

DECLARATION OF NATHANIEL E FRANK-WHITE

1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.

4. The archived data made viewable and browseable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.

5. The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL] aka an "extended URL". Thus, the extended URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.

6. Attached hereto as Exhibit A are true and accurate copies of browser screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each printout.

INTERNET ARCHIVE
archive.org

7. Attached hereto as Exhibit B are true and accurate copies of the Internet Archive's records of the archived files for the URLs and the dates specified in the following table.

Folder	URL
001	https://web.archive.org/web/20070202020317/http://www.trustmatta.com/downloads/pdf/Matta_Attack_and_Penetration_Introduction.pdf
002	https://web.archive.org/web/20060131095431/http://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf
003	https://web.archive.org/web/20100107152443/https://www.blackhat.com/presentations/bh-usa-07/Moore_and_Valsmith/Whitepaper/bh-usa-07-moore_and_valsmith-WP.pdf
004	https://web.archive.org/web/20091229020339/http://www.edge-security.com/docs/OWASP-Christian_Martorella-InformationGathering.pdf
005	https://web.archive.org/web/20101122112311/http://www.paterva.com:80/web5/documentation/Maltego3_crash_course.pdf
006	https://web.archive.org/web/20101123012539/http://www.paterva.com:80/web5/documentation/3.0.2.addendum.pdf

8. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATE: August 30, 2024

Nathaniel E Frank-White

Nathaniel E Frank-White

EXHIBIT A

https://web.archive.org/web/20090302045813/https://vimeo.com/2745624

INTERNET ARCHIVE WayBackMachine
https://vimeo.com/2745624
Go
17 captures
12 Feb 2009 - 7 Jan 20
FEB MAR SEP
2008 02 2009 2011
About this capture



Toorcon X Gates: New School Information Gathering

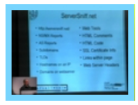
by carnal0wnage
2 months ago

More Add

Show me carnal0wnage's videos See all



4. Attacking Oracle with the Metasploit Framework Shm...
by carnal0wnage
23 days ago



3. Toorcon X Gates: New School Information Gathering
by carnal0wnage
2 months ago



2. Metasploit Auxiliary module for Oracle FTP Script ...
by carnal0wnage
2 months ago

Flag this video

Credits

carnal0wnage

Set credits

Tags

carnal0wnage 5
Chris Gates 1
toorconX 1
Add a tag



Add a new comment

Post Comment No HTML please

Sponsored by:

1 Related collections

Channels
carnal0wnage

Add to collections

Statistics

	plays	likes	comments
Total	305	0	0
Mar 1st	1	0	0
Feb 28th	1	0	0
Feb 27th	1	0	0
Feb 26th	3	0	0
Feb 25th	0	0	0
Feb 24th	1	0	0
Feb 23rd	5	0	0
Feb 22nd	1	0	0

‹ Previous Week

See referrers

Downloads

Sorry. This video is not available for download

Related Feeds
carnal0wnage's videos

Vimeo: About / Blog / Roadmap / Developers / Community Guidelines / Forums / Toys / Help! / Site Map / Get Vimeo Plus

Legal: ©2009 Vimeo, LLC / Terms & Conditions / Privacy Statement

https://web.archive.org/web/20070222133717/http://www.nessus.org/plugins/index.php?view=single&id=21725

INTERNET ARCHIVE WayBackMachine
http://www.nessus.org/plugins/index.php?view=single&id=21725
Go
11 captures
24 Sep 2006 - 9 Mar 20
SEP FEB SEP
22
2006 2007 2010
About this capture

PLUGINS

Direct Plugin Feed
Information on how to obtain the newest Nessus plugin feed.

Newest plugins
See the list of the newest security checks

All plugins
See the whole list of security checks performed by Nessus

Search plugins
Search the Nessus plugins

Nessus Licensing FAQ
Frequently asked questions about the licensing of Nessus and its plugins

QUICK LINKS

REGISTER
Register your Nessus installation to obtain the complete archive of Nessus Security Checks.

NEW PLUGINS
See the list of the newest security checks

DOWNLOAD
Download Nessus 3.0.5 now

BUY NOW
Buy a Nessus-related product today

DIRECT FEED SUPPORT
Log in to the Tenable Support Portal (Nessus Direct Feed Customers only)

BLOG
The official blog of Tenable and Nessus

WEBINARS
Register for a free webinar from Tenable Network Security, Inc.

Plugins

Symantec Anti Virus Corporate Edition Check

This script is Copyright (C) 2004-2005 Jeff Adams / Tenable Network Security

View the source code of this plugin here

Family	Windows
Nessus Plugin ID	21725
Bugtraq ID	
CVE ID	

Description:

This plugin checks that the remote host has Symantec AntiVirus Corporate installed and properly running, and makes sure that the latest Vdefs are loaded.

Solution : Make sure SAVCE is installed, running and using the latest VDEFS.
Risk factor : High

© Copyright 2002 - 2007 Tenable Network Security(R). All Rights Reserved.

https://web.archive.org/web/20120606172056/http:/ctas.paterva.com/view/Userguide

INTERNET ARCHIVE WayBackMachine http://ctas.paterva.com/view/Userguide Go DEC JUN JUN 06 2010 2012 2013 About this capture
47 captures 19 May 2008 - 23 May 202

Userguide

Contents [hide]

1 Maltego User Guide (Commercial edition)
2 Installation
  2.1 Windows
  2.2 Linux
  2.3 Mac
3 Running the first time & registering
4 Migrating From 2.0 to 2.0.1
5 Your first graph
6 Navigation
  6.1 Zoom
  6.2 Zoom to Pointer [As of 2.0.1]
  6.3 Zoom Lense [As of 2.0.1]
  6.4 Pan
  6.5 Copy And Paste [As Of 2.0.1]
    6.5.1 Copying
    6.5.2 Pasting Without Relationship Links
    6.5.3 Pasting Entities WITH Relationship Links
    6.5.4 Pasting From Text
7 Running transforms
8 Canceling Currently Running Transforms [As of 2.0.1]
9 Setting the number of results returned
10 Selecting entities
  10.1 Single select
  10.2 Multiple select
  10.3 Selecting entities one at a time
  10.4 Selection by child
  10.5 Selection by child (keep parent)
  10.6 Selecting parent
  10.7 Select a parent (keep)
  10.8 Selecting entities using 'Find'
  10.9 Invert Selection [As of 2.0.1]
  10.10 Combinations
  10.11 Quick list of incoming and outgoing nodes
11 Views and layout
  11.1 Layout
  11.2 Views
12 Entity Properties & Detailed view
  12.1 Entity properties
  12.2 Entity detailed view
13 Transform Manager
  13.1 Editing Transforms
    13.1.1 Changing Transform Display Names
    13.1.2 Cloning Transforms
  13.2 Discovery Process
  13.3 Sets
    13.3.1 Creating New Sets
    13.3.2 Adding/Removing Transforms from Sets
    13.3.3 Deleting Sets
14 Save/Load
15 Export
16 Printing

Maltego User Guide (Commercial edition)

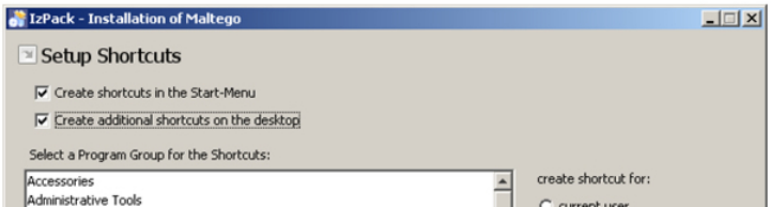
This user guide is for the commercial edition of Maltego. The community edition of Maltego is very similar; there are only a couple of differences in the startup.

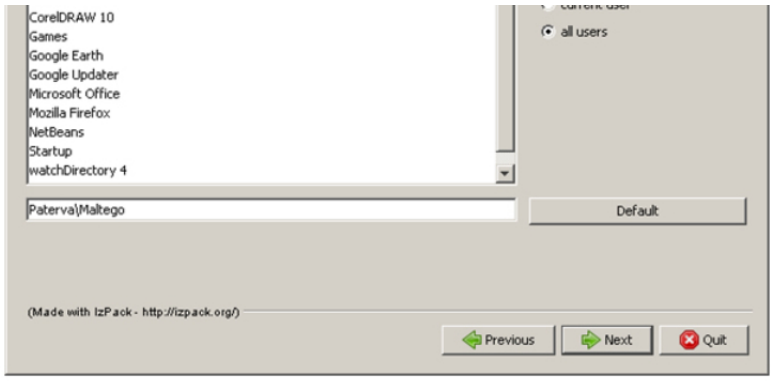
Maltego can run on Windows or Linux. This section of the guide assumes that you already have Java 1.6 installed. Should you have any questions not answered by this user guide please Contact Us

Installation

Windows

After downloading the MaltegoInstaller.exe file double click on it to start the installation process. The installer is built using Izpack – a generic Java installer that is not platform specific. You should follow the wizard – defaults will do, but you might want to add icons to your desktop on the last screen:





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

Linux

You will need to have a windows (X11) system – Maltego is a graphical application. After download you should open a terminal window. You should change to the directory to where you have downloaded the MaltegoInstaller.jar file – e.g.

> *cd downloads/maltego* (assuming that you've downloaded it here)

From here you can run the Java installer using the following command:

> *java –jar MaltegoInstaller.jar*

The installer should start the graphical wizard. As with the Windows install you can decide if you want a desktop item. The installer can normally add this for KDE or Gnome based desktops – others have not been tested.

Note 1: 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 is not good.

Note 2: 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/*

Mac

The mac release (commercial), can be downloaded as a .pkg from http://www.paterva.com/maltego/download/ . The .pkg file can then be executed and a simple wizard will guide you through the installation.

You will however need to install Java 1.6 (for dual core Mac users), or Soylatte Java (for 32bit Mac users). For more information this you can view the forum post here: http://www.paterva.com/forum/index.php/topic,84.0.html

Running the first time & registering

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

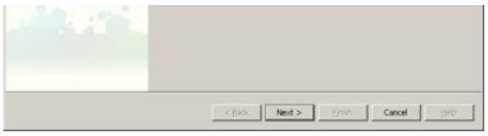


Note that parts of this screen are dynamic content and thus could change from time to time.

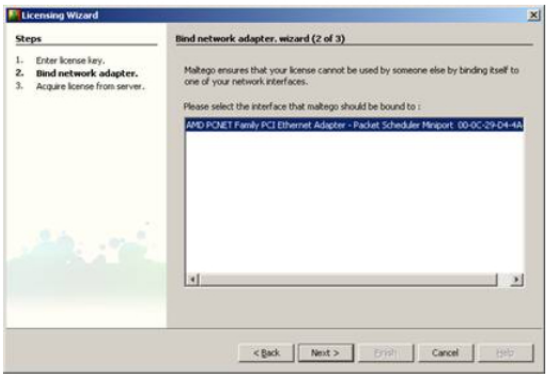
Maltego v2 is a commercial product and a license key is used to activate the product. The license key is valid for one year and is computer specific. Without a valid license key you can only use MaltegoV2 to view files created by other users – you cannot create new graphs and you cannot add or edit existing graphs. To register you can click on the red text that reads "You must register before you can use Maltego. Click here to register now". This will start the registration wizard.

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 the word 'Valid' appear. If not it the word 'Invalid' will appear:

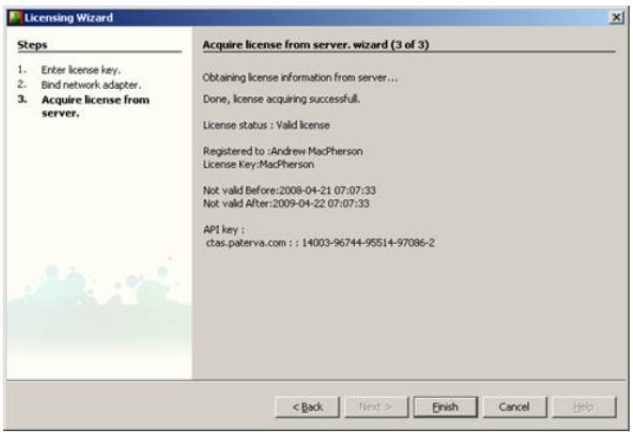




Click on next. Next you will be asked on which adaptor you want to bind the installation. Choose an adaptor that it not likely to change.



Under Linux you are encouraged to choose the 'eth0' adaptor. Click on Next. 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 enabled. The screen should show a summary of registration information. Don't worry about writing any of it down as you can get it from the application at a later stage.



The start page will now be updated with the registration information:



Migrating From 2.0 to 2.0.1

Click here to view the Migration Tutorial for Windows Vista, Windows XP and Linux

Your first graph

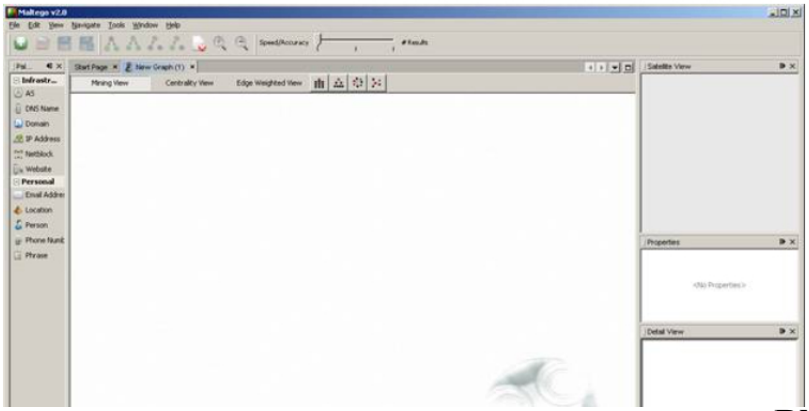


To start a new graph click on



You can also click on the 'New' icon that's right below [File]. 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).

You should get an empty graph which looks like this:





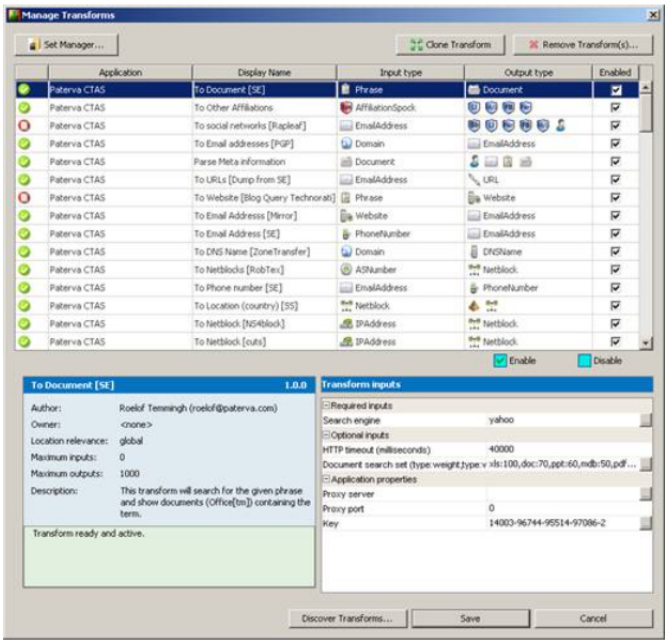
More than one graph can be opened. New graphs are added as tabs at the top of the screen.

You can go back to the start page by clicking on the 'Start Page' tab, or by going to Help -> Start Page. To get API and license keys, as well as a summary of registration information you can go to Help -> About Maltego. This should show a screen that looks like this:



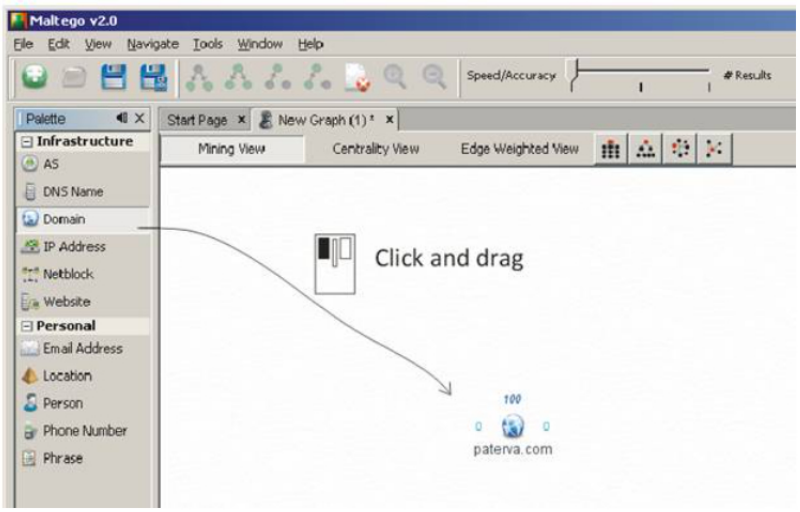
If you ever need to query the status of your license or if you've lost your API keys you can view your license key here.

At this stage you want to make sure that you have the preconfigured transforms discovered and keyed. Click on Tools->Manage transforms. You should see:

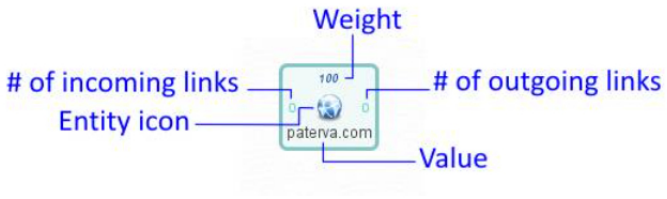


Note that there is a list of transforms and that most of them have a green icon on the left (which means they are ready to be used). For more information about managing transforms see the relevant section in this documentation.

Next, we want to put some entities on the graph window. Select the 'Domain' Entity from the Palette and drag it to the graph window:



The first thing that you will notice is that the entity contains three numbers and a value. The values are as follows:



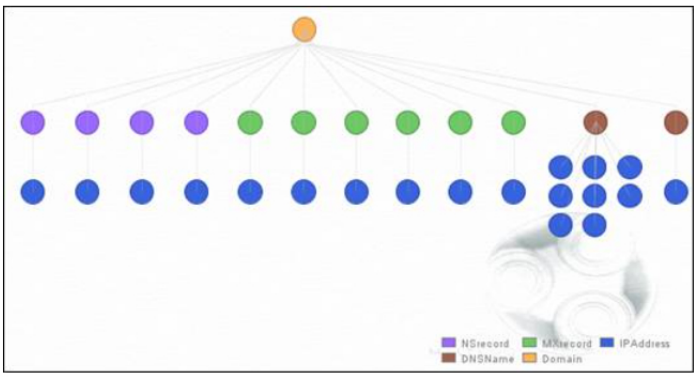
To edit the name of the entity (in this case a domain) double click on it. The entity will become selected and the text area underneath the entity will be highlighted – you can now edit it:



Navigation

Zoom

To zoom in and out use the mouse scroll wheel. If you are using a notebook without a scroll wheel you can use the  buttons. 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 colors, with a small legend for mapping colors to entity types in the right hand bottom corner of the graph:



Note that the colors 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.

Please Note: As of version 2.0.1 when zooming with the mouse scroll wheel the zoom to pointer method will be used (described below)

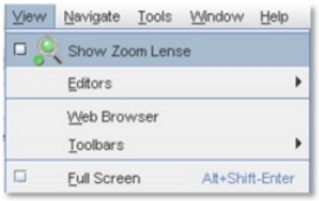
Zoom to Pointer [As of 2.0.1]

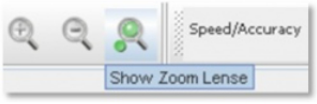
The zoom to pointer function is an enhanced zoom feature that has been implemented as of 2.0.1. Where the previous zoom method would zoom in or out based on the central display of the graph, zoom to pointer (the new 'zoom'), will zoom in and out based on the location of the mouse pointer within the graph.

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 center of the graph.

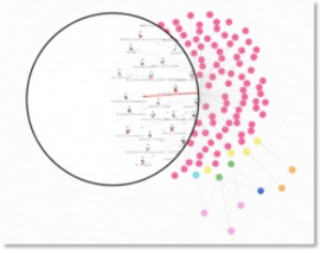
Zoom Lense [As of 2.0.1]

The zoom lense method of navigating a graph is a way of taking a virtual magnifying glass to your graph, whereby you can quickly see a magnified portion of the graph rather than have to zoom into it. This option can be turned on by either selecting view->show zoom Lense (as seen below left), or selecting the zoom lens icon within the top Maltego toolbar (below right)





With this option selected the mouse cursor is replaced by a single magnifying sphere. The zoom level on this can also be adjusted via the scroll button on the mouse to either increase or decrease the magnifying capacity of the lens. An example of this in use can be seen below:



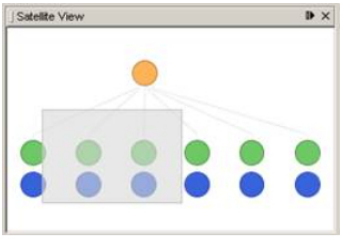
To turn this option off you can simply select either of the two methods used to turn the zoom lens on as described above.

Pan



To pan you can use the scroll bars at the sides of the graph window, or you can right-click and drag. This method of navigation is a lot faster than using the scroll bars.

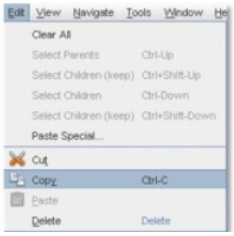
You can also use the Satellite view to navigate. This is useful navigation technique on large graphs.



You can move the visible frame (grey box) around on the Satellite view 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).

Copy And Paste [As Of 2.0.1]

Copying



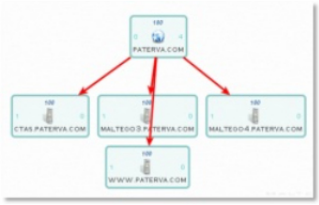
Entities can be copied by selecting the entities you wish to copy (via any of the selecting methods described elsewhere in this document) and then pressing CTRL + C or selecting Edit->Copy from the menu (as seen above).

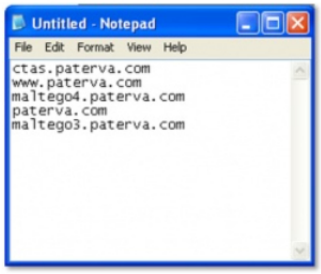
Pasting Without Relationship Links



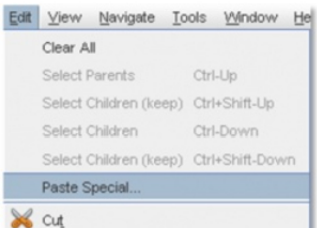
Entities can be pasted either into an external application or a Maltego graph (without relationship links). This can be done by either pressing CTRL + V or selecting Edit->Paste (as seen above)

Entities that are copied and have been pasted into any external application will have the value of the selected nodes. For example if we select the following entities in a graph, copy them and then paste them into a generic text editor (in this case windows notepad) you will see the values of the entities we copied have been pasted (second example)





Pasting Entities WITH Relationship Links





To retain the relationship links (links between entities) within graphs you can simply select Edit->Paste Special… (as seen above). You will then see a dialog window which allows you to either paste the copied entities with our without relationship links (below). Simply select the first option (Paste entities and links) and the relationships will be saved between graphs!



Pasting From Text

Entities can also be pasted from text by simple selecting the text, copying it (as you would with any word processor or other application), and then pasting using either of the paste methods described above.

Maltego will also try and determine what type of entity has been copied based on its value and try to select the correct entity within the graph.

For example, if you were to copy the following as text:

- Andrew@punks.co.za
- Andrew MacPherson
- Punks.co.za
- www.punks.co.za
- punk south Africa

Maltego would interpret the entities as the following in a graph

- Email Address
- Name
- Domain
- DNS Name
- Phrase

And the output would be as follows:



Please Note: The regular expression matching for pasted text is not perfect - but its pretty close!

Running transforms



To run your first transform you can right click on the entity. You will see a list that looks like this:

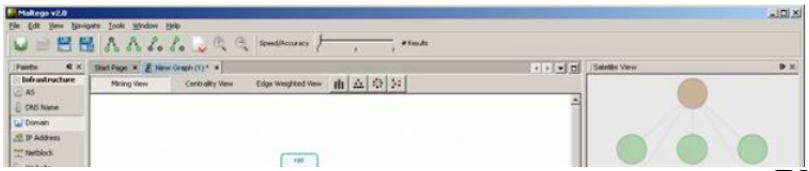


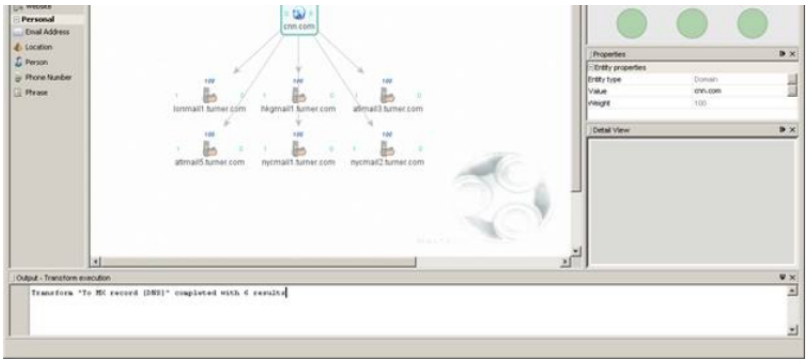
Let us assume that we want to find out what the MX (mail exchanger) records for the domain are. We want to use the 'To MX records [DNS]' transform and so we click on it. In the bottom right hand corner we can see the transform status bar indicating that we are running one transform on one entity.



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

The resultant screen should look something like this:

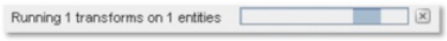




Note that the Output screen has appeared with details about the transform's execution. This information is very useful as some transforms will give additional information in this screen.

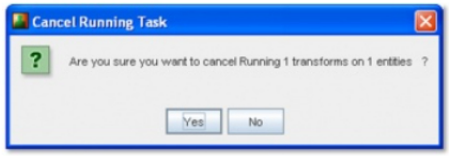
Canceling Currently Running Transforms [As of 2.0.1]

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:



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 all of the running transforms. 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.

Please Note: When running a set of transforms you can only cancel the entire set!

Setting the number of results returned

A slider is located at the top of the Maltego application:



When set to the very left Maltego will only show the top 12 results, based on weight. The middle setting corresponds to 50 results and the very right to 255 results. 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.

In upcoming versions of the tool the transforms will be categorized as either 'enumeration' or 'search' transforms – the slider will only apply to 'search' transforms. For now you have to be careful to understand how the slider works and spend time experimenting with it.

Selecting entities

There are a few way of selecting entities.

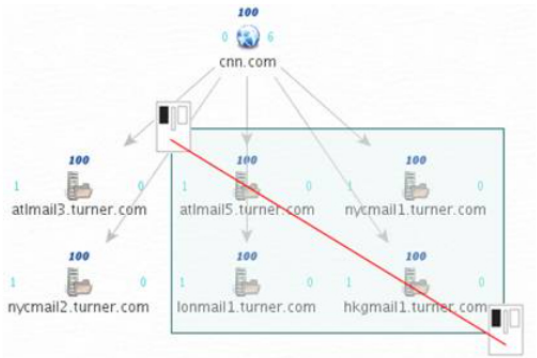
Single select



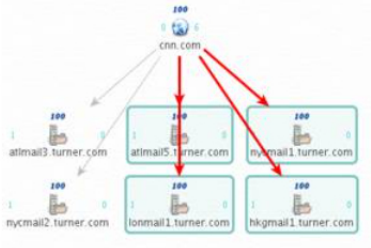
Simply click on the entity. The entity gets a blue frame around it. If zoomed out the entity's color is enhanced.

Multiple select

You can select more than one entity by left click dragging a box around it:



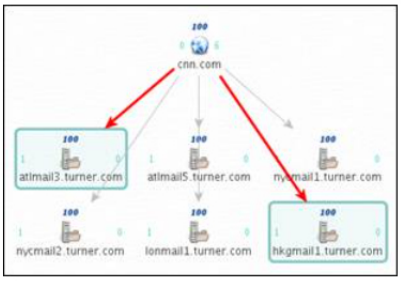
As soon as you release the left mouse button the entities are selected:



Selecting entities one at a time



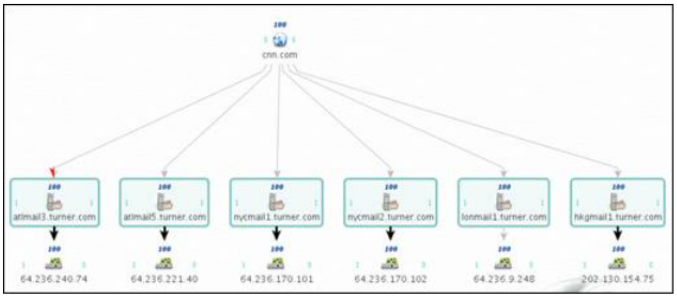
You can select entities one by one by click on it and holding in shift:



Selection by child



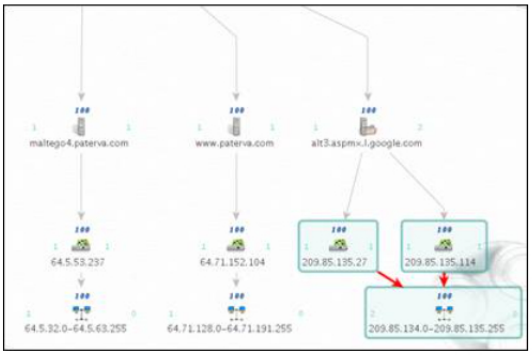
It is very useful to be able to select the children of a node (e.g. all the nodes that were created from the node). You can do this by selecting the parent and pressing Control + Down Arrow.



Selection by child (keep parent)



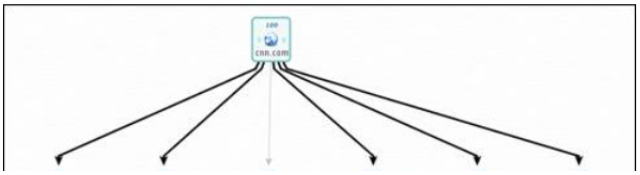
You can select child nodes and keep the parents selected by pressing Control + Shift + Down Arrow. This is useful to select an entire "family tree":

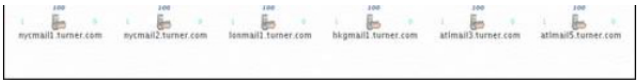


Selecting parent



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

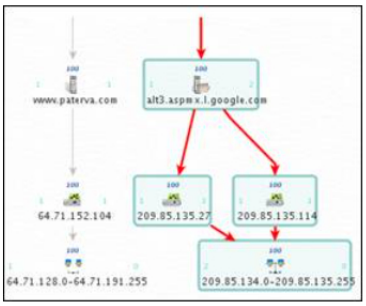




Select a parent (keep)



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.



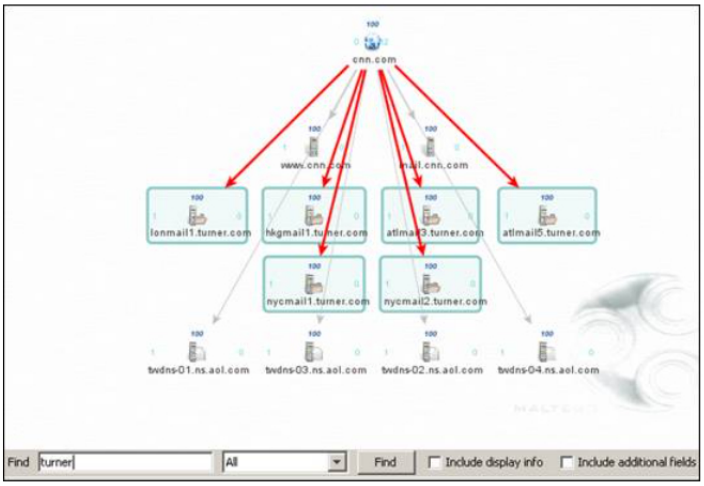
Selecting entities using 'Find'



To enable searching press Control F. The following window will appear:



Enter the search term and click on "Find" – entities that match the criteria will be selected:



For more information on finding entities please refer to the relevant section in this document.

Invert Selection [As of 2.0.1]



Invert Selection allows you to invert the selected nodes. For example if you had selected all the IP Addresses from a graph and then pressed the Invert Selection button (seen above - far left), everything except the IP Addresses would be selected.

Combinations

The best way to select entities is a combination of all of the above methods. For instance you might single select entities and use a combination of child/parent expansion to find what you are looking for.

Quick list of incoming and outgoing nodes



When working with large graphs it is very possible that parent and child nodes of a selected entity is outside the border of the current graph. A quick way to get a list of parent and child nodes is to Control click on the node. This show a separate window with all incoming (parents) and outgoing (children) nodes:





Views and layout

Layout

Maltego supports 4 types of layout algorithms:

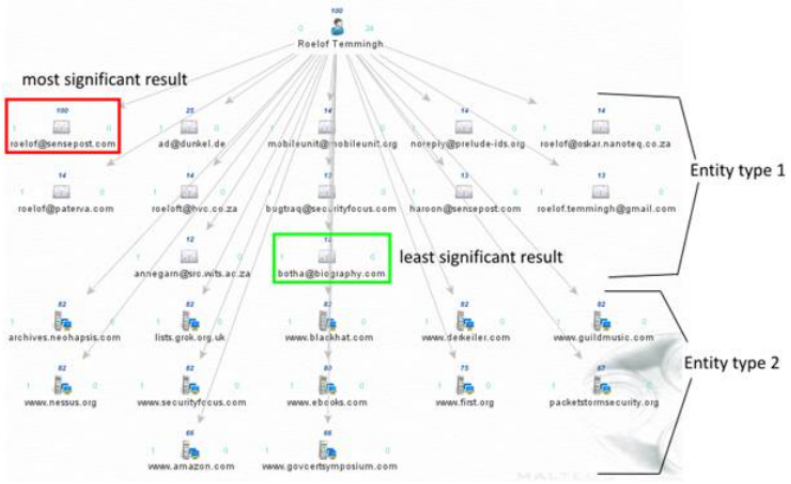
1. Block layout. This is the default layout and is also used during mining. This layout is discussed in more depth later.
2. Hierarchical layout. Think of this a tree based layout – like a file manager.
3. Centrality layout. Nodes that are most central to the graph (e.g. most incoming links) appear in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

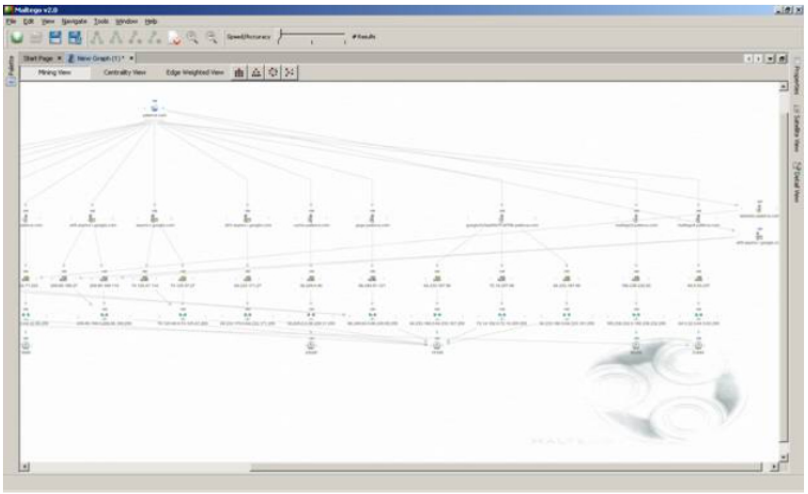
1. In a block of nodes
2. Sorted by entity type
3. Sorted by entity weight

Consider the following graph were two transforms were executed on the Person entity – Person2EmailAddress and Person2Website:

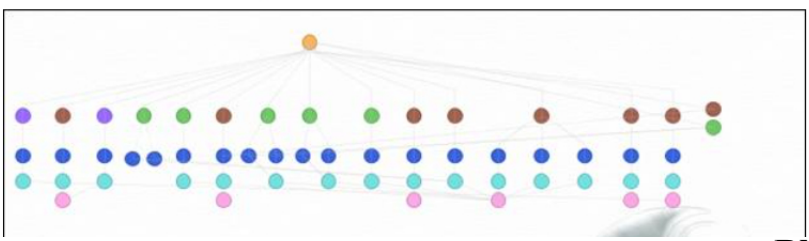


Note that entities are ordered by type and weight.

The following pictures show the same graph in different layout types. The graph shows all Paterva related DNS Names, their IP addresses, what netblocks they belong to and the AS numbers of those networks. Note that most of the graph has been viewed in 'overview' mode in order to see the layout properly Block layout (detailed):

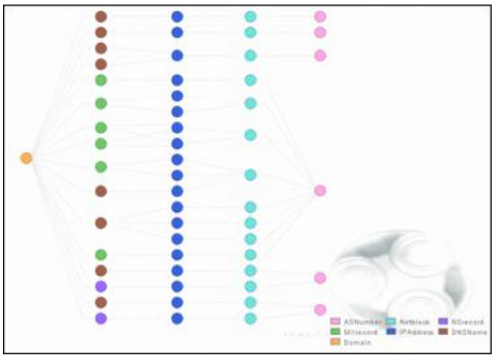


Block layout (zoomed out / overview):

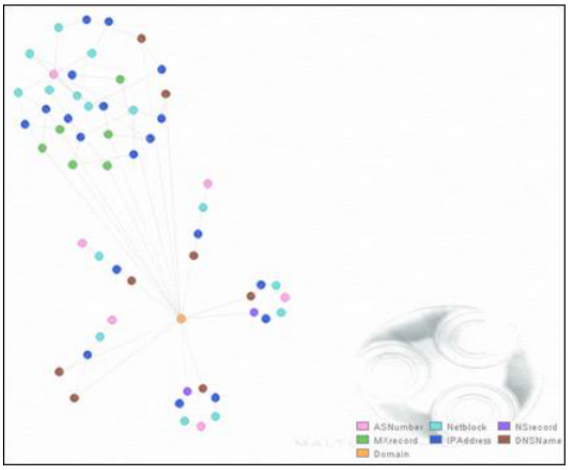




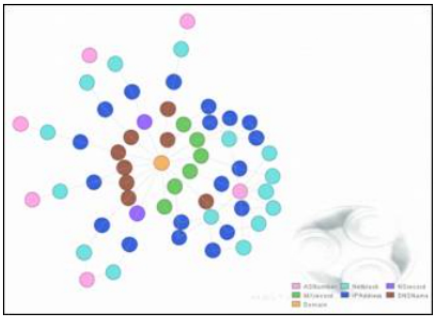
Tree layout:



Centrality layout:



Organic layout:



Different layouts work best of different situations – you need to experiment with it to see which layout works best for the situation at hand.

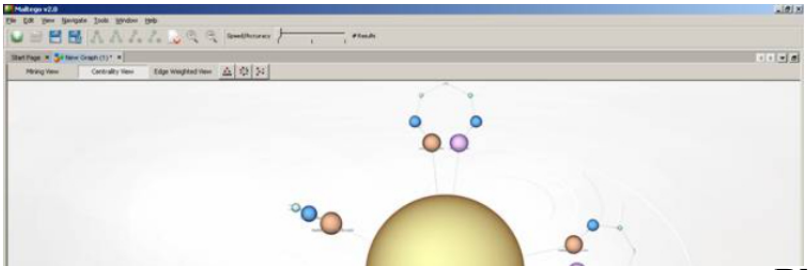
Views

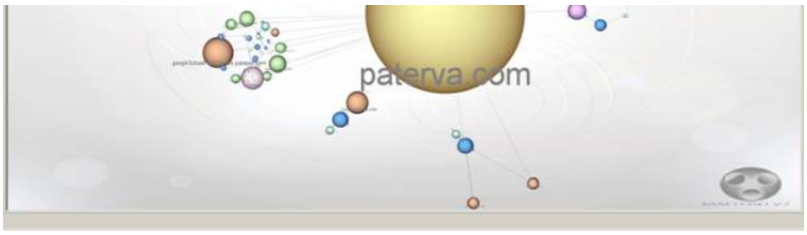
Views are used to extract non-obvious information from large graphs – where the analyst cannot see clear relationships by manual inspection of data. Other than the mining view, Maltego supports two other views:

1. Edge weighted view. Node sizes are based on number of incoming links.
2. Centrality view. Nodes that are calculated to be most central to the graph are given larger nodes.

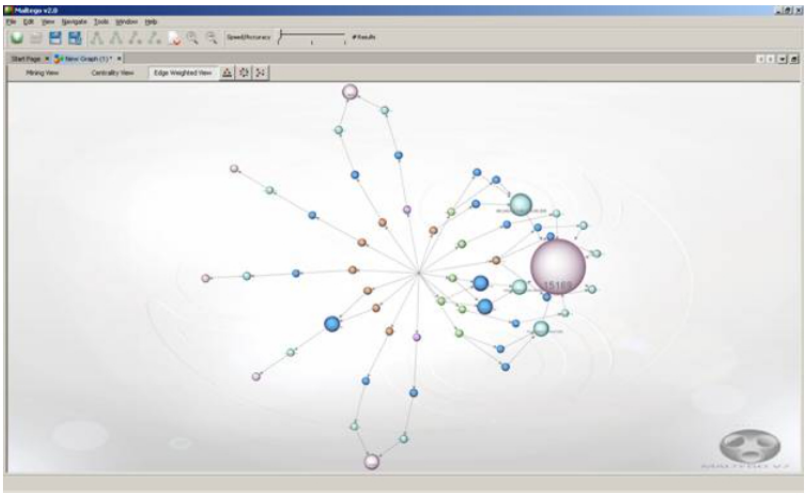
In views two and three entity details are not shown and no selection is possible. It is simply a view of the data with one exception - control clicking on a node still brings up a list of incoming and outgoing links.

The same graph used in the previous section is shown in different views. First the centrality view:



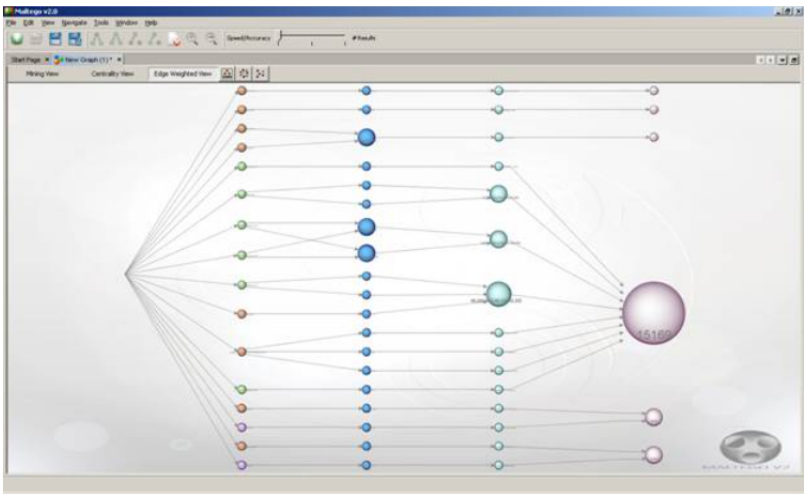


Clearly the domain paterva.com is central to the graph. When viewing the same graph in 'Edge weighted view' we see something more interesting:

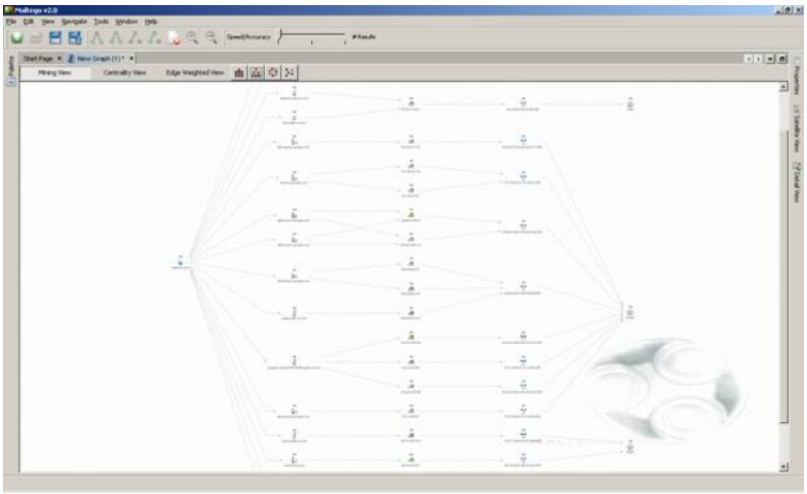


Now the AS number 15169 is clearly more 'inflated'. This is the expected result – this AS has the most incoming links.

The layout in these views can be modified. Consider the 'edge weighted view' in tree layout:

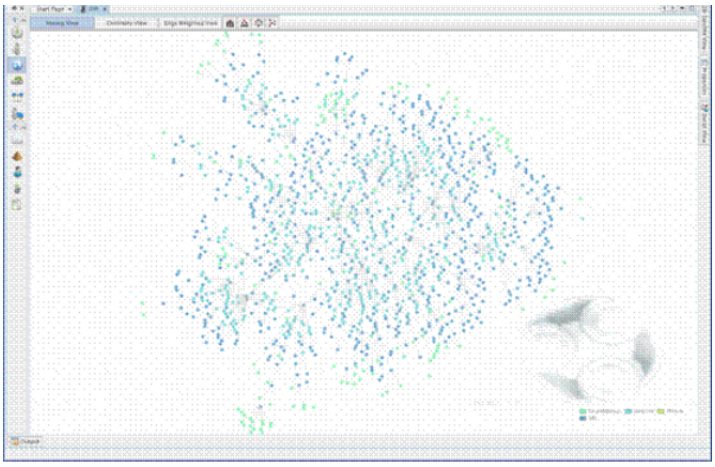


Comparing this view with the original view we can clearly see the relationship:

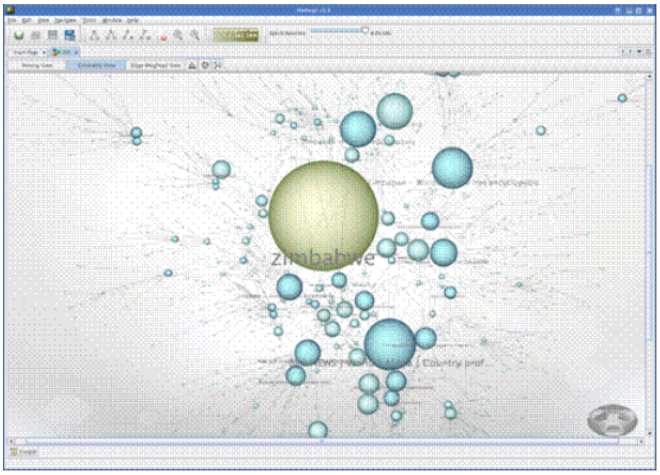


The graph showed above is rather simple and manual visual inspection would render the same results. However when graphs get very large these views proves invaluable. Consider this large graph:





It is practically impossible to extract any useful information from the graph. However – viewing the same graph in centrality view (organic):



This view makes it possible to identify the key entities in the graph with ease.

Entity Properties & Detailed view

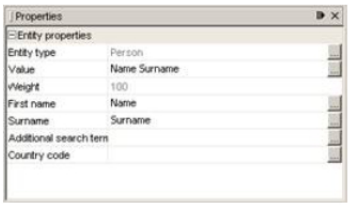
Each entity has a number of properties and may have a detailed view. Most of the properties of an entity can be set while the detailed view is read-only. The properties of an entity are used by transforms and are passed along with the entity's value to the transform. Detailed view information is not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

Entity properties

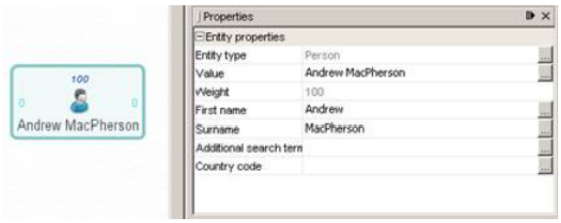
Entity properties are shown and can be edited in the Entity property window. Hereby the entity property of a netblock:



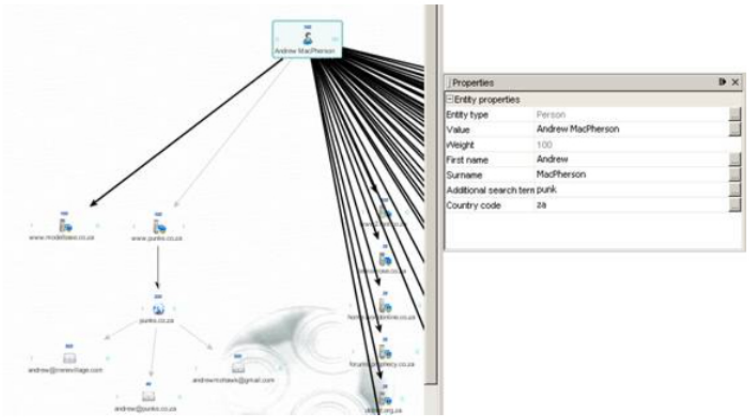
The properties can be changed. Consider a search for a person. We want to add additional search terms to our search. When a new person entity is created the entity's properties are blank:



When the Person entity is populated with the words "Andrew MacPherson" the properties is automatically updated. It now looks like this:



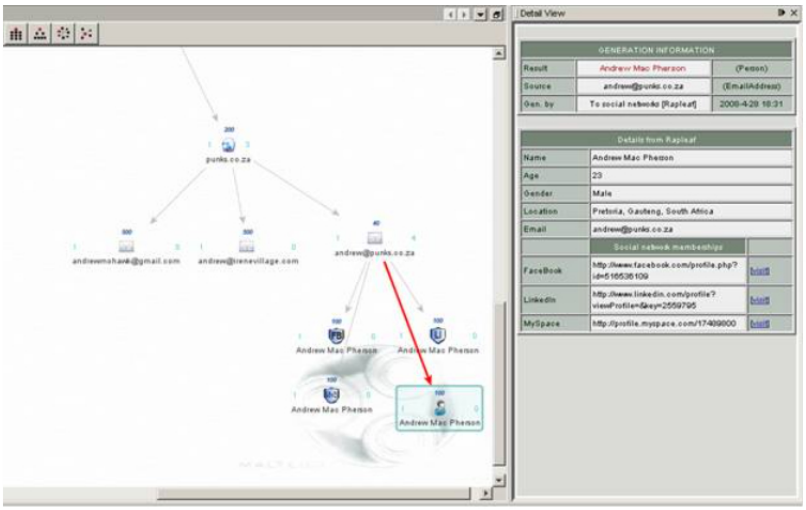
Running a PersonToWebsite transform on this PersonEntity leads to many results – clearly there are lots of Andrew MacPhersons active on the Internet. What we really want to do is looking for Andrew MacPherson in South Africa. We might also add an additional search term 'punks' because we know that the Andrew we are looking for has a mohawk. Running the transform again we now get results restricted to South Africa and related to punks:



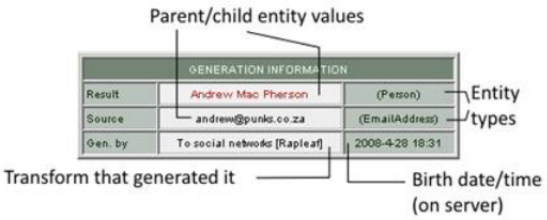
The first two results (coming in with weights of 100) are related to the Andrew MacPherson that we've had in mind. Setting entity properties for advanced searches is very important to focus searches.

Entity 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. Sticking with the graph above, when using the Rapleaf transform on an email address entity a lot of additional information is returned that cannot be fitted on the graph window itself:



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:

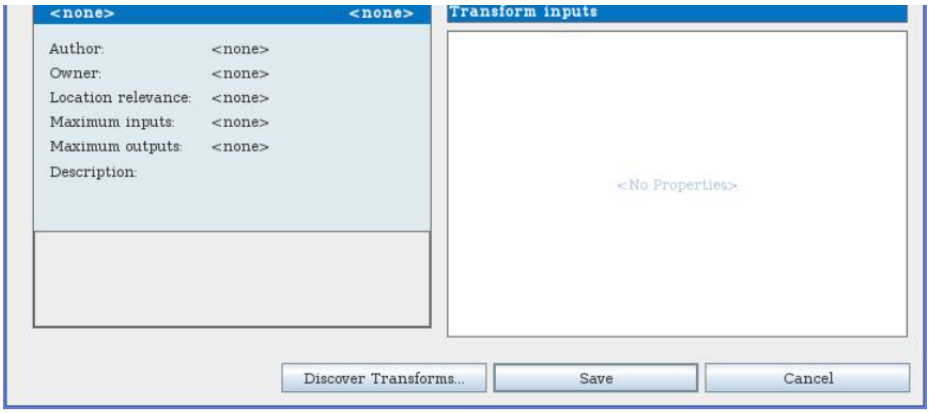


Transform Manager

The 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)

The transform manager can be found be selecting **Tools->Manage Transforms** and will look as follows:





Editing Transforms

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

- Application - The Transform Application Server (TAS)
- Display Name - The Transform Name in the GUI
- Input and Output Type - The entity types that a specific transform is run on and the entity types that are returned
- Enabled - Setting the transform to be Enabled or disabled.

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 and so on.
- Set Manager (Top Left) - This button allows you to access the Set Manager where sets (groups of transforms) can be added, deleted and modified.
- Clone and Remove Transforms (Top Right) - These buttons allow for the Removal and duplication of Transforms

Changing Transform Display Names

You can easily change transform display names by double clicking on the Display Name field of the transform you wish to edit.

Cloning Transforms

Cloning transforms creates a duplicate of an already existing transform and is very useful for transforms that require settings where you would like to use the same transform with multiple settings.



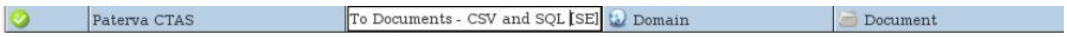
To clone a transform select the transform from the Transform Manager and click the "Clone Transform" button (seen above).

For example, to duplicate the To Documents[SE] transform so that we have one that searches for the standard set of documents and one that searches for .csv and .sql documents we will do the following:

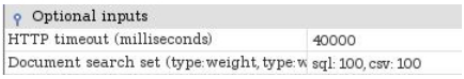
Step One: Select the ToDocuments[SE] Transform with a Domain entity as an input and a Document entity as an output type. Click "Clone Transform".



Step Two: Modify the name of the cloned transform (Seen as ToDocuments[SE]*) and change the name to something more descriptive.



Step Three: Modify the settings for this transform (Bottom right) and change the Document Search Set field to "sql:100,csv:100"



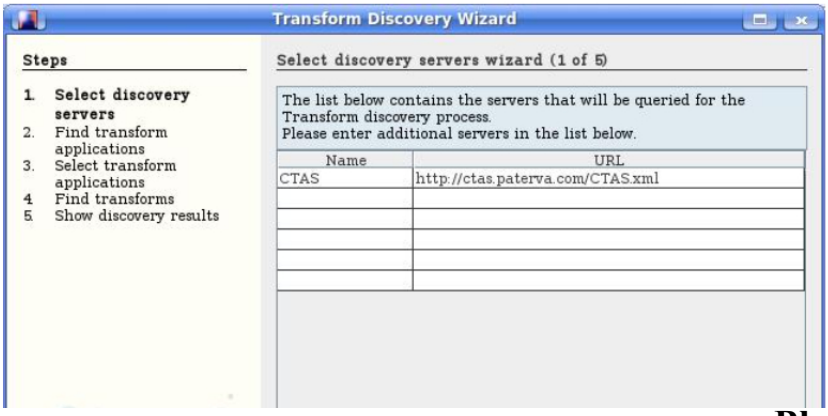

```
Note the field in this example is formatted as type:weight, the type denotes the
document extension and the weight is the relational weight that will be displayed in the graph.
```

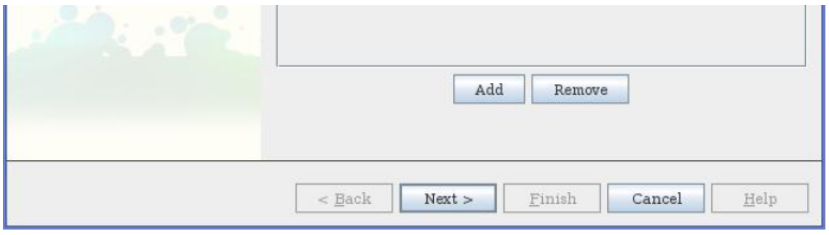
Step Four: Finally simply select save and your "new" transform will be ready to use!

Discovery Process

The discovery process is the method whereby Transform Applications are discovered and the transforms found so that they can be used within Maltego.To begin this process select the "Discover Transforms" button located at the bottom of the Transform Manager window.

Step One: After selecting Discover Transforms you will be greeted with a dialog whereby you can enter the Transform Application (or just application within the Transform Manager) - as seen below:

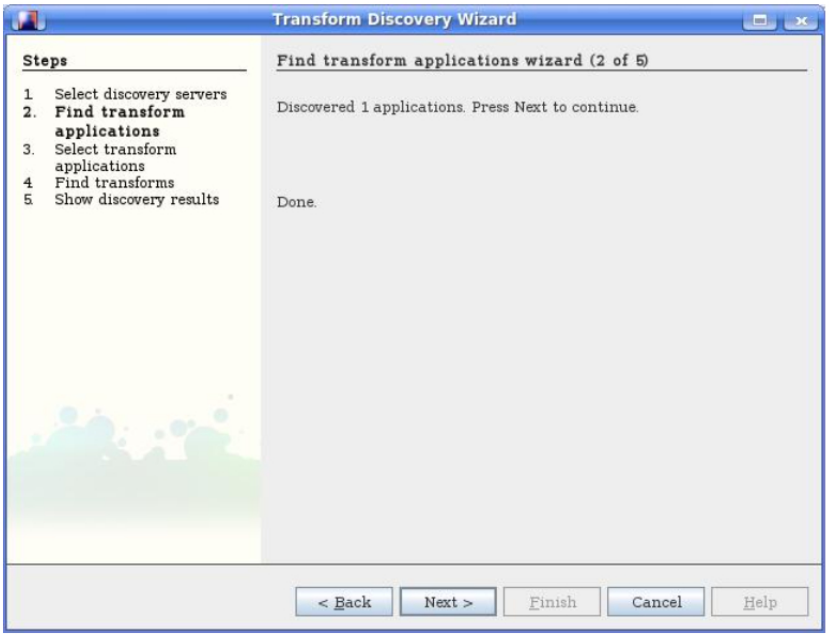




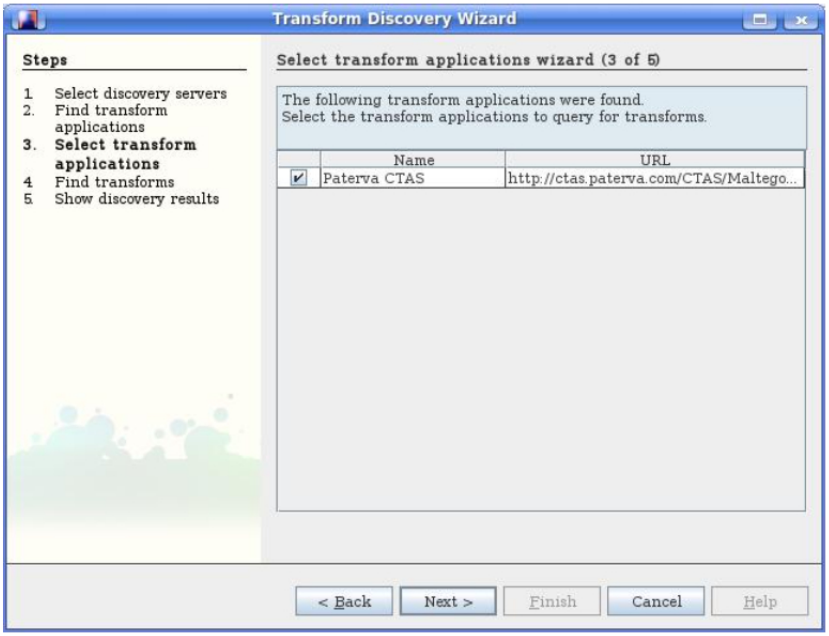
As seen above to proceed simply enter the transform application servers and a name for each of them before continuing. The publicly available servers are as follows:

Server	Description	URL
CTAS	The commercial TAS - only available to commercial users (Requires valid License Key)	http://ctas.paterva.com/CTAS.xml
CETAS	The Community Edition TAS	http://maltego4.paterva.com/CESeed.xml
MALTAS	The MALWARE TAS - Publicly Available to both CE and Commercial Users	http://ctas.paterva.com/MALTAS.xml

Step Two: After selecting Next you will see a confirmation screen indicating how many Transform Application Servers were found. If this number is not correct please go back to step one and double check the URLs of the servers.



Step Three: After confirming the amount of applications found you can select which servers Transforms you wish to use:



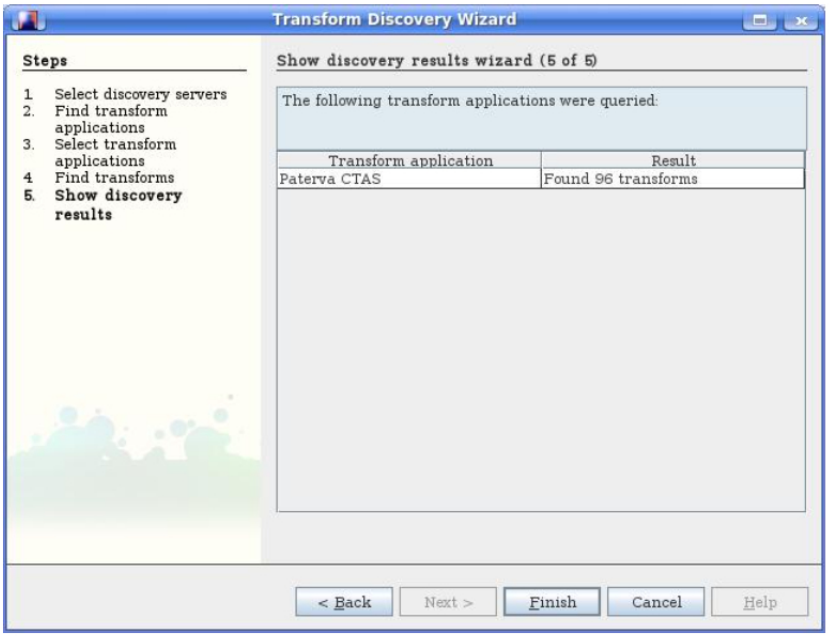

```
Note: Unselecting applications will *not* remove transforms from those servers that you
have already discovered, to remove transforms select the transforms in the Transform Manager
and click "Remove Transforms"
```

Step Four: After selecting the applications you wish to discover transforms from you can click next to identify how many transforms are located on this server:





You can then proceed to the next stage whereby the wizard will indicate how many transforms have been added:

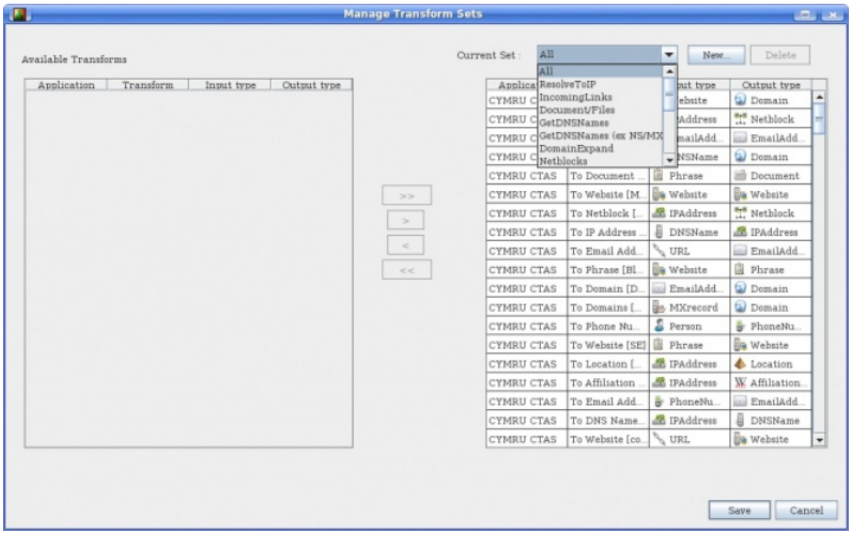


Clicking Finish will complete the cycle and your new transforms can be found within the Transform Manager:

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 button located within the Transform Manager (Top Left). The set manager is relatively straight forward with a basic interface to manage which transforms are within each set.

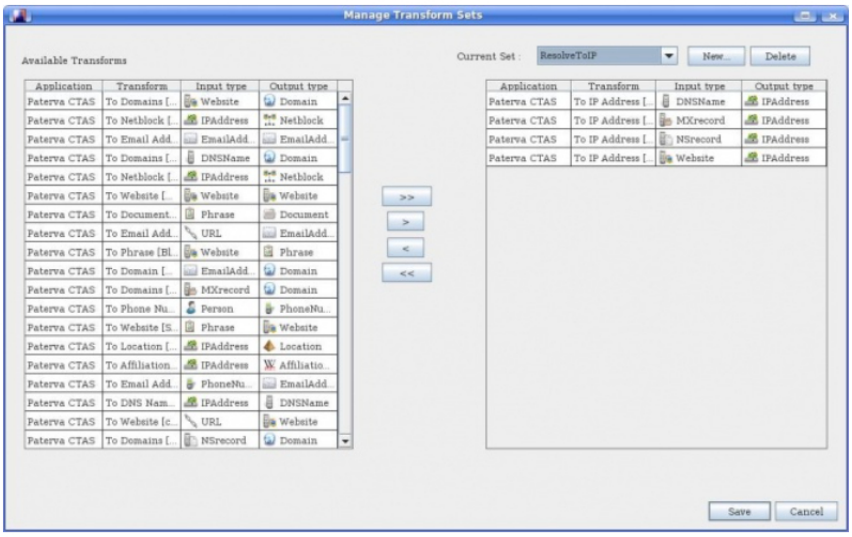


Creating New Sets

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

Adding/Removing Transforms from Sets

To add or remove transforms from a set start by selecting the set you wish to modify from the dropdown of available sets (located top right within the Set Manager) and then by using the arrow buttons located within the center of the set manager you can add and remove transforms in this set.



To add specific transforms to a set select the transforms that you wish to use within the selected set (available transforms are located in the table on the left) and select the ">" button to move those specific transforms. To add all of the available transforms to a set simply click the ">>" button located within the Set Manager.

To remove specific transforms to a set select the transforms that you wish to remove within the selected set (transforms currently in a set are located in the table on the right) and select the "<" button to remove those specific transforms. To remove all of the current transforms within the set simply click the ">>" button located within the Set Manager.

Deleting Sets

To Permanently delete a set select the set from the dropdown of available sets (located top right within the Set Manager) and click the Delete button. You will then be given a dialog to confirm that you wish to delete the set:



Selecting yes on this dialog will delete the set permanently.

Save/Load

Maltego can easily load and save graphs. Files are saved with a .MTG extension.

Export

Maltego can export entities in three ways:

1. Export all entities
2. Export selected entities
3. Export screen as PNG file

Entities are exported as CSV with the following fields:

- Value
- Weight
- Entity type

Printing

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.



Adding poster coordinates will help you to figure out which page goes where. Afterwards you need to manually cut the edges from the paper and stick it together. Here is a quick attempt of a 2x2 page poster by the author (picture taken with a cell phone in lowlight conditions…):





Some users told us that printing to PDF is possible. For this you should install a PDF printer driver.

https://web.archive.org/web/20120606172056/http:/ctas.paterva.com/view/Userguide

INTERNET ARCHIVE WayBackMachine
http://ctas.paterva.com/view/Userguide
Go
DEC JUN JUN
2010 06 2012 2013
47 captures
19 May 2008 - 23 May 202
page | discussion | view source | history
About this capture

Userguide

Contents [hide]

1 Maltego User Guide (Commercial edition)
2 Installation
  2.1 Windows
  2.2 Linux
  2.3 Mac
3 Running the first time & registering
4 Migrating From 2.0 to 2.0.1
5 Your first graph
6 Navigation
  6.1 Zoom
  6.2 Zoom to Pointer [As of 2.0.1]
  6.3 Zoom Lense [As of 2.0.1]
  6.4 Pan
  6.5 Copy And Paste [As Of 2.0.1]
    6.5.1 Copying
    6.5.2 Pasting Without Relationship Links
    6.5.3 Pasting Entities WITH Relationship Links
    6.5.4 Pasting From Text
7 Running transforms
8 Canceling Currently Running Transforms [As of 2.0.1]
9 Setting the number of results returned
10 Selecting entities
  10.1 Single select
  10.2 Multiple select
  10.3 Selecting entities one at a time
  10.4 Selection by child
  10.5 Selection by child (keep parent)
  10.6 Selecting parent
  10.7 Select a parent (keep)
  10.8 Selecting entities using 'Find'
  10.9 Invert Selection [As of 2.0.1]
  10.10 Combinations
  10.11 Quick list of incoming and outgoing nodes
11 Views and layout
  11.1 Layout
  11.2 Views
12 Entity Properties & Detailed view
  12.1 Entity properties
  12.2 Entity detailed view
13 Transform Manager
  13.1 Editing Transforms
    13.1.1 Changing Transform Display Names
    13.1.2 Cloning Transforms
  13.2 Discovery Process
  13.3 Sets
    13.3.1 Creating New Sets
    13.3.2 Adding/Removing Transforms from Sets
    13.3.3 Deleting Sets
14 Save/Load
15 Export
16 Printing

Maltego User Guide (Commercial edition)

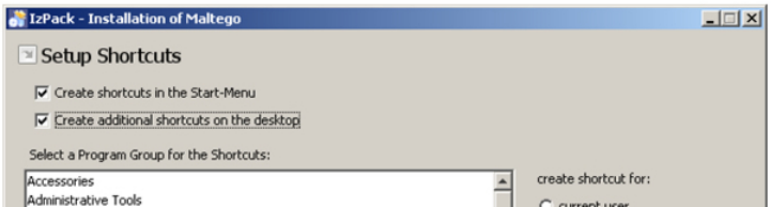
This user guide is for the commercial edition of Maltego. The community edition of Maltego is very similar; there are only a couple of differences in the startup.

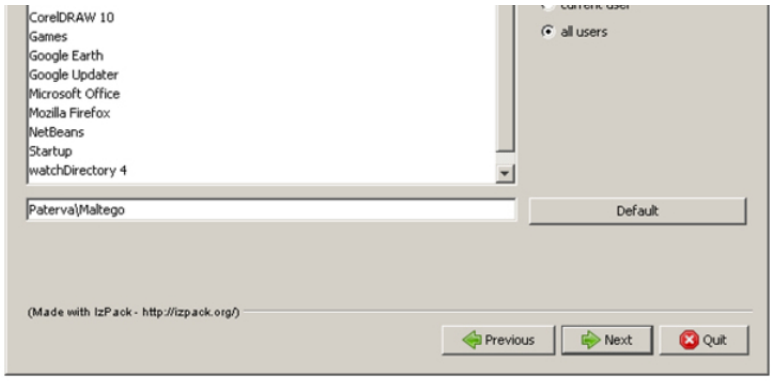
Maltego can run on Windows or Linux. This section of the guide assumes that you already have Java 1.6 installed. Should you have any questions not answered by this user guide please Contact Us

Installation

Windows

After downloading the MaltegoInstaller.exe file double click on it to start the installation process. The installer is built using Izpack – a generic Java installer that is not platform specific. You should follow the wizard – defaults will do, but you might want to add icons to your desktop on the last screen:





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

Linux

You will need to have a windows (X11) system – Maltego is a graphical application. After download you should open a terminal window. You should change to the directory to where you have downloaded the MaltegoInstaller.jar file – e.g.

> *cd downloads/maltego* (assuming that you've downloaded it here)

From here you can run the Java installer using the following command:

> *java –jar MaltegoInstaller.jar*

The installer should start the graphical wizard. As with the Windows install you can decide if you want a desktop item. The installer can normally add this for KDE or Gnome based desktops – others have not been tested.

Note 1: 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 is not good.

Note 2: 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/*

Mac

The mac release (commercial), can be downloaded as a .pkg from http://www.paterva.com/maltego/download/ . The .pkg file can then be executed and a simple wizard will guide you through the installation.

You will however need to install Java 1.6 (for dual core Mac users), or Soylatte Java (for 32bit Mac users). For more information this you can view the forum post here: http://www.paterva.com/forum/index.php/topic,84.0.html

Running the first time & registering

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

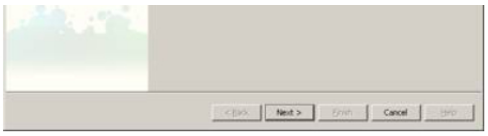


Note that parts of this screen are dynamic content and thus could change from time to time.

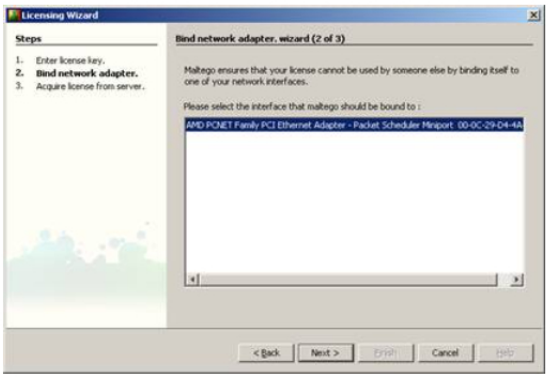
Maltego v2 is a commercial product and a license key is used to activate the product. The license key is valid for one year and is computer specific. Without a valid license key you can only use MaltegoV2 to view files created by other users – you cannot create new graphs and you cannot add or edit existing graphs. To register you can click on the red text that reads "You must register before you can use Maltego. Click here to register now". This will start the registration wizard.

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 the word 'Valid' appear. If not it the word 'Invalid' will appear:

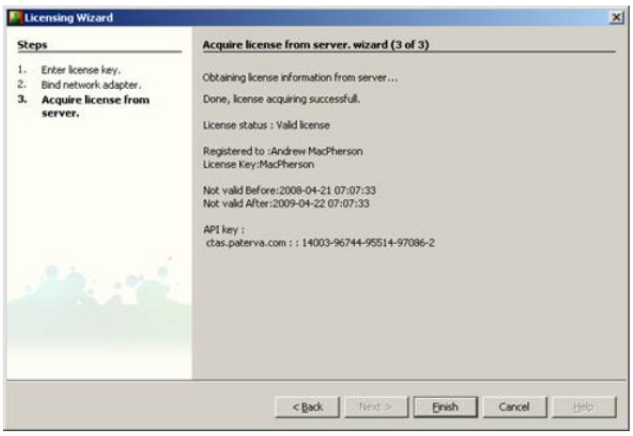




Click on next. Next you will be asked on which adaptor you want to bind the installation. Choose an adaptor that it not likely to change.



Under Linux you are encouraged to choose the 'eth0' adaptor. Click on Next. 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 enabled. The screen should show a summary of registration information. Don't worry about writing any of it down as you can get it from the application at a later stage.



The start page will now be updated with the registration information:



Migrating From 2.0 to 2.0.1

Click here to view the Migration Tutorial for Windows Vista, Windows XP and Linux

Your first graph

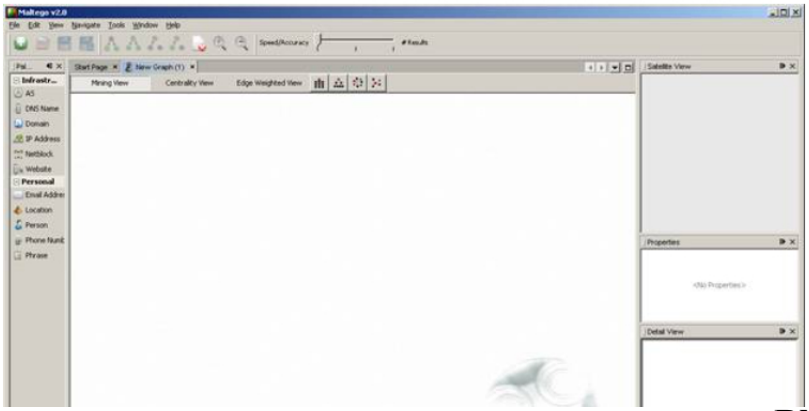


To start a new graph click on



You can also click on the 'New' icon that's right below [File]. 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).

You should get an empty graph which looks like this:





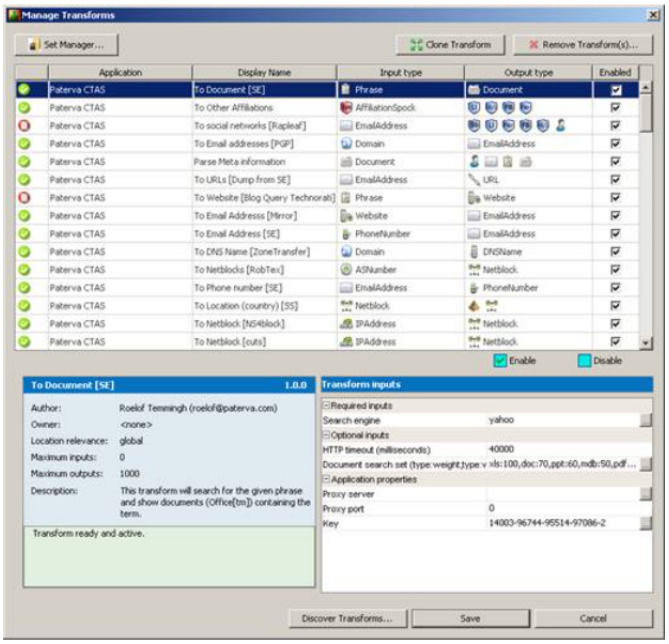
More than one graph can be opened. New graphs are added as tabs at the top of the screen.

You can go back to the start page by clicking on the 'Start Page' tab, or by going to Help -> Start Page. To get API and license keys, as well as a summary of registration information you can go to Help -> About Maltego. This should show a screen that looks like this:



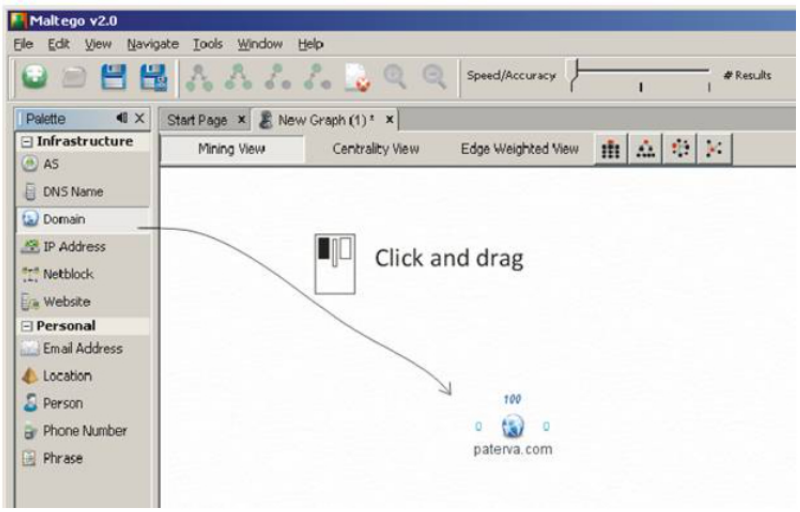
If you ever need to query the status of your license or if you've lost your API keys you can view your license key here.

At this stage you want to make sure that you have the preconfigured transforms discovered and keyed. Click on Tools->Manage transforms. You should see:

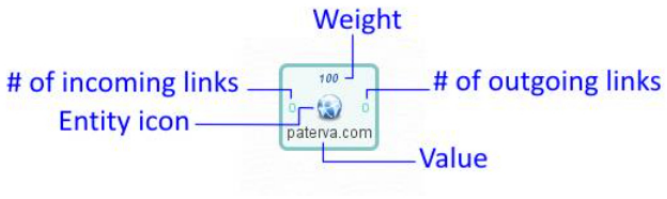


Note that there is a list of transforms and that most of them have a green icon on the left (which means they are ready to be used). For more information about managing transforms see the relevant section in this documentation.

Next, we want to put some entities on the graph window. Select the 'Domain' Entity from the Palette and drag it to the graph window:



The first thing that you will notice is that the entity contains three numbers and a value. The values are as follows:



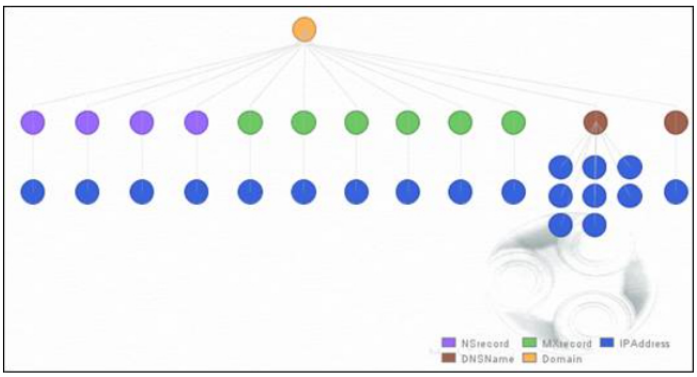
To edit the name of the entity (in this case a domain) double click on it. The entity will become selected and the text area underneath the entity will be highlighted – you can now edit it:



Navigation

Zoom

To zoom in and out use the mouse scroll wheel. If you are using a notebook without a scroll wheel you can use the  buttons. 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 colors, with a small legend for mapping colors to entity types in the right hand bottom corner of the graph:



Note that the colors 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.

Please Note: As of version 2.0.1 when zooming with the mouse scroll wheel the zoom to pointer method will be used (described below)

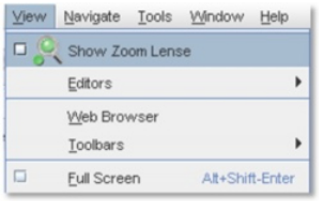
Zoom to Pointer [As of 2.0.1]

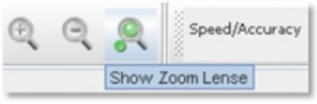
The zoom to pointer function is an enhanced zoom feature that has been implemented as of 2.0.1. Where the previous zoom method would zoom in or out based on the central display of the graph, zoom to pointer (the new 'zoom'), will zoom in and out based on the location of the mouse pointer within the graph.

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 center of the graph.

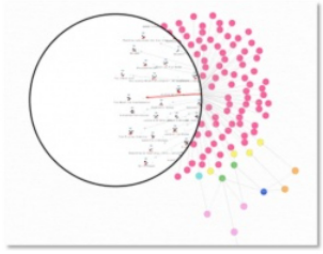
Zoom Lense [As of 2.0.1]

The zoom lense method of navigating a graph is a way of taking a virtual magnifying glass to your graph, whereby you can quickly see a magnified portion of the graph rather than have to zoom into it. This option can be turned on by either selecting view->show zoom Lense (as seen below left), or selecting the zoom lens icon within the top Maltego toolbar (below right)





With this option selected the mouse cursor is replaced by a single magnifying sphere. The zoom level on this can also be adjusted via the scroll button on the mouse to either increase or decrease the magnifying capacity of the lens. An example of this in use can be seen below:



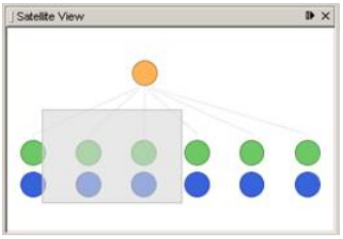
To turn this option off you can simply select either of the two methods used to turn the zoom lens on as described above.

Pan



To pan you can use the scroll bars at the sides of the graph window, or you can right-click and drag. This method of navigation is a lot faster than using the scroll bars.

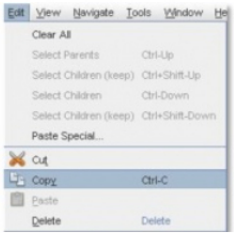
You can also use the Satellite view to navigate. This is useful navigation technique on large graphs.



You can move the visible frame (grey box) around on the Satellite view 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).

Copy And Paste [As Of 2.0.1]

Copying



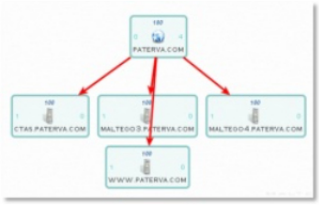
Entities can be copied by selecting the entities you wish to copy (via any of the selecting methods described elsewhere in this document) and then pressing CTRL + C or selecting Edit->Copy from the menu (as seen above).

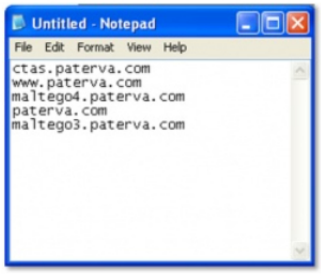
Pasting Without Relationship Links



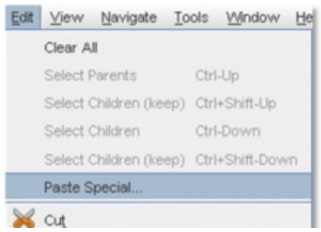
Entities can be pasted either into an external application or a Maltego graph (without relationship links). This can be done by either pressing CTRL + V or selecting Edit->Paste (as seen above)

Entities that are copied and have been pasted into any external application will have the value of the selected nodes. For example if we select the following entities in a graph, copy them and then paste them into a generic text editor (in this case windows notepad) you will see the values of the entities we copied have been pasted (second example)





Pasting Entities WITH Relationship Links





To retain the relationship links (links between entities) within graphs you can simply select Edit->Paste Special… (as seen above). You will then see a dialog window which allows you to either paste the copied entities with our without relationship links (below). Simply select the first option (Paste entities and links) and the relationships will be saved between graphs!



Pasting From Text

Entities can also be pasted from text by simple selecting the text, copying it (as you would with any word processor or other application), and then pasting using either of the paste methods described above.

Maltego will also try and determine what type of entity has been copied based on its value and try to select the correct entity within the graph.

For example, if you were to copy the following as text:

- Andrew@punks.co.za
- Andrew MacPherson
- Punks.co.za
- www.punks.co.za
- punk south Africa

Maltego would interpret the entities as the following in a graph

- Email Address
- Name
- Domain
- DNS Name
- Phrase

And the output would be as follows:

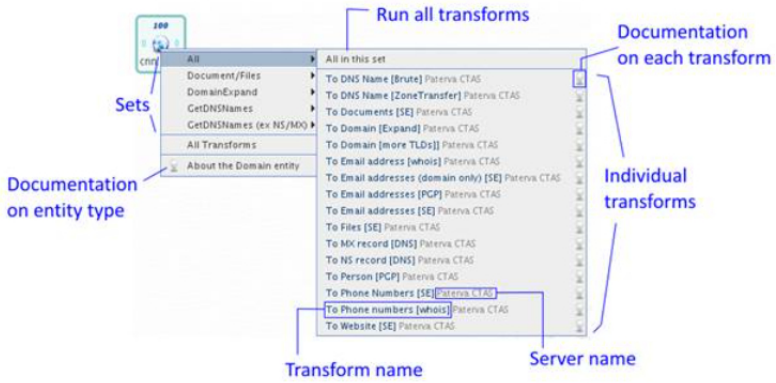


Please Note: The regular expression matching for pasted text is not perfect - but its pretty close!

Running transforms



To run your first transform you can right click on the entity. You will see a list that looks like this:

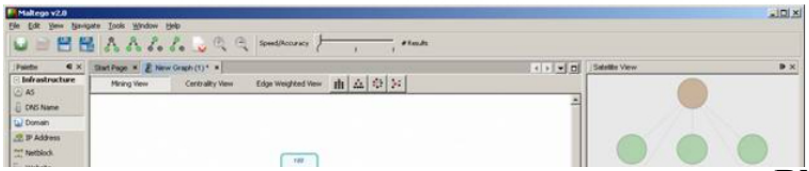


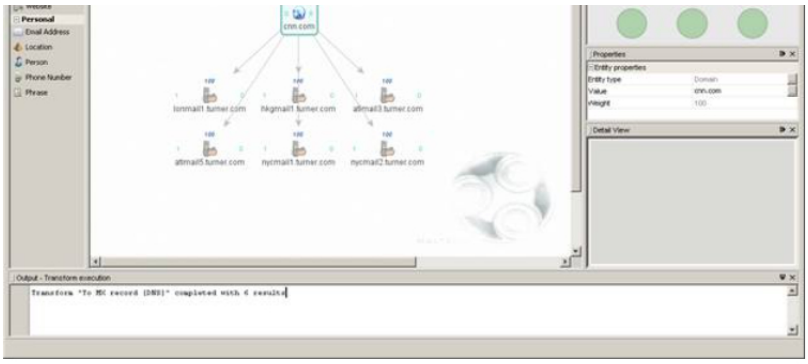
Let us assume that we want to find out what the MX (mail exchanger) records for the domain are. We want to use the 'To MX records [DNS]' transform and so we click on it. In the bottom right hand corner we can see the transform status bar indicating that we are running one transform on one entity.



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

The resultant screen should look something like this:

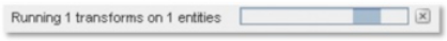




Note that the Output screen has appeared with details about the transform's execution. This information is very useful as some transforms will give additional information in this screen.

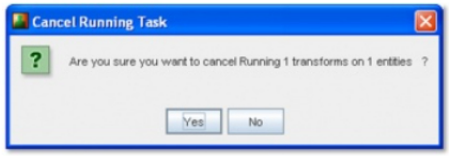
Canceling Currently Running Transforms [As of 2.0.1]

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:



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 all of the running transforms. 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.

Please Note: When running a set of transforms you can only cancel the entire set!

Setting the number of results returned

A slider is located at the top of the Maltego application:



When set to the very left Maltego will only show the top 12 results, based on weight. The middle setting corresponds to 50 results and the very right to 255 results. 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.

In upcoming versions of the tool the transforms will be categorized as either 'enumeration' or 'search' transforms – the slider will only apply to 'search' transforms. For now you have to be careful to understand how the slider works and spend time experimenting with it.

Selecting entities

There are a few way of selecting entities.

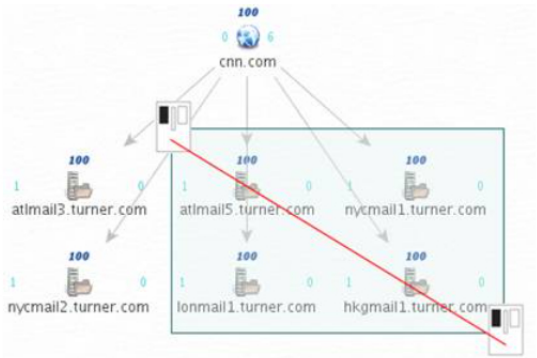
Single select



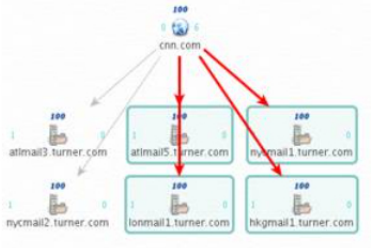
Simply click on the entity. The entity gets a blue frame around it. If zoomed out the entity's color is enhanced.

Multiple select

You can select more than one entity by left click dragging a box around it:



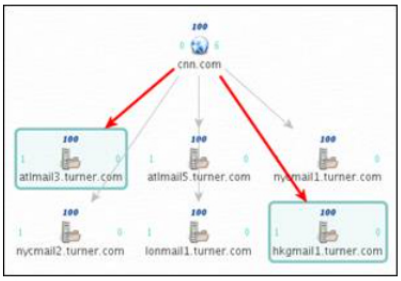
As soon as you release the left mouse button the entities are selected:



Selecting entities one at a time



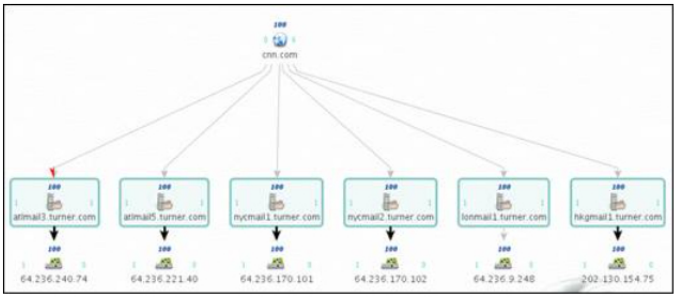
You can select entities one by one by click on it and holding in shift:



Selection by child



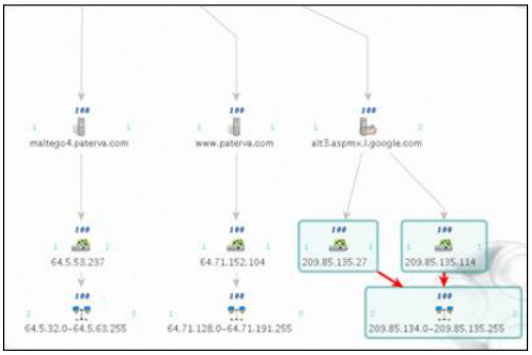
It is very useful to be able to select the children of a node (e.g. all the nodes that were created from the node). You can do this by selecting the parent and pressing Control + Down Arrow.



Selection by child (keep parent)



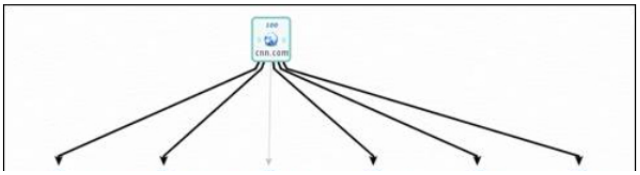
You can select child nodes and keep the parents selected by pressing Control + Shift + Down Arrow. This is useful to select an entire "family tree":

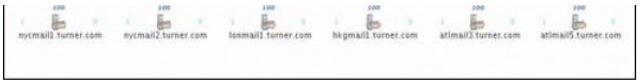


Selecting parent



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

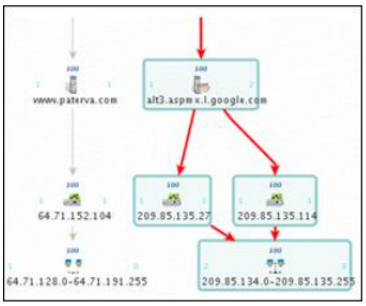




Select a parent (keep)



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.



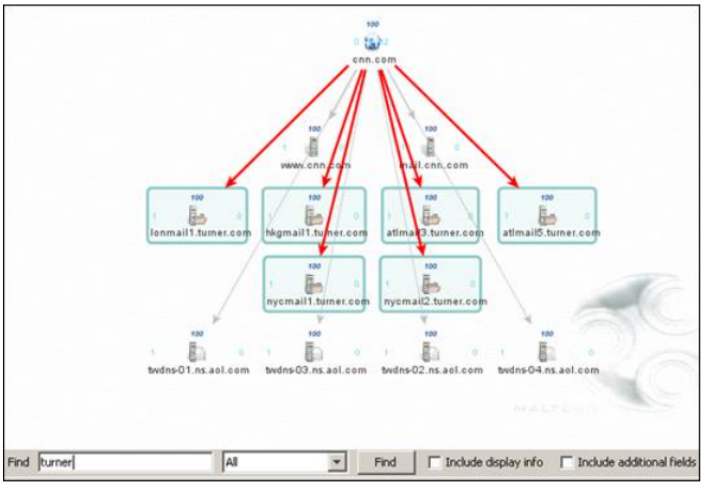
Selecting entities using 'Find'



To enable searching press Control F. The following window will appear:



Enter the search term and click on "Find" – entities that match the criteria will be selected:



For more information on finding entities please refer to the relevant section in this document.

Invert Selection [As of 2.0.1]



Invert Selection allows you to invert the selected nodes. For example if you had selected all the IP Addresses from a graph and then pressed the Invert Selection button (seen above - far left), everything except the IP Addresses would be selected.

Combinations

The best way to select entities is a combination of all of the above methods. For instance you might single select entities and use a combination of child/parent expansion to find what you are looking for.

Quick list of incoming and outgoing nodes



When working with large graphs it is very possible that parent and child nodes of a selected entity is outside the border of the current graph. A quick way to get a list of parent and child nodes is to Control click on the node. This show a separate window with all incoming (parents) and outgoing (children) nodes:





Views and layout

Layout

Maltego supports 4 types of layout algorithms:

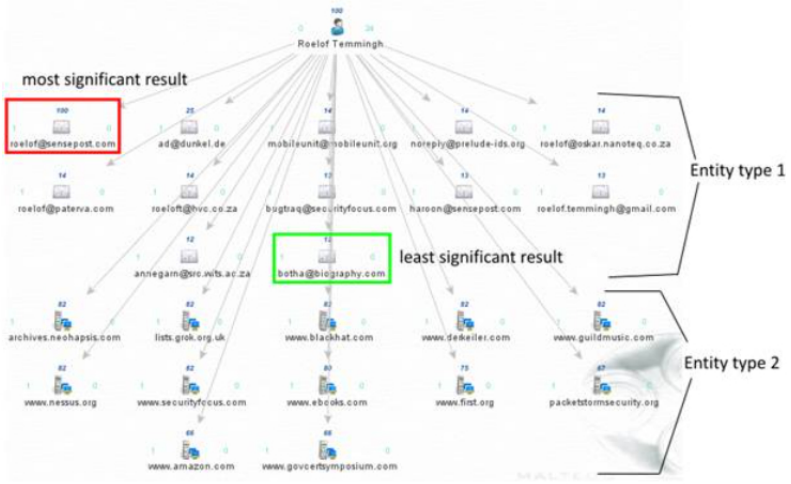
1. Block layout. This is the default layout and is also used during mining. This layout is discussed in more depth later.
2. Hierarchical layout. Think of this a tree based layout – like a file manager.
3. Centrality layout. Nodes that are most central to the graph (e.g. most incoming links) appear in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

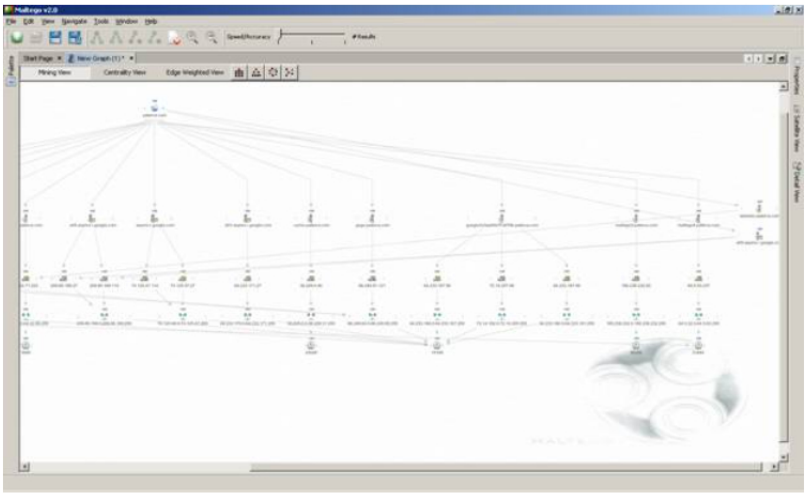
1. In a block of nodes
2. Sorted by entity type
3. Sorted by entity weight

Consider the following graph were two transforms were executed on the Person entity – Person2EmailAddress and Person2Website:

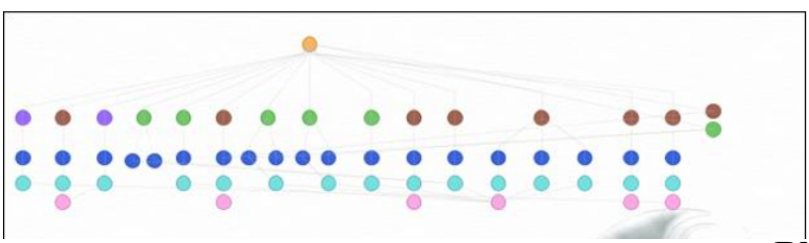


Note that entities are ordered by type and weight.

The following pictures show the same graph in different layout types. The graph shows all Paterva related DNS Names, their IP addresses, what netblocks they belong to and the AS numbers of those networks. Note that most of the graph has been viewed in 'overview' mode in order to see the layout properly Block layout (detailed):

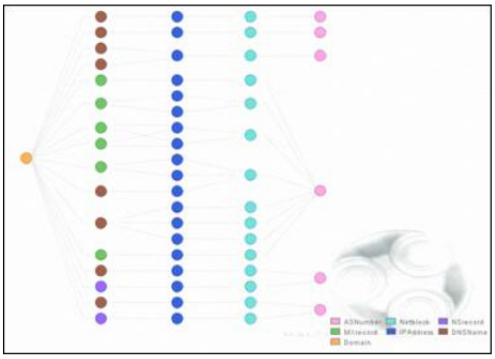


Block layout (zoomed out / overview):

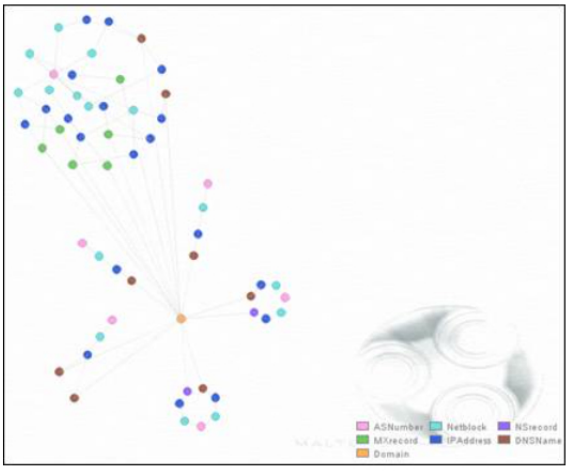




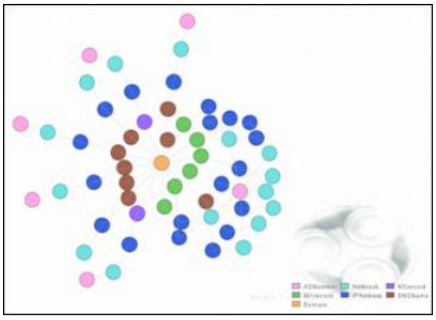
Tree layout:



Centrality layout:



Organic layout:



Different layouts work best of different situations – you need to experiment with it to see which layout works best for the situation at hand.

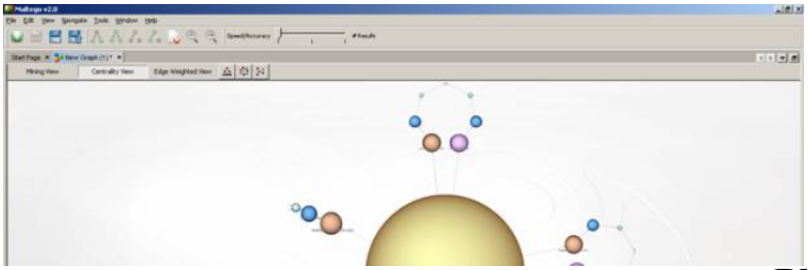
Views

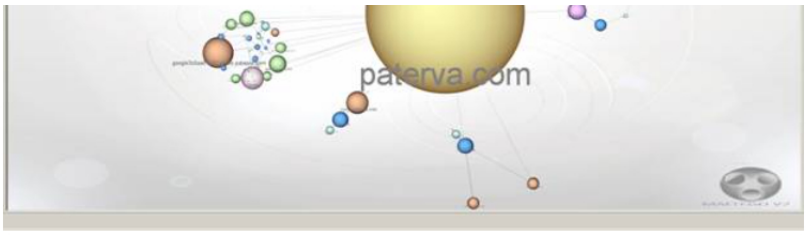
Views are used to extract non-obvious information from large graphs – where the analyst cannot see clear relationships by manual inspection of data. Other than the mining view, Maltego supports two other views:

1. Edge weighted view. Node sizes are based on number of incoming links.
2. Centrality view. Nodes that are calculated to be most central to the graph are given larger nodes.

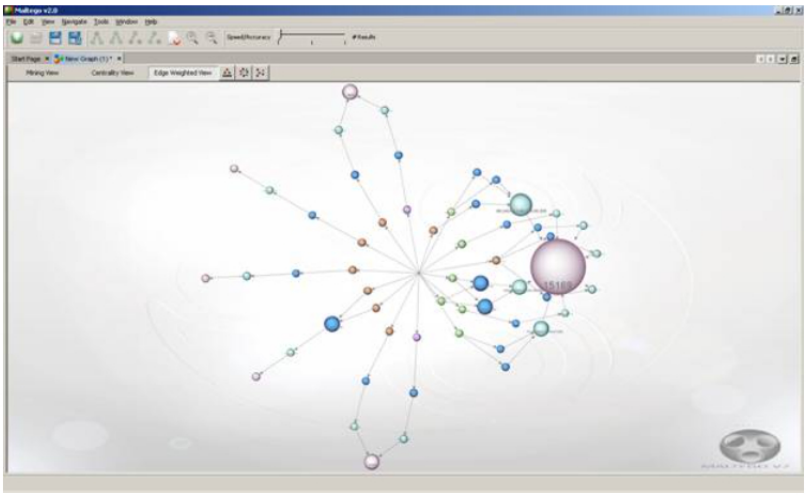
In views two and three entity details are not shown and no selection is possible. It is simply a view of the data with one exception - control clicking on a node still brings up a list of incoming and outgoing links.

The same graph used in the previous section is shown in different views. First the centrality view:



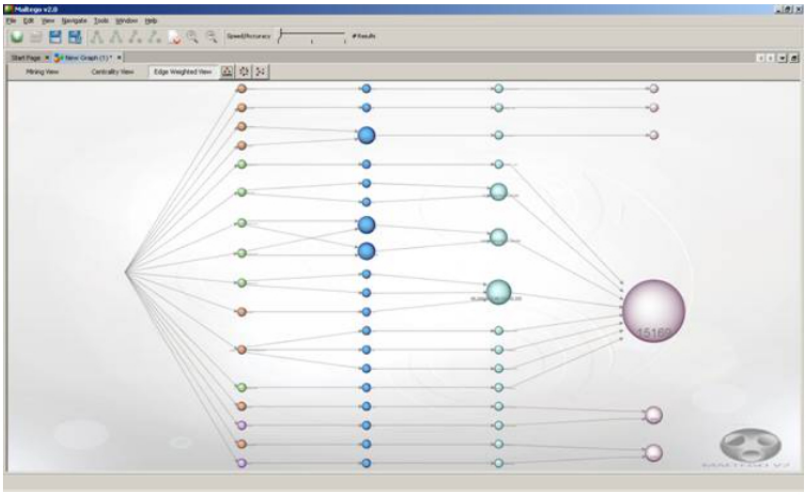


Clearly the domain paterva.com is central to the graph. When viewing the same graph in 'Edge weighted view' we see something more interesting:

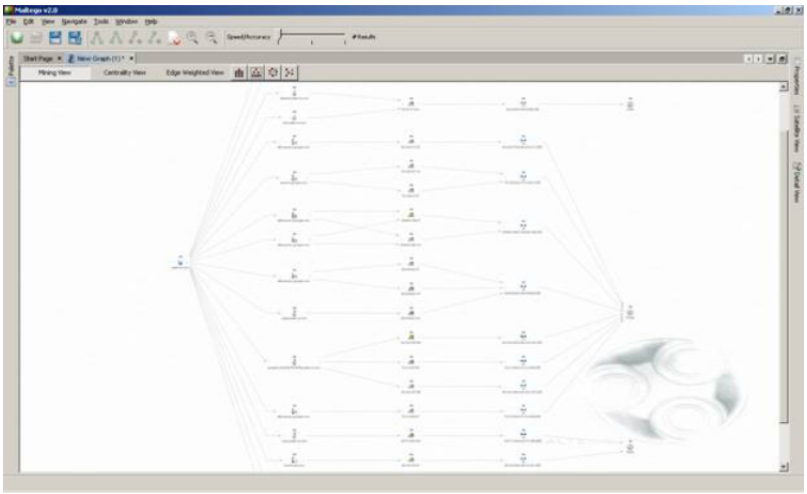


Now the AS number 15169 is clearly more 'inflated'. This is the expected result – this AS has the most incoming links.

The layout in these views can be modified. Consider the 'edge weighted view' in tree layout:

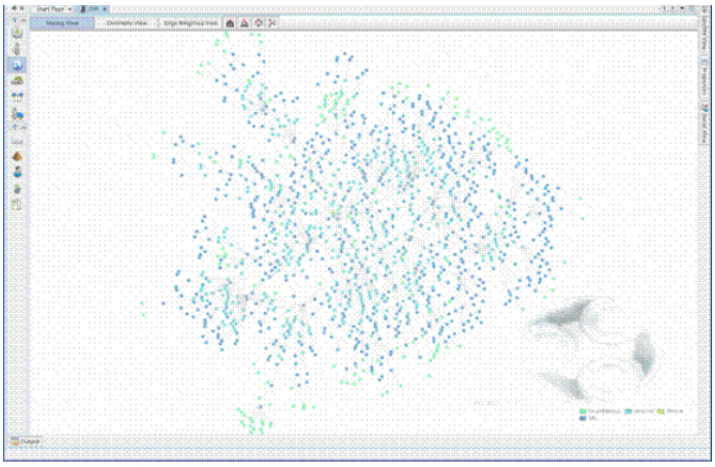


Comparing this view with the original view we can clearly see the relationship:

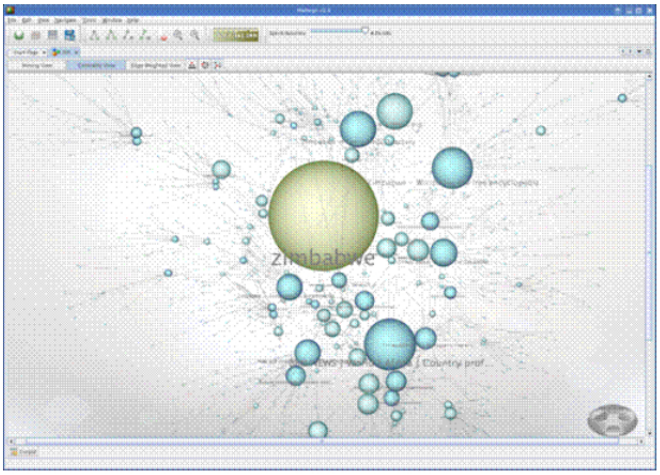


The graph showed above is rather simple and manual visual inspection would render the same results. However when graphs get very large these views proves invaluable. Consider this large graph:





It is practically impossible to extract any useful information from the graph. However – viewing the same graph in centrality view (organic):



This view makes it possible to identify the key entities in the graph with ease.

Entity Properties & Detailed view

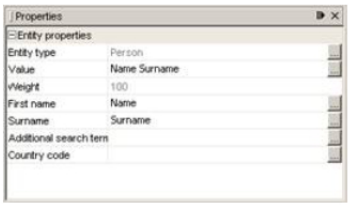
Each entity has a number of properties and may have a detailed view. Most of the properties of an entity can be set while the detailed view is read-only. The properties of an entity are used by transforms and are passed along with the entity's value to the transform. Detailed view information is not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

Entity properties

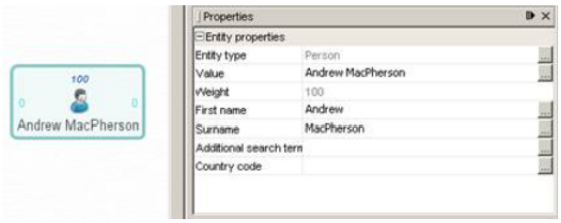
Entity properties are shown and can be edited in the Entity property window. Hereby the entity property of a netblock:



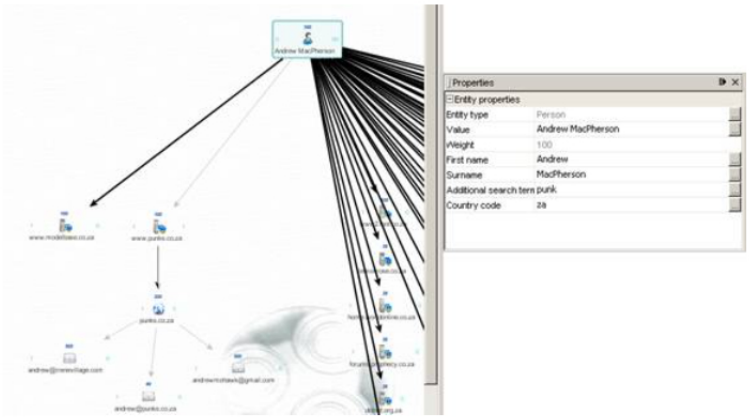
The properties can be changed. Consider a search for a person. We want to add additional search terms to our search. When a new person entity is created the entity's properties are blank:



When the Person entity is populated with the words "Andrew MacPherson" the properties is automatically updated. It now looks like this:



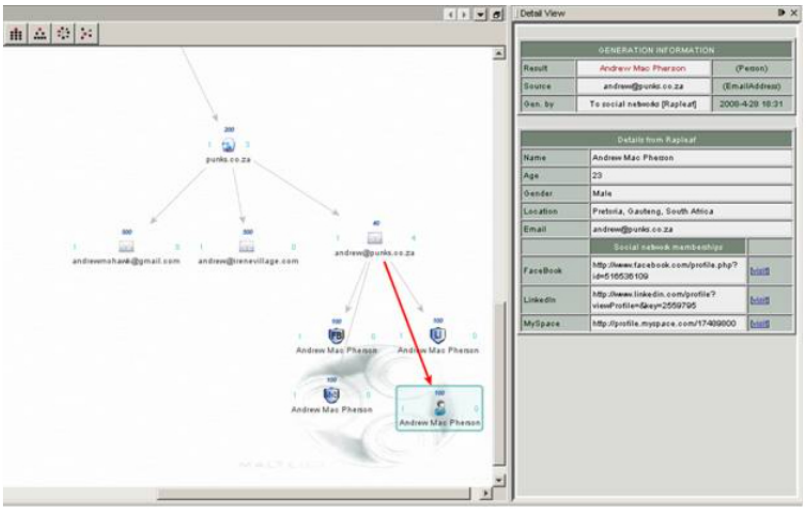
Running a PersonToWebsite transform on this PersonEntity leads to many results – clearly there are lots of Andrew MacPhersons active on the Internet. What we really want to do is looking for Andrew MacPherson in South Africa. We might also add an additional search term 'punks' because we know that the Andrew we are looking for has a mohawk. Running the transform again we now get results restricted to South Africa and related to punks:



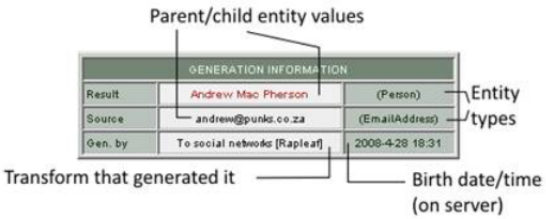
The first two results (coming in with weights of 100) are related to the Andrew MacPherson that we've had in mind. Setting entity properties for advanced searches is very important to focus searches.

Entity 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. Sticking with the graph above, when using the Rapleaf transform on an email address entity a lot of additional information is returned that cannot be fitted on the graph window itself:



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:

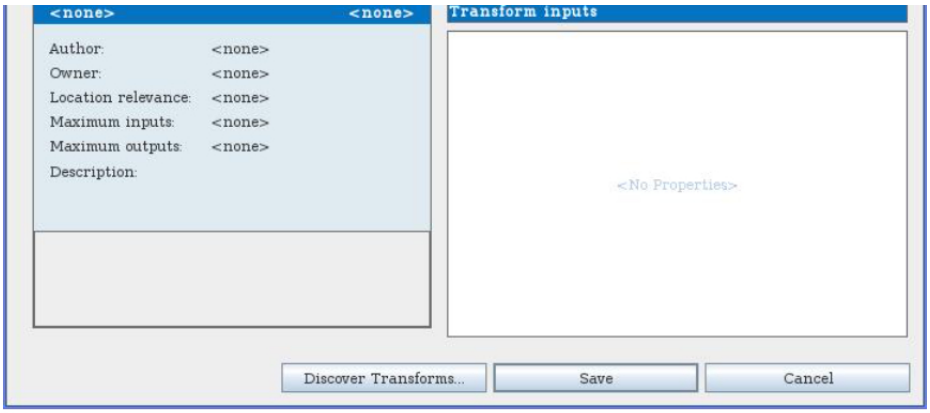


Transform Manager

The 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)

The transform manager can be found be selecting **Tools->Manage Transforms** and will look as follows:





Editing Transforms

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

- Application - The Transform Application Server (TAS)
- Display Name - The Transform Name in the GUI
- Input and Output Type - The entity types that a specific transform is run on and the entity types that are returned
- Enabled - Setting the transform to be Enabled or disabled.

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 and so on.
- Set Manager (Top Left) - This button allows you to access the Set Manager where sets (groups of transforms) can be added, deleted and modified.
- Clone and Remove Transforms (Top Right) - These buttons allow for the Removal and duplication of Transforms

Changing Transform Display Names

You can easily change transform display names by double clicking on the Display Name field of the transform you wish to edit.

Cloning Transforms

Cloning transforms creates a duplicate of an already existing transform and is very useful for transforms that require settings where you would like to use the same transform with multiple settings.



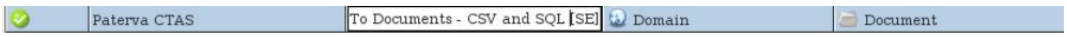
To clone a transform select the transform from the Transform Manager and click the "Clone Transform" button (seen above).

For example, to duplicate the To Documents[SE] transform so that we have one that searches for the standard set of documents and one that searches for .csv and .sql documents we will do the following:

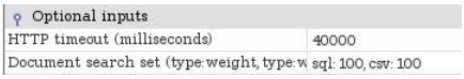
Step One: Select the ToDocuments[SE] Transform with a Domain entity as an input and a Document entity as an output type. Click "Clone Transform".



Step Two: Modify the name of the cloned transform (Seen as ToDocuments[SE]*) and change the name to something more descriptive.



Step Three: Modify the settings for this transform (Bottom right) and change the Document Search Set field to "sql:100,csv:100"



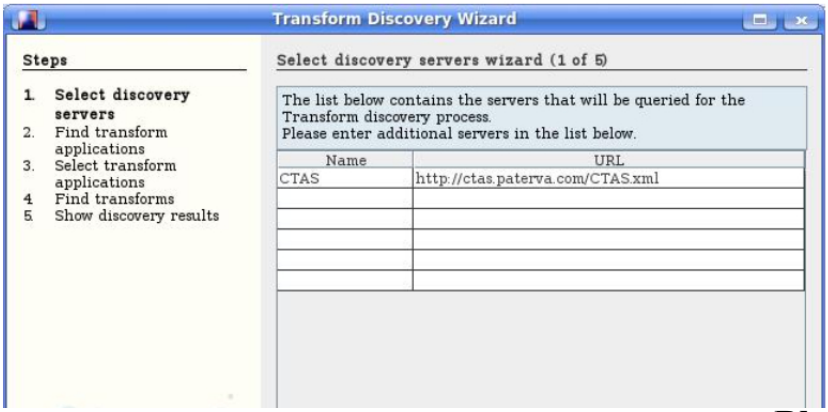

```
Note the field in this example is formatted as type:weight, the type denotes the
document extension and the weight is the relational weight that will be displayed in the graph.
```

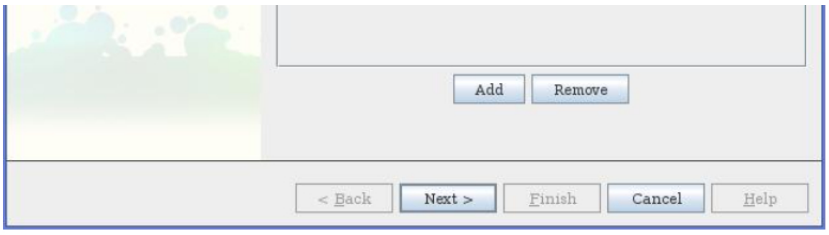
Step Four: Finally simply select save and your "new" transform will be ready to use!

Discovery Process

The discovery process is the method whereby Transform Applications are discovered and the transforms found so that they can be used within Maltego.To begin this process select the "Discover Transforms" button located at the bottom of the Transform Manager window.

Step One: After selecting Discover Transforms you will be greeted with a dialog whereby you can enter the Transform Application (or just application within the Transform Manager) - as seen below:

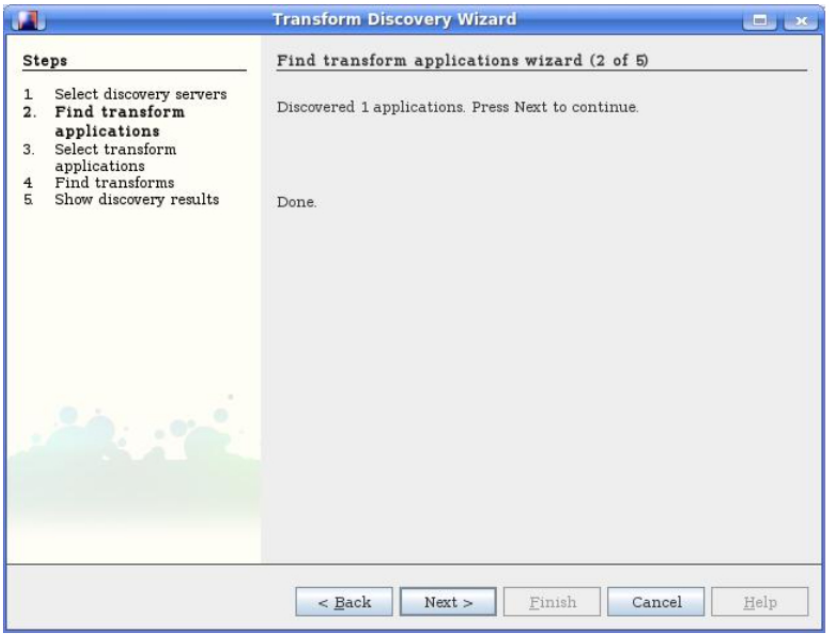




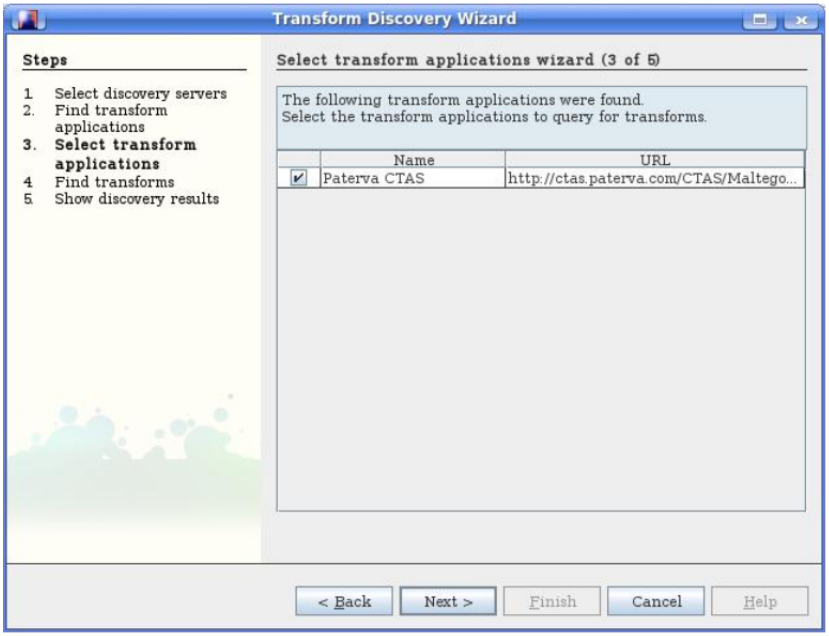
As seen above to proceed simply enter the transform application servers and a name for each of them before continuing. The publicly available servers are as follows:

Server	Description	URL
CTAS	The commercial TAS - only available to commercial users (Requires valid License Key)	http://ctas.paterva.com/CTAS.xml
CETAS	The Community Edition TAS	http://maltego4.paterva.com/CESeed.xml
MALTAS	The MALWARE TAS - Publicly Available to both CE and Commercial Users	http://ctas.paterva.com/MALTAS.xml

Step Two: After selecting Next you will see a confirmation screen indicating how many Transform Application Servers were found. If this number is not correct please go back to step one and double check the URLs of the servers.



Step Three: After confirming the amount of applications found you can select which servers Transforms you wish to use:



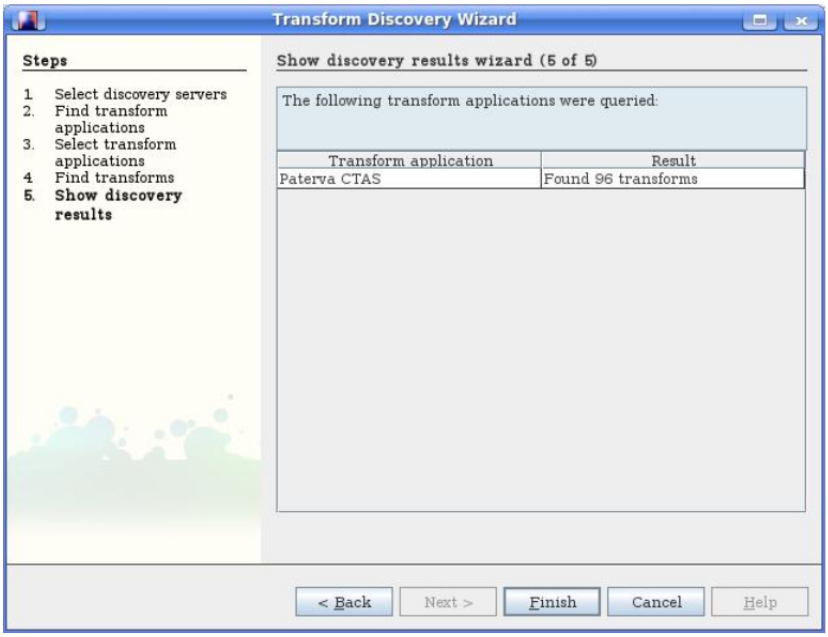

```
Note: Unselecting applications will *not* remove transforms from those servers that you
have already discovered, to remove transforms select the transforms in the Transform Manager
and click "Remove Transforms"
```

Step Four: After selecting the applications you wish to discover transforms from you can click next to identify how many transforms are located on this server:





You can then proceed to the next stage whereby the wizard will indicate how many transforms have been added:

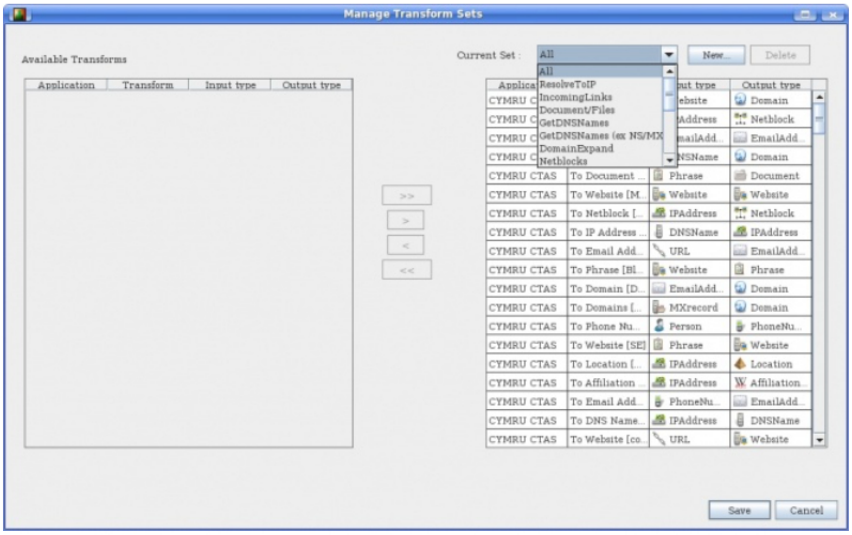


Clicking Finish will complete the cycle and your new transforms can be found within the Transform Manager:

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 button located within the Transform Manager (Top Left). The set manager is relatively straight forward with a basic interface to manage which transforms are within each set.

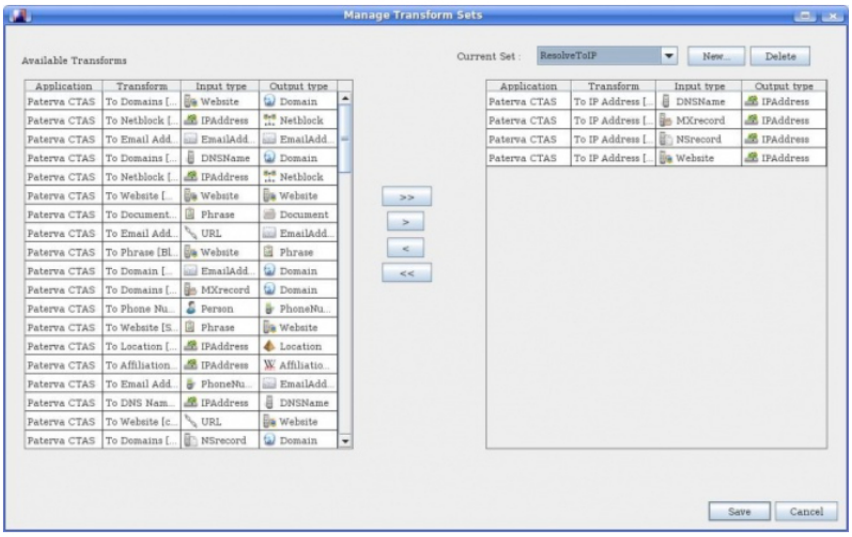


Creating New Sets

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

Adding/Removing Transforms from Sets

To add or remove transforms from a set start by selecting the set you wish to modify from the dropdown of available sets (located top right within the Set Manager) and then by using the arrow buttons located within the center of the set manager you can add and remove transforms in this set.



To add specific transforms to a set select the transforms that you wish to use within the selected set (available transforms are located in the table on the left) and select the ">" button to move those specific transforms. To add all of the available transforms to a set simply click the ">>" button located within the Set Manager.

To remove specific transforms to a set select the transforms that you wish to remove within the selected set (transforms currently in a set are located in the table on the right) and select the "<" button to remove those specific transforms. To remove all of the current transforms within the set simply click the ">>" button located within the Set Manager.

Deleting Sets

To Permanently delete a set select the set from the dropdown of available sets (located top right within the Set Manager) and click the Delete button. You will then be given a dialog to confirm that you wish to delete the set:



Selecting yes on this dialog will delete the set permanently.

Save/Load

Maltego can easily load and save graphs. Files are saved with a .MTG extension.

Export

Maltego can export entities in three ways:

1. Export all entities
2. Export selected entities
3. Export screen as PNG file

Entities are exported as CSV with the following fields:

- Value
- Weight
- Entity type

Printing

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.



Adding poster coordinates will help you to figure out which page goes where. Afterwards you need to manually cut the edges from the paper and stick it together. Here is a quick attempt of a 2x2 page poster by the author (picture taken with a cell phone in lowlight conditions…):





Some users told us that printing to PDF is possible. For this you should install a PDF printer driver.