https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-045

Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego

Klaus Schwarz[2,3]***, Reiner Creutzburg***[1,2]

[1] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany***
Email: creutzburg@th-brandenburg.de

[2] ***SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany***
Email: klaus.schwarz@srh.de, reiner.creutzburg@srh.de

[3] ***The University of Texas at San Antonio, College of Engineering, 1 UTSA Circle, San Antonio, TX 78249-0669, USA***

Abstract

Open-source technologies (OSINT) are becoming increasingly popular with investigative and government agencies, intelligence services, media companies, and corporations [22].
These OSINT technologies use sophisticated techniques and special tools to analyze the continually growing sources of information efficiently [17].
There is a great need for professional training and further education in this field worldwide.
After having already presented the overall structure of a professional training concept in this field in a previous paper [25], this series of articles offers individual further training modules for the worldwide standard state-of-the-art OSINT tools.
The modules presented here are suitable for a professional training program and an OSINT course in a bachelor's or master's computer science or cybersecurity study at a university.
In part 1 of a series of 4 articles, the OSINT tool RiskIQ PassivTotal [26] is introduced, and its application possibilities are explained using concrete examples. In part 2 the OSINT tool Censys is explained [27]. This part 3 deals with Maltego [28] and Part 4 compares the 3 different tools of Part 1-3 [29].

Introduction and Motivation

Accompanying theory

MALTEGO uses the idea of transformations to automate the process of querying different data sources. This information is then displayed in a node-based graph suitable for performing connection analysis.
There are currently three versions of the MALTEGO client, namely MALTEGO CE, MALTEGO Classic and MALTEGO XL. All three MALTEGO versions will have access to a library of standard transformations for the discovery of data from a variety of public sources commonly used in online research and digital forensics [20].

For this exercise, MALTEGO CE is used.

MALTEGO CE is the community version of MALTEGO, which is available free of charge after quick online registration. MALTEGO CE contains most of the same features as the commercial version but has some limitations. The community version's main limitation is that the application cannot be used for commercial purposes, and there is also a limit on the maximum number of units that can be returned from a single transformation. In the community version of MALTEGO, there is no graphics export functionality available in the commercial versions.

MALTEGO can be used to determine the relationships between the following units:

- human,
- name,
- email addresses,
- aliases,
- groups of people (social networks),
- company,
- Websites.

and Internet infrastructures such as:

- domains,
- DNA name,
- network block,
- IP addresses,
- connections,
- documents and files.

Links between this information are found using open source intelligence techniques (OSINT) by querying sources such as DNS records, whois records, search engines, social networks, various online APIs, and metadata extraction.

MALTEGO provides results in various graphical layouts that allow information to be aggregated and relationships to be immediately and accurately visible. Even hidden connections can be detected, even if they are three or four degrees apart [20].

For the analyses in this exercise, MALTEGO-CE is used. It offers the following features:

- link analysis for up to 10,000 objects in a single diagram,
- is possible to return up to 12 units per executed transformation,
- collection node that automatically groups entities with common characteristics and finds the key relationships searched for,
- possibility of sharing charts in real-time and with multiple analysts in a single session,
- options for exporting graphics like:
  - GraphML,
  - entity lists.
- options for importing graphics like:
  - table formats - csv, xlx and xlsx,
  - copy and paste.

This information is then displayed in a node-based graph. Such a visual representation is best suited for link analysis. Real relationships (e.g., computer networks or social networks) between people, websites, domains, and other **objects** can be analyzed.

Concept of MALTEGO

The concept of MALTEGO consists of a combination of entities, transformations, and machines. **Entities** are real objects, such as a person, DNS name, phone number, email address. A **entity** is visually represented as a node on the graph. The MALTEGO client (Classic/XL) contains approximately 20 entities, specifically for online investigations. However, one can also create own entities.

Transformations represent relationships between the entities. This is done by querying a data source and returning the results as a new **entity** on their graphs. The sources of the data are places like DNS servers, search engines, social networks, whois information, own databases, etc.

Machines assemble transformations using a script to automate tasks intelligently. They then either run entirely on their own or wait at predefined points for interaction with the user.

Creation of a Graph

To create a new graph in MALTEGO, click on the Maltego icon in the upper left corner of the application and then on the icon below with the green (+) (Fig. 1).

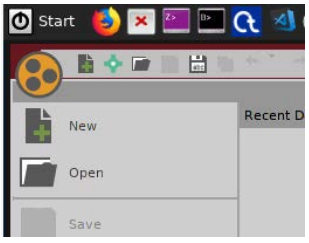


Figure 1. *Locate the submenu to create a new graph [31]*

This opens a window for a new graph.

Entity Palette

Entities in MALTEGO are used to represent different types of information. They are represented as nodes in the diagram. All entities available in the MALTEGO client are found in the entity palette, which is located by default on the left side of the graph. The entities in the palette are divided into groups, with the main categories being **Infrastructure** and **Personal** (Fig. 2).

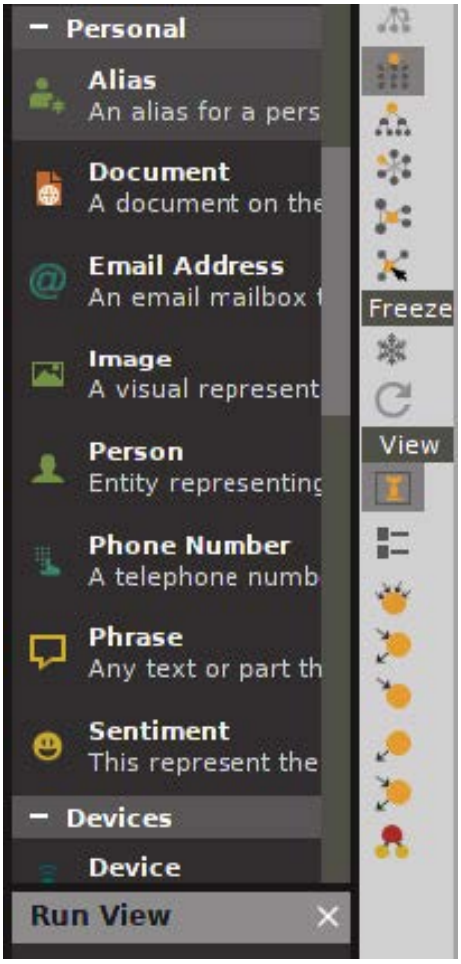


Figure 2. *Entity Palette [31]*

There are three aspects to an entity:

- **type** - type of information representing the entity
- **value** - Primary information field of the entity, always displayed in the diagram (Fig. 3):
- **properties** - Additional information fields for the entity

Adding an Entity to the Graph

To add a new entity to the diagram, click and hold the desired entity and drag it to the diagram area as shown in Fig. 4:

Figure 3. *Example of an Entity value [31]*

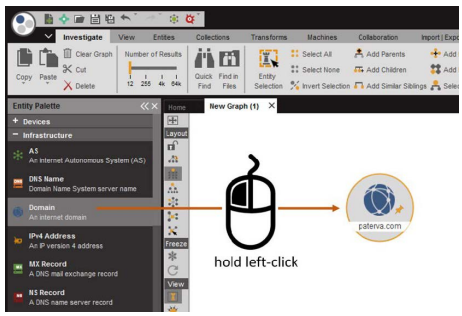


Figure 4. *Action to add an entity to the graph [31]*

Once an element has been dragged into the graph, it becomes one of the graph's nodes.

Editing an Entity Value

By double-clicking on the entity's text, it becomes possible to edit the value of the entity (Fig. 5). The text is highlighted and can be edited so fast (Fig. 6):

Figure 5. *Action for editing an entity value [31]*

Figure 6. *Edit an entity value [31]*

Selection of an Entity

By clicking with the left mouse button on the node, a selection circle appears around it (Fig. 7).

Selection of Multiple Entities

If several entities are to be selected, a block must be dragged with the mouse over the objects to be selected while the left mouse button is pressed (Fig. 8).

Figure 7. *Selection of an entity value [31]*

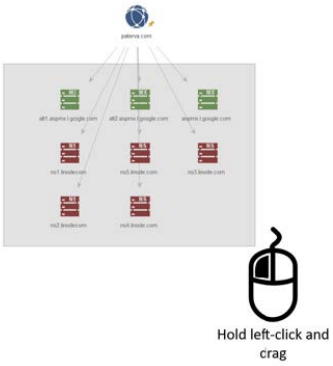


Figure 8. *Action to select multiple entities [31]*

After selection, the nodes are marked as shown in the figure below (Fig. 9).

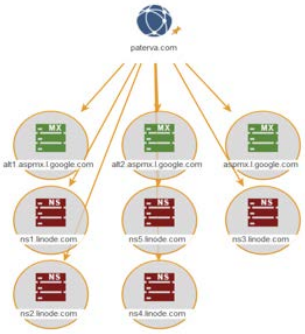


Figure 9. *Selection of multiple entities [31]*

Selecting Multiple Elements One After the Other

If one is working with multiple nodes but want to select only certain nodes, one uses **Shift+Leftclick** (Fig. 10). This adds individual nodes to the selection.

Entity Details

The full entity detail window opens with a double click on

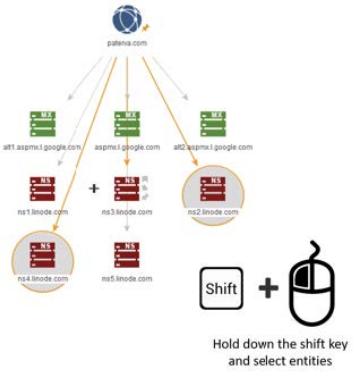


Figure 10. *Action to select several elements one after another [31]*

the entity icon next to the entity's value. The entity detail window contains four separate tabs that are described below:

Summary

The **Summary** tab appears first when the Entity Details window is opened. The tab contains a summary of all the entity information that can be found in more detail in the following tabs in the Entity window.

The following image shows a domain entity (Fig. 11). Thumbnails for all attachments of entities are also displayed at the bottom of the summary window. There is also a large text area where notes can be added or edited.

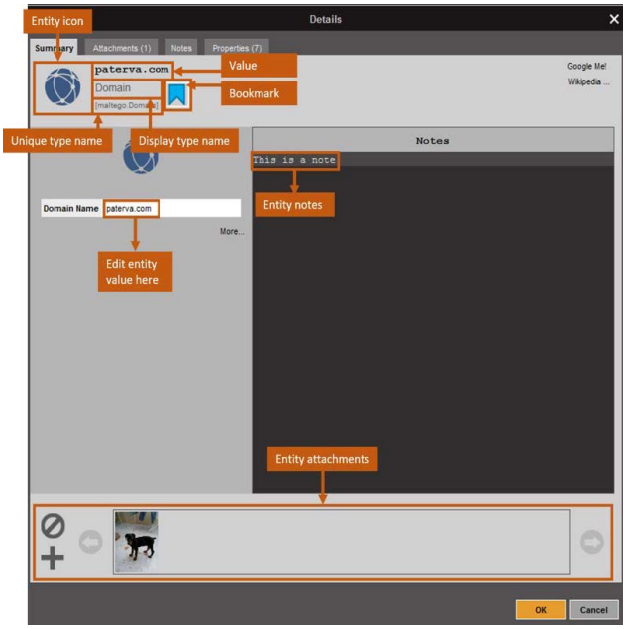


Figure 11. *Summary page of a domain entity [31]*

Attachments

On the **Attachments** tab page (Attachments) a list of all file attachments for the entity can be viewed, if available (Fig. 12).

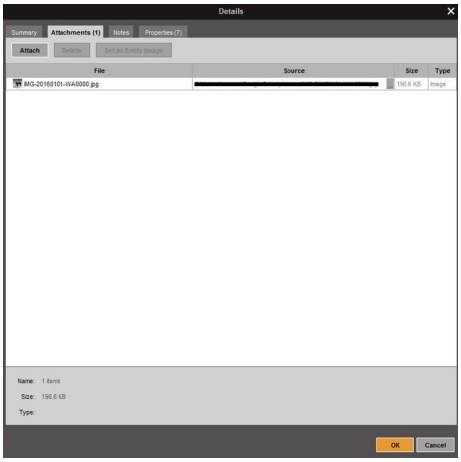


Figure 12. *Attachments Tab [31]*

New file attachments can be added by clicking the **Attach** button. A dialog opens where you can select a local file or specify a URL to a file retrieved by the MALTEGO client (Fig. 13). File

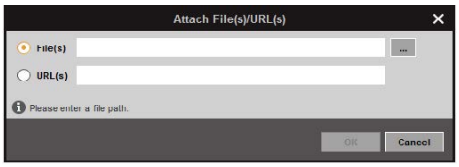


Figure 13. *Dialog for adding file attachments [31]*

attachments can also be added to an entity by dragging and dropping them from the file manager onto an entity in the diagram.

In a MALTEGO diagram, file attachments of an entity are displayed with a pin symbol visible on the left side of the entity symbol, as shown in the figure below (Fig. 14):

Figure 14. *File attachments of an entity [31]*

Notes

The tab **Notes** (Notes) contains a large text area in which a note for an object can be added or changed (Fig. 15).

In a MALTEGO diagram, entities with notes can be identified by the yellow note symbol on the right side of the entity symbol, as shown below. Double-clicking the icon displays the note in

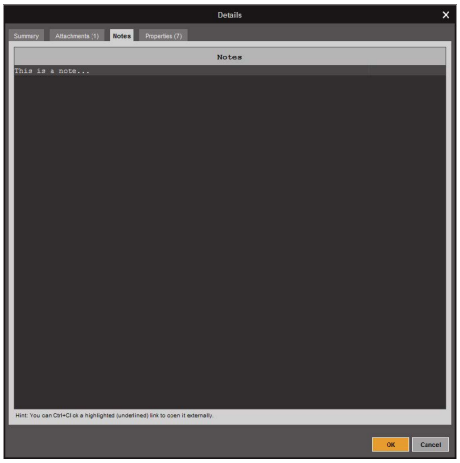


Figure 15. *Notes tab [31]*

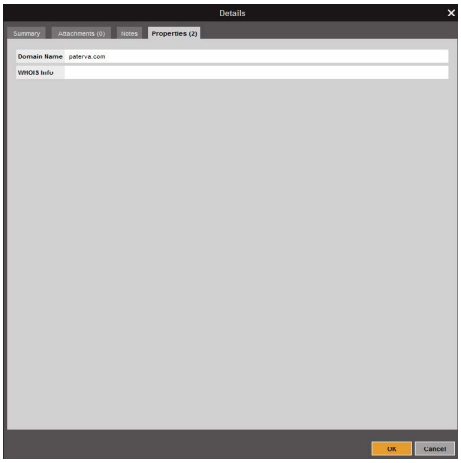


Figure 17. *Properties tab [31]*

a dialog box on the chart, as shown below. This dialog can be closed again by clicking the **X** in the upper right corner of the dialog box (Fig. 16).

Figure 16. *Attaching a note to an entity [31]*

Properties

The tab **Properties** (Properties) in the entity window **Details** displays a list of key-value pairs for the various properties the entity contains. The values for the properties of an entity can also be edited in this window (Fig. 17).

Context Menu

The context menu allows performing the transformation for the selected objects in a diagram. Right-clicking on an entity (or group of entities) displays a context menu. The context menu is divided into three different levels, the **Top-Level**, the **Set-Level** and the **Transform-Level**, each of which is explained in the following subsections.

Top-Level

The top level of the context menu lists the various transform hub items that are currently installed (Fig. 18). By default, only the PATERVA CTAS Transform Hub element from the Transform Hub is installed on the MALTEGO client. If MALTEGO has only one Transform Hub entry installed, the context menu will open at the set level, as there is only one entry to choose from at the top level.

Set Level

A left-click on a transform hub element leads to the set level. In MALTEGO, sets are used to group transformations into categories that perform similar tasks and/or are often performed together.

The following figure shows the different sets available for a domain entity and located in the PATERVA CTAS Transform Hub Item (Fig. 19). A left-click on the sidebar to the left of the context menu will navigate the user one level up again (in this case, back to the transform hub level). If one right-clicks anywhere in the context menu, it will also navigate one level up. Each set also has a Configuration button that, when pressed, opens the Set Configuration window to configure the transformations contained in the set.

Transform Level

The transform level of the context menu is the place from which transformations are executed. If one clicks with the left mouse button on a single transformation, it will be executed. Alternatively, one can click with the left mouse button on the single arrow symbol (>) on the right side of the context menu.

Clicking on the configuration icon in the transform line opens the transform manager with the correct transformation (Fig. 20). The Transform Manager displays more information about the transformation and allows one to configure the settings - it will be explained in later sections.

Clicking on the star symbol in a transform line adds the transformation to the favorites, which are always listed at the top of the context menu as a separate category, regardless of which level of the context menu you are on (Fig. 21).

It is important to note that the context menu is entity-

Figure 18. *Top level of the context menu [31]*

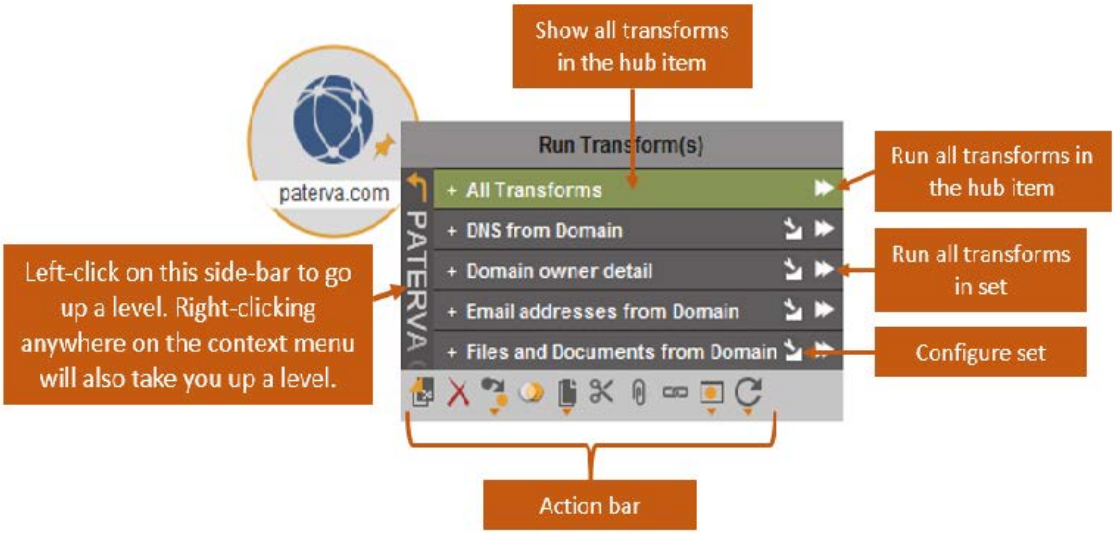


Figure 19. *Available sets of a domain entity [31]*

specific, i.e., the elements displayed in the context menu refer to the selected entity type's transformations.

Action Bar

The action bar, located at the bottom of the context menu, allows one to perform a series of actions for the graph's selected part. The ten actions from the action bar are labeled in the image below and are described in more detail below (Fig. reffig:Malt41).

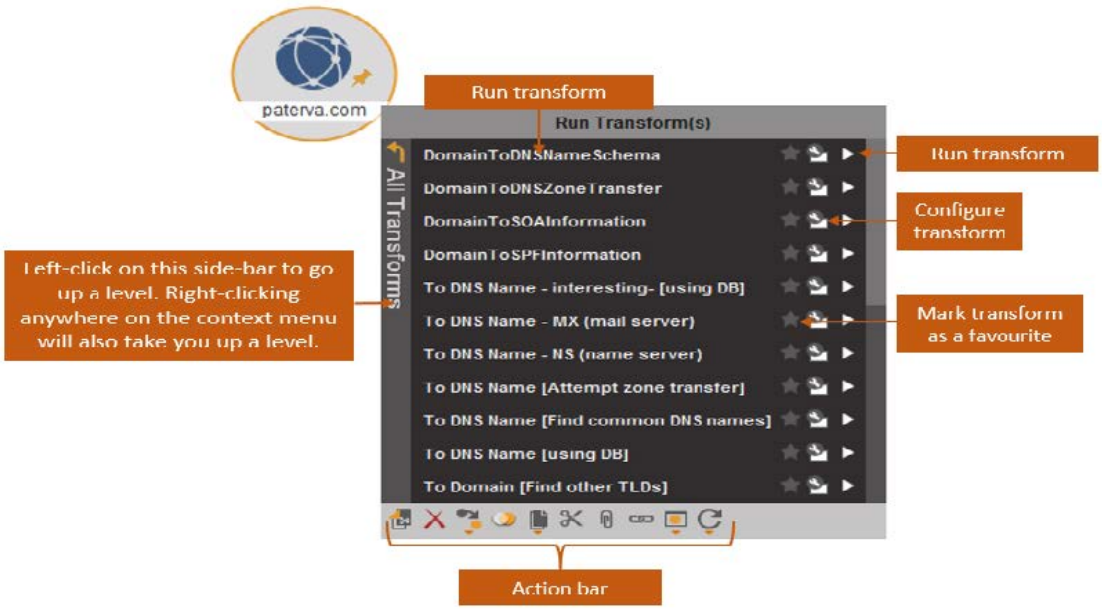


Figure 20. *Possibilities of the Transform Manager [31]*

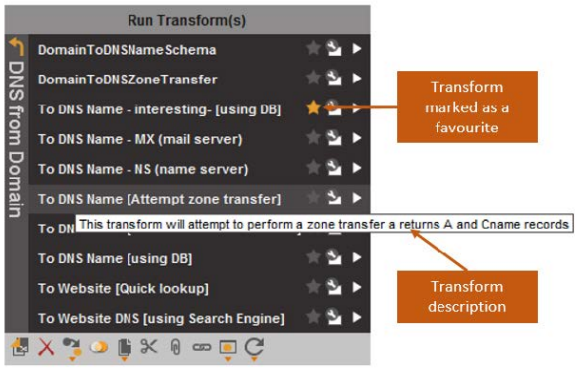


Figure 21. *Favouring a Transformation [31]*

1. **Copy to New Graph** - Copies the current selection to a new graph.
2. **Delete Entities** - Deletes the selected objects. This can also be done using the Delete key on the keyboard.
3. **Change Entity Type** - Opens a drop-down menu containing all objects from the entity palette. If one selects an entity from the drop-down list, all selected entities will be converted to this type (Fig. 23).

4. **Merge Entities** - Creates a single entity with properties from all merged entities. Clicking on the merge action opens a window in which a primary entity can be selected for merging. The primary unit takes precedence over the other units, and its entity type is used for the newly merged unit. The following image shows the merge window for three units to merge: a person, an alias, and a Twitter membership (Fig. 24).

   Combining these three units, which makes Twitter membership the primary unit, leads to the following picture (Fig. 25). Note that the properties of the other two entities are now in the dynamic properties of the merged entity:

5. **Copy in Different Formats** - Copy the graphic selection to different formats (Fig. 26). Each format is described below:

   - **Copy (as GraphML)** - copies the graph to the system clipboard as an XML-based graphics format. This format contains information about the entities and their connections.
   - **Copy (as 'value' list')** - Copies a list of objects currently selected in the graph. The list contains only the entity's value and no information about the connections between the entities in the diagram.
   - **Copy (as 'type#value' list**) - Copies a list of objects currently selected on the diagram and the entity type. Each element in the list has the format**'type#value'**. The list contains no information about the connections between the elements in the diagram.
   - **Copy (as'type#value#weight' list)** - Copies a list of the entities currently selected on the graph, as well as the entity type and weighting. Each element in the list has the format **'type#value#weight'**. The list contains no information about the connections between the elements in the diagram.

6. **Cut Entities** - Cuts out the entity selection and places put it

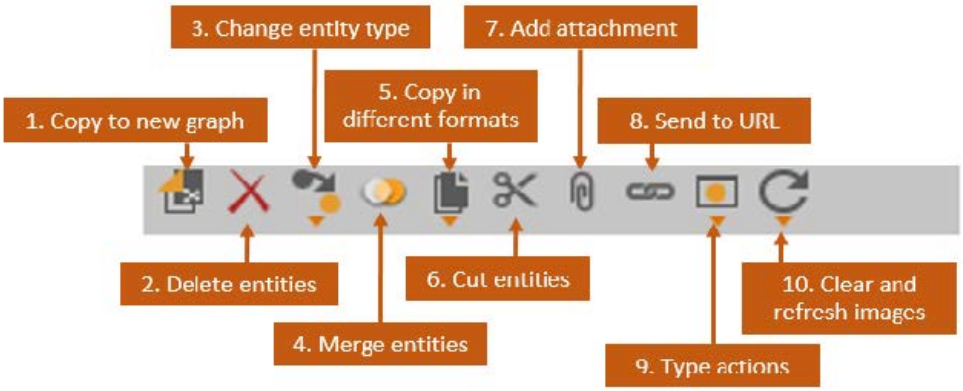


Figure 22. *Action bar [31]*

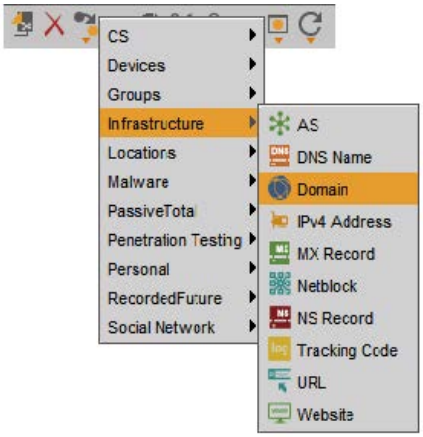


Figure 23. *Change entity type dropdown menu [31]*

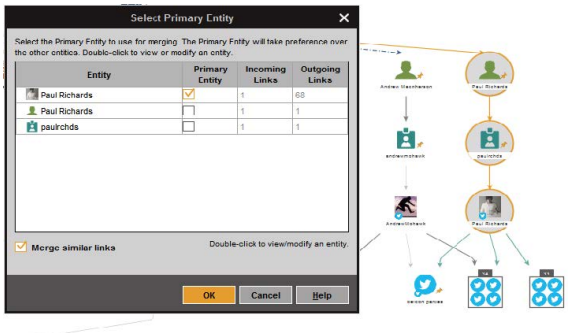


Figure 24. *Entity merge menu [31]*

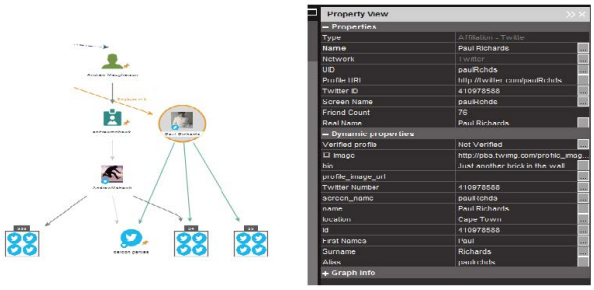


Figure 25. *Merging result [31]*

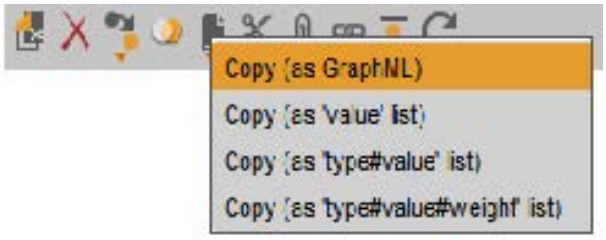


Figure 26. *Menu for copying the graphic selection into different formats [31]*

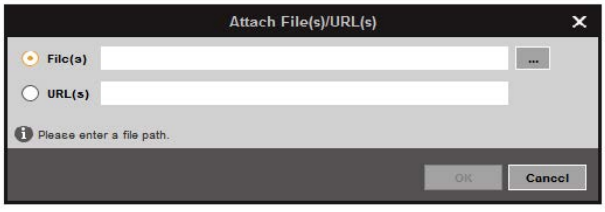


Figure 27. *Attaching files to an entity [31]*

on the clipboard.

7. **Add Attachment** - Attach files to the entity. Clicking this button opens a window where one can select the file to attach (Fig. 27):

8. **Send to URL** - Opens a **developer friendly** Function in MALTEGO. The function takes the selected segment of the graph and sends a hybrid GraphML/XML to a page that then returns a URL that Maltego opens in a browser.

9. **Type Actions** - Quick search in Google or Wikipedia for an entity value. When a type action is performed, the default

web browser is opened and the search is performed there.

10. **Clear and Refresh Images** - Retrieves all downloaded images in the diagram again.

Graph Options

Layout Sidebar

The layout sidebar is always located on the left side of the graphics window. It allows one to configure various view and layout options for MALTEGO graphics. The following figure shows an overview and explanation for each element in the layout sidebar (Fig. 28).

Graph Controls (1-3)

1. **Full Screen Mode -** Switches to full screen mode (alternatively **Alt**+**Enter**). Press the **Esc-** button to exit full screen mode.
2. **Lock Layout -** Locks all objects currently on the chart from moving. The new entities returned by transformations continue to be created.
3. **Full vs Incremental Layouts -** This option should be used during joint meetings if the personal chart layout is to be maintained.

Layouts (4-8)

The buttons 4 to 8 in the layout sidebar are used to define how the objects are to be arranged in the diagram. There are four standard layouts.

4. **Block Layout** - In this layout, nodes are represented according to the following rules:
   - in blocks of knots,
   - sorted by entity types,
   - sorted by entity weighting.

The weighting of the entities represents the relevance of entities [23]. For example, entities returned by one of the search engine transformations are weighted according to how relevant they are (their page rank). The following figure shows an example of a block layout (Fig. 29).

5. **Hierarchical Layout** - In hierarchical layouts, entities are grouped by layers that are stacked on top of each other (Fig. 30).

6. **Circular Layout** - nodes that are most central to the diagram (e.g., most links) appear in the center of circles, while the other nodes are distributed around them (Fig. 31).

7. **Organic Layout** - In an organic layout, the nodes are packed so tightly that the distance between each entity and all other entities is minimized. The closer the entities are to each other, the more interconnected they are (Fig. 32).

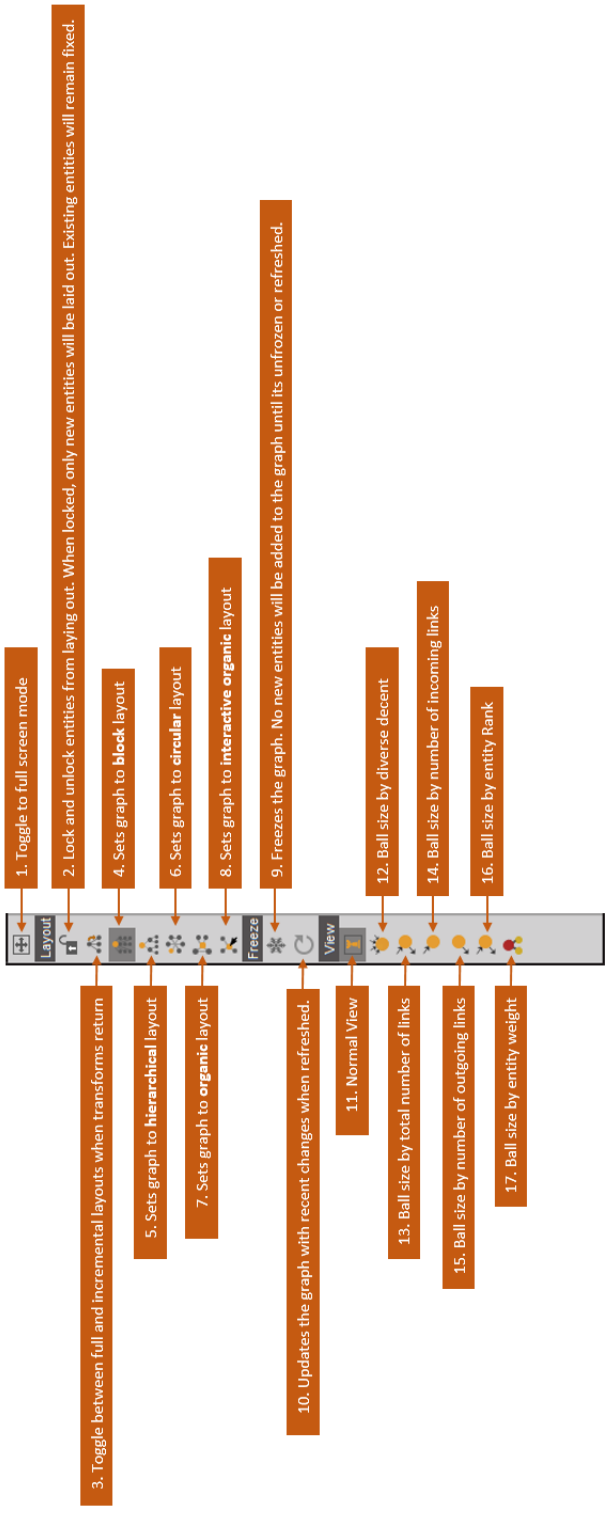


Figure 28. *Layout sidebar overview [31]*

8. **Interactive Organic Layout** - This layout is similar to the organic layout. The elements are positioned as they are con-

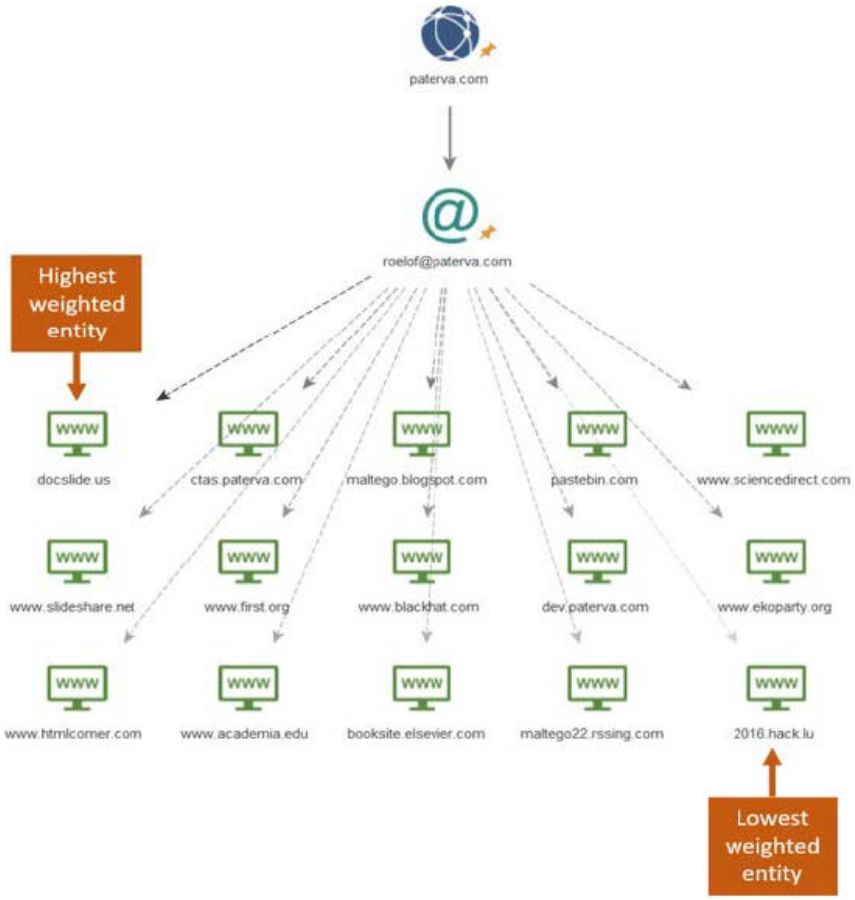


Figure 29. *Block layout [31]*

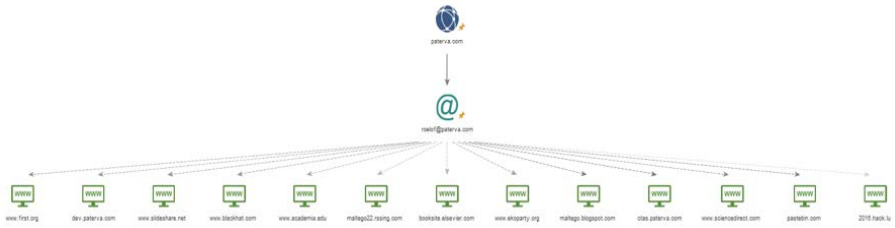


Figure 30. *Hierarchical layout [31]*

nected to the rest of the graphic. The two differences in interactive organic layouts are:

- When new elements are returned to the graph, only elements closely associated with the returned elements are moved, rather than recreating the entire graph layout each time. For this reason, inserting a graph into an interactive organic layout will improve performance with larger graphs because fewer layout calculations are required.
- The units are not as close together as in the organic layout.

The following graphic shows the same graphic as above, but in an interactive organic layout. It can be seen that the units are less densely packed (Fig. 33).

Freezing and Updating the Graphic (9-10)

9. **Freezing the Graph** - The Freezing key is used when there are many nodes in the graph (e.g., if many transformations are performed on many nodes) and the layout should not be constantly updated. By delaying the layout, the application can process transformations faster because it does not have to update the display after each transformation. To unfreeze the graphic, simply press the same key, and the graphic will

Figure 31. *Circular layout [31]*

Figure 32. *Organic layout [31]*

continue as usual [24].

10. **Update Graph** - Allows you to update the graph layout manually.

Views (11-18)

The next section in the layout sidebar is under **View**. Views can be used to determine the size and color of objects based on various properties of the diagram. It is possible to write one's views, but this goes beyond this exercise's scope. The seven views provided with MALTEGO out-of-the-box size units correspond to different properties.

11. **Normal View** - If you zoom close to objects, the entity icon is displayed in the diagram. When zooming into the Legend view, each element is represented by a sphere of equal size with a color corresponding to the entity type. This view is the default view when a new diagram is started.

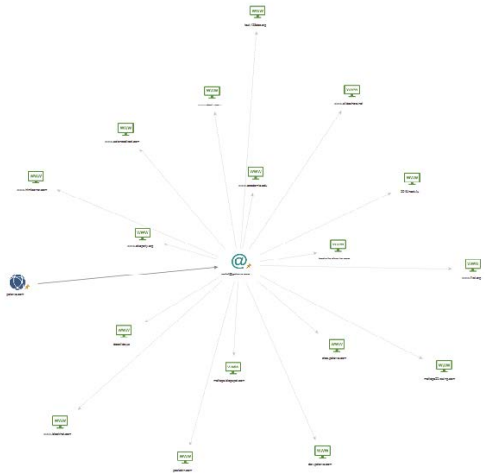


Figure 33. *Interactive organic layout [31]*

12. **Diverse Decent -** Entities are dimensioned according to the number of incoming links that the entity has. However, incoming links with different **grandparents** are weighted higher (Fig. 34).

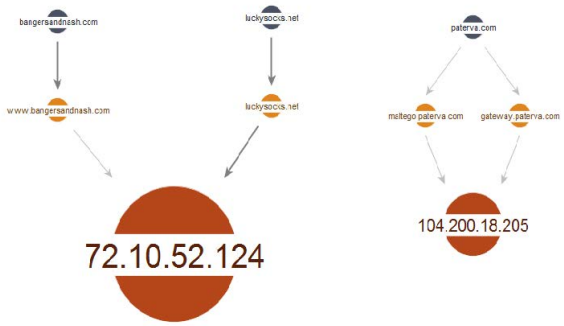


Figure 34. *Various decent - view [31]*

In the picture above (Fig. 34), the IP address units are different in size, although they both have two incoming links. This is because the IP address on the left has two incoming links coming from two different sources, while the IP address on the right has two incoming links both coming from the same source. There are many cases where this view is useful. In this case, IP addresses associated with different domains are pointed out.

13. **Ball Size Through All Links** - The entities' size depends on the total number of links (incoming and outgoing). The more links an object has, the larger it is shown in the diagram (Fig. 35).
14. **Ball Size by Incoming Links** - The units' size depends on the total number of incoming links. The more incoming

links an object has, the larger the diagram (Fig. 35).

15. **Ball Size by Outbound Links** - The size of the units depends on the total number of outbound links. The more outbound links an entity has, the larger it is in the diagram (Fig. 35).
16. **Ball Size Rank** - This size is based on the own number of links and the sum of the neighbor's links (Fig. 35).
17. **Ball Size by Weight** - This size is based on the weight of the objects. Some transformations (such as that of the search engine) return a weight field representing the entity's relevance. The following graph shows the results of a search engine transformation (Fig. 35).

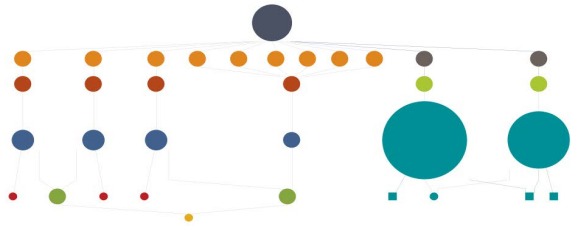


Figure 35. *Exemplary representation of the weighting of entities visualized by balls of different sizes [31]*

18. **List View** - The List view can be used as an alternative to the entity views above to display the graph information in a tabular layout. The List view behaves the same as an Entity View. The items selected in the List view are displayed in the Details view. The entity selection behavior and functionality are identical between the entity view and the list view. When switching from "entity selection" to "link selection", all graphic links are displayed in a list view instead of the entities (Fig. 36).

Multifunction Toolbar

Investigate Tab - The tab page **Investigate** (Examine) is open by default when you start a graphic in MALTEGO and offers numerous options for editing and navigating a graphic. The available options are grouped in logical groups (Fig. 37).

Clipboard

The Clipboard tool offers the following intuitive functionalities:

- Paste (to paste nodes that have been cut or copied),
- Delete all (deletes the entire contents of the diagram),
- Copy (to copy selected nodes),
- Cut (cut selected nodes),
- Delete (deletes selected nodes).

Transform Results

The transformation results slider is used to set the number of results returned when a transformation is performed (Fig. 38). The numbers to which the transform slider can be set differ between the different versions of the MALTEGO client as follows:

- MALTEGO CE 12,
- MALTEGO Classic 12, 50, 255, 10k,
- MALTEGO XL 12, 255, 4k, 64k, 64k.

Quick Find

The Quick Search option on the tab is a convenient tool to find something specific in a huge graph. A toolbar opens at the bottom of the diagram (the search toolbar can also be opened by clicking **Ctrl**+**F**)..

Find in Files

Find in Files does exactly what the title suggests, allowing one to search text in multiple MALTEGO graphics stored in a specific folder on your computer.

Entity Selection

The entity selection panel provides several options to manipulate the graph selection (Fig. 39).

- **Link vs. Entity Mode** - MALTEGO can be operated in two different modes. The Link Selection Mode or the Entity Selection Mode. The default mode is Entity Selection Mode. To switch between modes, press **Ctrl**+**M** or click on the mode selection icon at the top (this icon indicates the current mode) (Fig. 40).
- **Add Parents** - With this option (Fig. 41) you can add parents to a child node by using the key combination shown in Fig. 42.

- **Add Children** - Selects subnodes while retaining parents (Fig. 43).

- **Add Path** - Selects the nodes in the path between multiple nodes (this function is disabled unless multiple nodes are selected). An example best illustrates this. The following nodes are assumed to be selected (Fig. 44):

  In a complicated diagram like the one above, finding all the entities that connect the person and the email address would be quite challenging. Clicking the **Add Path** button will select all the elements that connect the two selected elements, as shown in Fig. 45. The detail view shows all selected objects.
  Copying the selection into a new diagram shows how that person and email address are connected (Fig. 46):

View Tab

On the **View** tab in the MALTEGO client, settings can be configured to view the graph (Fig. 47). The different views are listed above.

Entities Tab

On the **Entities** tab you can manage entities that are available in the MALTEGO client. New entities can be added, and own entities can be created (Fig. 48).

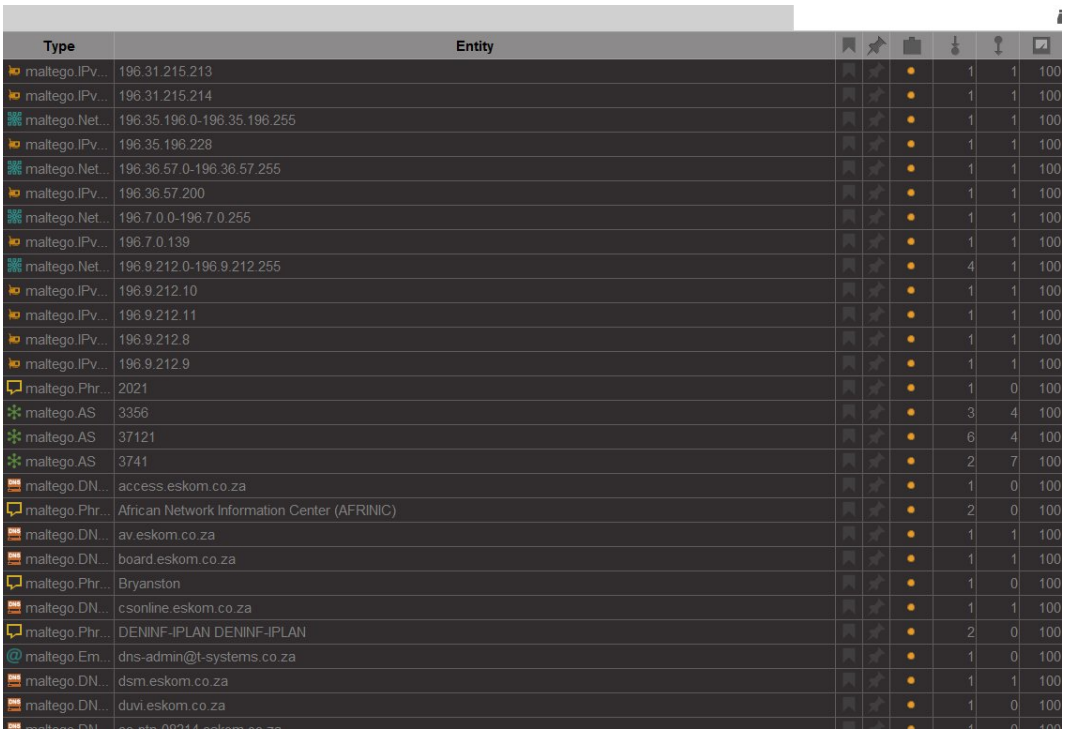


Figure 36. *List view [31]*

Figure 37. *Investigate tab of the multifunction toolbar [31]*

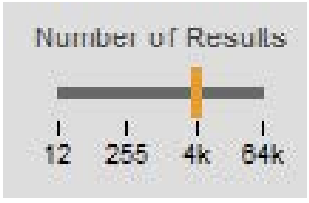


Figure 38. *Slider for the transformation results [31]*

Create New Entities

The first button under the Entities area allows one to create a new entity type. To do this, click the drop-down menu. This will open a submenu that offers the creation of two different entity types (Fig. 49):

The entity type (Advanced) provides more options when creating a new entity. When set to **New Entity Type** (Advanced) is clicked, a wizard opens that guides you through the process of creating a new custom entity. The first step of the New Item Wizard is shown in (Fig. 49):

- **Display Name -** This is the entity's name in the entity palette.
- **Short Description -** This field should display the entity in an Describe sentence. This description is also used in the entity palette is displayed.
- **Unique Type Name -** This is a unique identifier for the new entity and must be unique. Unique type names are defined with the Alias of the creator prefixed. For example, all entities have, delivered with MALTEGO have a unique type name preceded by MALTEGO.
- **Inheritance -** In the MALTEGO inheritance, transformations can inherit from a basic entity. If the new user-defined entity inherits from another (the parent) entity, all transformations executed on the parent entity will also be executed on the new entity.
- **Icons -** For the new entity type, an entity icon must be selected. The MALTEGO client has standard entity icons, from which can be selected. More symbols can also be added to **Manage Icons**.

Figure 39. *Panel for entity selection [31]*

Figure 40. *Link vs. Entity mode [31]*

Figure 41. *Add Parents - menu [31]*

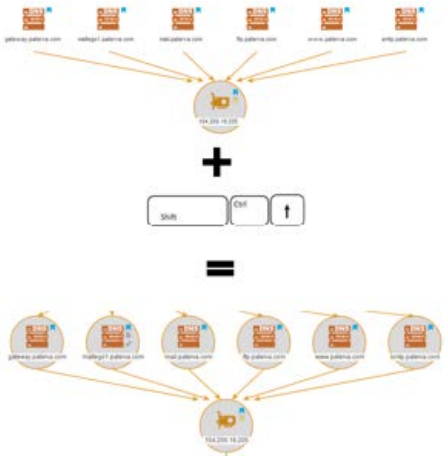


Figure 42. *Key combination for the option Add Parents [31]*

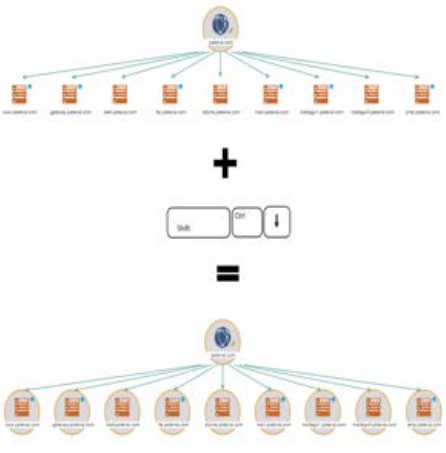


Figure 43. *Key combination for the Add Children option [31]*

An example input shows Fig. 51. Here a new entity ”Police Officer” is created as an example. The example input contains some important details and should therefore be considered carefully. After clicking **Next**, the main properties for the new entity can be configured (Fig. 52).

The main properties (also called entity value) are the entity’s properties to be represented in the diagram. For our example ”Police Officer” the data type ”string” is selected.

- **Property Display Name -** This is the name of the property specified in is displayed in the properties view (e.g. ”Police Officer”).
- **Short Description -** This enables a description of the Property in a record (for example, ”The Police Officers name”).
- **Unique Property Name -** This name identifies this property. and should not be reused (e.g. ”properties.policeofficer”).
- **Data Type -** Here you can specify the type of information, that represents the property. When selecting the data type, the following can be selected are between: string, date, integer or double (e.g. ”string”).
- **Sample Value -** The Sample value is the default value for this Entity type when a new entity of this type is created (for example, ”Paul Richards”).

Once these fields are filled in, click **Next** to proceed to the next step of the wizard. In the next step, one can select the category under which the new entity type should be located (Fig. 53):

The category **Personal** is selected for the new unit ”Police Officer”. Clicking on **Next** takes you to the assistant’s **Additional Properties** section.

Properties for an entity describe the additional fields that an entity contains. Many entities contain only a single field, such as a DNS name, and for most entities, it is sufficient to create a single field.

In the **Additional Properties** step, as the name implies, additional properties can be added to the entity to represent information that is often found with the new entity type (Fig. 54). At this stage, it is essential to consider whether new properties should be added to the entity type or whether an entirely new entity type should be created from it.

By default, the property that is the leading property (entity value) is filled in; this was set at the beginning of the process.

To add new properties, click the **Add property...** button in the upper left corner of the wizard window. This opens a new window in which the new property can be configured. In this

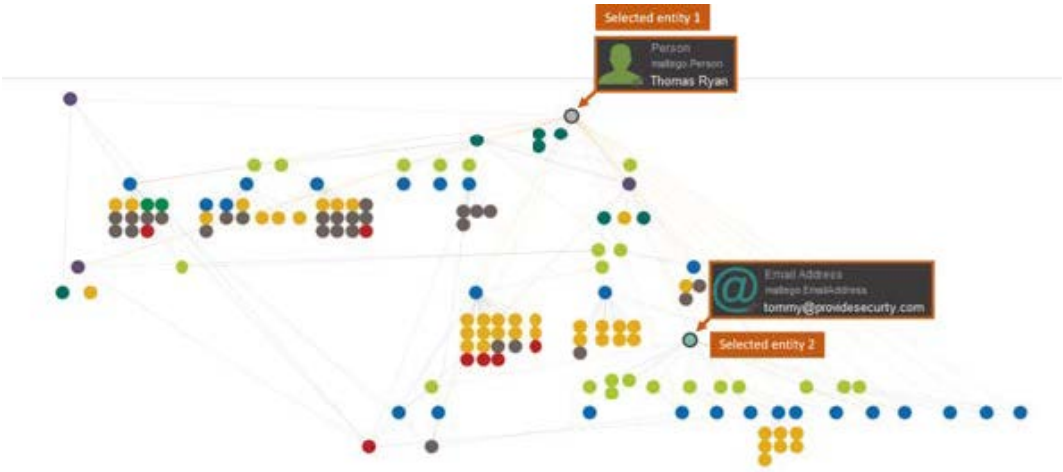


Figure 44. *Add Path – Selection of two nodes [31]*

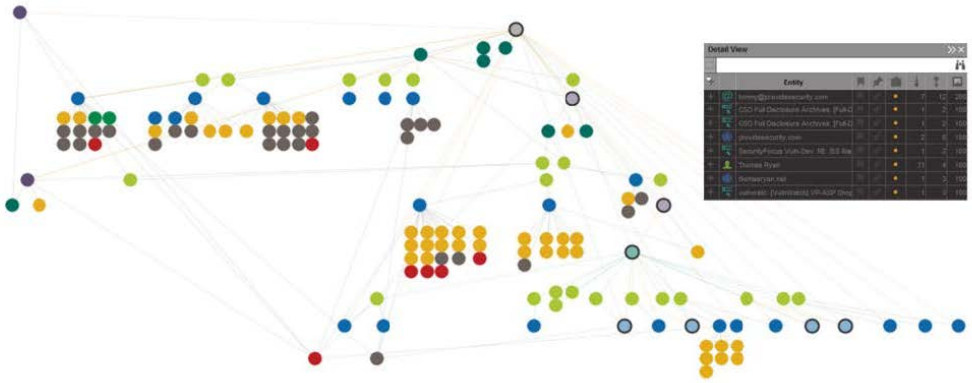


Figure 45. *Add Path – Detail view [31]*

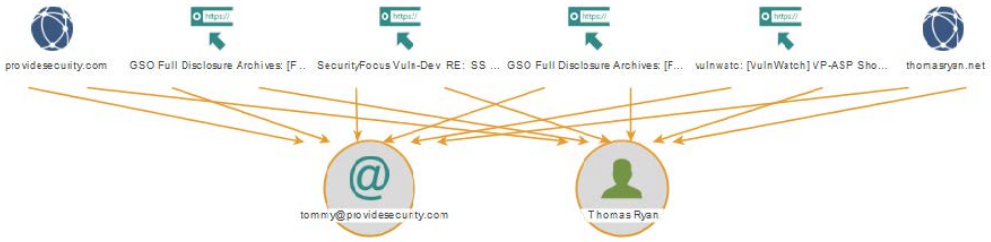


Figure 46. *Add Path – Result [31]*

case, a ”Badge number” is added for the new unit **Police Officer** (Fig. 55):

The following fields must be filled in for the new property (Fig. 56):

- **Name** - This name uniquely identifies the property (e.g. ”badgenumber”).
- **Display Name** - This is the name displayed in the MALTEGO usersurface in the property view (e.g. ”Badge Number”).
- **Type** - Here you can specify the data type the property

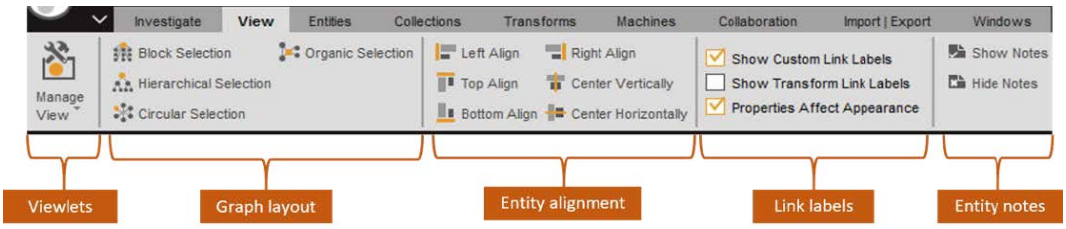


Figure 47. *View tab [31]*

Figure 48. *Entities tab [31]*

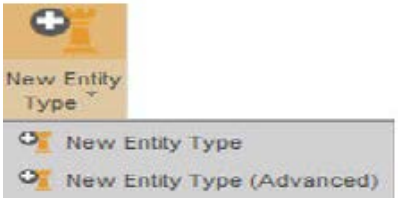


Figure 49. *Menu for creating new entities [31]*

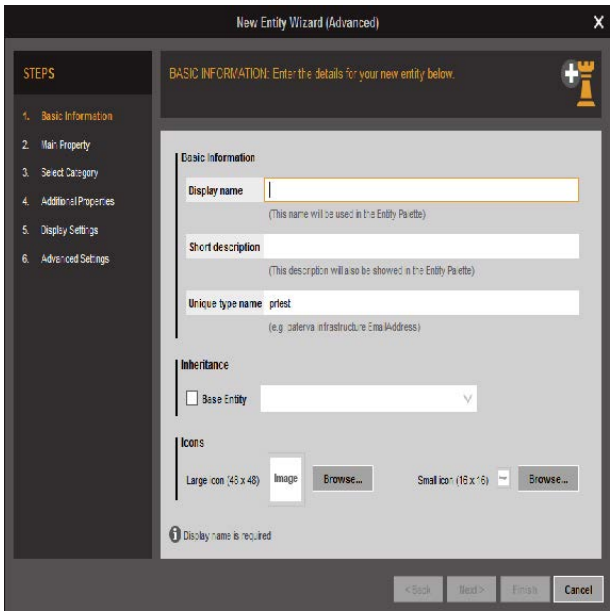


Figure 50. *Entity type creation wizard (advanced) [31]*

should represent. There are a number of data types that can be selected from the drop-down menu (e.g. ”string[]”).

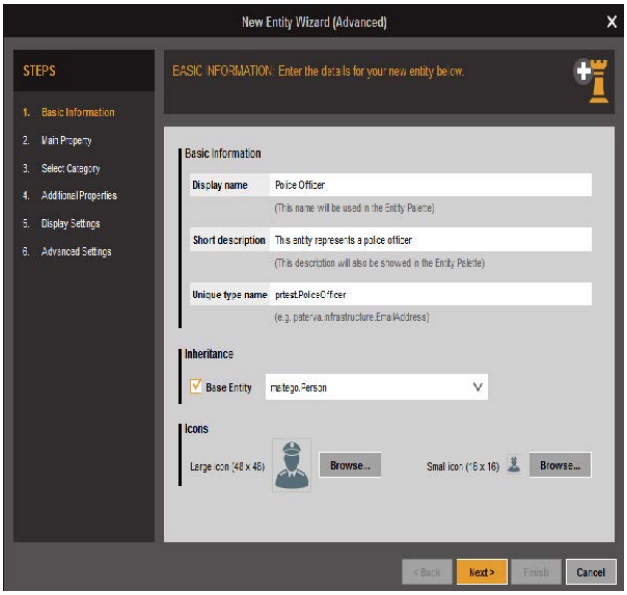


Figure 51. *Sample input for creating an entity [31]*

Once these three fields have been selected, click **OK** to add the new property to the entity.

- **Required** - If this entity type is added to the diagram, this property cannot be left blank.
- **Read Only** - If this option is enabled, the property can only be set by transformations, not by the user itself.
- **Description** - This field can be used to set a short description for the property.
- **Default Value** - This is the default value of the property.
- **Sample Value** - Corresponds to the property value when it is dragged from the entity palette to a graph.

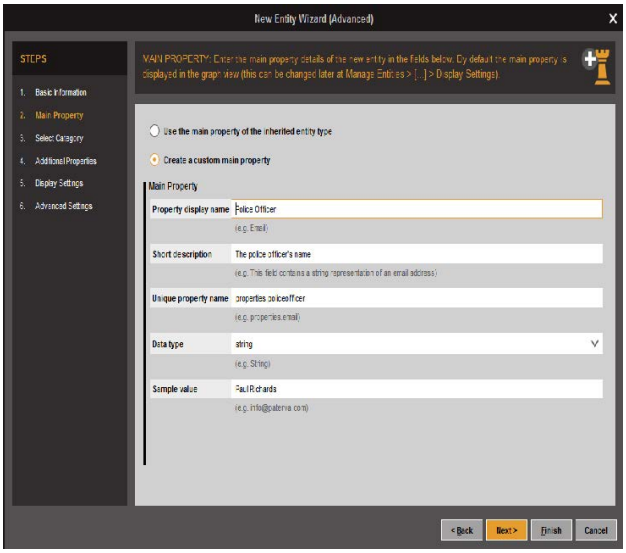


Figure 52. *Main features of the new entity [31]*

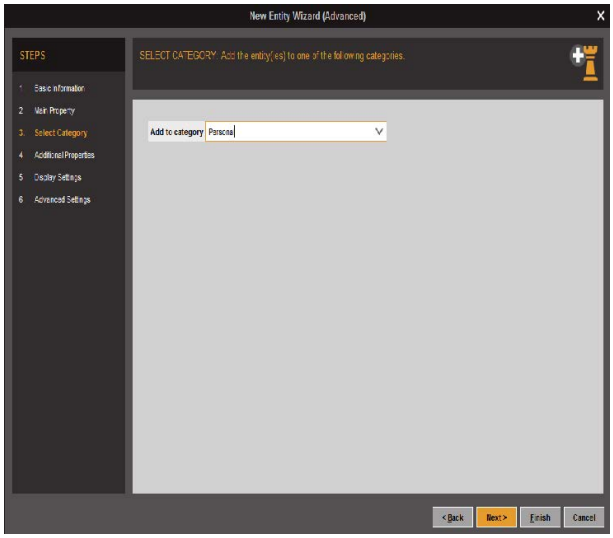


Figure 53. *Selection of the category of the new entity type [31]*

In the next step of the wizard, one can set the display settings for the new entity. Here one can also decide which property is displayed in the diagram (Fig. 57).

The display settings determine three different properties for an entity:

1. What is edited when changing the value in the diagram?
2. Which value is displayed in the diagram?
3. Which symbol should be used instead of the default symbol?

Although the actual URL of a page (which can be very long) is required, it is often undesirable for it to be displayed in full length in the diagram. Better would be something like the title of the page. This is where the display settings become essential.

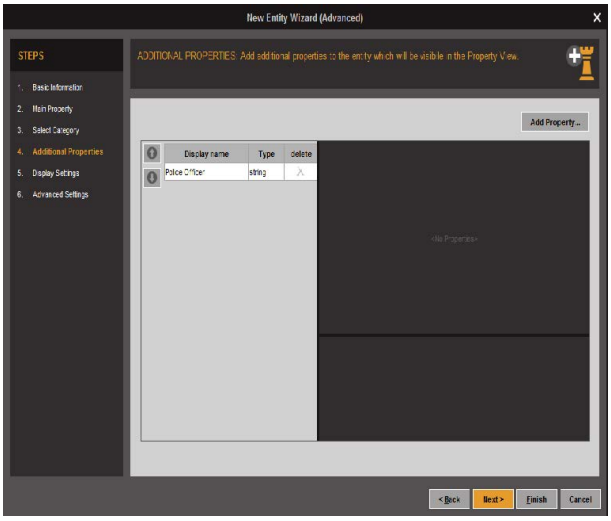


Figure 54. *Submenu - additional properties [31]*

Figure 55. *Menu for adding additional properties [31]*

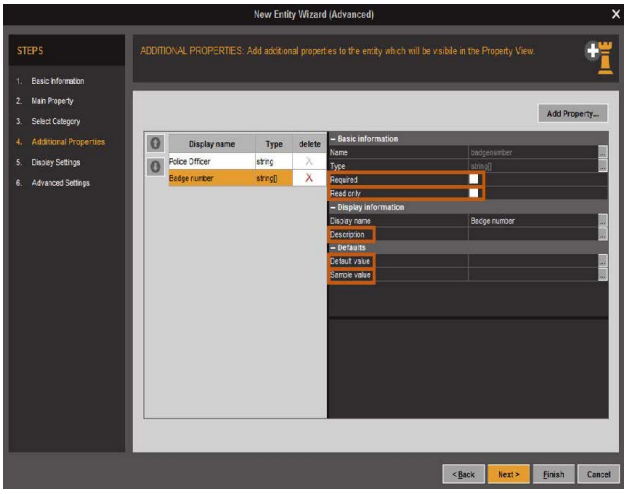


Figure 56. *Submenu for adding further properties [31]*

- **Edit Value** - This property determines which field is edited.
- **Display Value** - The property shown in the graph.
- **Large Image** - If a property is a URL to an image, this option can be used to replace the icon on the graph (useful for

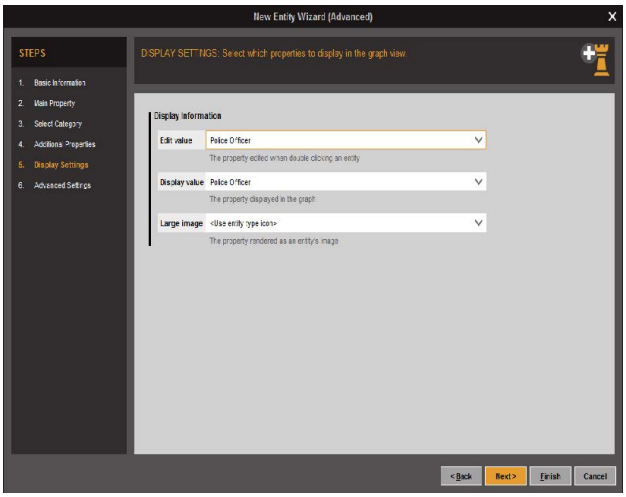


Figure 57. *Setting the display settings of an entity [31]*

displaying things like a thumbnail image of a Web site).

The last step in the wizard is the **Advanced Settings** page (Fig. 58).

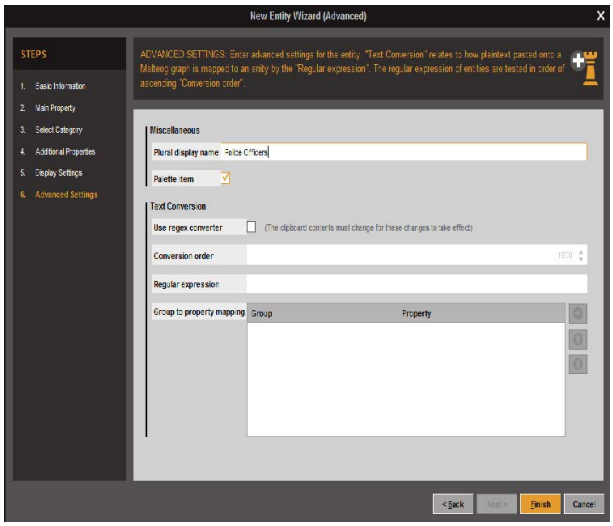


Figure 58. *Advanced settings [31]*

The following ranges can be specified on the **Advanced Settings** page:

- **Plural Display Name** - This allows you to set the plural options when multiple objects are described.
- **Palette Item** - This allows you to choose whether to display the new entity type in the entity palette. By default, this option is enabled. If one wants an entity type to return only one transformation and not be manually added to the graph, this field should be disabled.
- **Use Regex Converter** - This check box allows you to select whether to use a regular expression to identify an element automatically.
- **Conversion Order** - The priority given to this entity when inserting text corresponds to multiple regex expressions.
- **Regular Expression** - The Fig. 59 describes the regular expression used to match a domain entity. When this is inserted into the diagram, the tool compares the inserted text with the regular expression and automatically creates an entity of this type if it matches. The regular expression for a domain is as follows:
  [-\w]{1,120}\.[-\w]{1,4}\.*[-\w]{0,4}

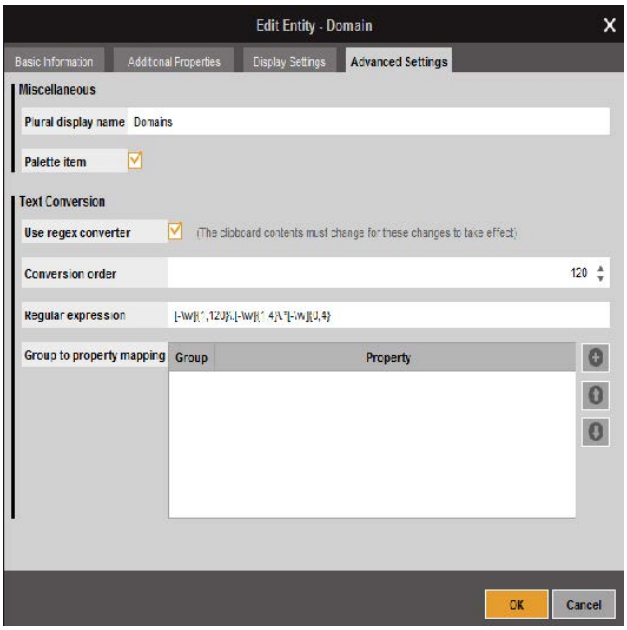


Figure 59. *Regular expression for matching with a domain entity [31]*

- **Group to Property Mapping** - In addition to the comparison, certain fields within the tool can also be filled in automatically. An example of this is the person entity, which automatically fills the first and last name fields of the entity when inserting something like **Andrew MacPherson** into the tool (Fig. 60). The regular expression for this is as follows:
  ([A-Z]{1,15}[a-z]{0,15}) ([A-Z]{0,15}[a-z]{0,15}*[A-Z]{0,15}[a-z]{0,15}*[A-Z]{0,15}[a-z]{0,15})

In the current example **Police Officer** both the regular expression and the fields **Group to property mapping** remain empty.

Once the Finish button has been clicked (Fig. 60), the wizard closes. The new entity type can be found in the entity palette under the category **Personal** (Fig. 61):

Entity Management

When the **Manage Entities** button is clicked (Fig. 62), the

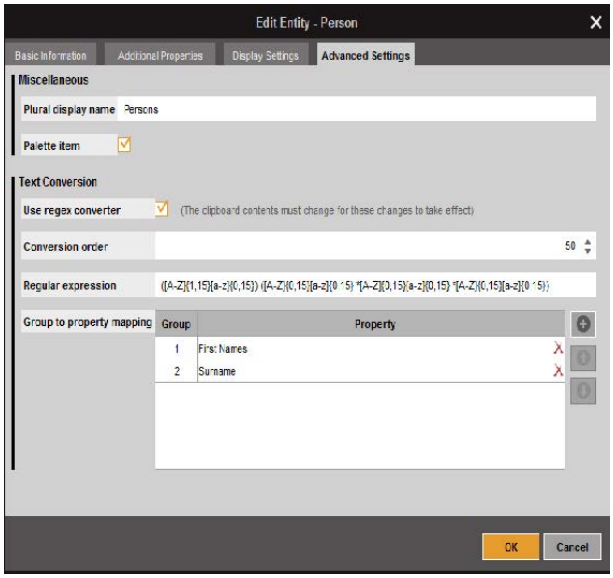


Figure 60. *Regular expression for comparison with a person entity [31]*

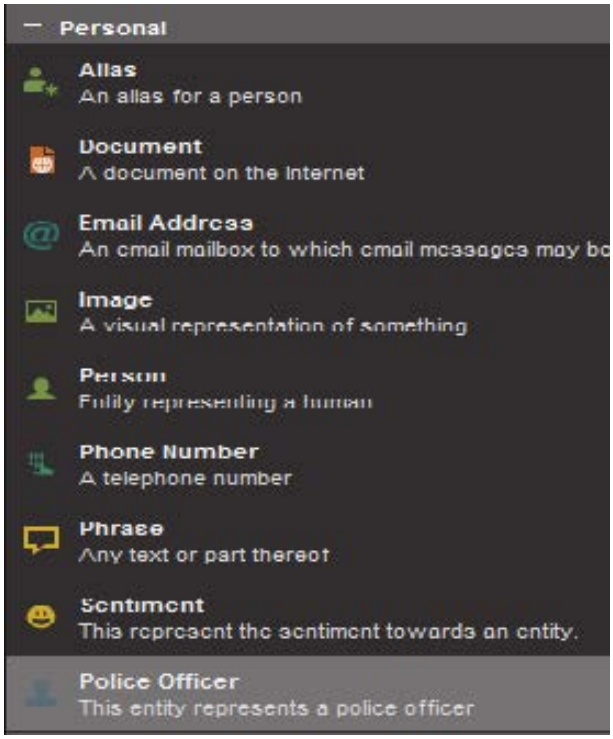


Figure 61. *Result of the addition of an entity [31]*

Entity Manager window (Fig. 63) opens and entities can be added or deleted.

Machines Tab

In MALTEGO, a machine is a script/macro that performs multiple transformations with different filter types. Machines are useful for performing common tasks, such as the forward

Figure 62. *Menu Entry - manage entities [31]*

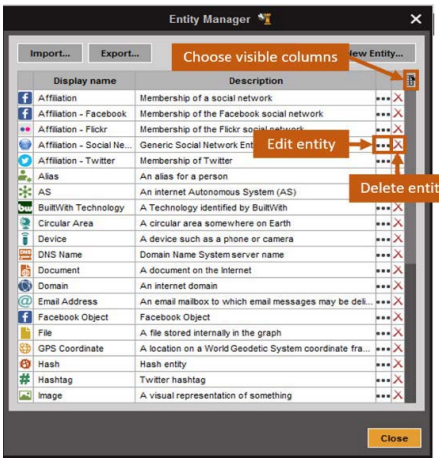


Figure 63. *Menu - manage entities [31]*

footprint of domains. The Fig. 64 shows the Machines tab.

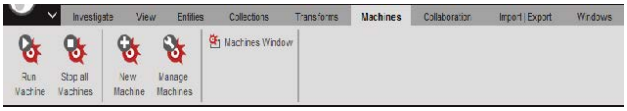


Figure 64. *Machines tab [31]*

MALTEGO has a custom scripting language that can be used to create new machines.

Running a Machine

Clicking on **Run Machine** (Fig. 65) opens the **Start a Machine** window, which can help start a first machine.

Figure 65. *Menu - run machine [31]*

The first step to starting a machine is to select the machine to run (Fig. 66). This can be done using the list of available machines in the MALTEGO client.

By default, the options **Show on startup** and **Show on**

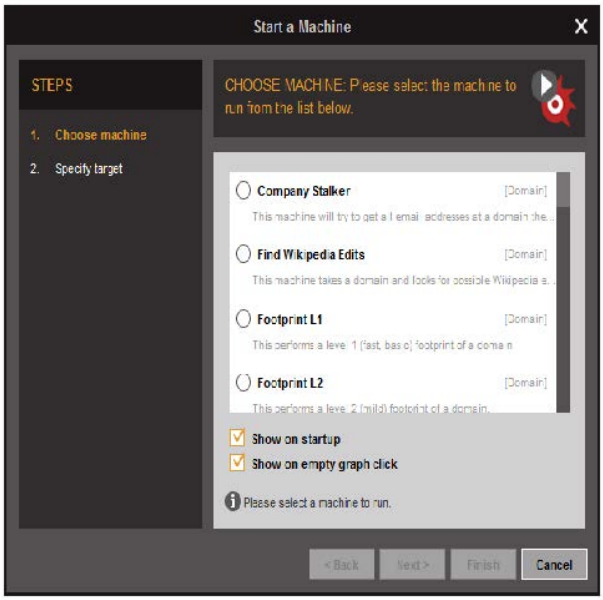


Figure 66. *Starting a machine - machine selection [31]*

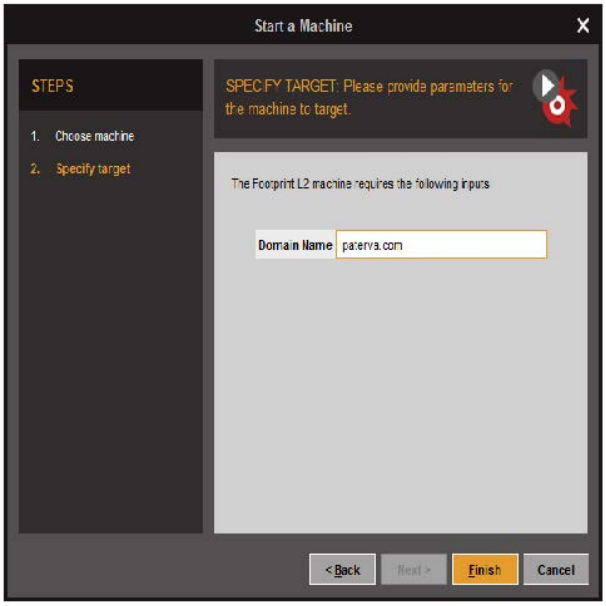


Figure 67. *Starting a machine - start parameters [31]*

empty graph click are enabled. This means that under these two conditions, the **Start a Machine** window opens automatically. This option can be disabled.

Clicking on **Next** takes you to the next page. Here you can enter the start parameter (Fig. 67).

Machines need a start parameter from which subsequent transformations can be executed. For example, the **Footprint L2 device** needs a target domain as an input unit.

If **Finish** is clicked, the machine is started at the specified destination. The **Machines** window opens containing details about the running machine's status, as described in the next section.

The following figure shows the labels for each function in the machine window (Fig. 68):

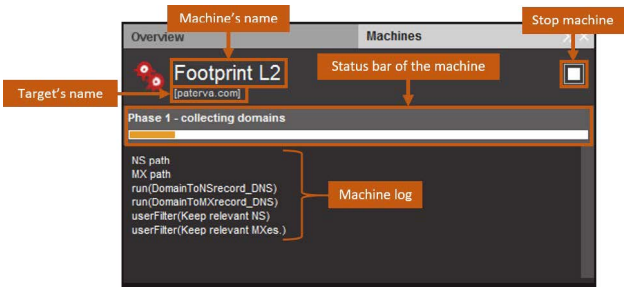


Figure 68. *Starting a Machine - summary [31]*

Machine User Filter

Some of the machines supplied with MALTEGO have a user filter that can select which objects to continue in the machine's pipeline. This is important because it generally allows one to specify what is relevant and what is not and prevents the machine from collecting information about irrelevant entities to the current investigation.

In the case of the **Footprint L2 machine** (Fig. 49), a user filter appears asking if the machine should search for additional domains that use the same MX and NS records as the target domain:

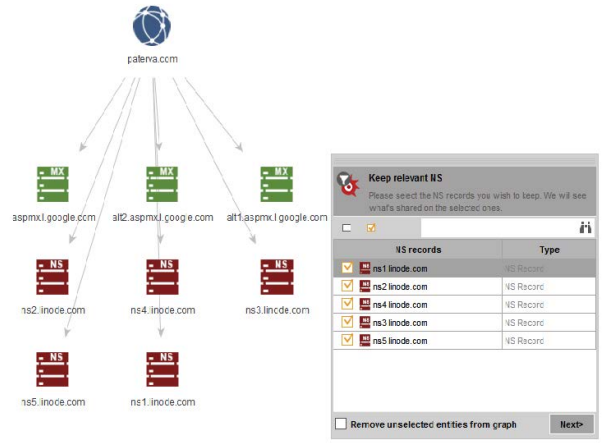


Figure 69. *Machine user filter [31]*

It seems that **paterva.com** uses Google for its MX records and Linode for its NS records. If one were to investigate **paterva.com**, one would not want the machine to search for domains that use these records, as it would provide thousands of independent results for companies and organizations that use Google for their mail servers and Linode for their name surcharges. In this case, one should uncheck these objects in the filter window, then click the **Next** button, and the machine will continue to run.

User Filter Window - In Detail

In the case of **Footprint L2**, after clicking **Next**, the device will pause again to display the User Filter window for the MX records of **paterva.com**, as shown in Fig. 70:

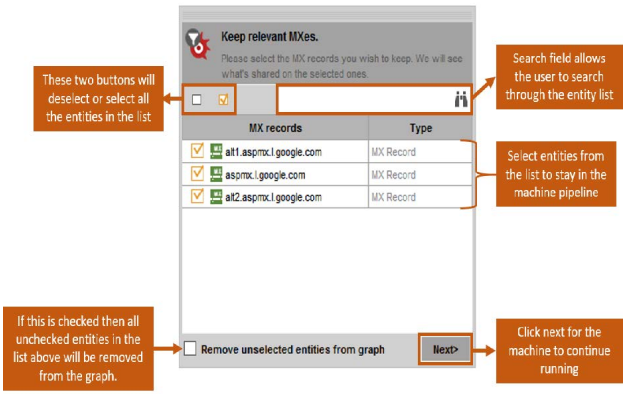


Figure 70. *User filter window - detail view [31]*

Once a selection has been made for each user filter, the machine continues all of its transformations except for the objects disabled in the user filter. When the machine is finished, the MALTEGO client beeps to indicate that the machine is complete.

In MALTEGO there is also something like a "eternal machine". A permanent machine can be configured to run every n second. This is useful for monitoring data that changes regularly. When a "perpetual machine" has stopped operating, a countdown timer appears in the Machines window that counts down until it is time for the machine to run again (Fig. 71).

Stop All Machines

Clicking the **Stop all machines** button (Fig. 72) will stop all machines currently running in the MALTEGO client. This is useful when multiple computers in the client are running on different tabs, and they all need to be stopped at once.

New Machine

Clicking the **New Machine** button (Fig. 73) opens the New Machine Wizard, which then guides you through the process of creating a new machine. The creation of a new machine is outside the scope of this document; more information on building special

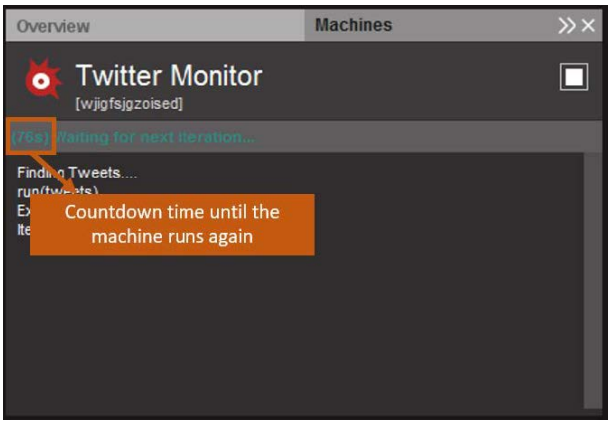


Figure 71. *Timer of a "perpetual machine" [31]*

Figure 72. *Menu entry - stop all machines [31]*

Figure 73. *Menu item - new machine [31]*

machines can be found in the developer portal of **paterva.com**.

Manage Machines

Figure 74. *Menu entry - manage machines [31]*

With a clich on **Manage Machines** (Fig. 74), the **Machine Manager** window opens, listing all machines currently in the MALTEGO client. The Fig. 75 shows the labels for all buttons in the machine manager:

The list in the Machine Manager can be sorted by the following fields:

- **Name** - The name of the system,
- **Status** - Readiness of the machine,
- **Author** - The person or company who built the machine,
- **Description** - A brief description of what the machine does,
- **Read-only** - If a machine is write-protected, the machine's script cannot be edited by the user. All machines installed from the transform hub are read-only and cannot be edited.

If one wants to edit one of the transformations installed by a transform hub element, one can clone the transformation and

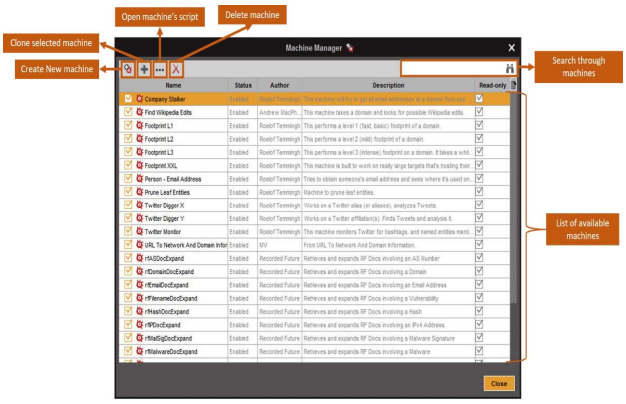


Figure 75. *Machine manager [31]*

then edit the clone because the original is read-only.

Machines Window

The **Machines Window** button opens the Machines window in the MALTEGO client if it is not already open.

Summary

MALTEGO is proprietary software for open-source intelligence and forensics, developed by Paterva. MALTEGO focuses on providing a library of transformations for finding and linking data from open sources and visualizing this information in a graphical format suitable for link analysis and data mining [18].

MALTEGO is a visual link analysis tool that comes with open-source Intelligence plugins called transformations. The tool offers real-time data mining. Collected information is displayed on a node-based graph that makes patterns and connections of multiple orders between the information easily identifiable. MALTEGO focuses on analyzing real relationships between publicly accessible information about Internet infrastructures, individuals, and organizations [21].

MALTEGO allows the creation of user-defined entities to represent any information in addition to the basic entity types that are part of the software. The primary focus of the application is on the analysis of real relationships between people, groups, websites, domains, networks, Internet infrastructures, and connections to online services such as Twitter and Facebook.

Collecting all publicly available information using search engines and manual techniques is tedious and time-consuming. By automating the information gathering process to a large extent, MALTEGO saves a lot of time for researchers. The graphical representation of the information gathered by the software also aids the researcher's thought process in identifying connections between entities, Internet infrastructures, individuals, and organizations [19].

In today's dynamic IT environment, many organizations struggle to find every system and application at risk before the attackers do [9]. CENSYS empowers defenders with the automated visibility they need to truly understand and to get ahead of these risks, enabling even small security teams to have an outsized impact. For this reason, it is important to have trained operators who have the necessary expertise and can use this tool effectively and profitably.

The course created in this work gives participants a comprehensive overview of the topic of Open Source Intelligence. It allows them to work independently with the newly taught tools, collect data from freely available sources, and aggregate it into investigation results. For this purpose, the tasks were designed for several laboratory exercises.

References

[1] Mercado, Stephen C. "Sailing the Sea of OSINT in the Information Age." Secret intelligence: A reader 78 (2009).
[2] Best Jr, Richard A., and Alfred Cumming. "Open source intelligence (OSINT): issues for congress." December 5 (2007): 28.
[3] Glassman, Michael, and Min Ju Kang. "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)." Computers in Human Behavior 28.2 (2012): 673-682.
[4] Quick, Darren, and Kim-Kwang Raymond Choo. "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix." Future Generation Computer Systems 78 (2018): 558-567.
[5] Williams, Heather J., and Ilana Blum. "Defining second generation open source intelligence (OSINT) for the defense enterprise." RAND Corporation Santa Monica United States, 2018.
[6] Benes, Libor. "OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm." Journal of Strategic Security 6.3 (2013): 22-37.
[7] Schaurer, Florian, and Jan Störger. "The evolution of open source intelligence (OSINT)." Journal of US Intelligence Studies 19.3 (2013): 53-56.
[8] Pringle, Robert W. "The limits of OSINT: Diagnosing the Soviet media, 1985-1989." International Journal of Intelligence and CounterIntelligence 16.2 (2003): 280-289.
[9] Gibson, Helen. "Acquisition and preparation of data for OSINT investigations." Open Source Intelligence Investigation. Springer, Cham, 2016. 69-93.
[10] Carroll, Jami M. "OSINT Analysis using Adaptive Resonance Theory for Conterterrorism Warnings." Artificial Intelligence and Applications. 2005.
[11] Best, Clive. "OSINT, the Internet and Privacy." EISIC. 2012.
[12] Casanovas, Pompeu. "Cyber warfare and organised crime. A regulatory model and meta-model for open source intelligence (OSINT)." Ethics and Policies for Cyber Operations. Springer, Cham, 2017. 139-167.
[13] Layton, Robert, and Paul A. Watters. "Automating Open Source Intelligence: Algorithms for OSINT." Syngress, 2015.
[14] Steele, Robert David. "Open Source Intelligence (OSINT)."
[15] Berghel, Hal. "Robert David Steele on OSINT." Computer 47.7 (2014): 76-81.
[16] Weaver, Greg S. "Open Source Intelligence (OSINT)." The Police and the Military: Future Challenges and Opportunities in Public Safety 4.
[17] Revell, Quentin, Tom Smith, and Robert Stacey. "Tools for

OSINT-Based Investigations." Open Source Intelligence Investigation. Springer, Cham, 2016. 153-165.
[18] Kalpakis, George, et al. "OSINT and the Dark Web." Open Source Intelligence Investigation. Springer, Cham, 2016. 111-132.
[19] Tabatabaei, Fahimeh, and Douglas Wells. "OSINT in the Context of Cyber-Security." Open Source Intelligence Investigation. Springer, Cham, 2016. 213-231.
[20] Danda, Matthew. "Open Source Intelligence and Cybersecurity." (2019).
[21] Steele, Robert D. "1997 OSINT What Is It – Why Is It Important to the Military (White Paper)." Academia.edu **www.academia.edu/9817888/1997_OSINT_What_Is_It_Why_Is_It_Important_to_the_Military_White_Paper_**.
[22] "Social Media Prisma 2017/2018, Ethority, **ethority.de/social-media-prisma/**.
[23] Mohsin, Maryam, et al. "10 Social Media Statistics You Need to Know in 2020 [Infographic]." Oberlo, Oberlo, 15 Jan. 2020, **www.oberlo.com/blog/social-media-marketing-statistics**.
[24] Tenzer: "Daten - Volumen Der Weltweit Generierten Daten 2025." Statista, Statista, 13 Feb. 2020, **de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/**.
[25] Schwarz, Klaus; Franziska Schwarz, Reiner Creutzburg: "Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020, **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-278**
[26] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 1: RiskIQ PassiveTotal". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
[27] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 2: Censys". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
[28] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
[29] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
[30] Schwarz, Klaus: "Conception and Implementation of Professional Laboratory Exercises in the Field of Open Source Intelligence (OSINT) for use in English and German Training Market for Security Authorities". Master Thesis, Technische Hochschule Brandenburg, Department of Computing and Media, April 2020
[31] **https://www.maltego.com/**.
[32] Kant, Daniel; Reiner Creutzburg: 'Investigation of risks for Critical Infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253**
[33] Pilgermann, Michael; Thomas Bocklisch; Reiner Creutzburg: "Conception and implementation of a course for professional training and education in the field of IoT and smart home security". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-277**

Author Biography

Klaus Schwarz received his B. Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. His research interests include IoT and Smart Home Security, OSINT, Mechatronics, Sensorics, Embedded Systems, Artificial Intelligence, and Cloud Security. As a faculty member, he is developing a graduate program in Applied Mechatronic Systems focusing on Artificial Intelligence at SRH Berlin University of Applied Sciences.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

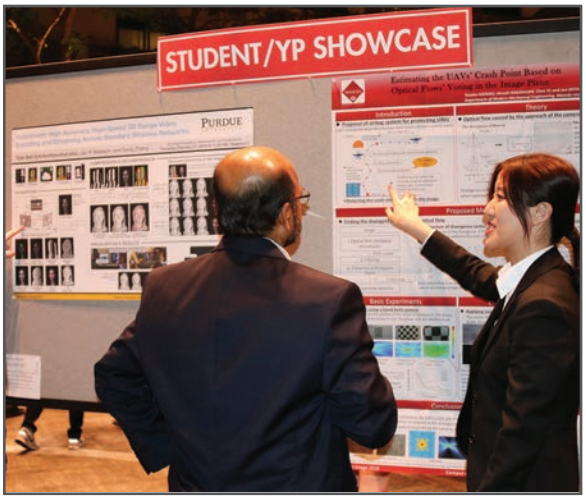
JOIN US AT THE NEXT EI!

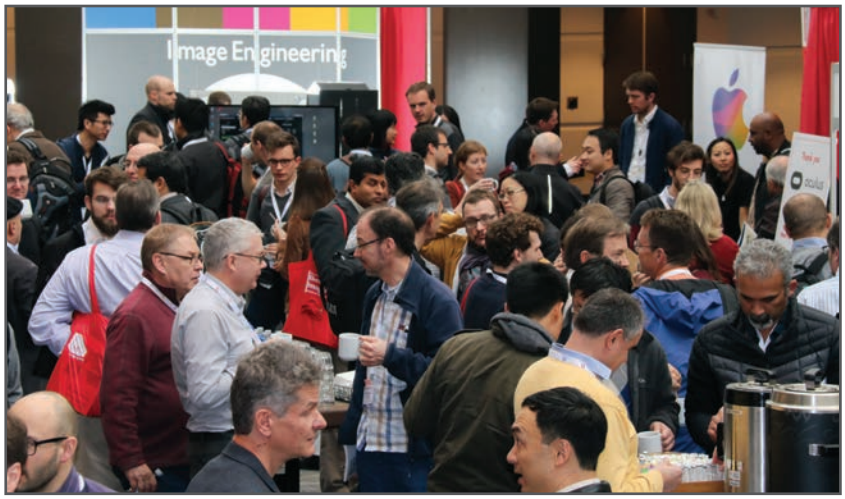
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org