

Security and Trust in Distributed Systems

Master Degree in New Technologies in Computer Science

2022/23

Open Source Intelligence (OSINT)

**Antonio Ruiz Martínez, Pantaleone Nespoli,
Félix Gómez Mármol**

Outline

Part I

- What's OSINT?
- OSINT Techniques
- OSINT Tools
- OSINT Workflows

Part II

- Maltego
 - Getting started
 - Developing a new transform

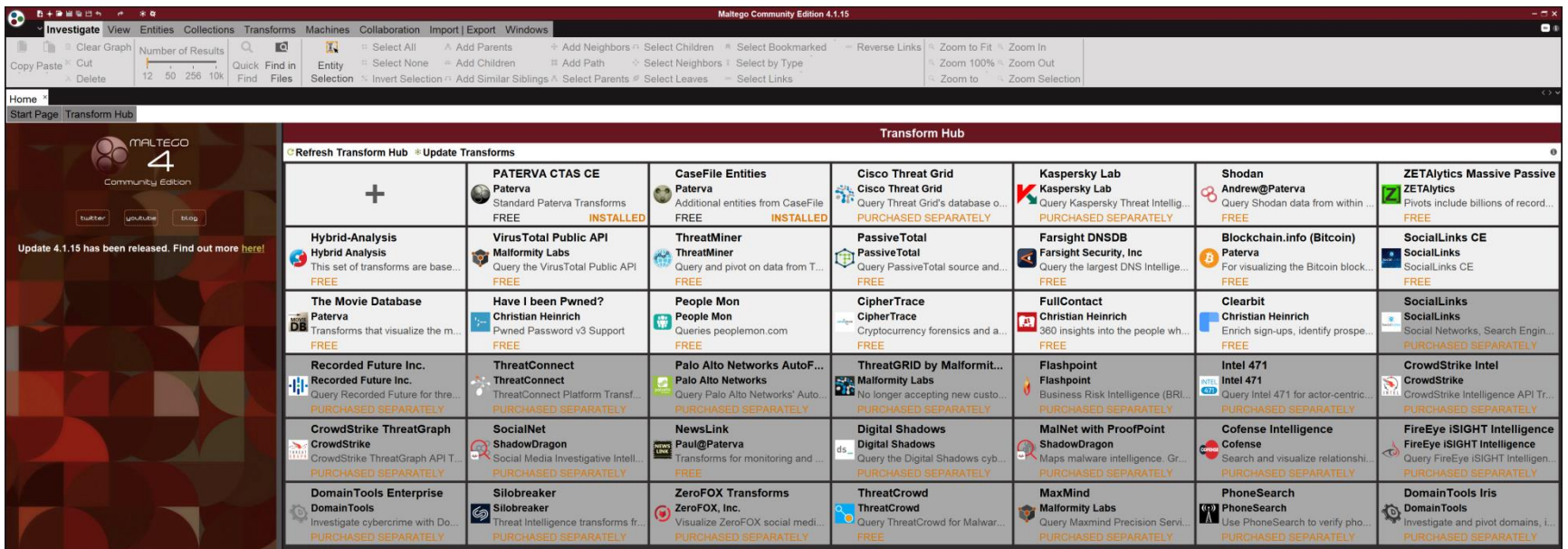
Maltego: Getting started

<https://docs.maltego.com>



Maltego: Getting started

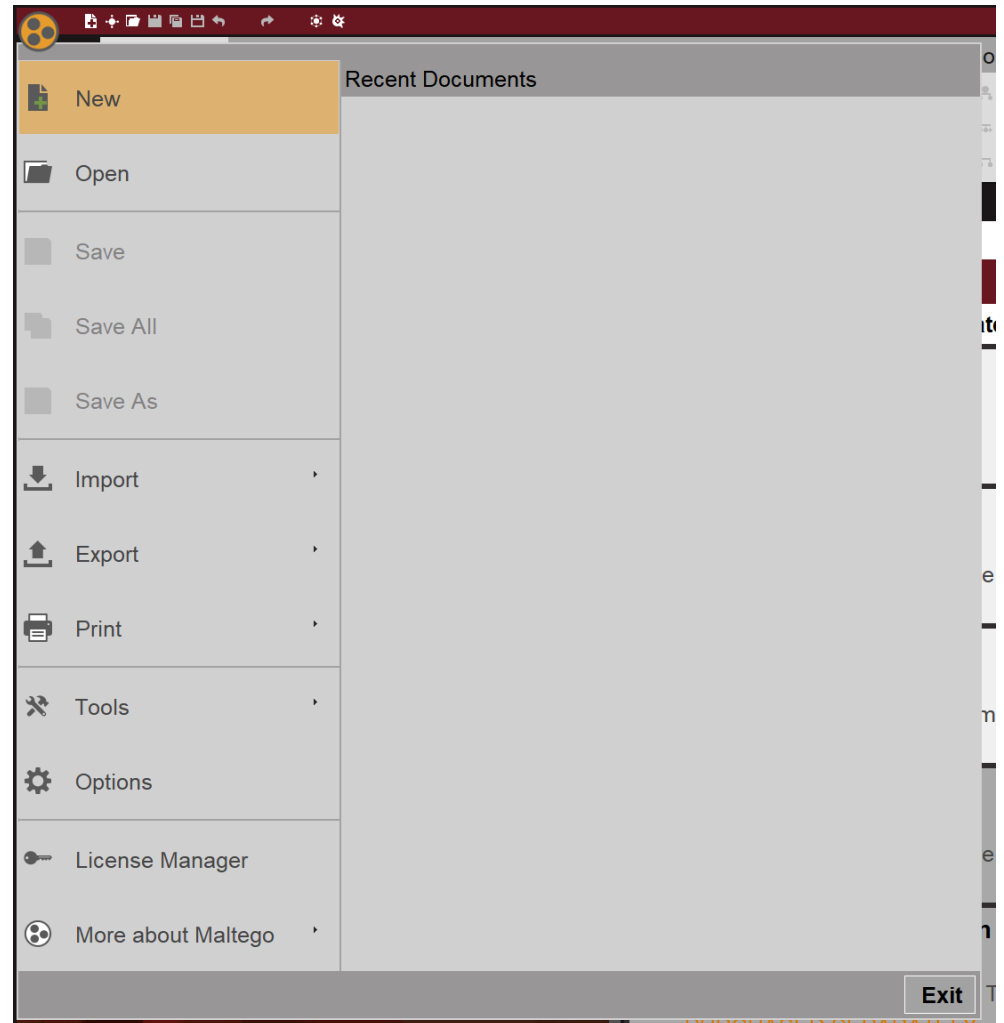
- Home



- Transform Hub
 - Free and purchased separately sets of transforms
 - Some require API key or authentication token to be used

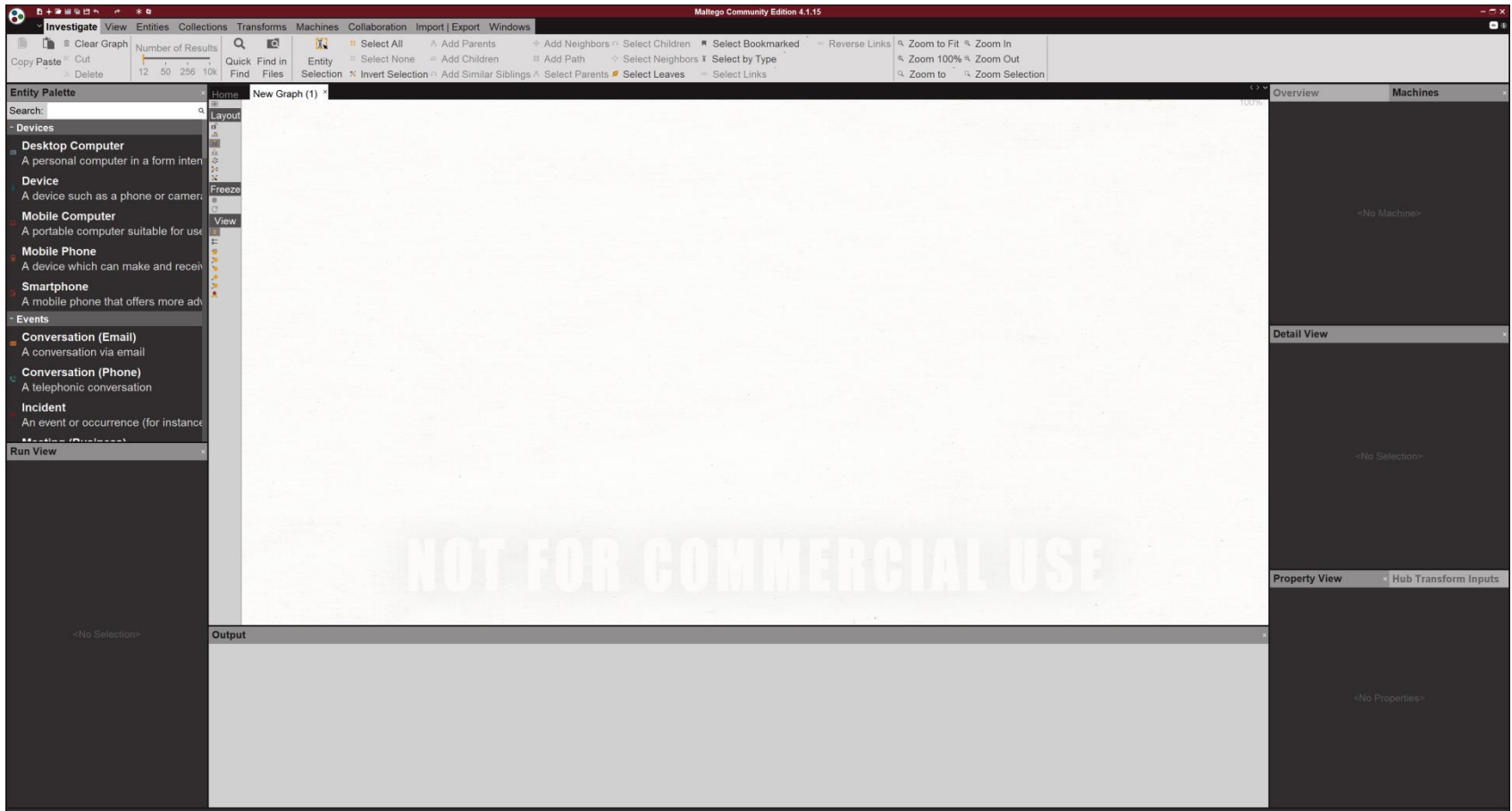
Maltego: Getting started

- Create a new Graph
(Ctrl+T | Cmd+T)



Maltego: Getting started

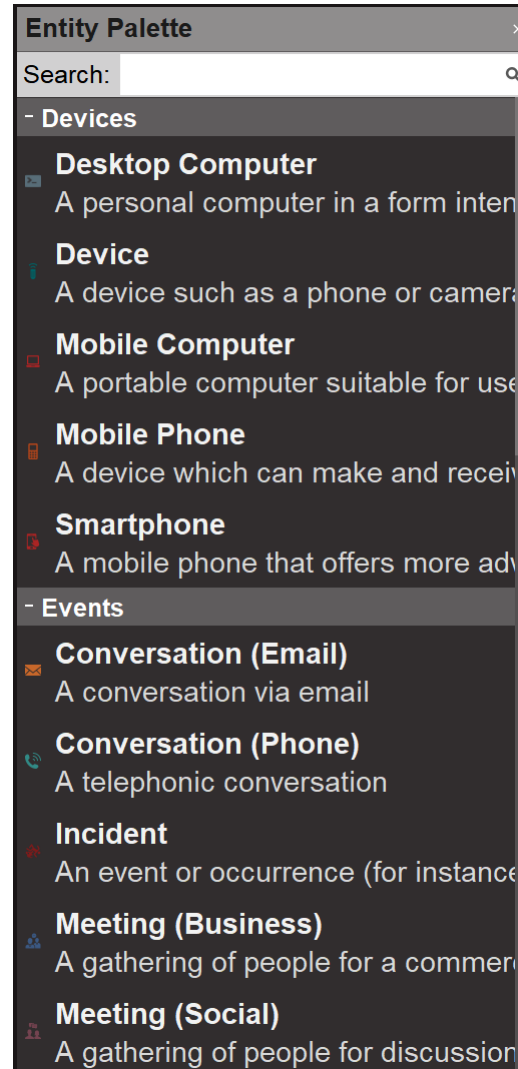
- Create a new Graph



Maltego: Getting started

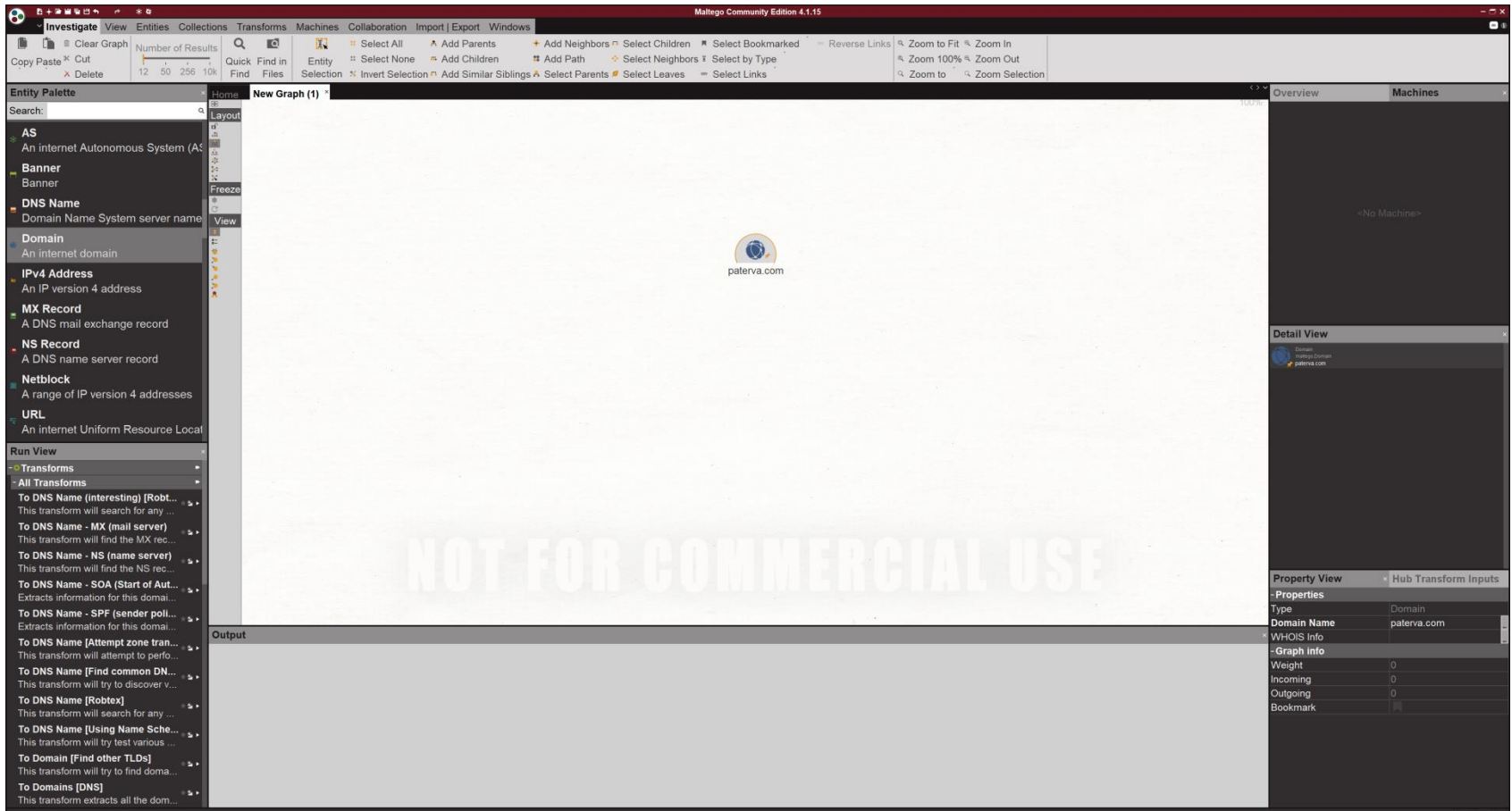
- **Entity Palette**

- Devices
- Events
- Groups
- Infrastructure
- Locations
- Malware
- Penetration Testing
- People
- Personal
- Social Network
- Tracking
- Transportation
- Weapons



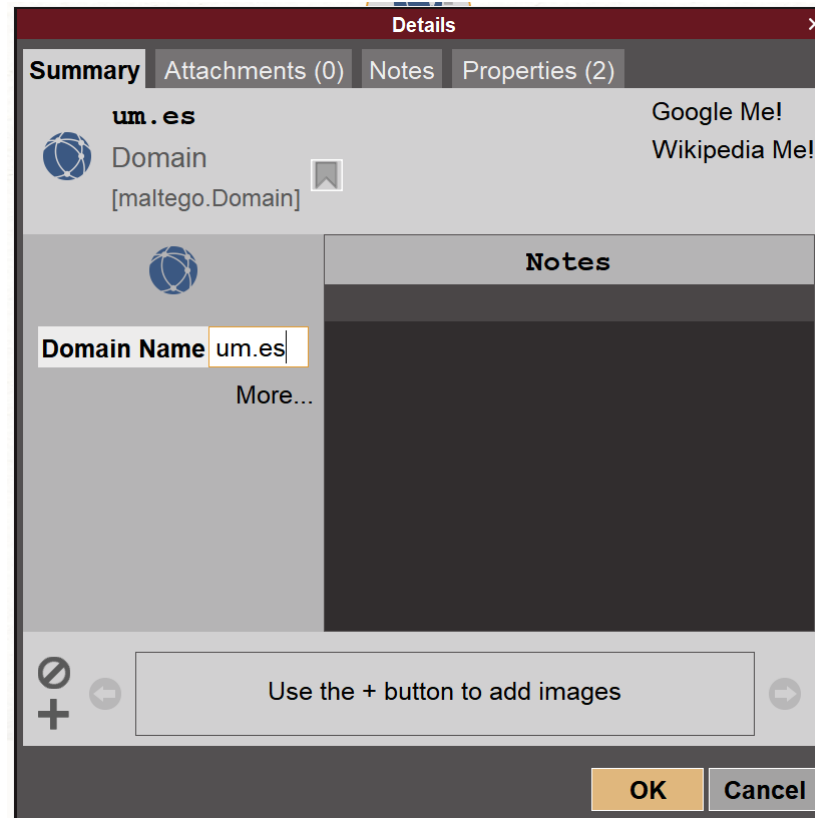
Maltego: Getting started

- Add a new Domain entity



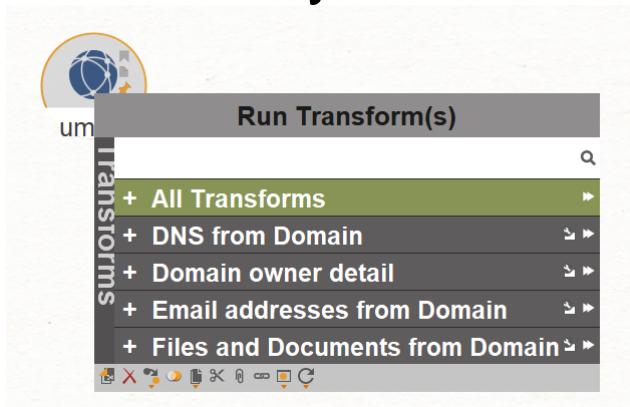
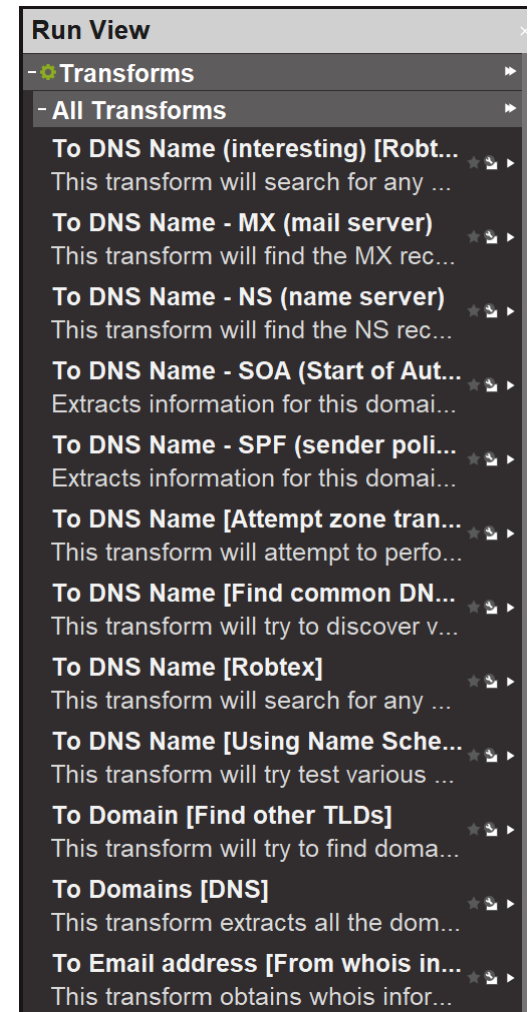
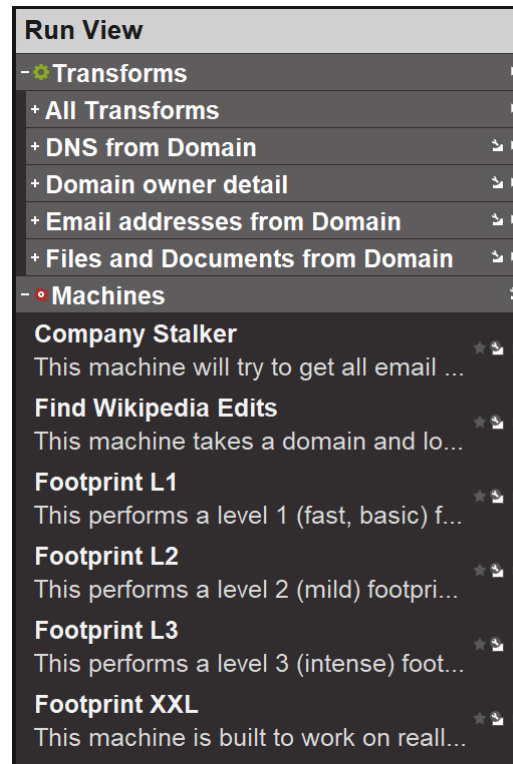
Maltego: Getting started

- Modify Domain entity's name to um.es



Maltego: Getting started

- **Run View**
 - Transforms
 - All transforms having a Domain entity as an Input
 - Machines
 - All machines having a Domain entity as an Input
- Also right-click on the entity



Maltego: Getting started

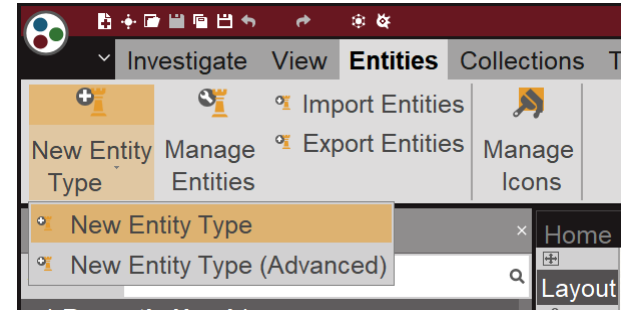
- Run All Transforms

The screenshot displays the Maltego interface with a central graph of entities. The root entity is 'um.es'. It branches into several subdomains: 'www.um.es', 'dns1.um.es', 'um.city', 'um.cx', 'mx01.puc.rediris.es', 'um.ac', 'um.cl', 'um.cz', 'um.be', 'um.cm', 'um.de', 'um.ca', 'um.co', 'chico.rediris.es', 'um.center', 'um.com', 'hostmaster@um.es', 'mx02.puc.rediris.es', and 'sun.rediris.es'. Each entity is represented by a globe icon, except for the email address and the rediris.es domains which have their respective logos. The interface includes a sidebar on the left with 'Layout', 'Freeze', and 'View' options. On the right, there are panels for 'Overview', 'Detail View', and 'Property View'. The 'Output - Transform Output' panel at the bottom shows the results of running transforms on the 'um.es' entity.

```
Output - Transform Output
Transform To DNS Name [Using Name Schema dictionary] returned with 10 entities (from entity "um.es")
Transform To DNS Name [Using Name Schema dictionary] done (from entity "um.es")
Too much content for http://keyserver.ubuntu.com:11371/pks/lookup?exact=off&op=vindex&search=um.es (from entity "um.es")
Too much content for http://pool.sks-keyservers.net:11371/pks/lookup?exact=off&op=vindex&search=um.es (from entity "um.es")
Transform To Person [PGP] returned with 0 entities (from entity "um.es")
Transform To Person [PGP] done (from entity "um.es")
Too much content for http://keyserver.ubuntu.com:11371/pks/lookup?exact=off&op=vindex&search=um.es (from entity "um.es")
Request read time out for http://pgp.mit.edu:11371/pks/lookup?exact=off&op=vindex&search=um.es (from entity "um.es")
Request read time out for http://pool.sks-keyservers.net:11371/pks/lookup?exact=off&op=vindex&search=um.es (from entity "um.es")
Transform To Email addresses [PGP] returned with 0 entities (from entity "um.es")
Transform To Email addresses [PGP] done (from entity "um.es")
```

Maltego: Getting started

- Play around a bit
 - Add new entities manually
 - Explore entities' properties
 - Run specific transforms
 - Change layout of the graph
 - Save and open a graph
- Create a new entity type
 - University
 - Unique type name
 - es.um.university
 - Category Locations
 - Inherited from Location

A screenshot of the 'New Entity Wizard (Basic)' dialog box. The dialog is titled 'New Entity Wizard (Basic)' and contains a 'BASIC INFORMATION: Enter the details for your new entity below.' section. The 'BASIC INFORMATION' section includes fields for 'Display name', 'Short description', 'Unique type name', and 'Category'. Below these are 'Inheritance' options, including a checkbox for 'Base Entity' and a dropdown menu. At the bottom, there are 'Icons' sections for 'Large icon (48 x 48)' and 'Small icon (16 x 16)', each with a 'Browse...' button. A note at the bottom left states 'Display name is required'. At the bottom right, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

Maltego: Developing a new transform

<https://docs.maltego.com/support/solutions/articles/15000015758-writing-transforms>

Maltego: Developing a new transform

- **iTDS (internal Transform Distribution Server) Transforms**
 - Web application allowing distribution and management of transforms, seeds and settings
 - Transforms are written as a web services (or application/pages), and the iTDS will call these scripts
 - **PROS**
 - Once setup transforms are easily distributed to multiple Maltego clients
 - No configuration needed client side, scripts all live in one place
 - Updating instantly impacts all clients
 - Deeper into the protocol (Slider value + Transform settings/Popups)
 - **CONS**
 - Cannot integrate with applications local to the Maltego client
 - All requests come from a single point (may impact things like rate limiting APIs)
 - Server infrastructure setup is required

Maltego: Developing a new transform

- **Local Transforms**
 - Pieces of code running on the same machine that the Maltego client application is on
 - Very useful for integrating in machine specific tasks
 - Written in any language and merely rely on output to be sent via STDOUT
 - PROS
 - Machine Specific
 - Nothing ever goes 'over the wire' - unless you want it to
 - Simple to write in any language
 - Does not require any server infrastructure setup
 - CONS
 - Requires setup on each machine you wish to install them
 - Does not go as deep into the Transform Specification - no slider or settings
 - Updating a transform means it needs to be updated on every machine
 - Sensitive data such as usernames and passwords could reside on the computer of the analysts

Maltego: Developing a new transform

- **Local Transforms**

- Interacted with via **STDIN** and **STDOUT**

- **STDIN**

- **Entity Value** (what is displayed on the graph) → this is the first argument.
 - **Entity Fields** (the fields contained in the entity), separated by #'s and each field is separated - name and value by an '=' sign.
 - e.g., "Félix Gómez Mármol" person.fullname=Félix Gómez Mármol#person.firstnames=Félix#person.lastname=Gómez Mármol

- **STDOUT**

```
<MaltegoMessage>
  <MaltegoTransformResponseMessage>
    <Entities>
      <Entity Type="maltego.Phrase">
        <Value>Hello Félix Gómez Mármol</Value>
        <Weight>100</Weight>
      </Entity>
    </Entities>
    <UIMessages>
    </UIMessages>
  </MaltegoTransformResponseMessage>
</MaltegoMessage>
```