fwhibbit.es

Introducción a Maltego

6-8 minutos

Introducción

Buenas conejetes!!

Maltego (de la compañía Paterva) es una potente herramienta desarrollada en Java (seguro que ya os estáis quejando unos cuantos, sobre todo los defensores de .net :P), que recopila información y la muestra en forma de grafos, ayudando así en el análisis posterior de la información obtenida por los equipos de inteligencia y forense. Contiene una serie de módulos de aplicaciones externas (*transforms*) que complementan su potencial.

La vista en grafos de la información recopilada permite analizar las relaciones entre actores y sus redes sociales (como Twitter y Facebook) con la infraestructura de las entidades investigadas, como son grupos, dominios, y redes.

Cuenta además con la funcionalidad de crear entidades propias, permitiendo así representar cualquier tipo de información y no sólo la relacionada con el software analizado.

Versiones de Maltego y diferencias

Existen principalmente 4 versiones, dos de pago y dos gratuitas. El

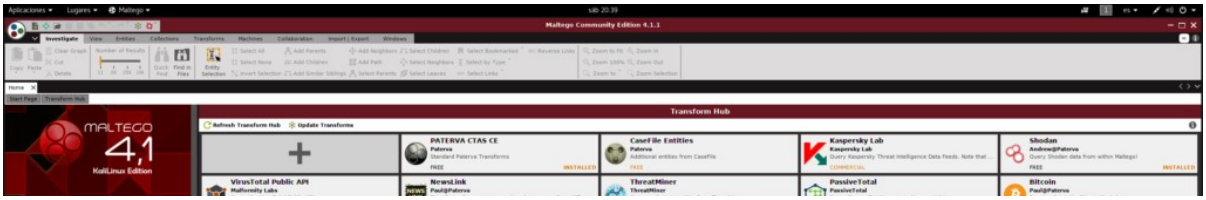
precio de las versiones de pago (Maltego XL y Maltego Classic) al menos para mi es muy elevado, por lo que al utilizar Maltego sin fines comerciales y para demostrar su potencial, he optado por la versión Maltego CE, ya que es igual que la versión Classic pero con limitaciones. Entre estas limitaciones está que tan sólo se nos mostrará 12 resultados como máximo por transformada analizada.

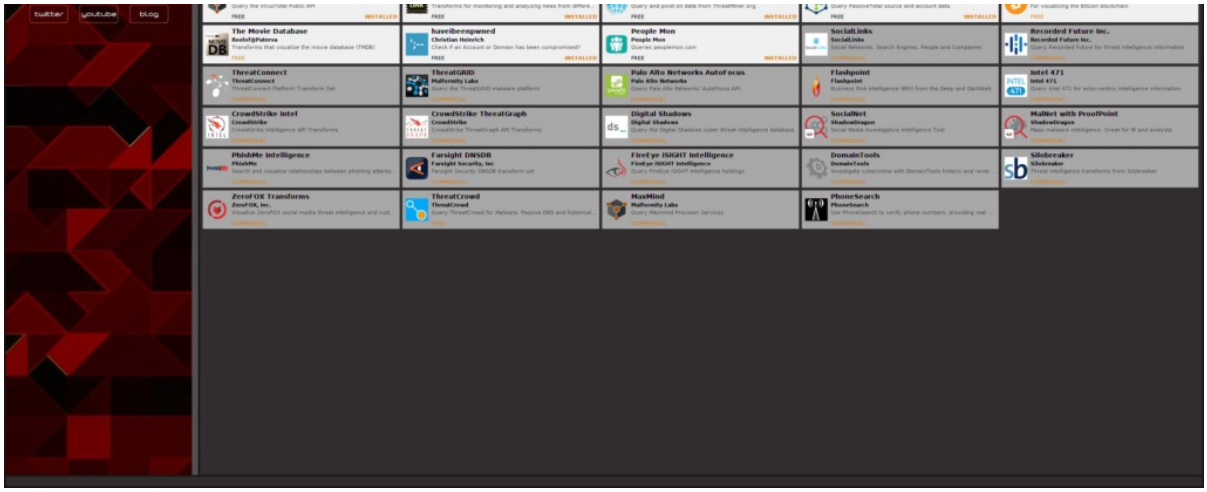
	Maltego XL	Maltego Classic	Maltego CE	CaseFile
Initial Cost	1800 USD	760 USD	Free	Free
Yearly Renewal Cost	760 USD	320 USD	Free	Free
Commercial Use	✓	✓	✗	✓
Access to commercial Transform Hub	✓	✓	✗	N/A
Use with Internal Transform servers	✓	✓	✗	N/A
Standard OSINT Transforms	✓	✓	✓	✗
Max number of results per transform	64,000	10,000	12	N/A
Max number of entities on a graph	1, 000, 000	10,000	10, 000	N/A
Technical support	✓	✓	✗	✗
Graph Export (CSV, XLS, XLSX, PDF and Image formats)	✓	✓	✓	✗
Graph Import (CSV, XLS, XLSX)	✓	✓	✓	✓
Shared Graph Sessions (Collaboration)	✓	✓	✓	✓
Machines (Transform Macros)	✓	✓	✓	N/A
	Buy	Buy	Register	Read More

Para poder utilizar Maltego, necesitaremos registrarnos en su página web. Tras unos breves pasos, ya podremos empezar a disfrutar de la herramienta.

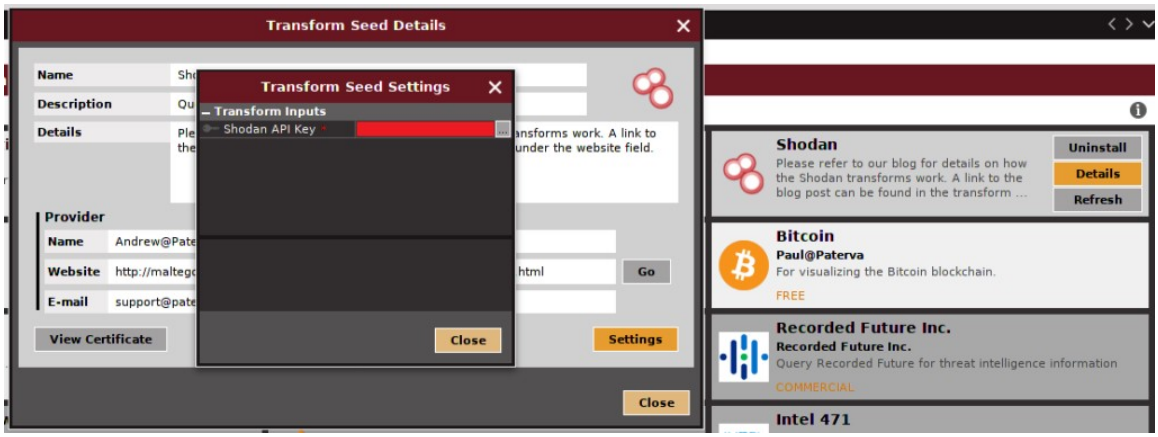
Configuración de las transformadas

Nada más abrir Maltego, se nos pedirá loguearnos con el usuario que nos hemos registrado. Tras realizar esto, se nos presentará la siguiente interfaz:



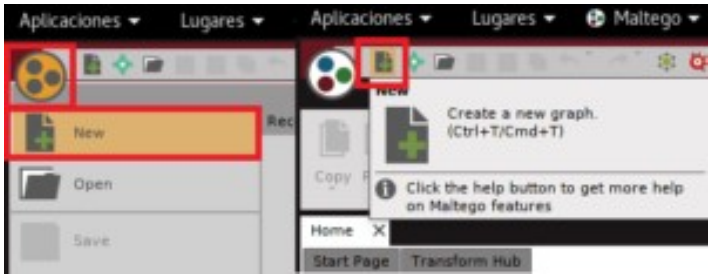


En la pantalla principal (*Transform Hub*) se nos muestra el conjunto de transformadas predefinidas por el programa. Las que se encuentran sobre un fondo gris pertenecen a las versiones de pago, por lo que en este caso no estarán disponibles. De las transformadas disponibles, podéis instalar cuantas necesitéis, pero tened en cuenta que algunas necesitarán que se introduzca su **API Key**, como por ejemplo la de Shodan. Si no disponéis de la misma, al realizar una búsqueda de una transformada el programa os la pedirá, y en caso de no introducir nada, no realizará la búsqueda sobre la transformada. Para introducir vuestra API Key deberéis seleccionar la transformada en cuestión (una vez instalada) y pulsar en *Details/Settings*:

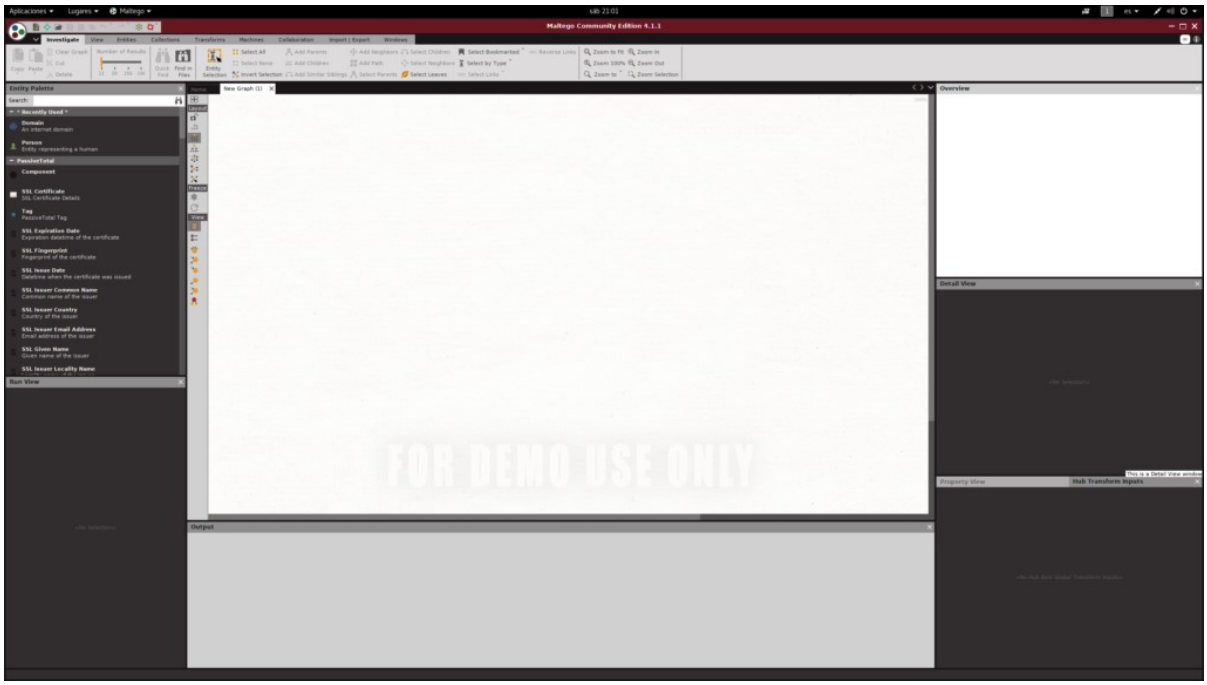


Empecemos a jugar

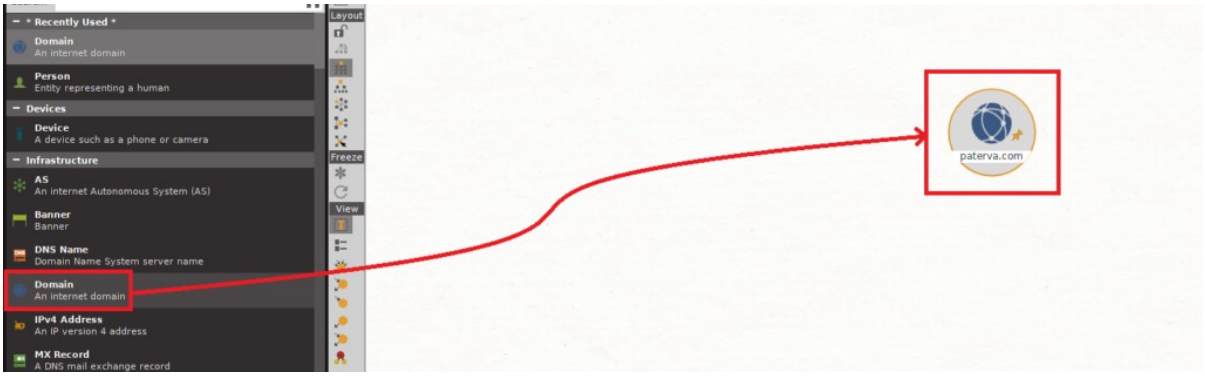
Para comenzar a trastear, deberemos crear un nuevo grafo. Para ello, podremos usar el atajo **Ctrl + t/Cmd + t**, o crearlo desde el panel desde una de estas dos opciones:



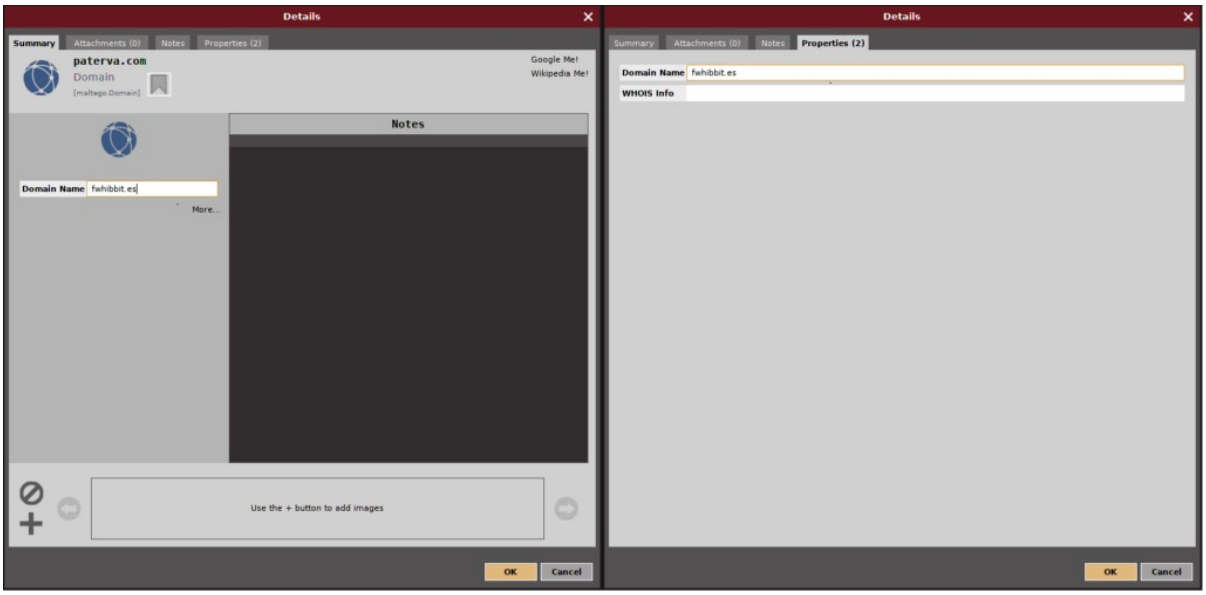
Una vez hecho esto, se nos mostrará una pantalla principal nueva, con un menú de entidades a la izquierda, y varios paneles de información a la derecha:



Lo primero que vamos a probar es como funciona respecto a un dominio público. En este caso, vamos a investigar a estos pequeños conejos. Para ello, desde la paleta de entidades, deberemos buscar en el módulo *Infrastructure*, la entidad con nombre *Domain* y arrastrarla hasta el grafo creado anteriormente:

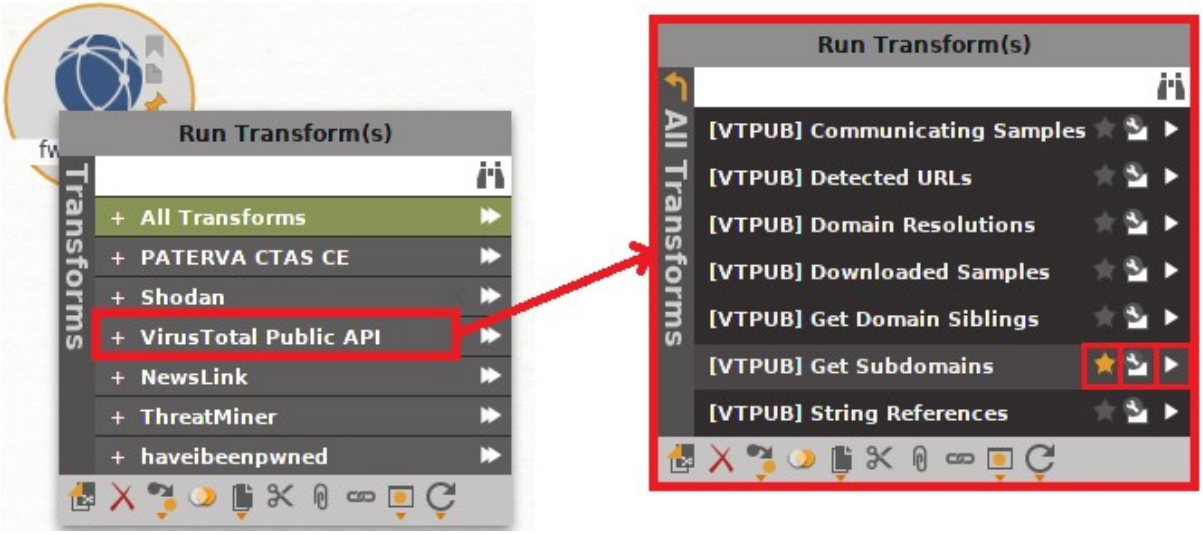


Si hacemos doble click en la entidad de dominio creada, entraremos a la forma detalle de la entidad y podremos modificar sus valores. En este caso modificaremos el nombre del dominio, ya sea en la parte de *summary* o bien en *properties* (también es posible cambiarlo directamente sin entrar a la forma del detalle de la entidad, pulsando directamente sobre el nombre y modificándolo):

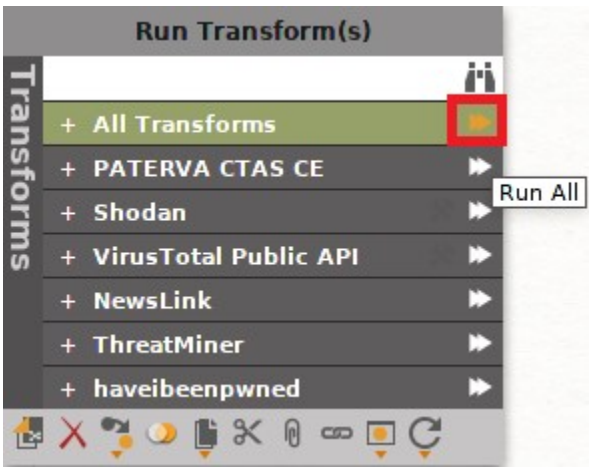


Una vez indicado el dominio a investigar, al pulsar botón derecho sobre la entidad nos aparecerá un pequeño menú de módulos para indicar que transformadas queremos ejecutar. Cómo podemos observar, se pueden ver o bien todas las transformadas, o ir específicamente a una determinada. Para acceder a cada transformada, podremos pulsar en el nombre de la misma. Una vez hecho esto, nos aparecerá un listado de las distintas partes de la

transformada, por si queremos ser más específicos. Además, podremos seleccionar a una transformada como favorita pulsando en la estrella, o configurar sus opciones pulsando en la llave para configurar más detalladamente la transformada. Si queremos ejecutar una transformada, deberemos pulsar sobre el icono de *play*.



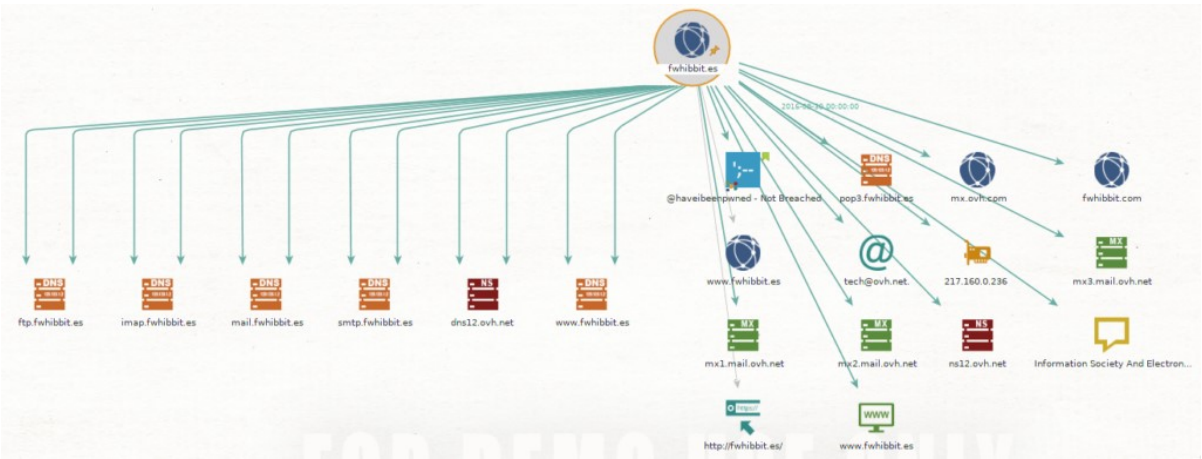
Existe también lo opción de ejecutar todas las transformadas directamente desde el menú principal de la entidad, pulsando sobre el icono de *play* doble en *All Transforms*.



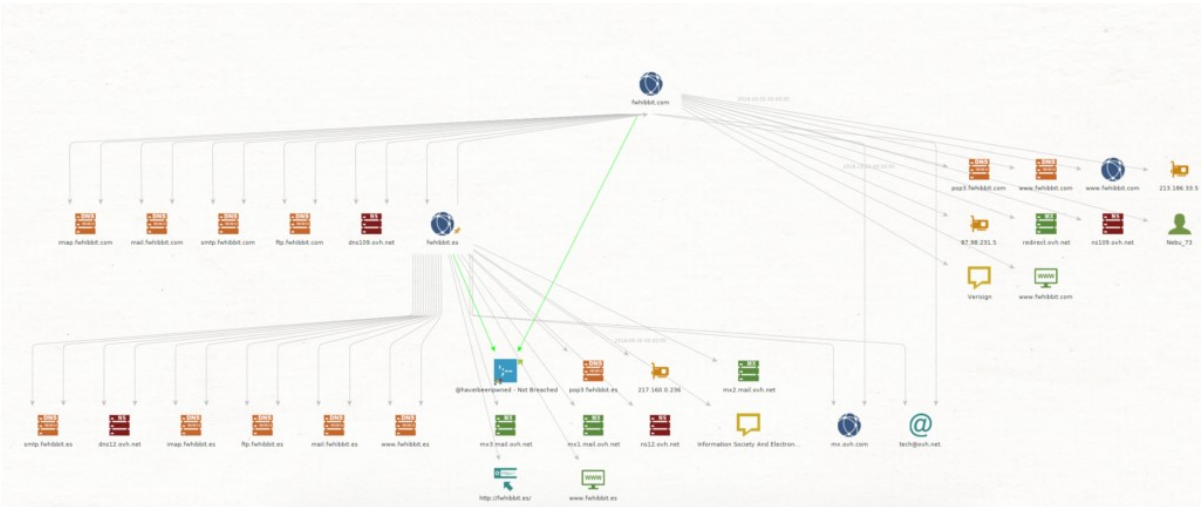
Para este ejemplo, vamos a ejecutar todas las transformadas. Dependiendo de las que tengáis instaladas y si disponéis o no de APIs para ellas, os aparecerán resultados distintos. Además, dependiendo de las transformadas que ejecutéis, os podrá pedir

cierta información al respecto.

Al ser este un ejemplo pequeño puede no haber una gran diferencia, pero si pretendéis investigar (guiño guiño) a una gran corporación, una buena configuración puede marcar la diferencia y ayudar mucho en el trabajo de análisis posterior.



Como podéis ver, rápidamente saca bastante información general sobre el dominio. En este caso nos podemos fijar que encuentra otro dominio (fwhibbit.com). Podemos investigar que información comparte con el principal volviendo a correr todas sus transformadas para así tener una imagen más global de este objetivo.



Si analizamos los datos obtenidos, podemos ver que comparten algo de información… esperad, oh no!! ¿Un conejo ha sido

conejeado? ¡¡¡Cerramos transmisión!!!

Entender esta entrada como una introducción a Maltego. En la siguientes entradas especificaremos más algunos de los módulos y transformadas, y lo relacionaremos con aplicaciones como VirusTotal, realizaremos una investigación sobre una persona física demostrando el potencial de Maltego, entenderemos como correlaciona los datos y explicaremos como recoger la información que arroja Maltego con otras aplicaciones (para lo que contaré con la colaboración de un **gran profesional** y compañero de trabajo). Además, se explicará por qué puede llegar a ser malo utilizar Maltego para un uso comercial.

Saludos conejiles!!

"*I am Ubik. Before the universe was, I am. I made the suns. I made the worlds. I created the lives and the places they inhabit; I move them here, I put them there. They go as I say, then do as I tell them. I am the word and my name is never spoken, the name which no one knows. I am called Ubik, but that is not my name. I am. I shall always be.*"

Gonx0