
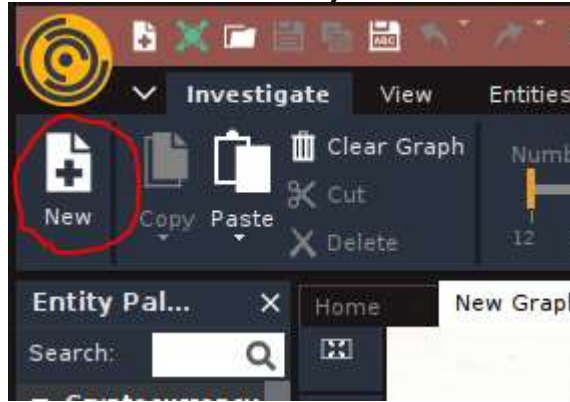


<b>Materia:</b>	Ethical Hacking
<b>Unidad:</b>	2
<b>Práctica:</b>	3 Maltego
<b>Versión:</b>	1.0
<b>Objetivo:</b>	¿Quién? El alumno, ¿Qué? Entenderá qué es una herramienta OSINT, ¿Cómo? usando la herramienta Maltego, ¿Para qué? en orden a conocer la fase de rastreo y reconocimiento.
<b>Horas teórico-prácticas:</b>	1.5 hrs
<b>Puntuación:</b>	% de la calificación final
<b>Logística:</b>	<p>Tarea personal.</p> <p>La recopilación de la información es la forma de adquirir los datos relevantes disponibles de manera pública de fuentes disponibles. A menudo se le conoce como <b>Open Source Intelligence (OSINT)</b>. Un atacante dedicará aproximadamente el 75% del esfuerzo de trabajo únicamente para el reconocimiento, ya que es la fase que permite mapear y definir el objetivo, explorando las vulnerabilidades que eventualmente conducirán a una explotación.</p> <p>Uno de los mejores softwares disponibles actualmente para el OSINT es <b>Maltego</b>. Dicho software proporciona una biblioteca de transformaciones para el descubrimiento de datos de fuentes abiertas y visualizar esa información en un formato gráfico adecuado para análisis de enlaces y minería de datos.</p> <ol style="list-style-type: none"> <li>1. Bajar e instalar el software <b>Maltego</b> (<a href="https://www.maltego.com/downloads/">https://www.maltego.com/downloads/</a>).</li> <li>2. Activar <b>Maltego</b> con <b>Maltego ID</b></li> </ol>  <p>A continuación solicitará datos para crear el perfil de nuestro usuario. Se puede usar una dirección e-mail desechable (yopmail.com). Se puede decir que se es un “estudiante” y que la organización es la UADY. En algún momento, desde el asistente de instalación, habrá que identificarse con el usuario recién creado a través de un link</p>

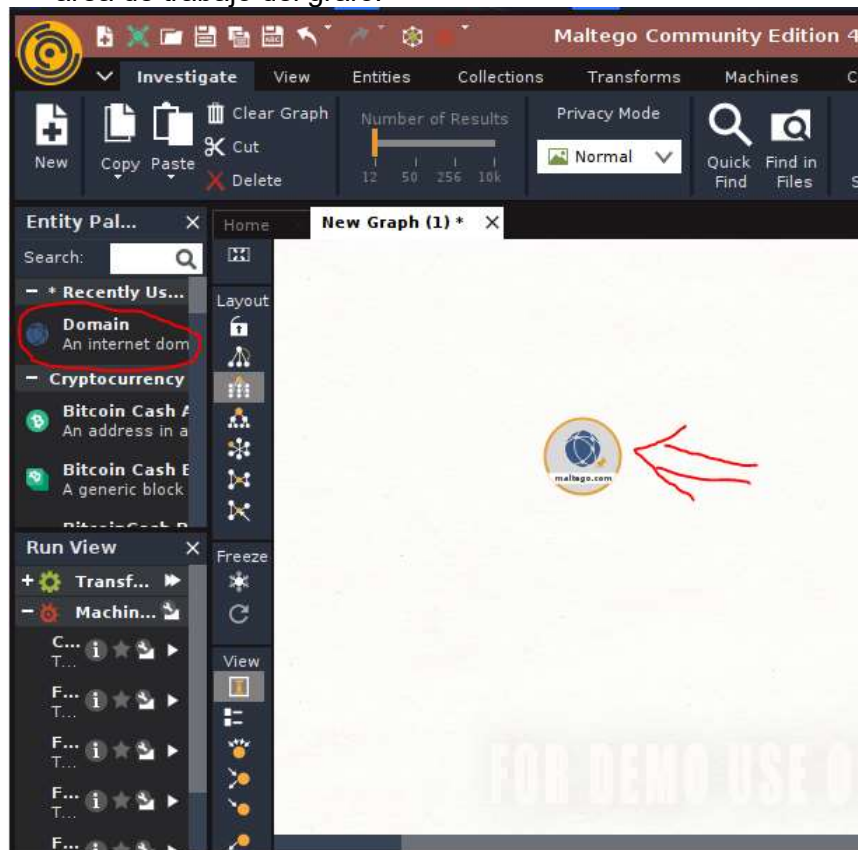
proporcionado por el propio asistente, y después de ello continuar la instalación con los valores por default y aceptar los términos.

Continuar con el proceso de instalación hasta terminar.

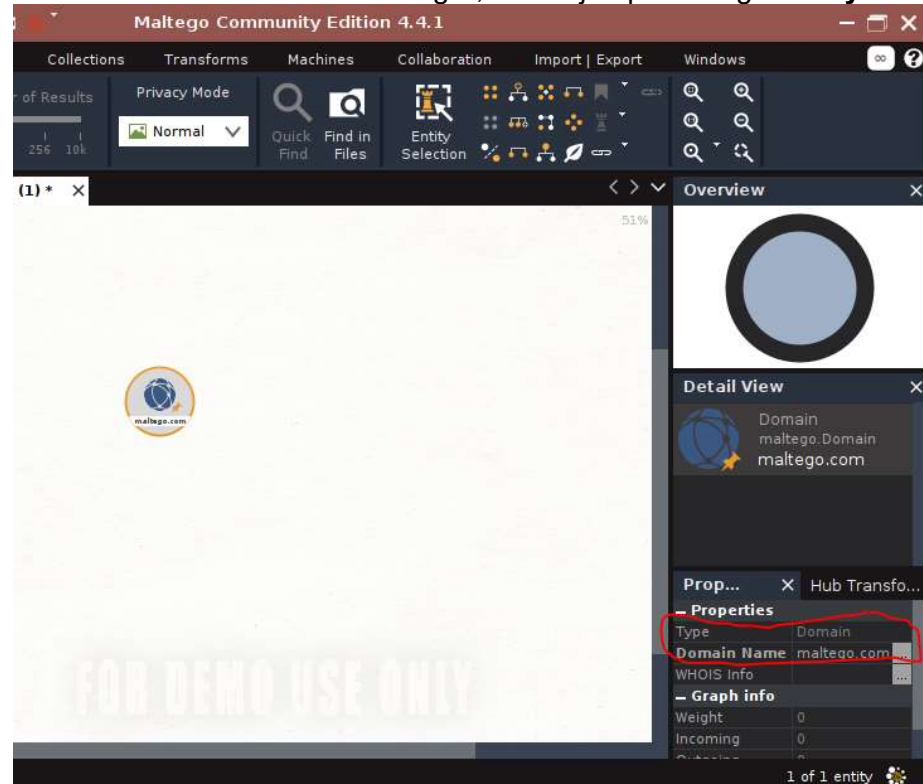
3. Crear un nuevo trabajo:



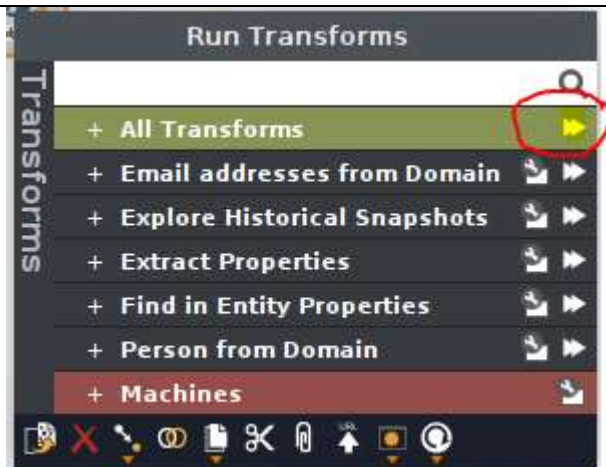
4. Inmediatamente nos ofrecerá abrir una nueva gráfica. En la paleta de opciones del lado izquierdo denominada “**Entity Palette**”, buscar y seleccionar el elemento “**Domain**”, dar click sobre él y arrastrarlo al área de trabajo del grafo:



5. Sobre el objeto “**Domain**” dar doble click y editar el registro con el nombre del dominio a investigar, en el ejemplo se digitó **uady.mx**.



6. Ya que el objetivo ha sido configurado, con un click sobre el objeto “**Domain**” se abrirá un menú de transformaciones de información. Para este caso se elegirán y correrán todas las transformaciones disponibles:



Nota: En caso que las transformaciones seleccionadas requieran información adicional, se solicitará en este momento, por ejemplo: rangos de fechas para limitar las búsquedas. Se pueden dejar los datos por default, donde sea posible.

Required inputs

×

The following transforms require inputs:

– To Snapshots between Dates [Wayback Machine]

Search Date Range

18Oct'13 19:00:00 EDT → 17Oct'23 14:00:10 EDT

▼

Search Date Range

+ Extract Property To Phrase

☐ Remember these settings

Run!

Cancel

7. Analizar y verificar toda la información que se pueda para el dominio **uady.mx**:

The screenshot displays the Maltego interface with a central network diagram. Nodes include email addresses like 'chcamara@uady.mx', 'hcorrea@uady.mx', and 'inzel@uady.mx', as well as domains like 'mail2.uady.mx' and 'mail.uady.mx'. A 'YESLI' node is also visible. A 'Detail View' window is open on the right, showing a list of 32 links. The table below represents the data shown in this window.

Link	Source	Target
transform	uady.mx	revista.c
transform	uady.mx	transpar
transform	uady.mx	revbiome
transform	uady.mx	uady.mx
transform	uady.mx	cirsocia
transform	uady.mx	mayas.u
transform	uady.mx	ingquim
transform	uady.mx	odontolo
transform	uady.mx	s2.medi
transform	uady.mx	dgda.ua
transform	uady.mx	intranet
transform	uady.mx	unidadad
transform	uady.mx	ftp.uady

**Entregable:**

- Screenshot de los gráficos obtenidos
- ¿qué información arrojó maltego del dominio uady.mx?
- Si fueras hacker de sombrero negro ¿para qué te sería útil maltego?
- Como hacker de sombrero blanco ¿qué sugieres hacer para mitigar el riesgo de que un pirata use maltego en su beneficio?

**Bibliografía:** <https://www.maltego.com>