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

UNIVERSIDAD DE MURCIA

Outline

Part I

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

Part II

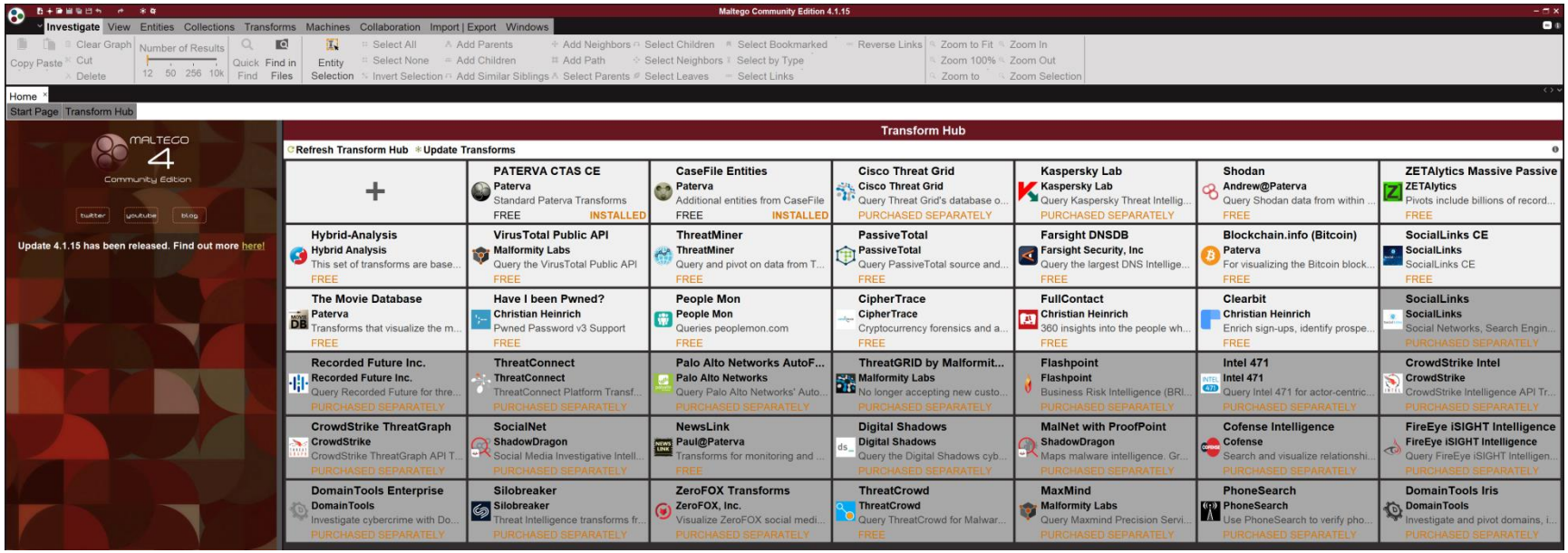
- Maltego
  - Getting started
  - Developing a new transform

Maltego: Getting started

https://docs.maltego.com

Maltego: Getting started

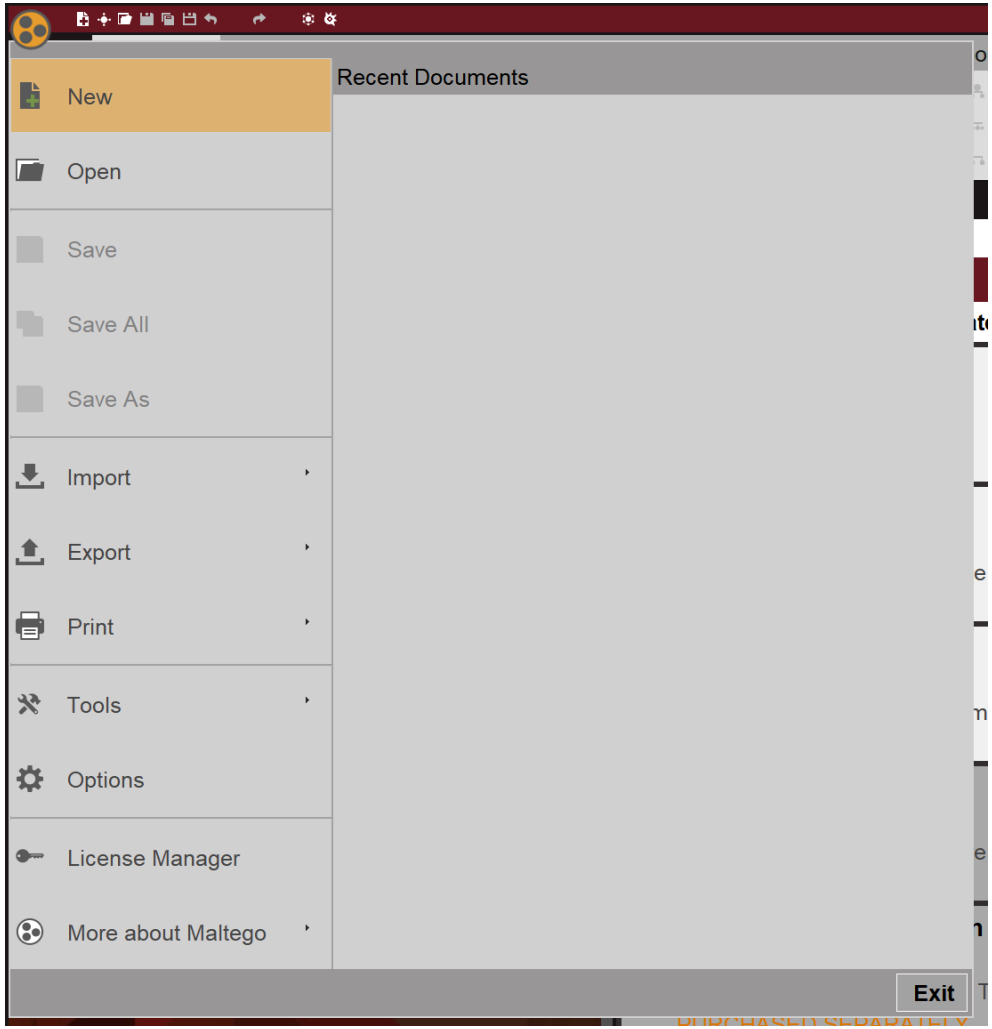
- Home



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

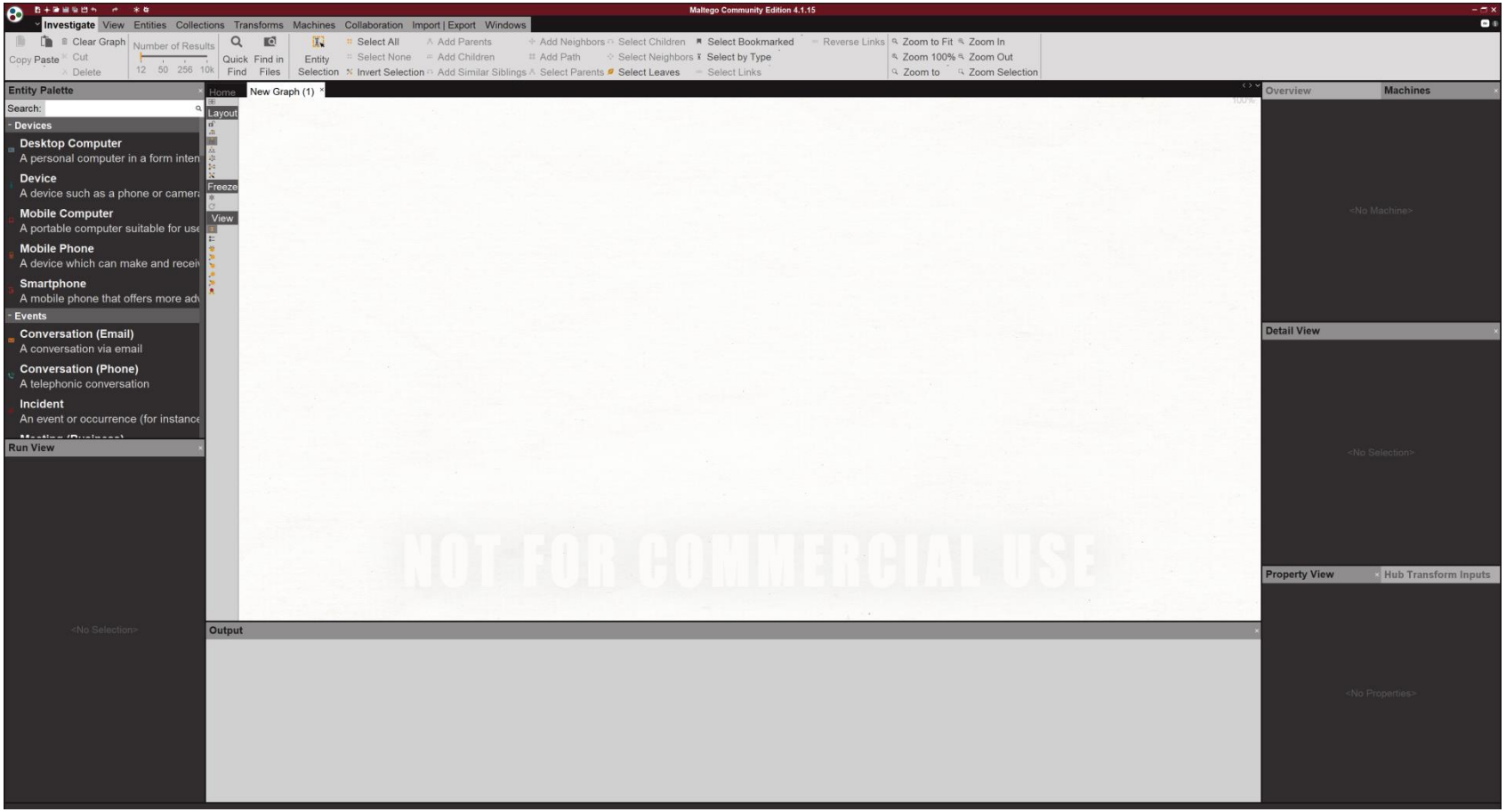
Maltego: Getting started

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



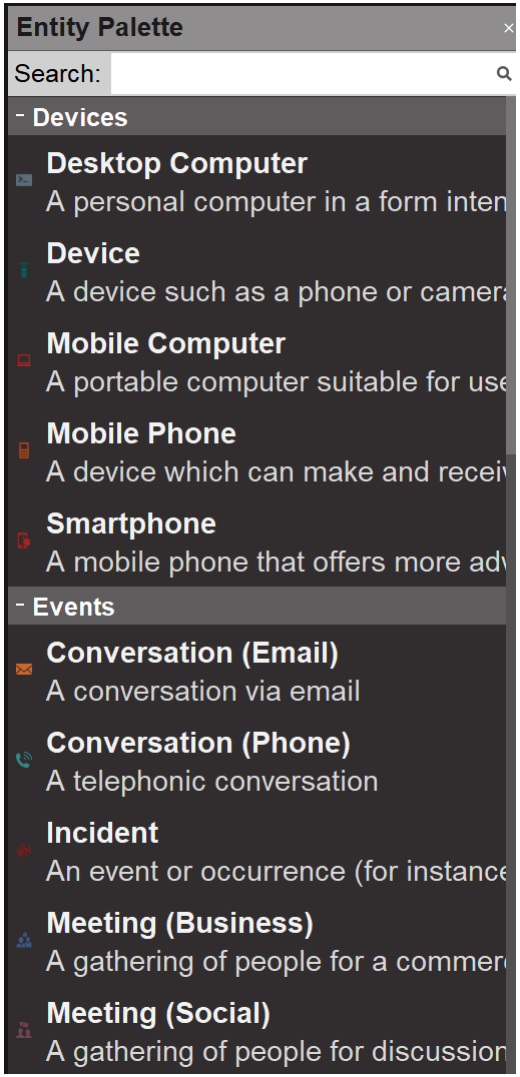
Maltego: Getting started

- Create a new Graph



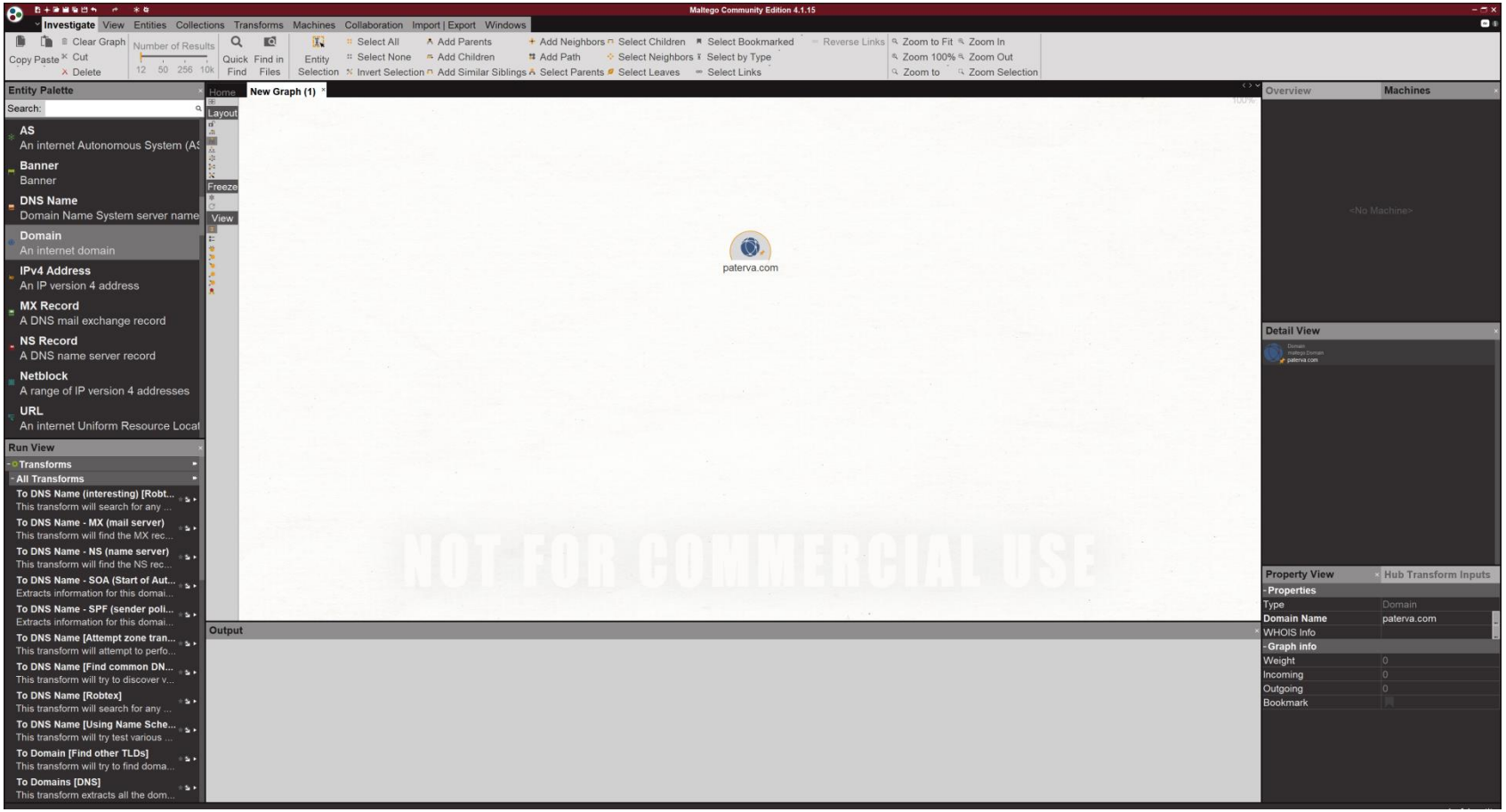
Maltego: Getting started

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



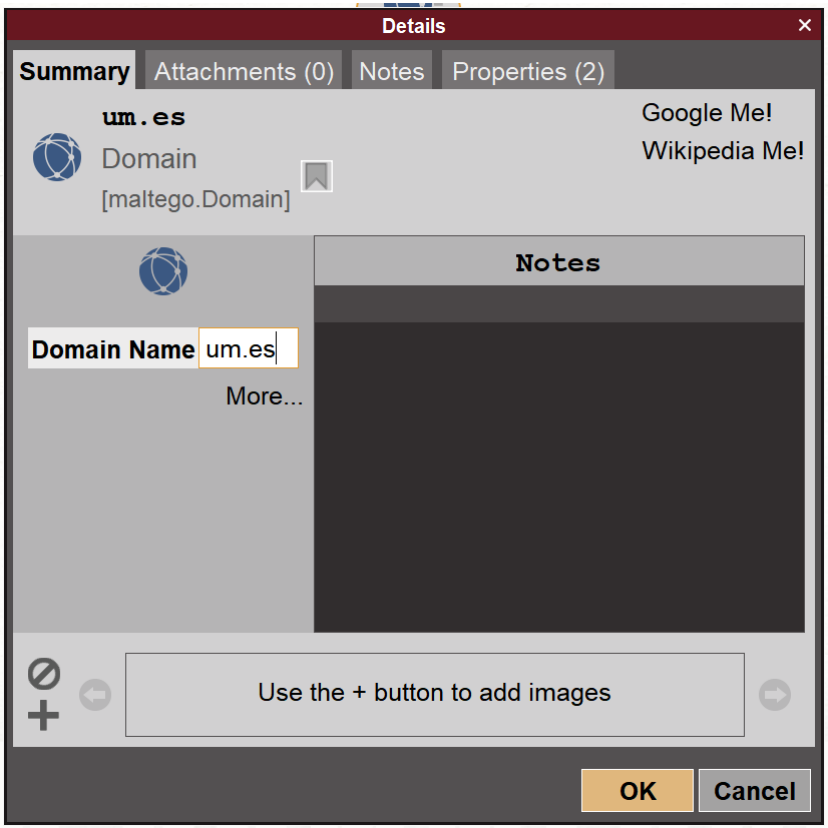
Maltego: Getting started

- Add a new `Domain` entity



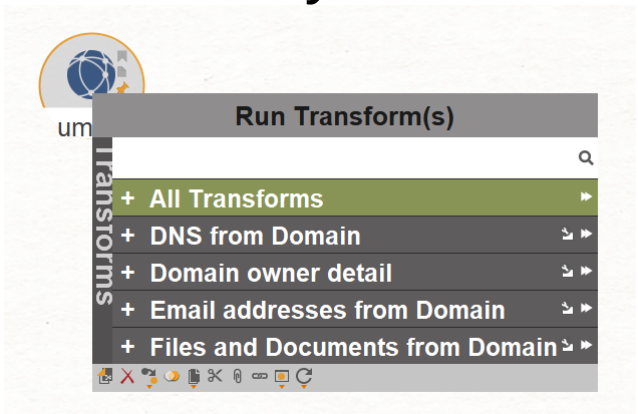
Maltego: Getting started

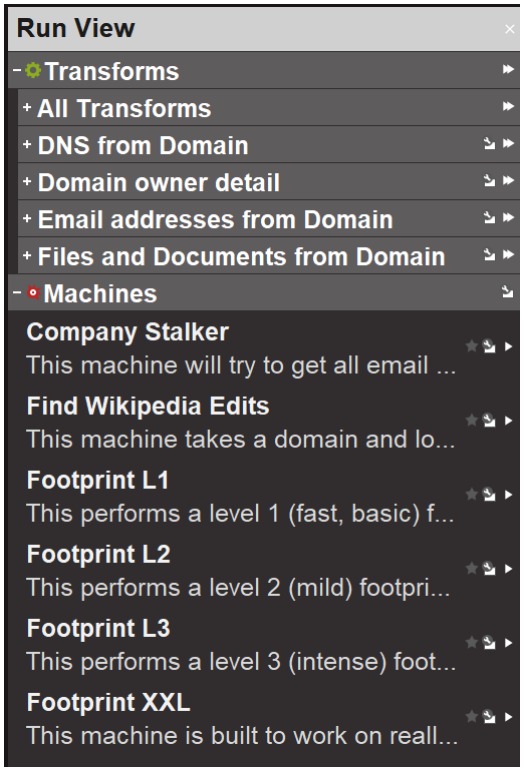
- Modify `Domain` entity's name to `um.es`

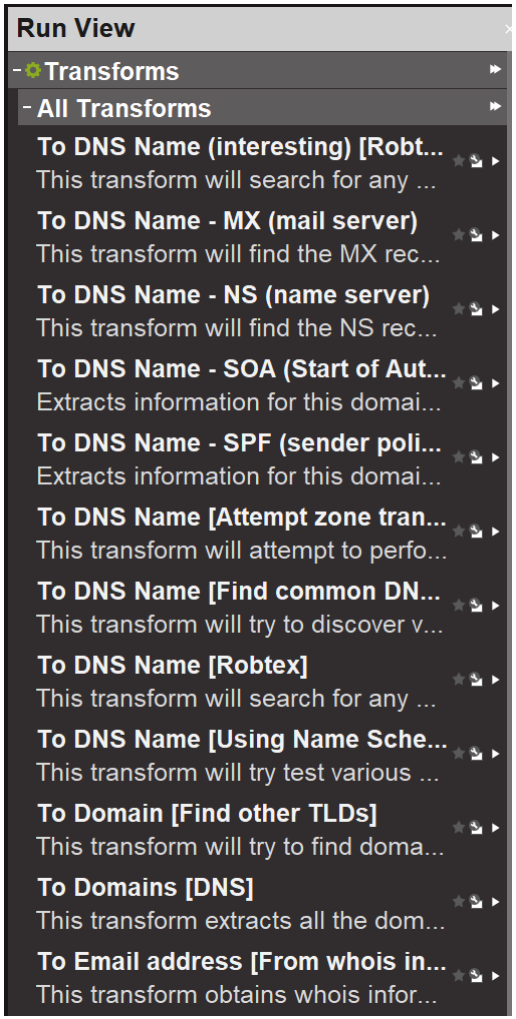


Maltego: Getting started

- 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



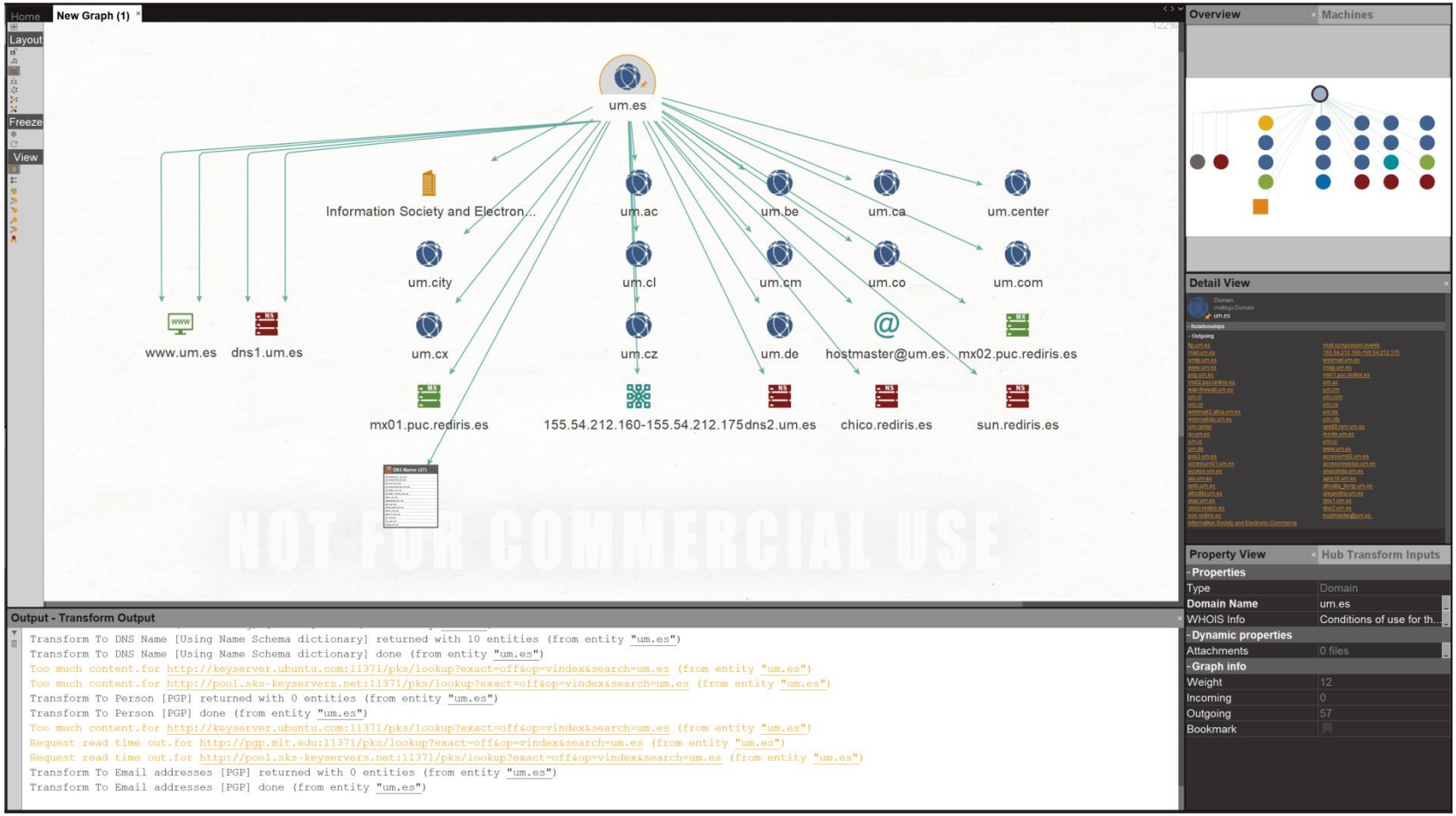




UNIVERSIDAD DE MURCIA

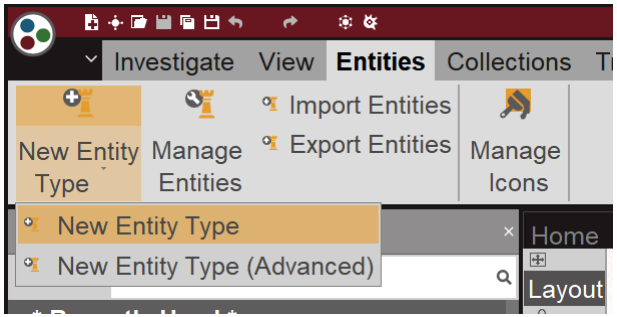
Maltego: Getting started

- Run All Transforms

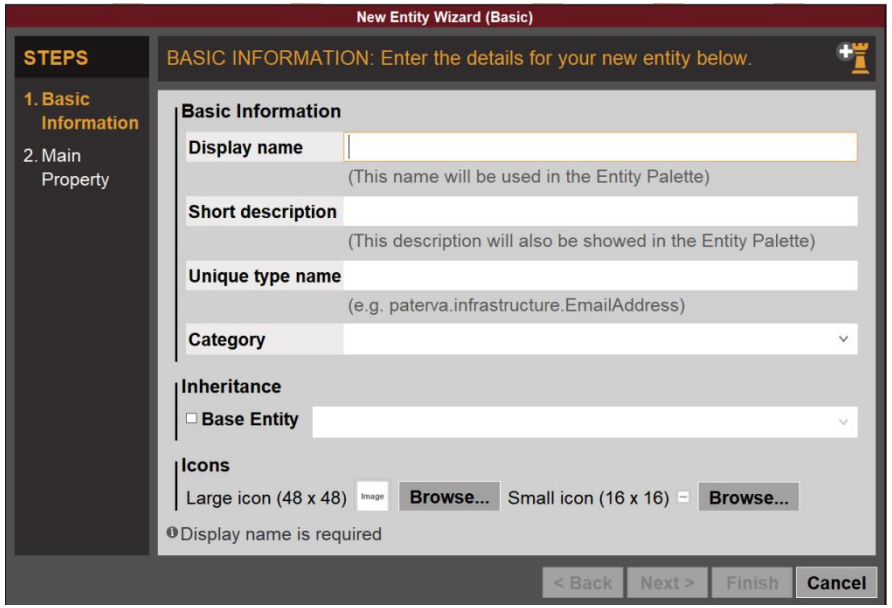


Maltego: Getting started

- 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`



Maltego: Developing a new transform

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

Maltego: Developing a new transform

- iTDS (**i**nternal **T**ransform **D**istribution **S**erver) 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>
```