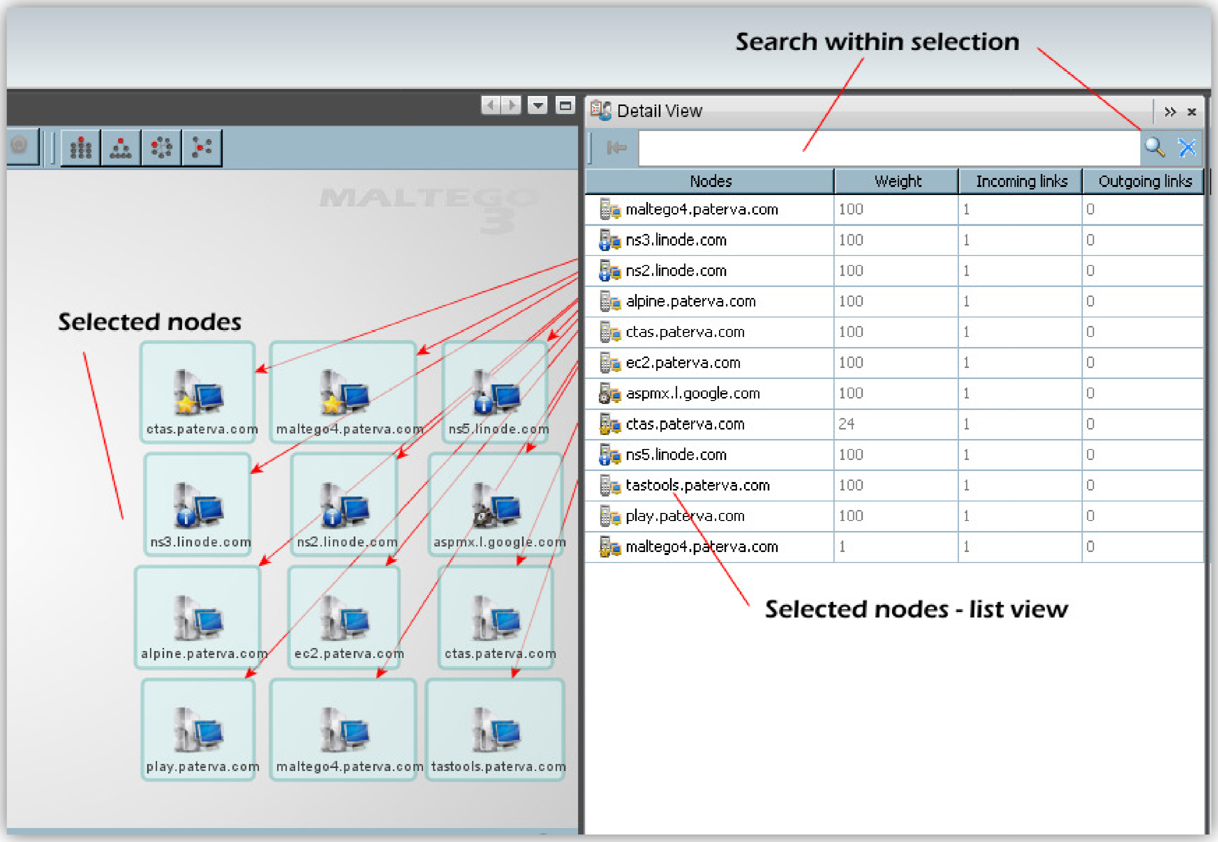
Birth date/time (on server)

Transform that generated it

Detail View

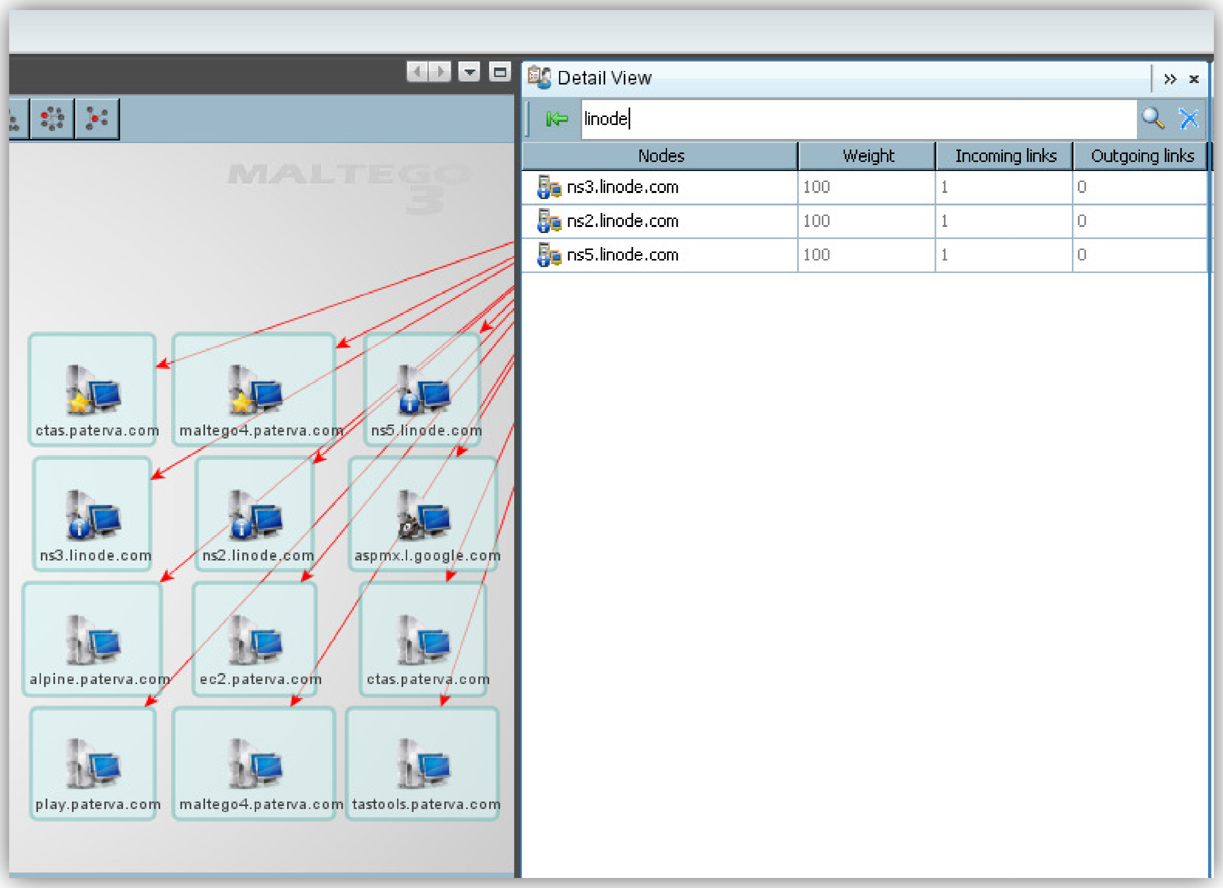
7.3 Selecting multiple entities

In Maltego 3 the detail view change to a multi column item list when more than one node is selected. This gives the user a lot more flexibility in terms of selection. Here is how to use it:



Nodes	Weight	Incoming links	Outgoing links
maltego4.paterva.com	100	1	0
ns3.linode.com	100	1	0
ns2.linode.com	100	1	0
alpine.paterva.com	100	1	0
ctas.paterva.com	100	1	0
ec2.paterva.com	100	1	0
aspmx.l.google.com	100	1	0
ctas.paterva.com	24	1	0
ns5.linode.com	100	1	0
tastools.paterva.com	100	1	0
play.paterva.com	100	1	0
maltego4.paterva.com	1	1	0

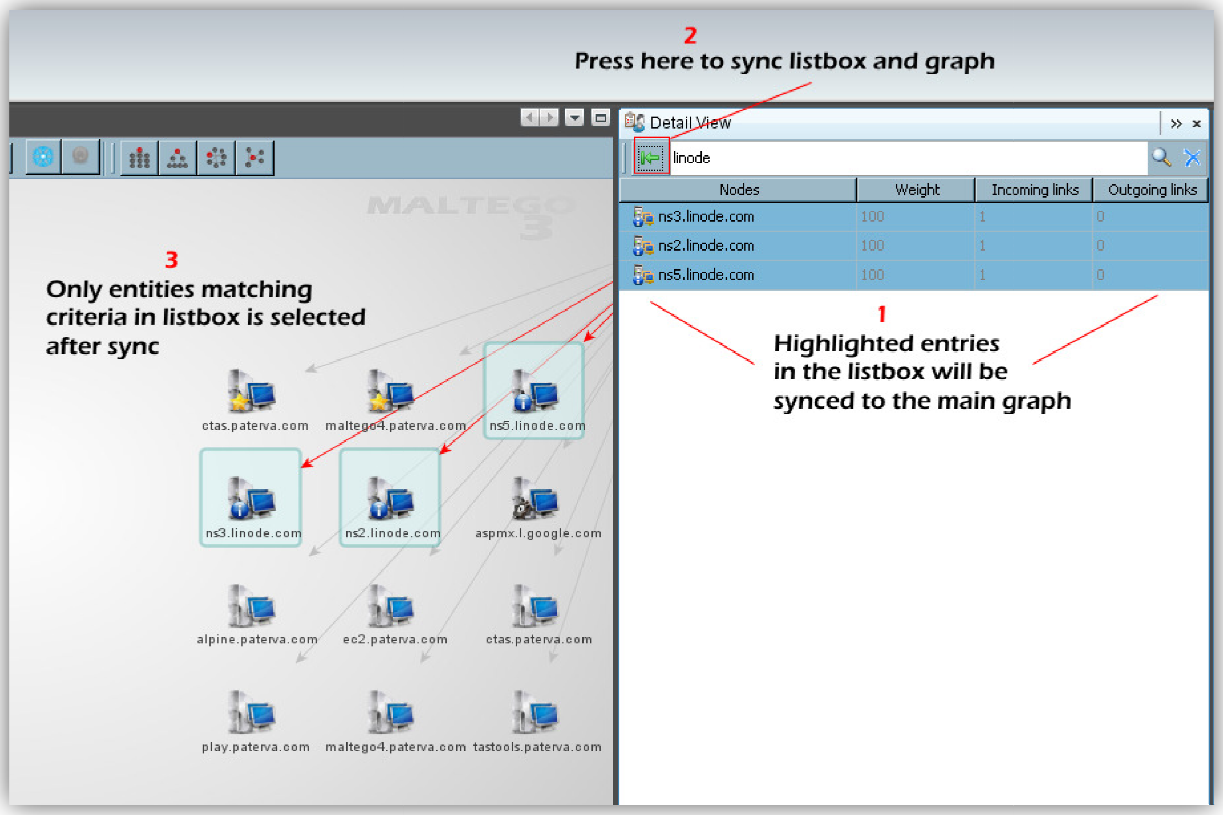
You can now search for nodes in the text area and press Enter to see which nodes match. The selection on the graph will remain at this stage as can be seen in the screen shot below:



linode

Nodes	Weight	Incoming links	Outgoing links
ns3.linode.com	100	1	0
ns2.linode.com	100	1	0
ns5.linode.com	100	1	0

Note that the green arrow button (just left of the word 'linode') has turned green. This is the sync button. You can now select nodes within the list (eg Control A for all, Shift selects ranges and Control select to select one by one) and when the sync button is pressed the selected nodes on the graph will update according to the selection:



2
Press here to sync listbox and graph

3
Only entities matching criteria in listbox is selected after sync

1
Highlighted entries in the listbox will be synced to the main graph

Detail View

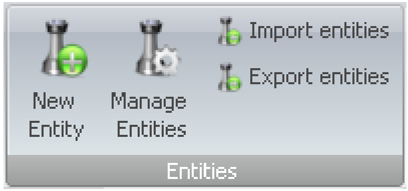
linode

Nodes	Weight	Incoming links	Outgoing links
ns3.linode.com	100	1	0
ns2.linode.com	100	1	0
ns5.linode.com	100	1	0

By putting an exclamation mark in front of a phrase you can invert the selection – e.g. if you want to find all entities that do not match the word ‘linode’ you need to search for ‘!linode’.

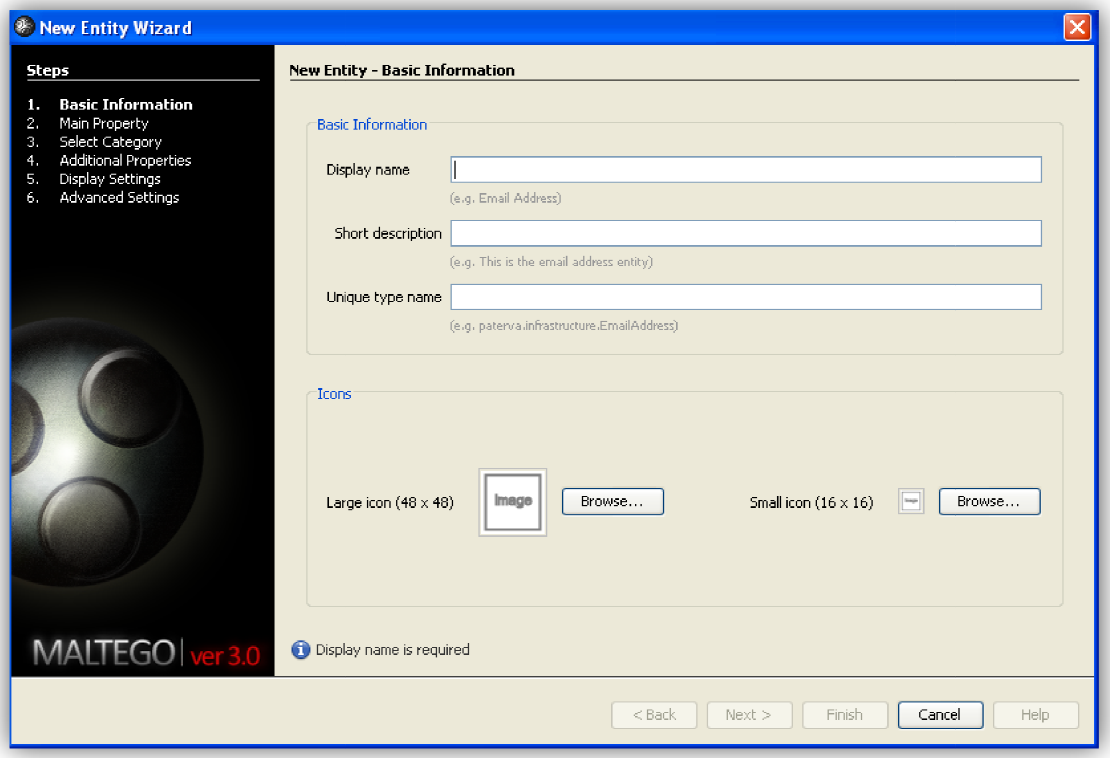
The Find (Control F) functionality with the secondary search in the Detail View gives a lot a flexibility and power.

8 Custom Entity Creation



Entity management

To create a custom entity select “New Entity” on the Manage tab of Maltego. This selection opens a wizard that will guide you through the process of creating a new custom entity.



New Entity Wizard

Steps

1. **Basic Information**
2. Main Property
3. Select Category
4. Additional Properties
5. Display Settings
6. Advanced Settings

New Entity - Basic Information

Basic Information

Display name

(e.g. Email Address)

Short description

(e.g. This is the email address entity)

Unique type name

(e.g. paterva.infrastructure.EmailAddress)

Icons

Large icon (48 x 48)

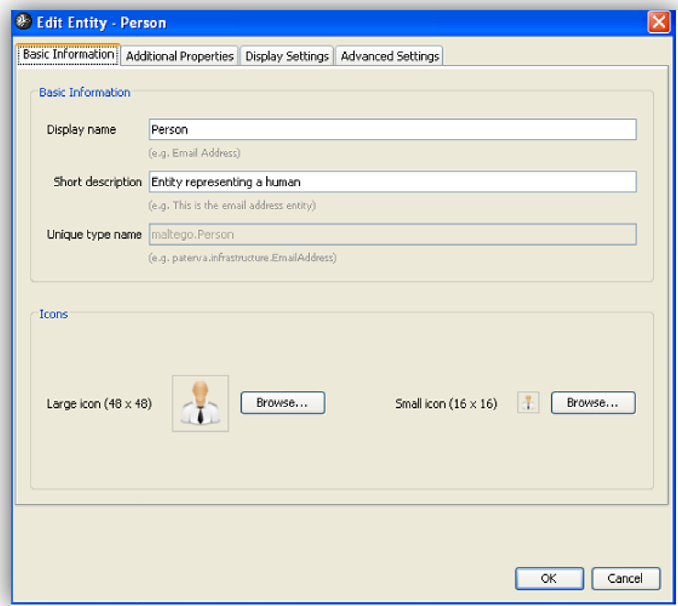
Small icon (16 x 16)

Display name is required

New Entity Wizard

8.1 Edit Entity

<u>Note</u>. The Name is important for use with the TDS/local transforms.

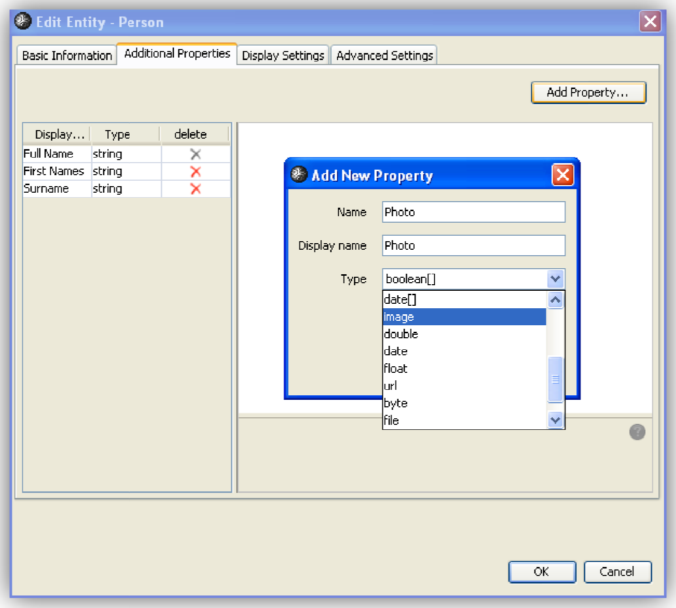


Display name: Person

Short description: Entity representing a human

Unique type name: maltego.Person

Choose a name, description and icon for the entity



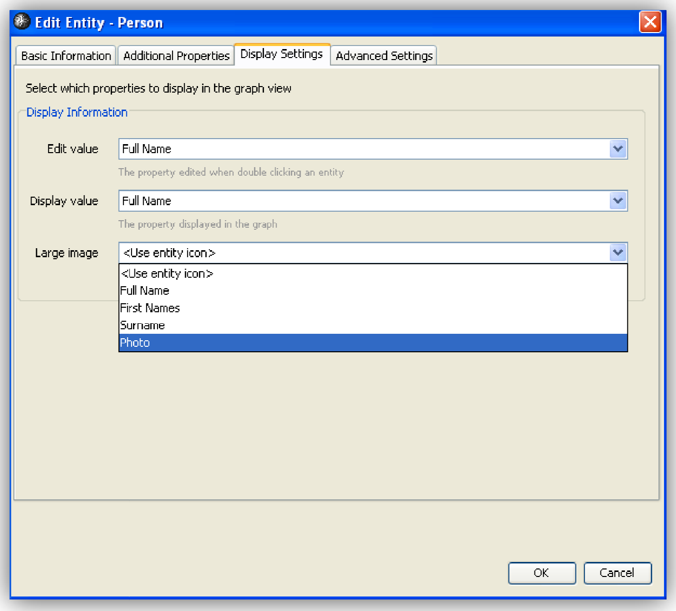
Display...	Type	delete
Full Name	string	✕
First Names	string	✕
Surname	string	✕

Name: Photo

Display name: Photo

Type: boolean[]

Add properties to the entity



Select which properties to display in the graph view

Display Information

Edit value: Full Name

The property edited when double clicking an entity

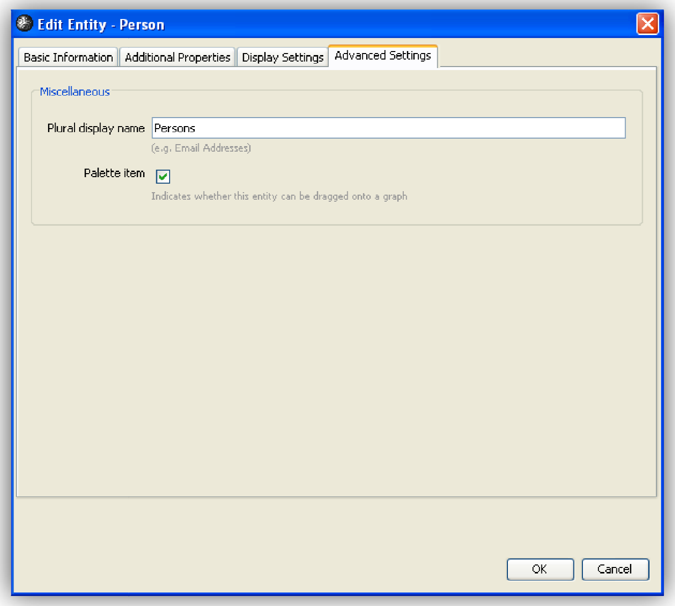
Display value: Full Name

The property displayed in the graph

Large image: <Use entity icon>

<Use entity icon>
Full Name
First Names
Surname
Photo

Choose display settings



Miscellaneous

Plural display name: Persons

(e.g. Email Addresses)

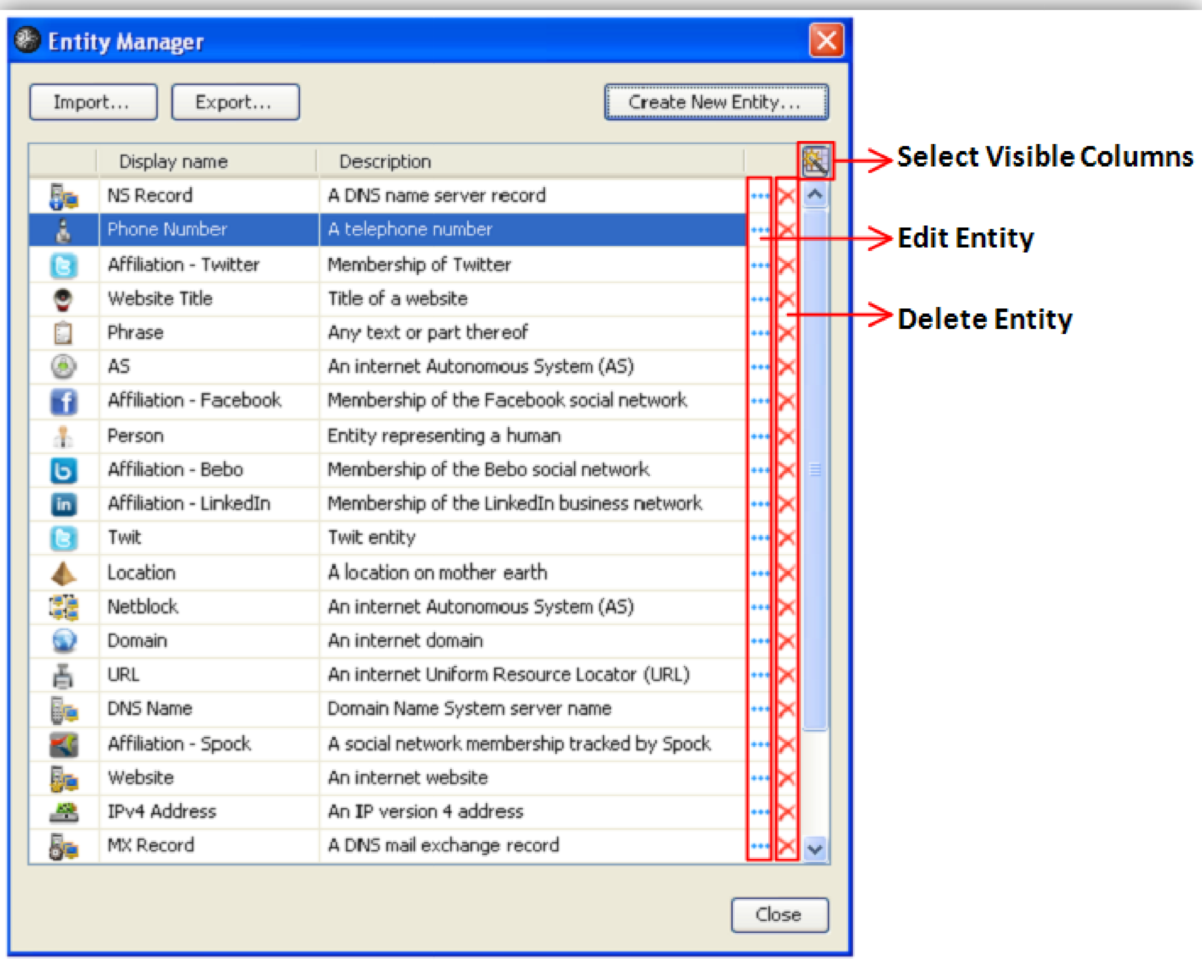
Palette item: ☑

Indicates whether this entity can be dragged onto a graph

Plural display name

8.2 Deleting a custom entity

To delete a custom entity, or any entity for that matter, go to the “Entity Manager” on the Manage tab and select the delete option as highlighted in the image below:



Display name	Description
NS Record	A DNS name server record
Phone Number	A telephone number
Affiliation - Twitter	Membership of Twitter
Website Title	Title of a website
Phrase	Any text or part thereof
AS	An internet Autonomous System (AS)
Affiliation - Facebook	Membership of the Facebook social network
Person	Entity representing a human
Affiliation - Bebo	Membership of the Bebo social network
Affiliation - LinkedIn	Membership of the LinkedIn business network
Twit	Twit entity
Location	A location on mother earth
Netblock	An internet Autonomous System (AS)
Domain	An internet domain
URL	An internet Uniform Resource Locator (URL)
DNS Name	Domain Name System server name
Affiliation - Spock	A social network membership tracked by Spock
Website	An internet website
IPv4 Address	An IP version 4 address
MX Record	A DNS mail exchange record

Select Visible Columns

Edit Entity

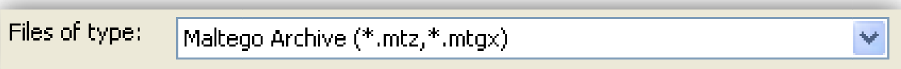
Delete Entity

Entity Manager

8.3 Sharing entities

Custom entities can easily be shared between users by exporting and importing them. It’s also possible to share entities by simply saving a graph containing custom entities and loading it in another (clean) Maltego.

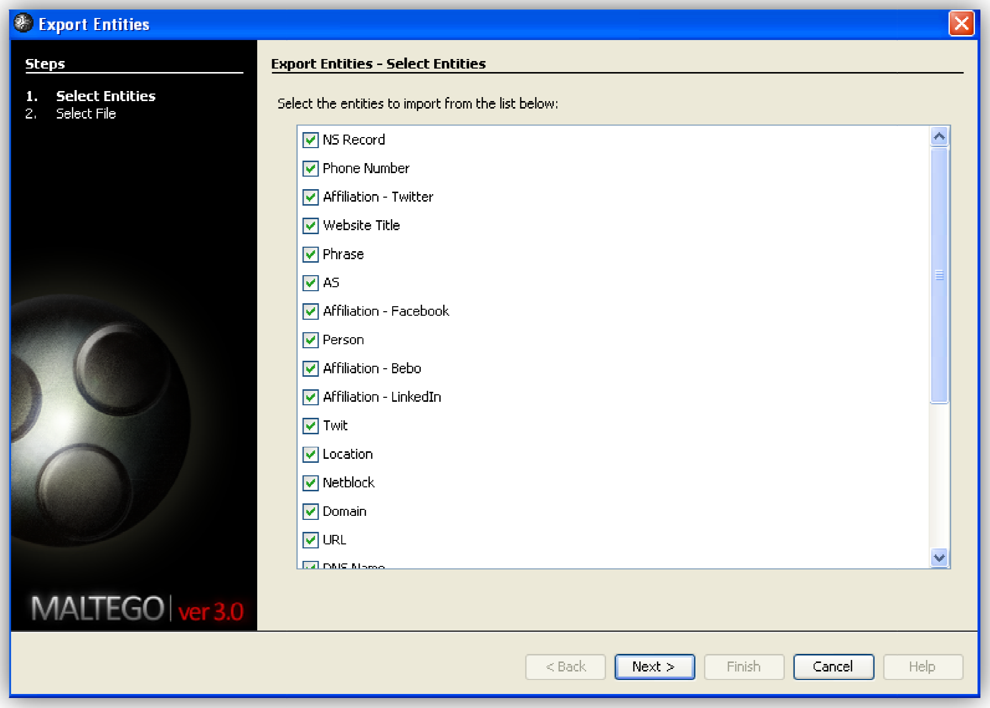
8.3.1 Import



Files of type: Maltego Archive (*.mtz,*.mtgx)

Valid Import file formats (mtz – entities, mtgx – Maltego 3 graph)

8.3.2 Export



Export Entities

Steps

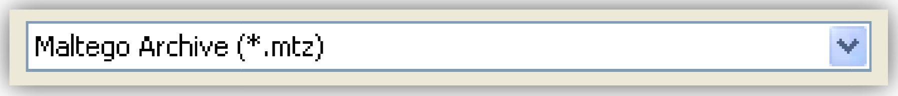
1. Select Entities
2. Select File

Export Entities - Select Entities

Select the entities to import from the list below:

- ☑ NS Record
- ☑ Phone Number
- ☑ Affiliation - Twitter
- ☑ Website Title
- ☑ Phrase
- ☑ AS
- ☑ Affiliation - Facebook
- ☑ Person
- ☑ Affiliation - Bebo
- ☑ Affiliation - LinkedIn
- ☑ Twit
- ☑ Location
- ☑ Netblock
- ☑ Domain
- ☑ URL
- ☑ DNS Name

Select entities to export



Maltego Archive (*.mtz)

Export file format