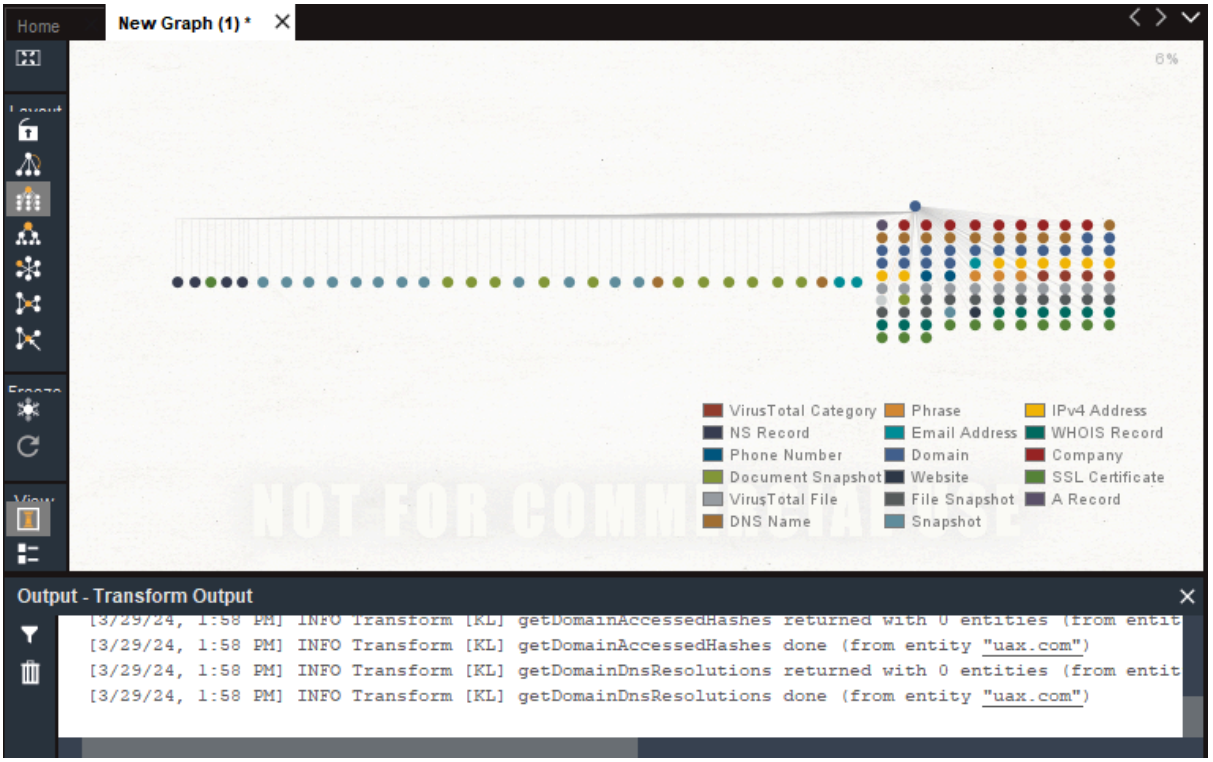
TRABAJO MALTEGO

Maltego es una herramienta avanzada de recolección de información y análisis de datos utilizada para la investigación de seguridad cibernética y la inteligencia de fuentes abiertas. Maltego utiliza transformaciones para buscar datos como y luego presenta esos datos en un formato de grafo, mostrando las conexiones entre ellos.

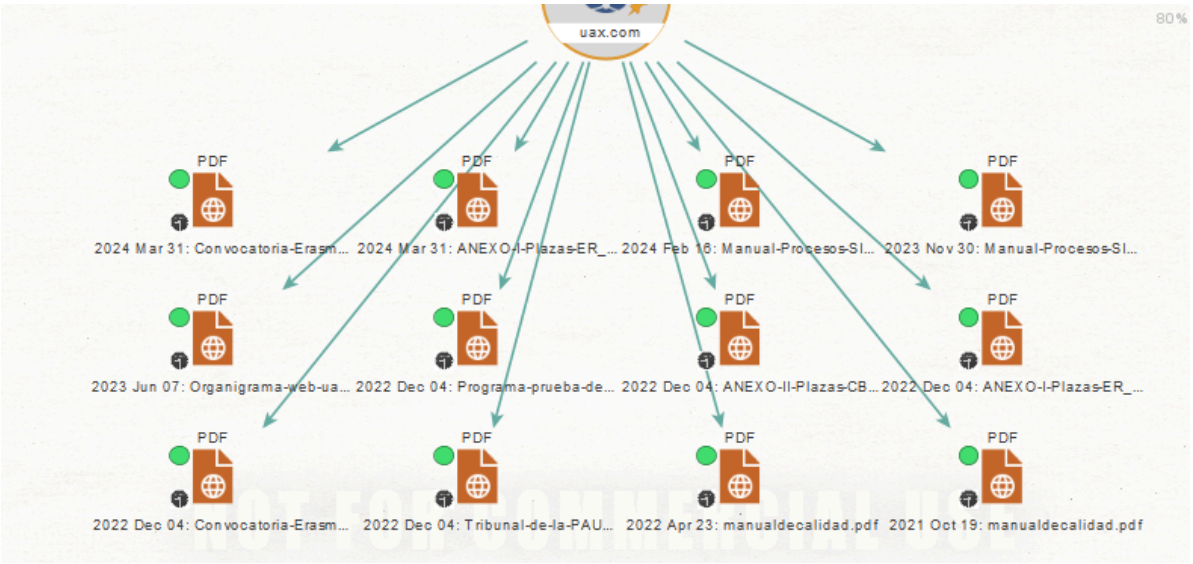
El objetivo principal de esta tarea es aplicar las transformaciones óptimas para sacar información de interés acerca de la web de la UAX, demostrando dominio sobre esta herramienta de trabajo.

Para empezar con el trabajo en cuestión, se han aplicado todas las transformaciones a nuestro alcance empleando el comando All transforms. De esta forma se aplican todas las transformaciones posibles sobre la web “uax.com”. Cabe destacar que esta no es una práctica recomendada bajo ningún concepto, pero nos sirve para saber qué potencial tenemos al inspeccionar determinado elemento y qué caminos podemos tomar en el análisis.



A continuación, se enumerarán algunas transformaciones más específicas que se han utilizado para inspeccionar la web en cuestión:

1. **To Snapshots of Files (Extensions) [Wayback Machine]**



Esta transformación busca capturas de versiones antiguas de archivos, basándose en sus extensiones, en la Wayback Machine de Internet Archive.

Algunos pdf que podemos usar para obtener información interesante son los siguientes:

- Convocatoria erasmus:

https://www.uax.com/download/10131/file/ANEXO-I-Plazas-ER_23-24.pdf

UAX
UNIVERSIDAD ALFONSO X EL SABIO

Erasmus+

1

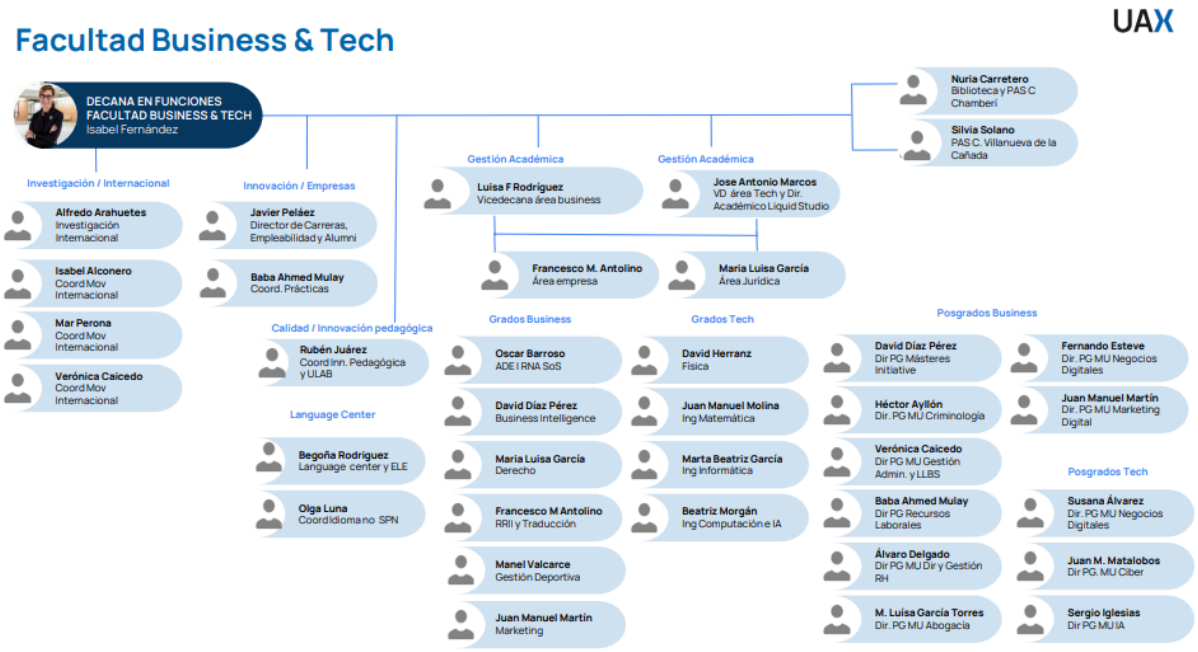
CONVOCATORIA PROGRAMA ERASMUS+ 2023-24

Relación de plazas convocadas por la Oficina de Relaciones Internacionales de la Universidad Alfonso X el Sabio.
El plazo de solicitud será del 21 de noviembre de 2022 al 31 de enero de 2023.

FACULTAD DE ESTUDIOS SOCIALES Y LENGUAS APLICADAS		
EMPRESAS Y MARKETING	**PLAZAS**	**MESES**
Alemania		
Karlsruhe- Karlshochschule International University*	2	9
Schmalkalden - Fachhochschule Schmalkalden	1	5
Siegen – Universitäta Siegen	2	5
Austria		
St. Pölten -St. Pölten Unversity of Applied Sciences *	2	5
Bélgica		
Bruxelles – ICHEC Bussels Management School	3	5
Bruxelles – Haute Ecole Ichec - Ecam - Isfsc	3	5
Liège – Haute École de la Province de Liège*	4	12
Dinamarca		
Aalborg – Aalborg Universitet * - Requiere TOEFL	2	5
Francia		
Cholet - École de Commerce, Management International - ESIAME	2	9

- Profesorado:

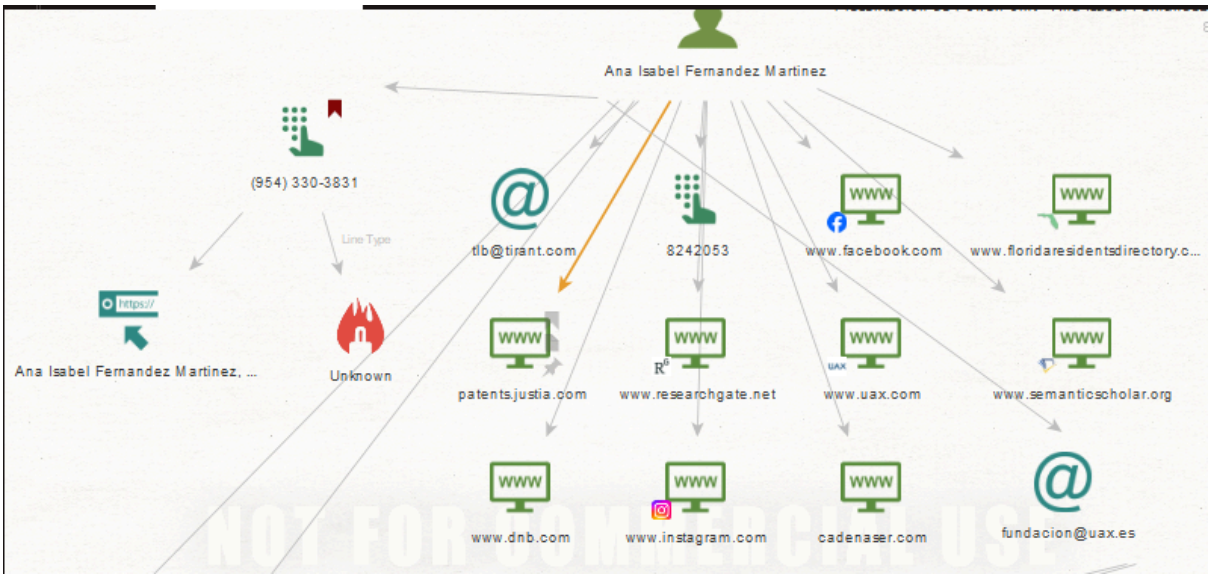
https://www.uax.com/download/10102/file/Organigrama-web-uax.pdf



De este pdf del organigrama aplicando todas las transformadas podemos obtener:

En esta parte del gráfico podemos encontrar la compañía ULAB, o nombres importantes de la universidad como bien puede ser el nombre de la rectora: Ana Isabel Fernández Martinez.

Aplicando alguna transformada más conseguimos:



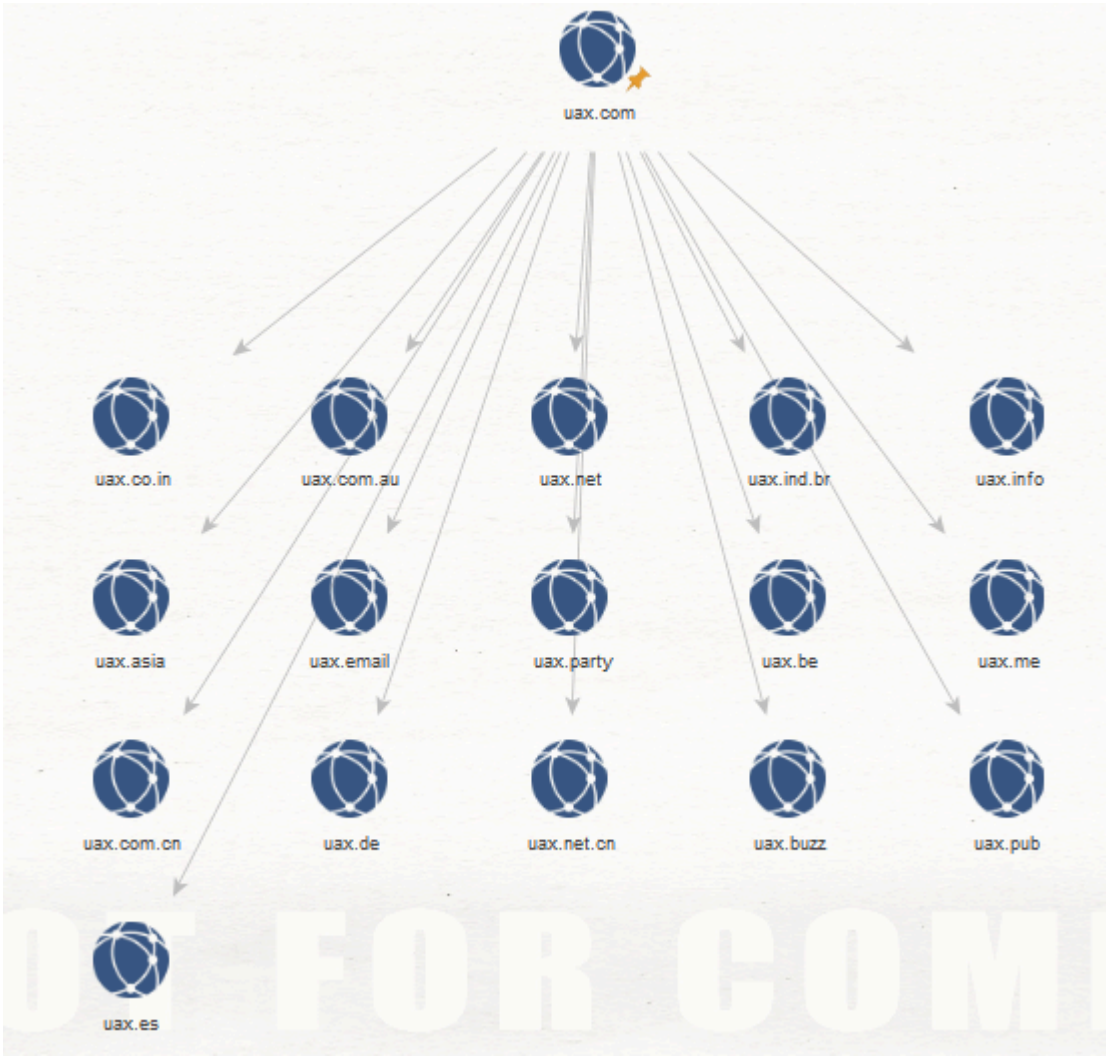
- Un número de teléfono asociado a su nombre el cuál pertenece a la página https://www.floridaresidentsdirectory.com. Esta página nos da datos como su edad pero nos podemos dar cuenta de que se trata de otra persona que se llama igual que ella.

-Sus redes sociales tanto de facebook, instagram…

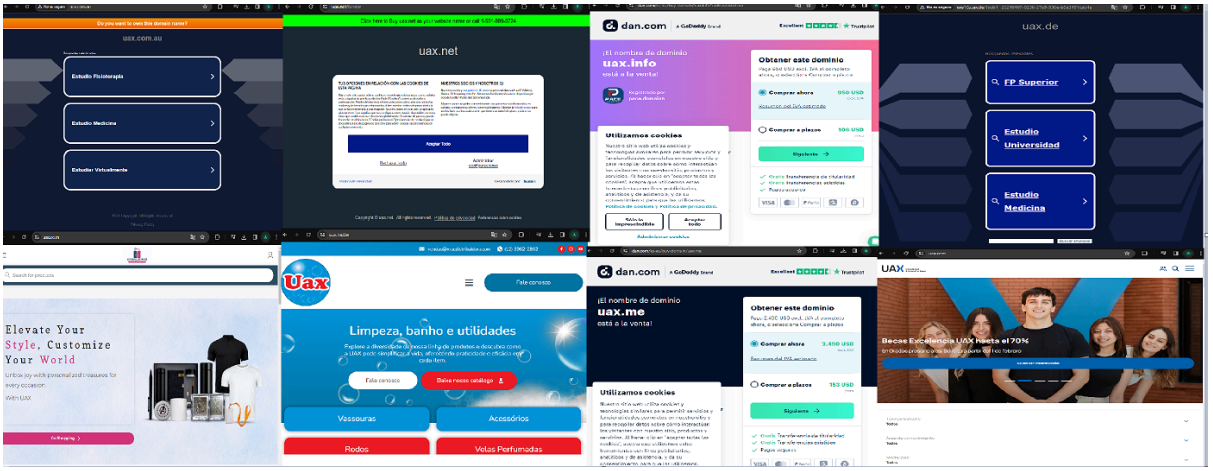
-Un correo llamado fundacion@uax.es el cual pertenece a la fundación de la UAX, creada para impulsar las actividades de carácter científico, cultural y de interés social.

2. **To Domain**

Como con los DNS, también tenemos una gran variedad de transformadas relacionadas con los Dominios, la transformada con la que he recibido más resultados ha sido **To Domain (Find other TLDs) [WhoisXML]**. Esta transformación busca otros dominios de nivel superior (TLD) relacionados con el nombre de dominio objetivo, utilizando el servicio WhoisXML.:

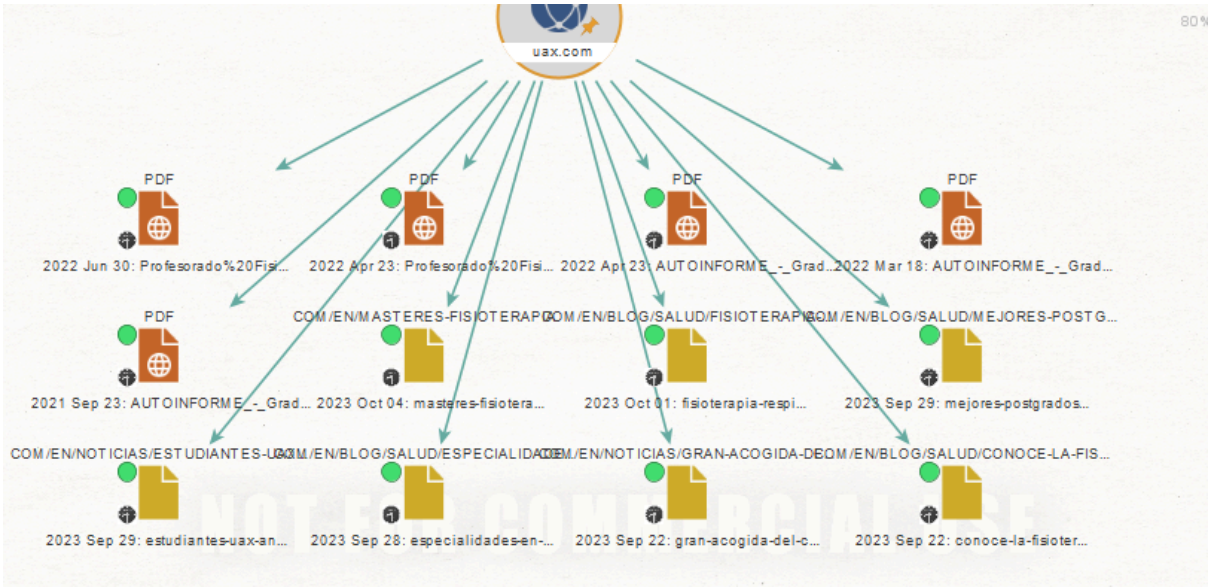


Algunas de las webs mostradas parece ser que no ya no existen ya que no se nos permite acceder a estos sitios web. Estas son: uax.email, uax.party, uax.be, uax.com.cn, uax.net.cn, uax.buzz y uax.pub. Sin embargo, algunas sí que se nos muestran.



Como podemos observar el único relacionado con la UAX es uax.es el cual nos redirigirá a uax.com.

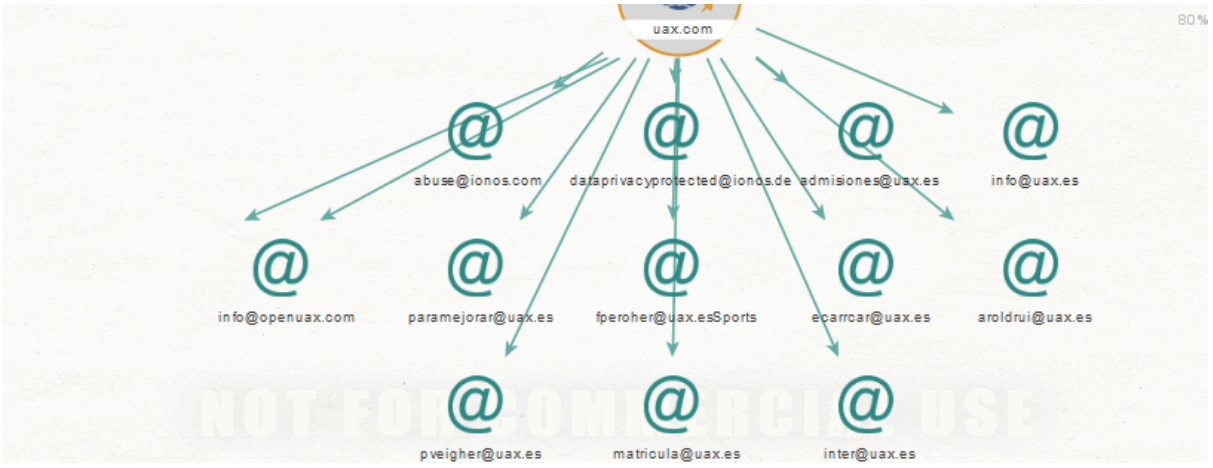
3. **To Snapshots Containing Phrase [Wayback Machine]**



Esta transformación encuentra capturas de páginas web en la Wayback Machine que contienen una frase específica.

Aquí podemos ver información sobre el grado en fisioterapia, lo cual no nos resulta demasiado interesante de analizar.

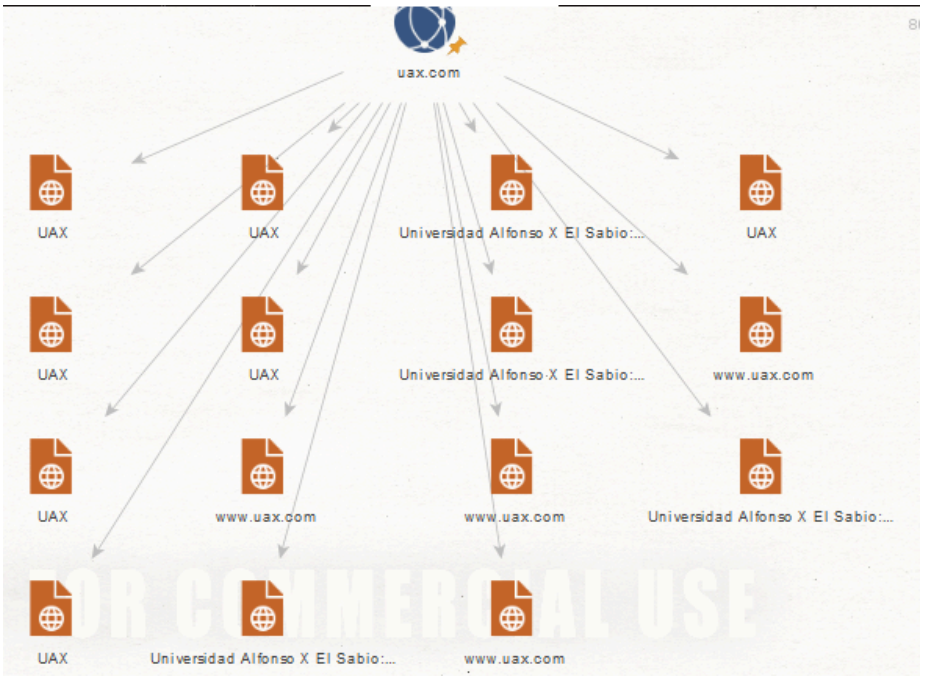
4. **To email**



Esta transformación identifica direcciones de correo electrónico relacionadas con el objetivo o entidad analizada.

Tal y como se muestra en el nombre de la transformación, esta resulta en distintos correos interesantes como el de admisiones, información de la universidad, información de los “Open Day” o el de las matrículas.

5. **To Files (Office) [using Search Engine]**

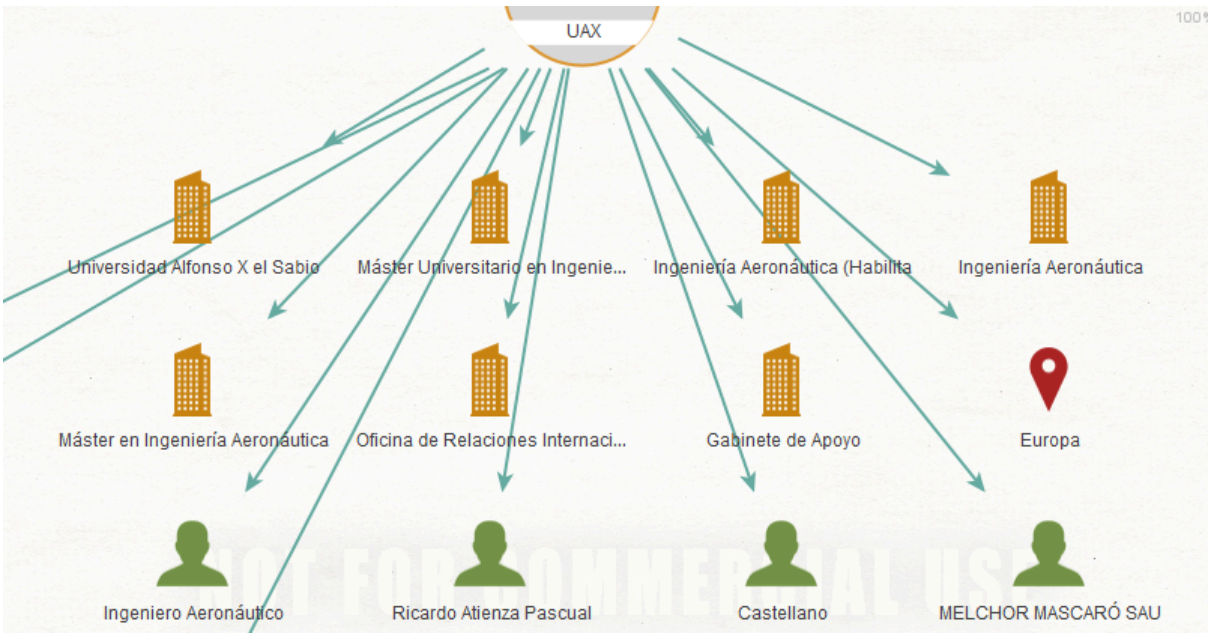


De esta forma se buscan archivos de Office (como documentos de Word, hojas de cálculo de Excel y presentaciones de PowerPoint) relacionados con uax.com, utilizando un motor de búsqueda.

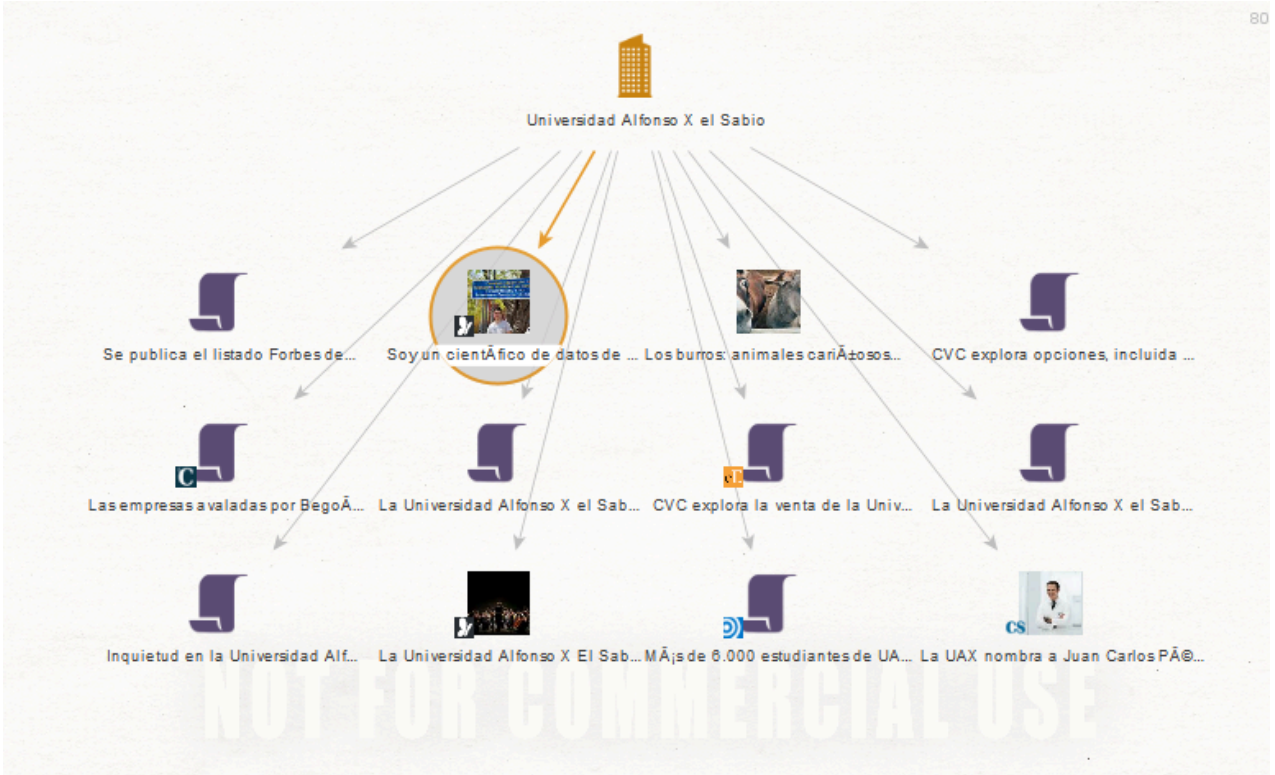
Los resultados más relevantes son:

- Un word con información sobre el máster de ingeniería aeronáutica y otro de psicología.
- Un word con las competencias básicas del grado en ingeniería electrónica industrial y automática, otro del grado de mecánica.
- información relevante sobre otros grados y de la universidad.

Si profundizamos en el máster de ingeniería aeronáutica podemos obtener la siguiente información:



En la cual obtenemos las compañías registradas dentro del máster, y profesorado del máster.
Si nos enfocamos en la compañia de la UAX y le aplicamos transformadas para sacar artículos interesantes, podemos encontrar el siguiente grafo:



El cual nos proporciona artículos interesantes como bien puede ser:

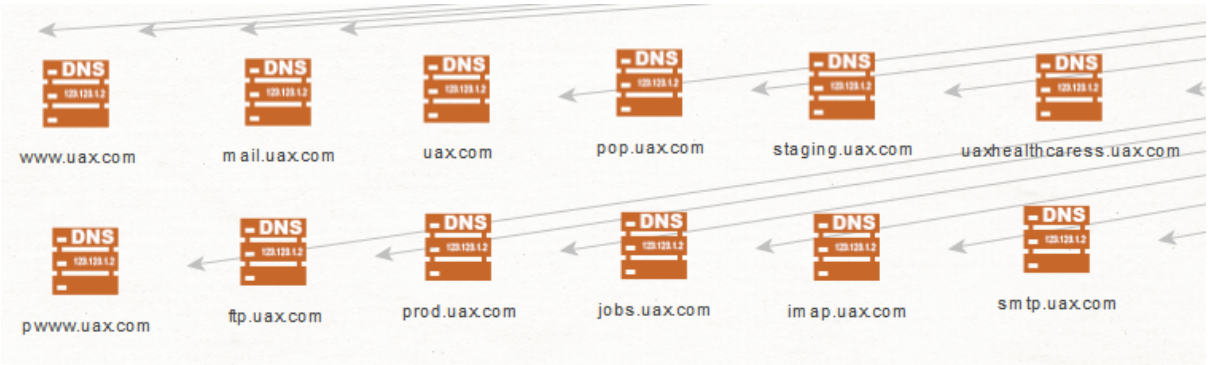
- La intención de CVC de vender parte de sus acciones de la UAX.
- La UAX impulsa la innovación con el Avanade PocketLab.
- La UAX se encuentra en el listado de Forbes de las 10 universidades más innovadoras de España.

6. **To DNS**

El DNS, o Sistema de Nombres de Dominio, es una tecnología clave de internet que traduce nombres de dominio fácilmente legibles por humanos (como "ejemplo.com") a direcciones IP numéricas que las computadoras utilizan para comunicarse entre sí. Maltego puede utilizar datos de DNS para ayudar en la investigación de seguridad cibernética, como el rastreo de la infraestructura de red de una entidad sospechosa, al revelar cómo diferentes nombres de dominio se conectan a ciertas direcciones IP, ayudando a desenmascarar redes de phishing, malware, o infraestructuras de comando y control.

Maltego nos ofrece distintas transformadas relacionadas con los DNS, como por ejemplo: **To DNS Name [Enumerate Hostname numerically]** , **To DNSNames [within Properties]**, **To Domain [DNS]** , **To IP Address [DNS]**... las cuales a pesar de que apliquemos no obtendremos ninguna información relevante, pero aún así podemos mirar analizar brevemente lo que obtenemos.

Partiendo del dominio web de la uax, podemos aplicar la transformada **DNS Name**. Esta transformación identifica los nombres de dominio del Sistema de Nombres de Dominio (DNS) asociados con la entidad objetivo.

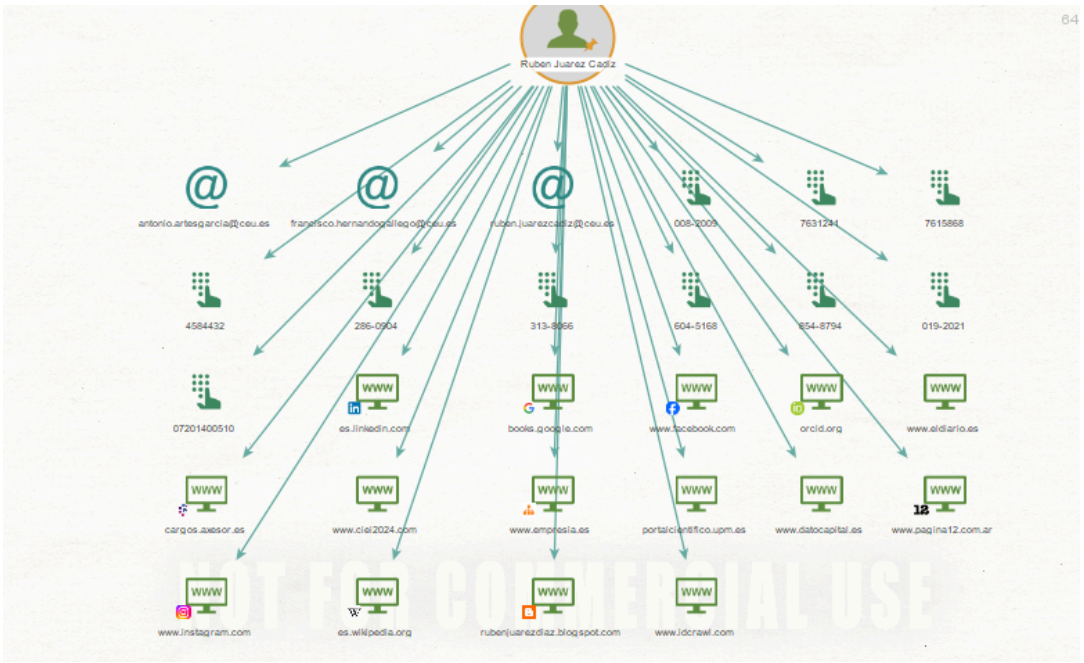


No encontraremos nada si buscamos en Internet estos registros de DNS.

Con otra transformada que obtendremos algo será con **To DNS Name - SOA(Start of Authority)**. Esta transformación encuentra el registro SOA (Start of Authority), que proporciona información sobre la zona DNS principal para el nombre de dominio objetivo.

Como podemos ver, hemos obtenido el correo postmaster@uax.es.

Finalmente, aplicando transformaciones parecidas a las usadas en el perfil de la decana, vamos a ver que nos ofrece el perfil de Rubén Juárez Cádiz, profesor que hemos encontrado en el organigrama también, en la facultad de Business and Tech:



Encontramos:

- Algunos correos pertenecientes a la universidad CEU, uno de ellos el suyo personal.
- Algunos números de teléfono que no parecen ser de gran utilidad.
- Algunas redes sociales como bien puede ser FaceBook o Instagram.
- Algunas web en las que tiene cuenta como puede ser linkedin, portal científico…
- Un Blog personal que no nos ofrece mucha información relevante.

Conclusiones

Maltego se erige como una herramienta fundamental para los profesionales en el ámbito de la ciberseguridad, gracias a su excepcional capacidad para recabar y examinar vastas cantidades de información. Esta capacidad la convierte en una herramienta esencial para la inteligencia sobre amenazas, la gestión de incidentes, entre otras aplicaciones críticas.

El análisis presentado en este trabajo apenas es la punta del iceberg de lo que Maltego ofrece. La razón de esta limitación radica en que, para explotar plenamente las capacidades de Maltego, es necesario invertir tanto en el coste asociado a su uso como en superar una curva de aprendizaje significativa. No obstante, los beneficios que aporta Maltego compensan ampliamente estos inconvenientes. Entre sus ventajas más notables se encuentra su intuitiva disposición de los datos en un formato de grafo, así como la aplicación lógica de diversas transformaciones para analizar los datos, lo cual subraya su valor inestimable para la ciberseguridad.