CASO PRÁCTICO

Enunciado

“Realizar la fase de reconocimiento o footprinting de la Web de la Universidad Alfonso X "El Sabio" para obtener toda la información posible del mismo, utilizando las técnicas de exploración pasivas”.

La web del sitio es: https://www.uax.com/

Las actividades o fases son las siguientes:

1. Estudio de las principales de las características, arquitectura, funcionalidades, uso y capacidades de las principales herramientas a utilizar en una Prueba de Penetración realizando especial hincapié en la fase de reconocimiento.

· Reconocimiento: Anubis, Spiderfoot, Maltego y Foca.

2. Determinar el alcance de las tareas y actividades de la fase de reconocimiento.

3. Obtención de información pública como información disponible de sitios web Internet Intranet, datos corporativos, webs personales de empleados, grupos de noticias, redes sociales, etc.

4. WHOIS y DNS enumeración. Búsquedas inversas.

5. DNS interrogación. Cuentas de correo.

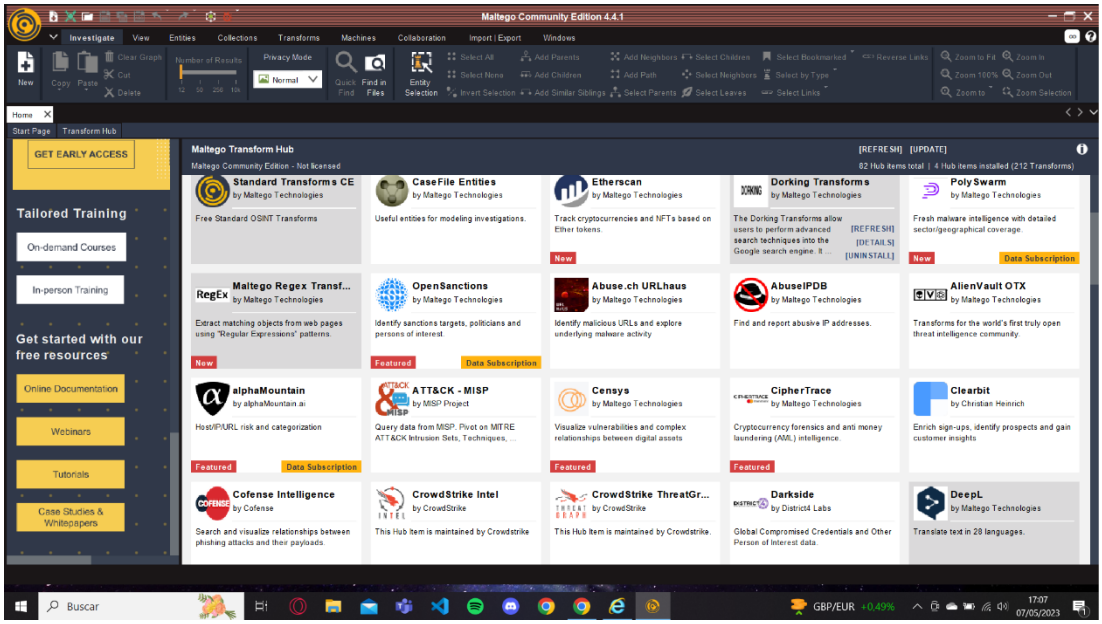
6. Reconocimiento de la red.

Resolución con Maltego

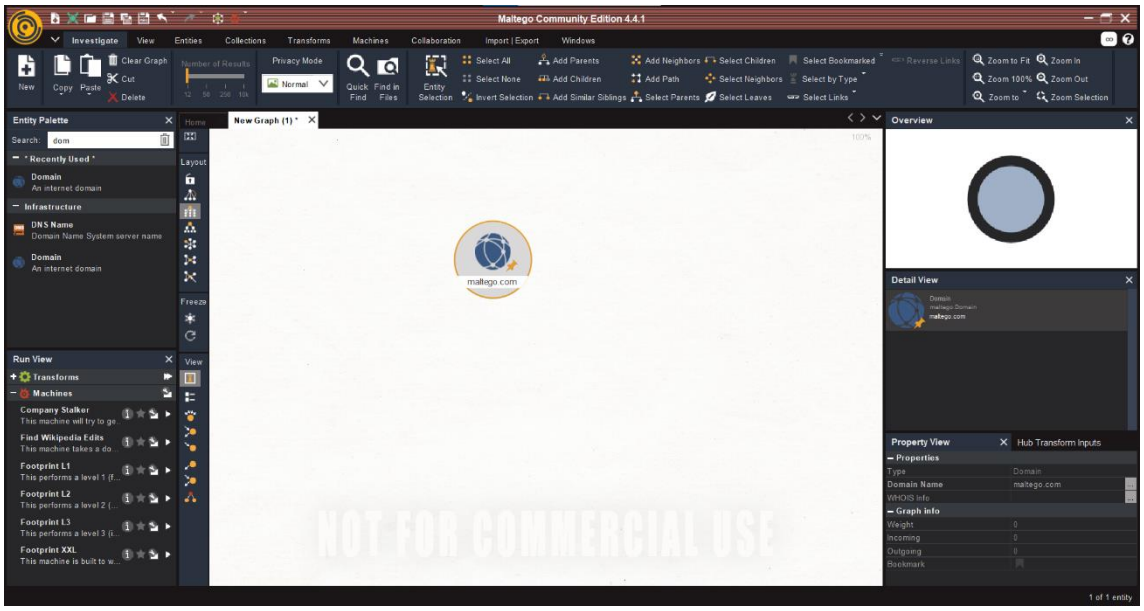
Para esta tarea de reconocimiento utilizaremos Maltego.

Maltego es una herramienta de inteligencia de código abierto que se utiliza para la recopilación y el análisis de información en línea. Permite a los usuarios realizar búsquedas en múltiples fuentes de datos públicos y privados para recopilar información sobre una entidad en particular, como una persona, una organización o un sitio web. Maltego visualiza los datos en un gráfico interactivo, lo que permite a los usuarios identificar patrones y relaciones entre las entidades. Además, Maltego cuenta con una gran cantidad de transformaciones que permiten automatizar muchas tareas de investigación.

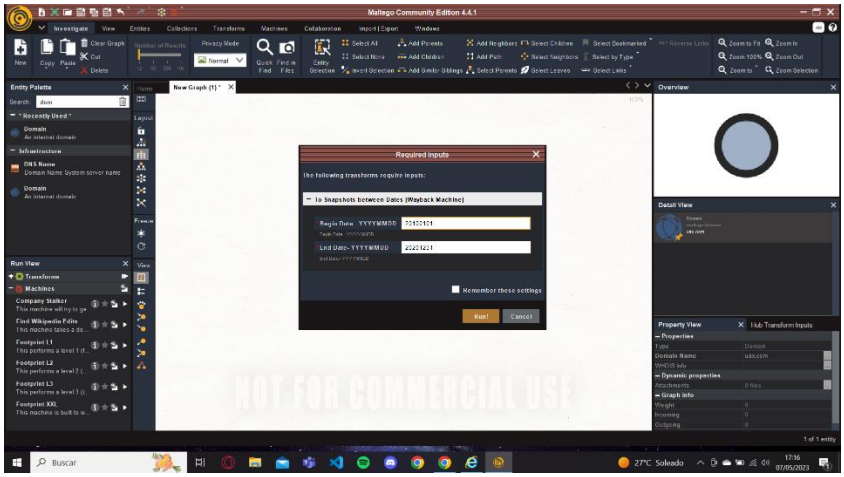
Instalaremos la versión CE por ser gratuita y tras iniciar la aplicación nos encontraremos con varias extensiones útiles para nuestra tarea.

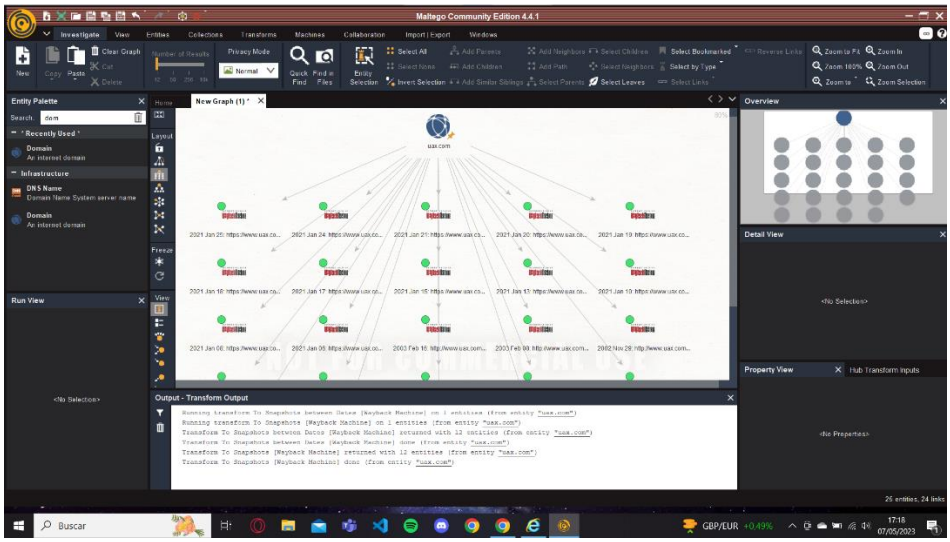


Para empezar, abriremos un script vacío en el que seleccionaremos un dominio como nodo principal, en este caso el dominio será [uax.com](uax.com)

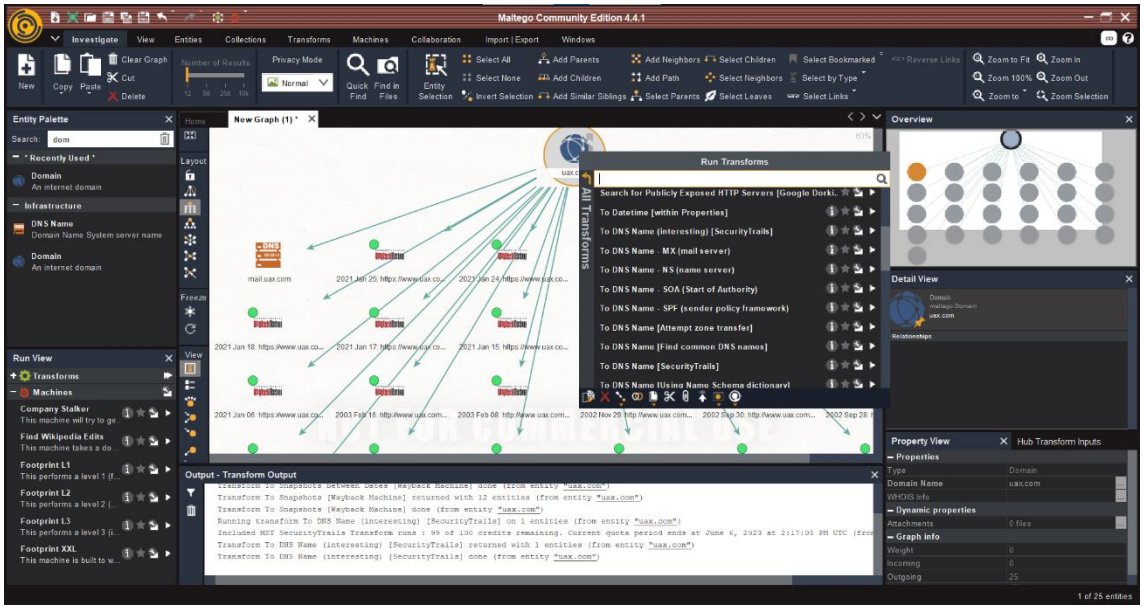


La primera transformación que haremos será con WAYBACKMACHINE la cual nos será útil para ver como ha ido evolucionando la página web de la UAX desde el 1 de enero de 2021 hasta el 31 de abril de 2023.



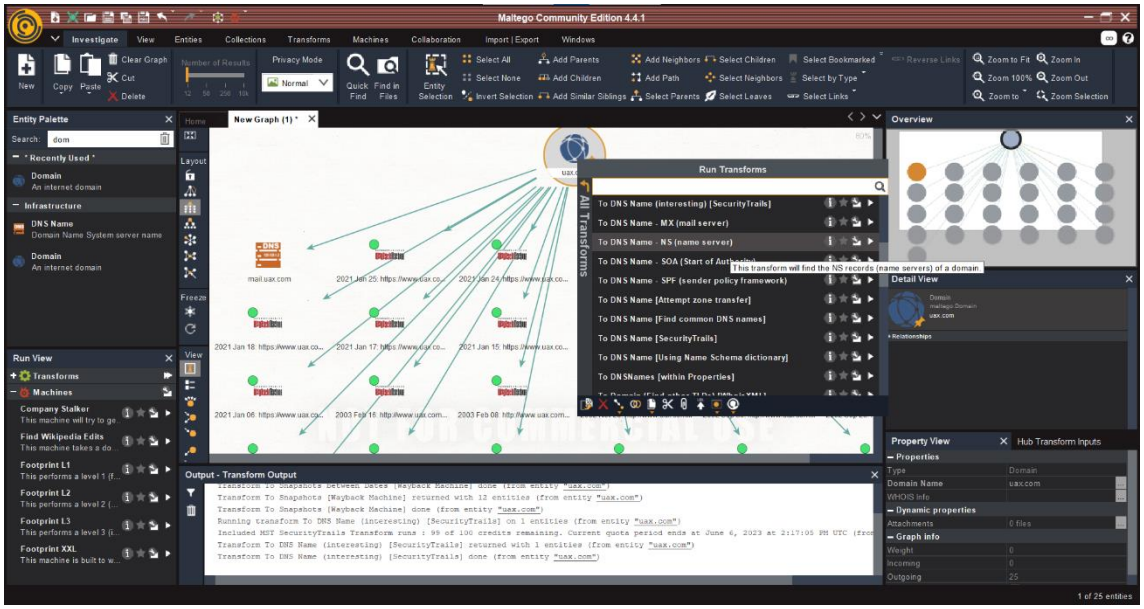


Ahora utilizaremos transformaciones del tipo To DNS Name , esta transformación nos proporcionará una lista de registros DNS asociados al dominio uax.com



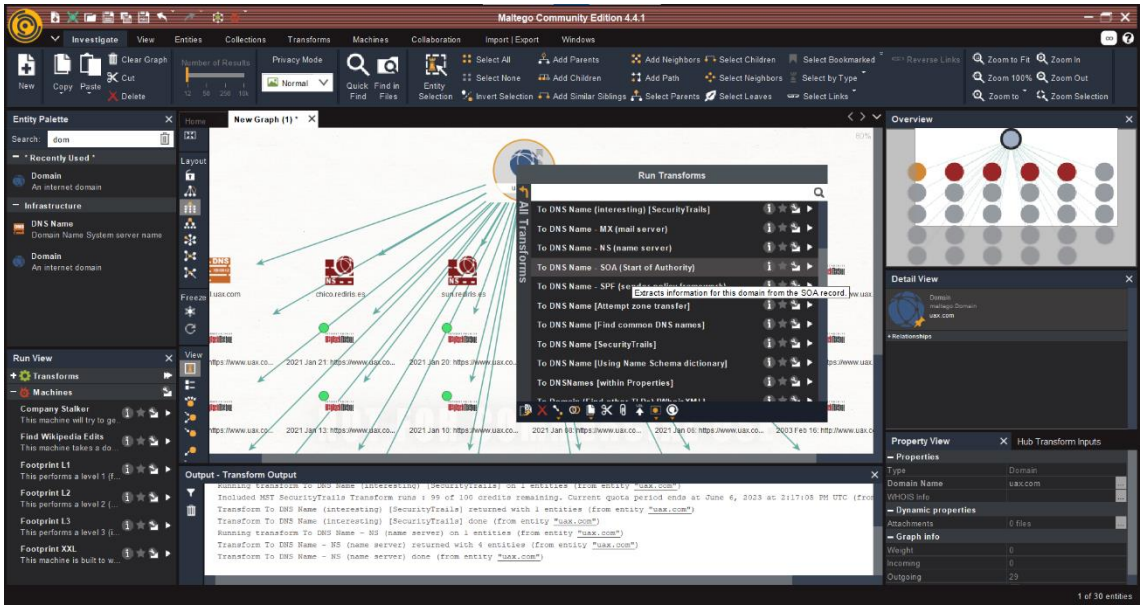
Aquí podemos ver el subdominio mail.uax.com, que se utiliza para enviar y recibir correros pero que da error al buscarlo desde nuestro navegador.

Apliquemos ahora otra transformación: To DNS Name – NS



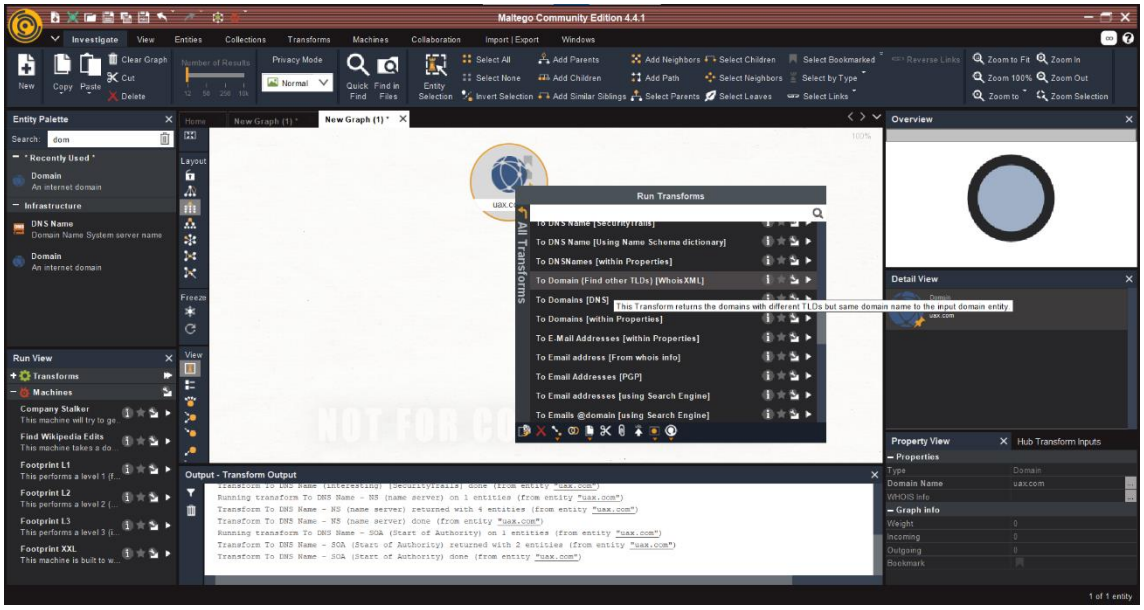
Estos nuevos dominios no nos aportan ninguna información relevante. También puede ser que estén protegidos por firewall que no nos permitan acceder.

Procederemos ahora con la transformación To DNS Name - SOA

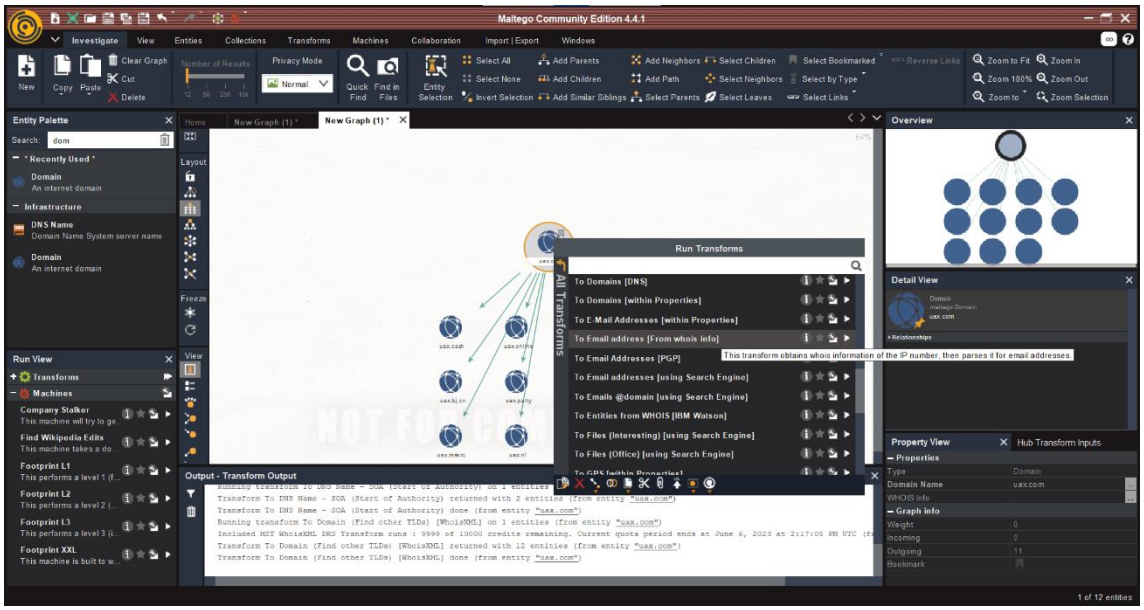


Hemos obtenido la dirección de correo postmaster@uax.es, utilizada para recibir informes de problemas con el correo electrónico.

En un nuevo script utilizaremos ahora la transformación To Domain:

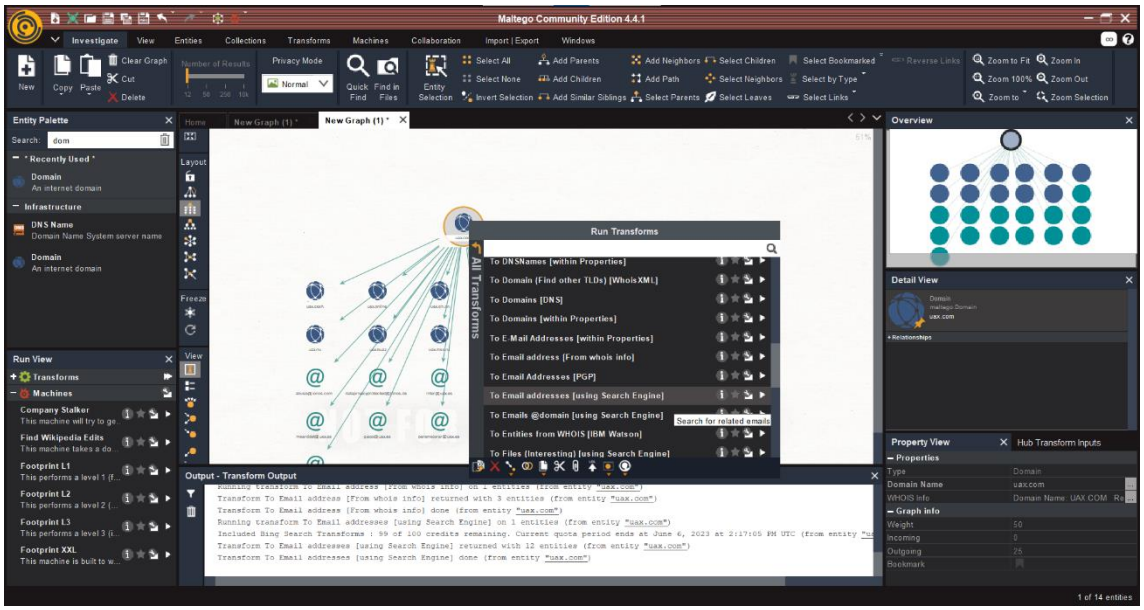


Aplicaremos ahora la transformación (Find other TDLs) [WhoisXML] que nos devuelve otros dominios con diferentes extensiones



Pero ninguno de estos dominios parece estar relacionado con la UAX por lo que deducimos que ninguno esta siendo utilizado con fines maliciosos del tipo phishing.

Ahora aplicaremos la transformación To emails



Esta transformación obtiene direcciones de correo asociada al dominio a partir de la información obtenida de únicamente de la base de datos WHOIS

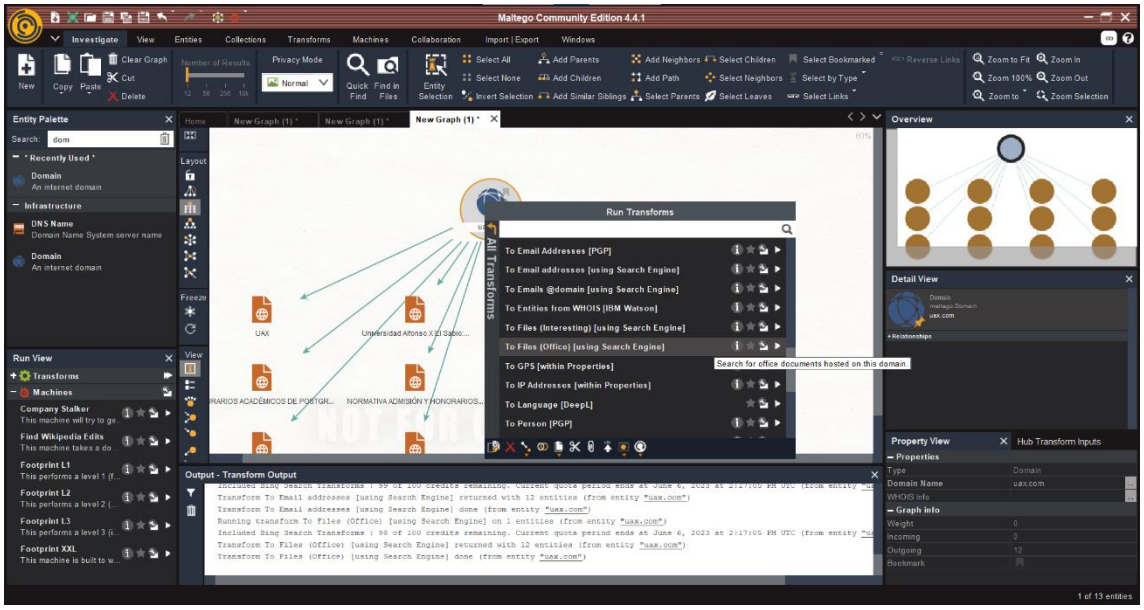
WHOIS

WHOIS es un protocolo de red utilizado para obtener información sobre los propietarios de nombres de dominio, direcciones IP y otros recursos de Internet. Esencialmente, WHOIS es una base de datos pública que contiene información sobre el registro de un nombre de dominio o dirección IP, incluyendo información de contacto del propietario, la fecha de registro, la fecha de vencimiento, el servidor de nombres, y más.

Al usar el protocolo WHOIS, los usuarios pueden realizar consultas en la base de datos y obtener información sobre un nombre de dominio o dirección IP en particular. Esta información puede ser útil para determinar la propiedad de un sitio web, identificar a los propietarios de un dominio en disputa, o incluso para identificar a los posibles responsables de actividades maliciosas en línea.

Sin embargo, es importante tener en cuenta que la información proporcionada por WHOIS puede variar según la región geográfica y las políticas de privacidad locales. Algunos registradores de nombres de dominio pueden ofrecer servicios de privacidad que ocultan la información de contacto del propietario, lo que hace que sea más difícil obtener información precisa a través de WHOIS.

Ahora procederemos a utilizar To Files, donde encontraremos dos transformaciones. Nos interesará la segunda



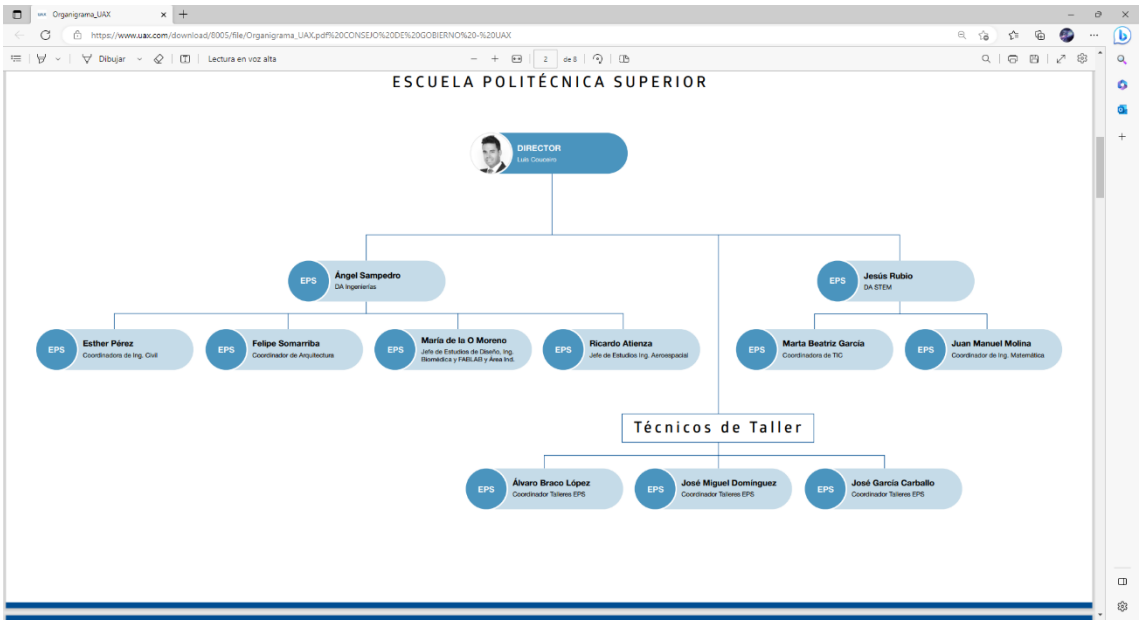
Vamos a proceder a un breve análisis de estos documentos:

- UAX: Información sobre el Máster en ingeniería aeronáutica.
- Calendario: Calendario académico. Aquí nos encontramos con los días lectivos y los de vacaciones.
- CAMPUS: Mapa del campus.
- Página no encontrada - UAX: El siguiente archivo ya no existe, es probable que en algún momento haya sido eliminado de la web.
- HONORARIOS: Coste de todos los postgrados de la universidad, incluyendo información sobre la matriculación, financiación y plan de ayudas.
- HONORARIOS: Este segundo pdf informativo es igual que el anterior solo que la información es sobre los grados online en vez de los postgrados.
- Uax: Este archivo word es una plantilla para una solicitud de ayuda para postgrado ESAME.
- HONORARIOS: Para grados presenciales.
- Calendario: Calendario académico del pasado año.
- EUROPEAN: Información sobre los intercambios académicos de la universidad (Generalmente ERASMUS).

- CONSEJO: Altos cargos de la universidad.

Este último pdf resulta el más interesante de todos los vistos para conocer a los responsables de la gestión y organización visible de la universidad.

Estos son los de nuestra escuela politécnica



Ahora utilizaremos To Phone Numbers

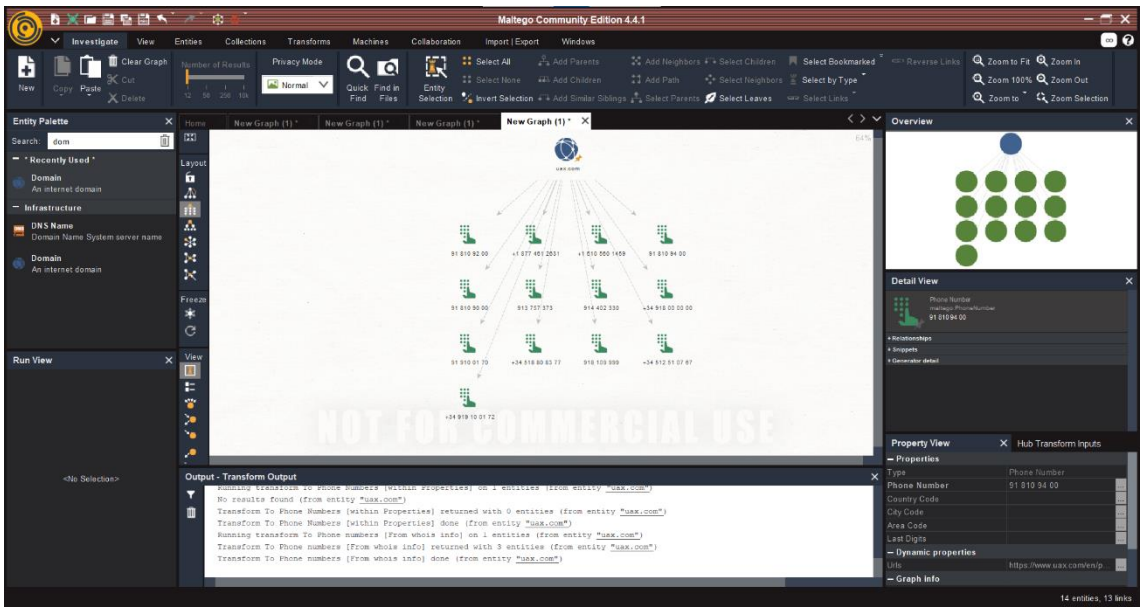
Buscando en la base de datos Whois:

- +1 877 461 2631: El prefijo +18 suele corresponderse con la región de Hawai.
- +1 610 560 1459: Este prefijo (+16), se puede corresponder a varias regiones ya que actualmente no se corresponde con ninguna región en específico.

Utilizando ingeniería de búsqueda:

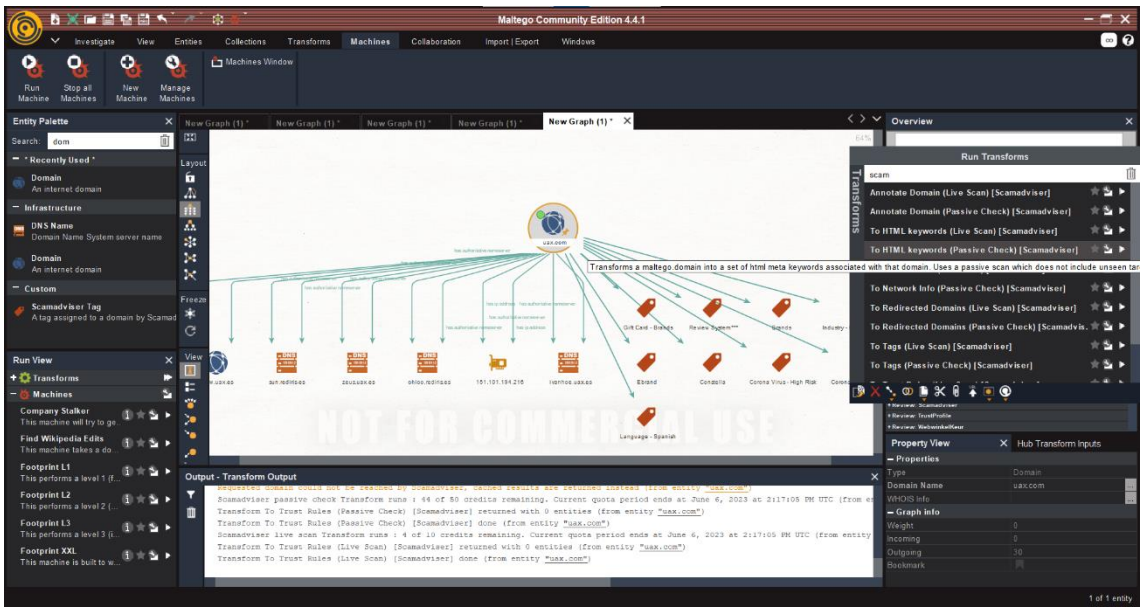
- 91 810 92 00
- +34 512 51 07 67
- 914 402 330
- +34 919 10 01 72
- 918 109 999
- +34 918 00 00 00

- 91 810 90 00
- 91 810 92 00
- 913 757 373



Los números de teléfono si suponen un riesgo potencial ya que presentan riesgos de spam, phishing o ataques de fuerza bruta.

Ahora vamos a utilizar Scamadviser, una herramienta en línea que permite verificar la confiabilidad de un sitio web. Utiliza una variedad de fuentes de datos públicos y privados para calcular una puntuación de confianza para un sitio web en particular. Esta puntuación se basa en la edad del sitio, la ubicación del servidor, la información de contacto disponible, la presencia de opiniones y comentarios de los usuarios, y otros factores relevantes para evaluar la legitimidad de un sitio web.



Además de ver los DNS y la IP asociada con el dominio que ya vimos con anterioridad, se nos muestran etiquetas bastante interesantes que nos aportan información muy valiosa. Vamos a ir analizándolas una a una:

- Como con todas las transformaciones ofrecemos un report además del grafo exportado como una XML.
- Industry - Essay/Thesis/Dissertation Writers – High Risk: Esta etiqueta indica que el sitio web está relacionado con servicios de escritura de tesis, ensayos o disertaciones, y que según los criterios de IPQS, es un sector de alto riesgo. Esto podría indicar que el sitio web está asociado con estafas académicas o académicos poco éticos.
- Corona - Vaccin Suppliers: Esta etiqueta indica que el sitio web está relacionado con proveedores de vacunas para el COVID-19.
- Gift Card - Brands: Esta etiqueta indica que el sitio web está relacionado con la venta o promoción de tarjetas de regalo de marcas específicas. La venta de tarjetas de regalo es una práctica común en el comercio en línea, pero también puede ser utilizada por estafadores para obtener información personal o financiera.
- Ebrand: Esta etiqueta no es muy descriptiva, pero podría indicar que el sitio web está relacionado con la creación o promoción de marcas en línea.
- Language - Spanish: Esta etiqueta indica que el idioma principal del sitio web es el español.
- Review System: Esta etiqueta indica que el sitio web tiene algún tipo de sistema de revisión o calificación para productos, servicios o experiencias.
- Constella: Esta etiqueta no es muy descriptiva, pero podría indicar que el sitio web está relacionado con algún tipo de servicio o producto llamado Constella.
- Brands: Esta etiqueta indica que el sitio web está relacionado con marcas o promoción de marcas.
- Corona Virus - High Risk: Esta etiqueta indica que el sitio web está relacionado con información o productos relacionados con el COVID-19 y, según los criterios de IPQS, se considera de alto riesgo. Es importante tener precaución al interactuar con sitios web relacionados con el COVID-19, ya que pueden ser utilizados por estafadores para obtener información personal o financiera.

FOOTPRINTING

Esta maquina ofrece tres niveles en su versión gratuita en función de tus necesidades:

- L1 para un nivel básico y rápido
- L2 para un nivel medio
- L3 para un nivel intensivo que requiere de tiempo y recursos

Este es el reporte del nivel 1: