

CASO PRÁCTICO: Expedición Digital: Navegando por el Ciberespacio de la Universidad Alfonso X

Introducción a la Aventura: Embárcate en la "Expedición Digital", una misión de inteligencia cibernética donde desentrañarás los secretos ocultos de la Universidad Alfonso X "El Sabio". Con herramientas de vanguardia y técnicas de exploración pasiva, tu tarea es navegar por el ciberespacio de <https://www.uax.com/> y extraer tesoros de información ocultos en la vastedad digital. ¡Prepárate para una odisea de conocimiento y descubrimiento!

1. SpiderFoot: El Rastreador Cibernético

Instalación:

Accede a la última versión en GitHub de SpiderFoot.

Clona el repositorio: `git clone https://github.com/smicallef/spiderfoot.git`.

Instala las dependencias: `cd spiderfoot && pip3 install -r requirements.txt`.

Ejecución:

Inicia SpiderFoot: `python3 sf.py -l 127.0.0.1:5001`.

Accede a la interfaz web en tu navegador: `http://127.0.0.1:5001`.

2. Anubis: El Descifrador de Subdominios

Instalación y Uso:

Visita la página de Anubis en GitHub para obtener la última versión.

Instalación vía pip: `pip3 install anubis-netsec`.

Ejecuta Anubis en la terminal: `anubis -t www.uax.com`.

3. FOCA: El Explorador de Metadatos

Instalación:

Descarga FOCA desde ElevenPaths.

Sigue las instrucciones de instalación proporcionadas en el sitio.

Ejecución:

Inicia FOCA y crea un nuevo proyecto apuntando a la URL de la Universidad.

Deja que FOCA analice y recolecte metadatos.

4. Maltego: La Red de Inteligencia Visual

Regístrate y descarga Maltego desde el sitio oficial.

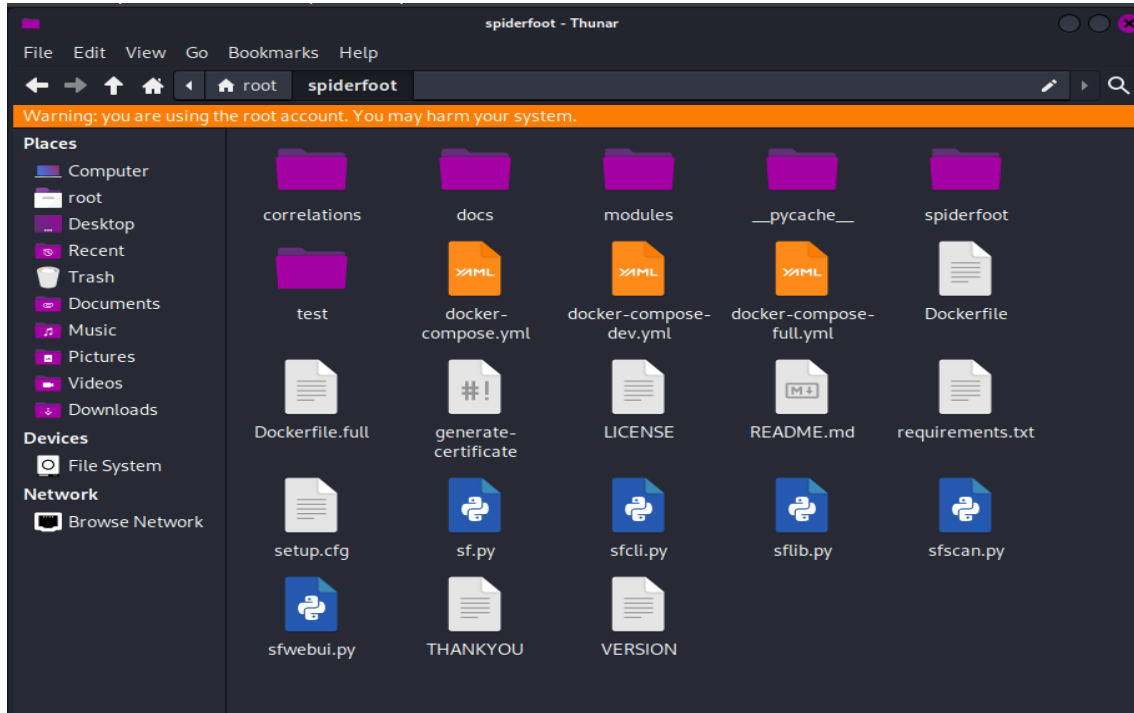
Ejecución:

Abre Maltego, configura tu cuenta y selecciona las transformaciones a usar.

Comienza tu investigación ingresando la URL o cualquier otro punto de interés.

- **Spiderfoot**

Comenzamos descargando Spiderfoot en nuestro Kali Linux:



Una vez descargado ejecutamos Spiderfoot en local:

```
Successfully installed ExifRead-2.3.2 Mako-1.3.2 PyPDF2-1.28.6 cryptography-3.4.8 ipaddr-2.2.0 ipwhois-1.1.0 networkx-2.6.3 phonenumbers-8.13.34 pyOpenSSL-21.0.0 python-docx-0.8.11 python-pptx-0.6.23 python-whois-0.7.3
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

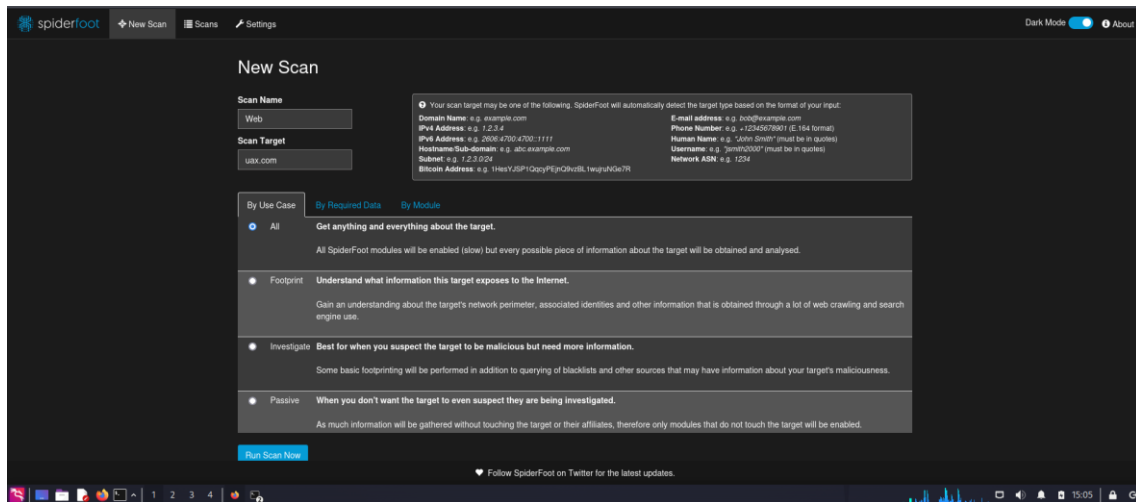
(root@kali)-[~/spiderfoot]
# python3 sf.py -l 127.0.0.1:5001

*****
2024-04-06 17:18:14,708 [INFO] sf : Starting web server at 127.0.0.1:5001 ..
.
2024-04-06 17:18:14,708 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****

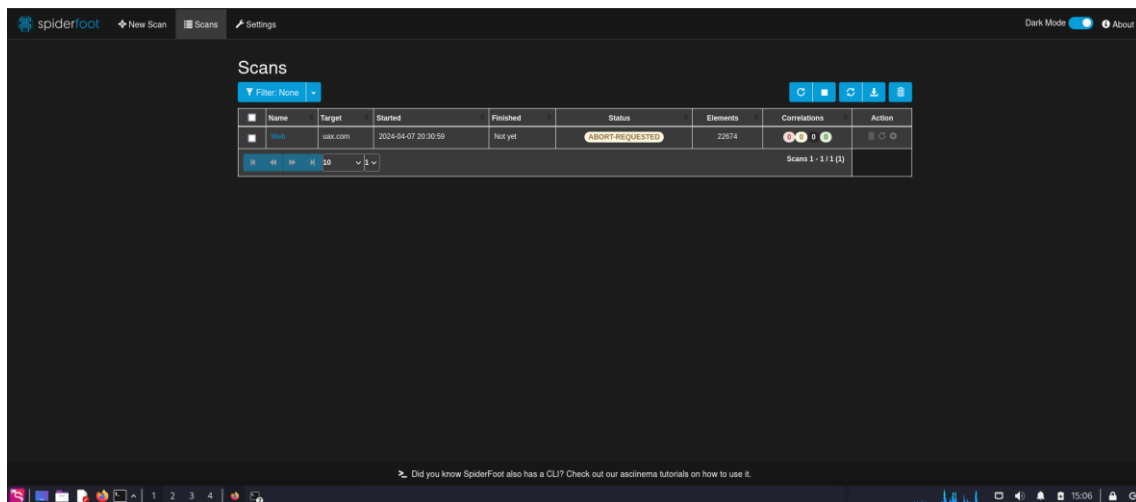
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/
*****
```

Una vez dentro tenemos que especificar que vamos a trabajar con la URL de la web, en este caso uax.com

Diego de Santos del Río NP: 138996
Javier Miguélez Yagüe NP: 138571



Pasadas 4 horas completamos el escáner:

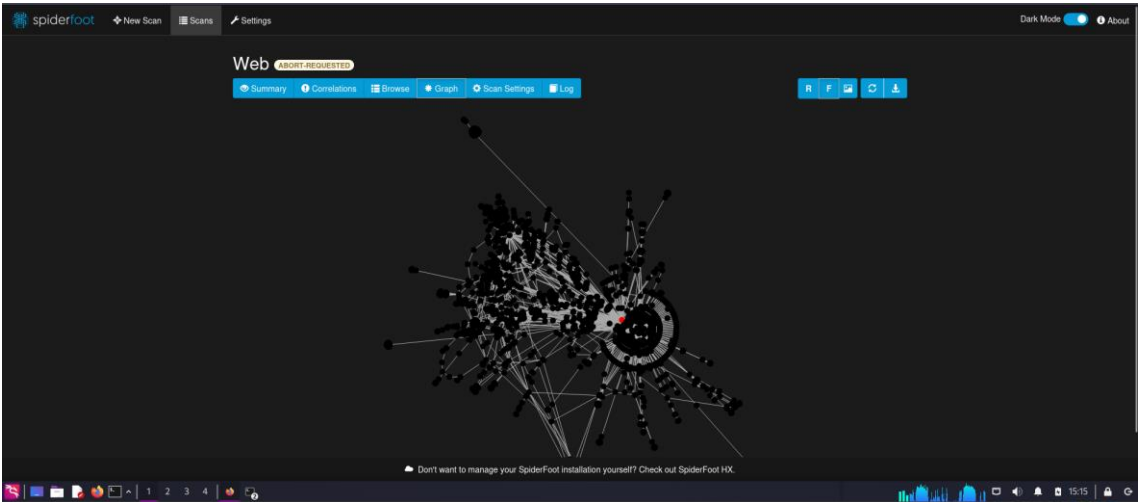


Dentro podemos observar la cantidad de datos únicos en los diferentes parámetros con los que trabaja Spiderfoot, desde URLs pasando por emails hasta subdominios y protocolos.



Podemos ver cómo están relacionados los datos en el apartado de grafos

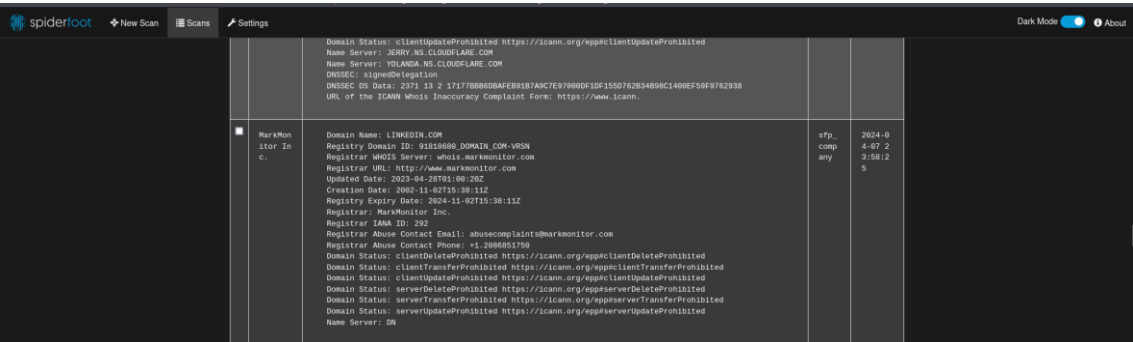
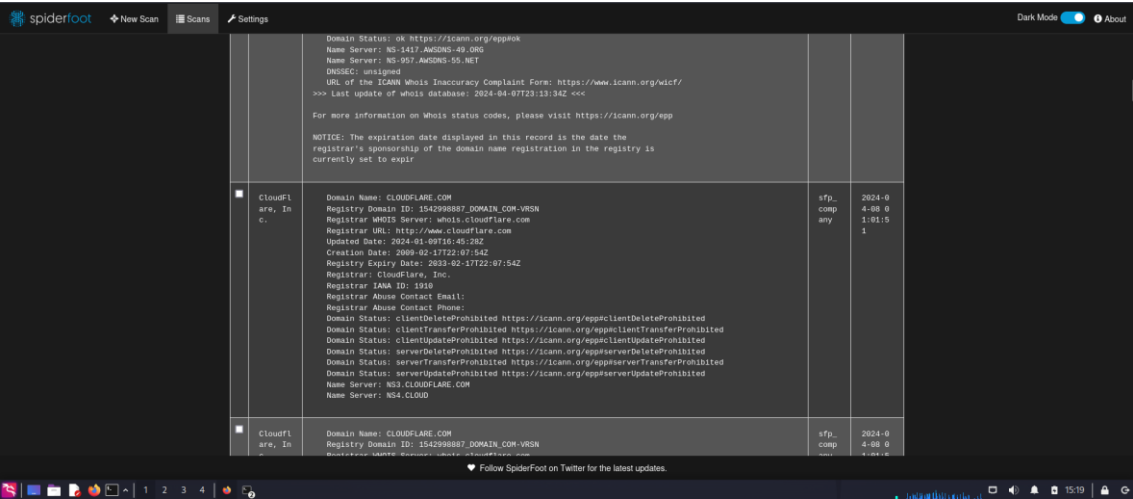
Diego de Santos del Río NP: 138996
Javier Miguélez Yagüe NP: 138571



Aquí podemos ver el resumen de todos los datos y sus tipos obtenidos:


Type	Unique Data Elements	Total Data Elements	Last Data Element
Linked URL - Internal	1241	1256	2024-04-08 01:29:47
Domain Name	869	869	2024-04-08 01:52:30
Non-Standard HTTP Header	467	1683	2024-04-08 00:12:29
Vendor Domain	405	405	2024-04-08 02:31:37
Raw File Meta Data	325	338	2024-04-08 02:09:49
Vendor Domain - Internal	367	341	2024-04-08 02:36:53
Attacks - Email Address	295	788	2024-04-08 02:26:54
HTTP Headers	230	230	2024-04-08 01:29:38
Linked URL - External	208	208	2024-04-08 01:29:38
Web Content	205	220	2024-04-08 01:29:38
URL (Point)	192	192	2024-04-08 00:12:29
URL (Valid Javascript)	192	192	2024-04-08 00:12:29
Attacks - Internet Name	191	234	2024-04-08 02:30:56
Discovery on Existing Site	179	179	2024-04-08 02:29:18
Attacks Description - Category	176	198	2024-04-08 01:04:50
Domains	169	171	2024-04-08 02:28:44


Una vez vistas las relaciones pasamos a ver la información obtenida como por ejemplo ver los diferentes plug-in que tiene la UAX como CLOUDFLARE para controlar el tráfico y seguridad de la red o LINKEDIN.















Javier Miguélez Yagüe NP: 138571

También obtenemos diferentes usuarios y geolocalizaciones dentro de uax.com

New Scan

Scans

Settings

	convenioslatinoam	Convenios Latinoam	sfp_accounts	2024-04-08 01:54:08
	cursos.adaptaci	Cursos Adaptaci	sfp_accounts	2024-04-07 21:41:54
	cursosadaptaci	Cursos Adaptaci	sfp_accounts	2024-04-07 21:41:54
	david.mart	David Mart	sfp_accounts	2024-04-08 22:11:35
	davidmart	David Mart	sfp_accounts	2024-04-07 22:11:35
	decana.veterinaria	Decana Veterinaria	sfp_accounts	2024-04-07 22:10:08
	decanaveterinaria	Decana Veterinaria	sfp_accounts	2024-04-07 22:10:08
	departamentos.client	Departamentos Client	sfp_accounts	2024-04-08 01:23:51
	departamentoscient	Departamentos Cient	sfp_accounts	2024-04-08 01:23:51
	deporte.afyd	Deporte AFYD	sfp_accounts	2024-04-07 21:50:34
	deporteafyd	Deporte AFYD	sfp_accounts	2024-04-07 21:50:34

Dark Mode

About

spiderfoot		New Scan	Scans	Settings	Dark Mode		About
	40.510584,-3.6674125	AVERIDA CAMINO DE SANTIAGO 40, Madrid, ES, 28056	sfp_openstreetmap	2024-04-07 22:00:25			
	40.8672395,-3.6100413	CALLE JOSE ORTEGA Y GASSET 40 2 / D, Madrid, ES, 28006	sfp_openstreetmap	2024-04-07 22:00:54			
	41.2196784,1.7217149	BALMES 36, Barcelona, ES, 08007	sfp_openstreetmap	2024-04-07 22:00:21			
	41.2008279,1.7703353	BALMES 36, Barcelona, ES, 08007	sfp_openstreetmap	2024-04-07 22:00:21			
	41.3173071,2.0719342	OSONA 1, Prat de Llobregat, EL, ES, 08820	sfp_openstreetmap	2024-04-07 22:00:05			
	41.3886832,2.163798915865469	BALMES 36, Barcelona, ES, 08007	sfp_openstreetmap	2024-04-07 22:00:21			
	41.558892,2.2212121	BALMES 36, Barcelona, ES, 08007	sfp_openstreetmap	2024-04-07 22:00:21			
	43.3373788,-8.374674632080307	PLAZA CHARLES DARWIN 2 BAJO, OLEIROS, ES-C, ES, 15172	sfp_openstreetmap	2024-04-07 22:01:18			
	43.3375147,-8.3747094	PLAZA CHARLES DARWIN 2 BAJO, OLEIROS, ES-C, ES, 15172	sfp_openstreetmap	2024-04-07 22:01:18			
	45.7585868,21.2325244	Popa Sapca, Timisoara, RO-TM, RO, 300057	sfp_openstreetmap	2024-04-07 22:00:59			
	45.7604969,21.2328116	Popa Sapca, Timisoara, RO-TM, RO, 300057	sfp_openstreetmap	2024-04-07 22:00:59			

- **Anubis**

```

root@kali: ~# /spiderfoot
# pip3 install anubis-netsec
Collecting anubis-netsec
  Downloading anubis-netsec-1.2.0-py2.py3-none-any.whl.metadata (8.6 kB)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from anubis-netsec) (68.1.2)
Collecting python-nmap=0.7.1 (from anubis-netsec)
  Downloading python-nmap-0.7.1.tar.gz (44 kB)
  44.4/44.4 kB 1.8 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting shodan>=1.31.0 (from anubis-netsec)
  Downloading shodan-1.31.0.tar.gz (57 kB)
  57.9/57.9 kB 3.4 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Requirement already satisfied: doctest=0.6.2 in /usr/lib/python3/dist-packages (from anubis-netsec) (0.6.2)
Requirement already satisfied: requests>=2.21.1 in /usr/lib/python3/dist-packages (from anubis-netsec) (2.31.0)
Collecting census=2.2.11 (from anubis-netsec)
  Downloading census-2.2.11-py3-none-any.whl.metadata (7.0 kB)
Collecting dnspython>=2.6.1 (from anubis-netsec)
  Downloading dnspython-2.6.1-py3-none-any.whl.metadata (5.8 kB)
Requirement already satisfied: argcomplete<4.0.0, >=2.0.0 in /usr/lib/python3/dist-packages (from census=2.2.11->anubis-netsec) (3.1.4)
Requirement already satisfied: backoff<3.0.0, >=2.0.0 in /usr/lib/python3/dist-packages (from census=2.2.11->anubis-netsec) (2.2.1)
Requirement already satisfied: rich>=10.6.2 in /usr/lib/python3/dist-packages (from census=2.2.11->anubis-netsec) (13.3.1)
Requirement already satisfied: urllib3<3.0.0 in /usr/lib/python3/dist-packages (from census=2.2.11->anubis-netsec) (1.26.18)
Requirement already satisfied: lxmlwriter in /usr/lib/python3/dist-packages (from shodan>=1.31.0->anubis-netsec) (3.0.2)
Requirement already satisfied: click in /usr/lib/python3/dist-packages (from shodan>=1.31.0->anubis-netsec) (8.1.6)
Requirement already satisfied: click-plugins in /usr/lib/python3/dist-packages (from shodan>=1.31.0->anubis-netsec) (1.1.1)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from shodan>=1.31.0->anubis-netsec) (0.4.6)
Requirement already satisfied: tqdm in /usr/lib/python3/dist-packages (from shodan>=1.31.0->anubis-netsec) (3.1.2)
Collecting markdown-it-py<3.0.0, >=2.1.0 (from rich>=10.6.2->census=2.2.11->anubis-netsec)
  Downloading markdown_it_py-2.2.0-py3-none-any.whl.metadata (6.8 kB)
Requirement already satisfied: pygments<3.0.0, >=2.14.0 in /usr/lib/python3/dist-packages (from rich>=10.6.2->census=2.2.11->anubis-netsec) (2.15.1)
Requirement already satisfied: mdurl<=0.1 in /usr/lib/python3/dist-packages (from markdown-it-py<3.0.0, >=2.1.0->rich>=10.6.2->census=2.2.11->anubis-netsec) (0.1.2)
Downloading anubis-netsec-1.2.0-py2.py3-none-any.whl (22 kB)
Downloading census-2.2.11-py3-none-any.whl (77 kB)
  77.7/77.7 kB 5.4 MB/s eta 0:00:00
Downloading dnspython-2.6.1-py3-none-any.whl (307 kB)
  307.7/307.7 kB 9.6 MB/s eta 0:00:00
Downloading markdown_it_py-2.2.0-py3-none-any.whl (84 kB)
  84.5/84.5 kB 7.8 MB/s eta 0:00:00
Building wheels for collected packages: python-nmap, shodan
  Building wheel for python-nmap (setup.py) ... done

```

Aquí podemos ver todos los subdominios que tiene la UAX

```
(root@kali)~/spiderfoot
# anubis -t www.uax.com

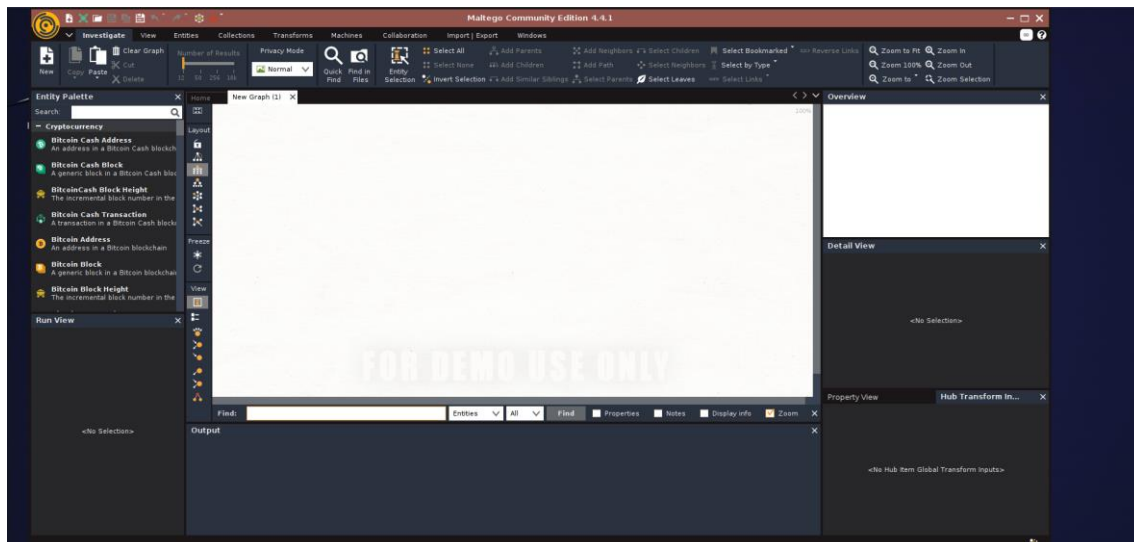
d8888      888      d8b
d888888    888      Y8P
d88P888    888
d88P 888 88888b. 888 888 88888b. 888 .d8888b
d88P 888 888 "88b 888 888 888 "88b 888 88K
d88P 888 888 888 888 888 888 888 "Y8888b.
d8888888888 888 888 Y88b 888 888 d88P 888 X88
d88P 888 888 888 "Y88888 88888P" 888 88888P'

Searching for subdomains for 151.101.130.216 (www.uax.com)
Working on target: www.uax.com
Testing for zone transfers
Searching HackerTarget
Searching for Subject Alt Names
Searching NetCraft.com
Searching crt.sh
Searching DNSDumpster
Searching Anubis-DB
Error checking for Zone Transfers
Found 22 subdomains

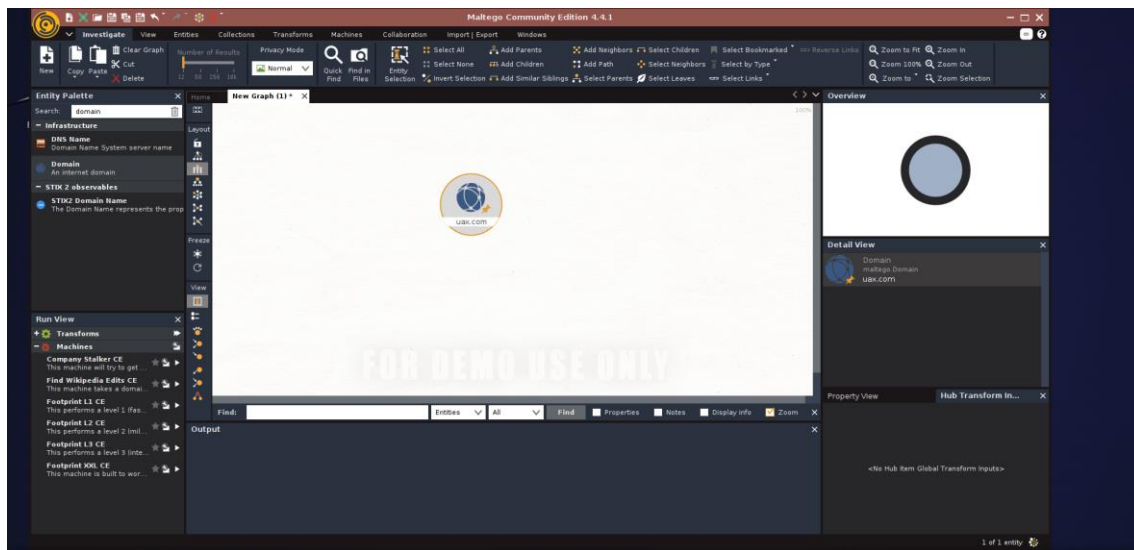
uax.es
staging.uax.com
www.uax.com
www.uax.es
www.clinicasuax.com
prod.uax.com
www.fpclaudiogaleno.es
www.hospitalveterinariouax.com
prod.xtart.com
uaxhealthcaress.uax.com
uax.com
hospitalveterinariouax.com
dwww.uax.com
www.xtart.com
clnicasuax.com
openuax.com
pwww.uax.com
www.openuax.com
xtart.com
jobs.uax.com
fpclaudiogaleno.es
```

- Maltego

Iniciamos maltego



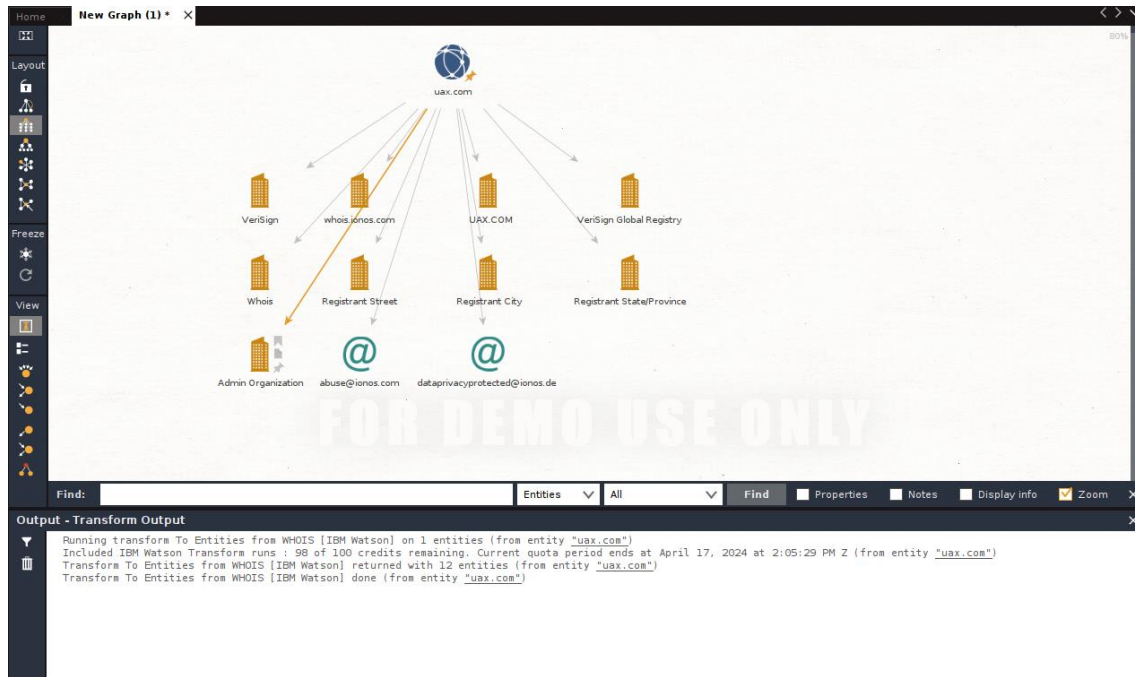
Ponemos el Dominio de la UAX



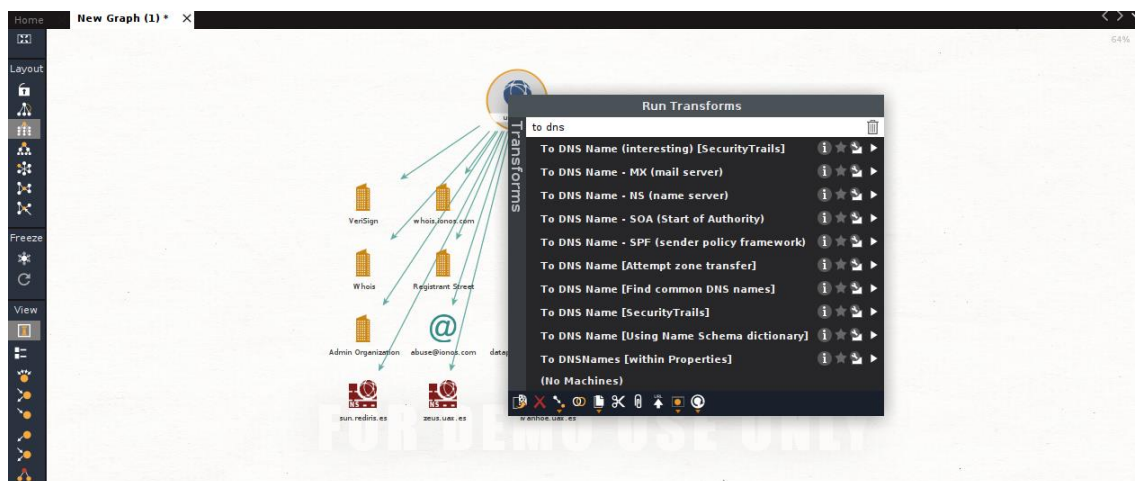
Y comenzamos el análisis, en este caso Entities from WHOIS



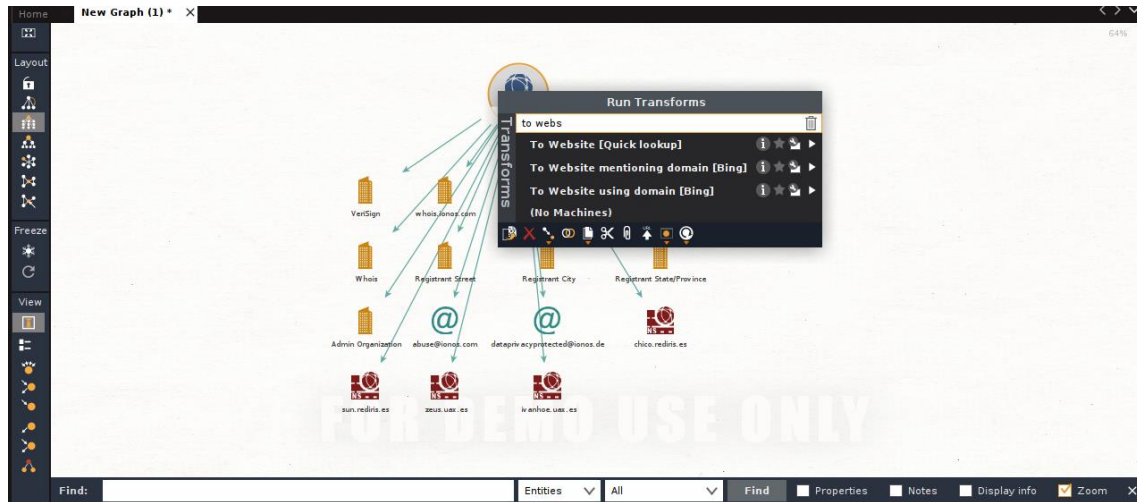
Aquí podemos ver la estructura básica de la web y vemos que tiene una capa de seguridad con IONOS.



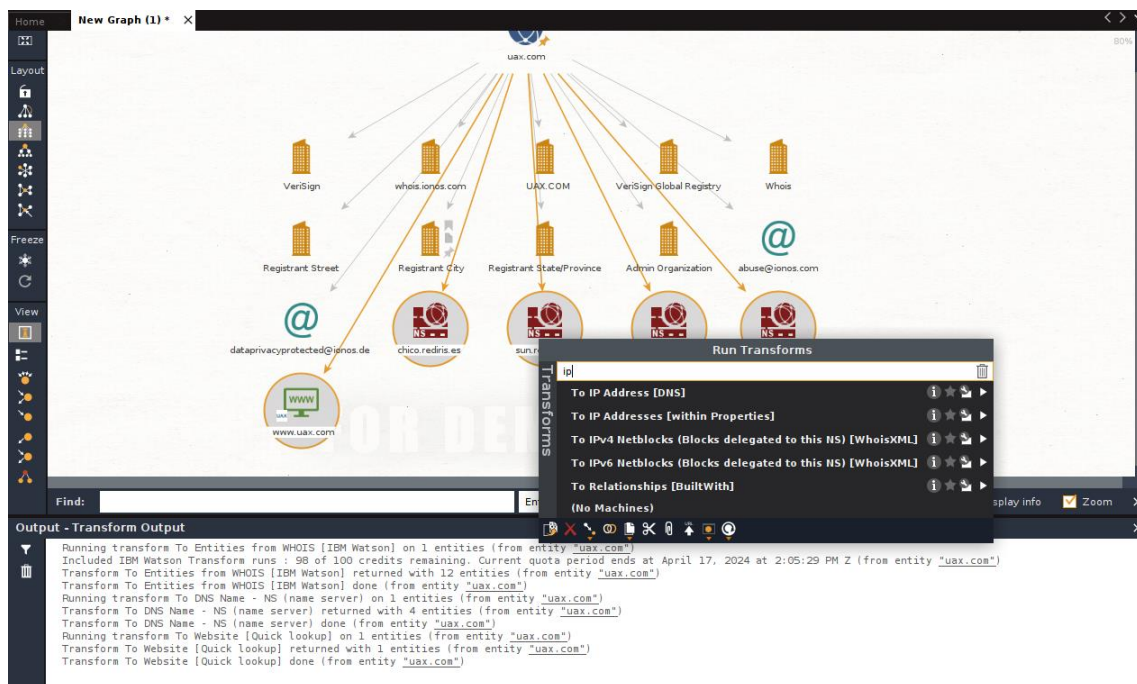
Ahora obtenemos los Nombres de las diferentes DNS asociadas:



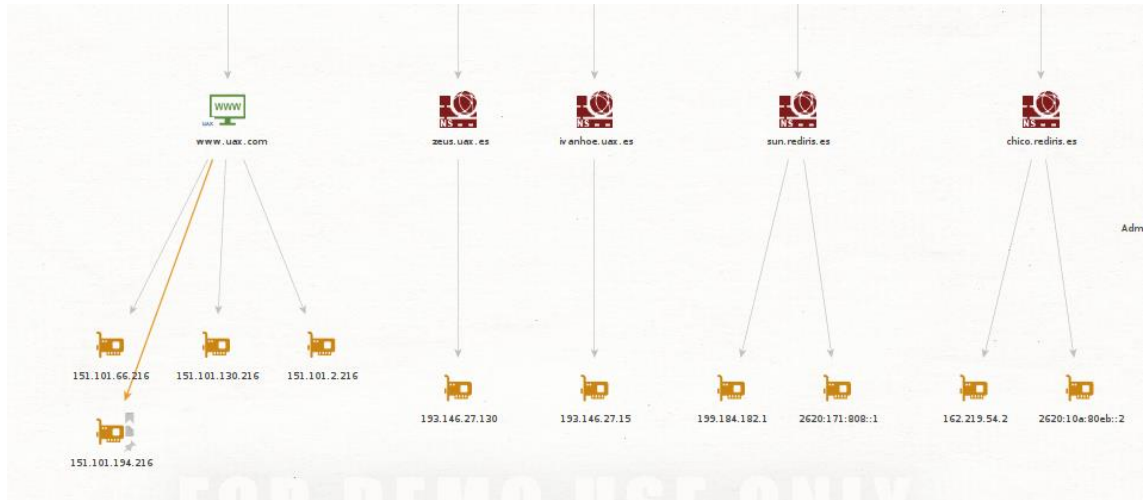
Y lo vemos aplicado en la web



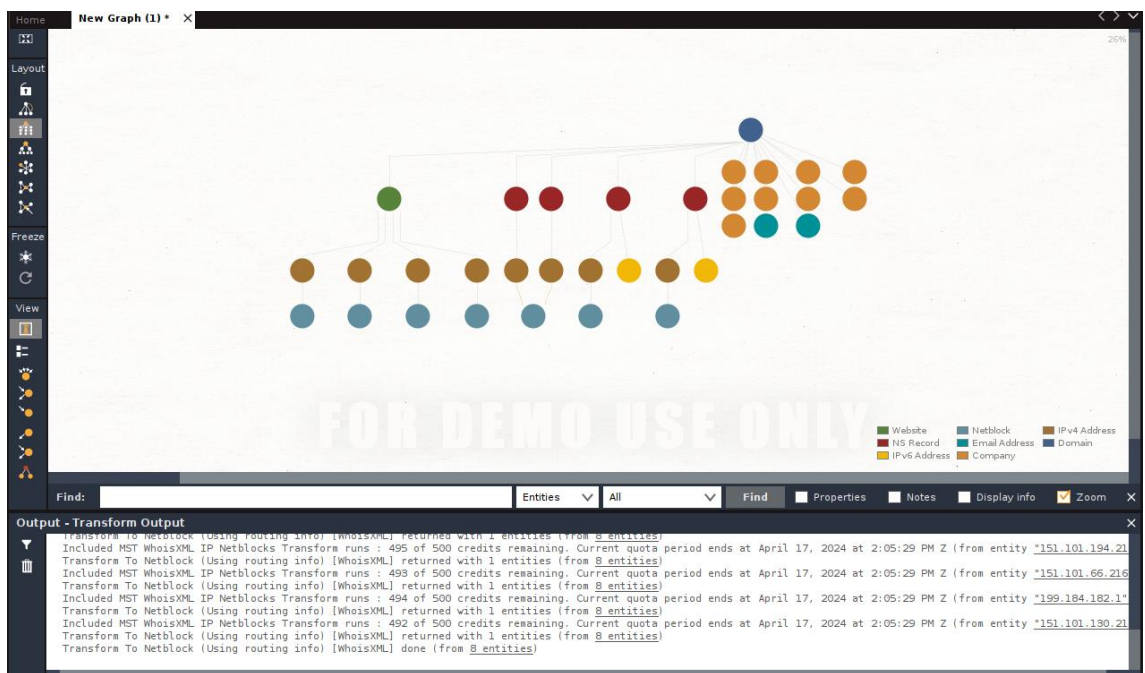
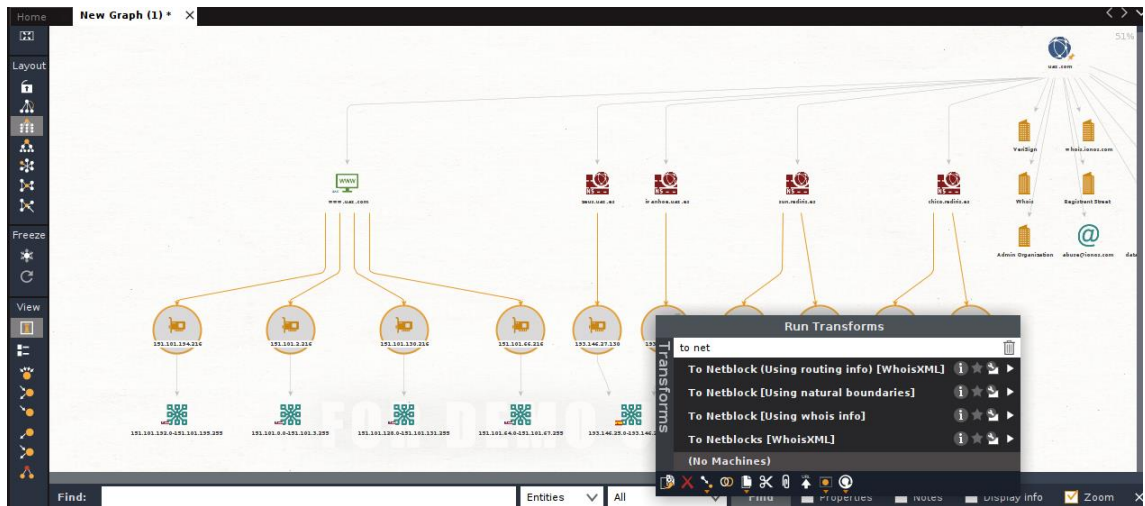
Lo pasamos a direcciones IP para sacarlas:



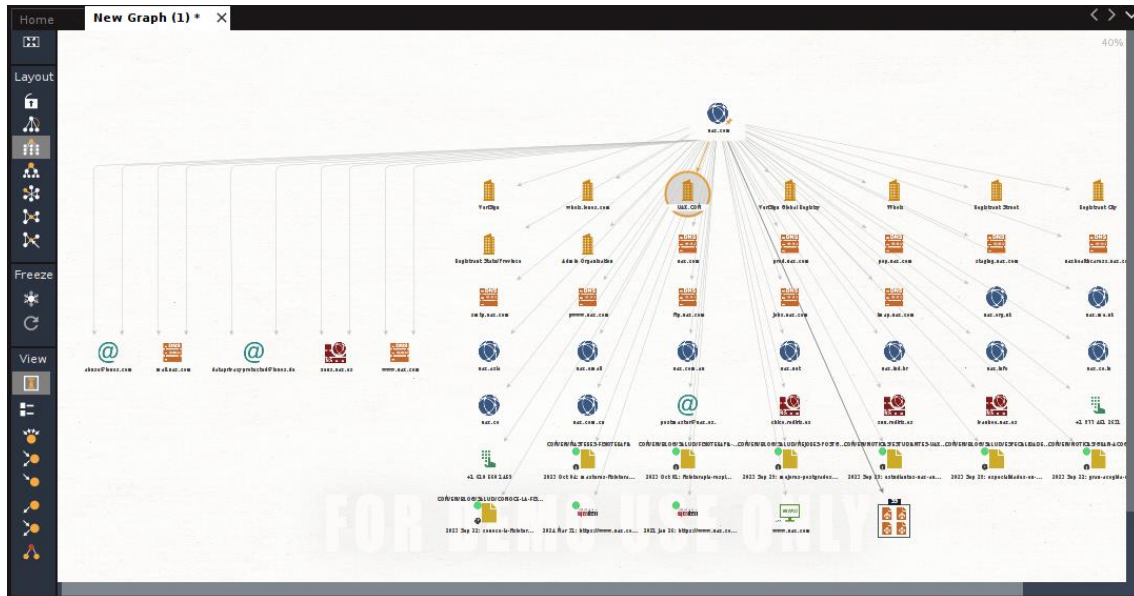
Aquí ya tenemos todas las direcciones IPs de la estructura principal de la UAX



Y para finalizar este análisis podemos ver a que routers están asociadas las diferentes IPs



Y si en cambio le pedimos todas las transformaciones podemos ver toda la información y estructura de la red obtenida, en este caso también encontramos documentos, correos etc



• Reflexiones y conclusiones:

En la "Expedición Digital" a través de la Universidad Alfonso X "El Sabio", se han empleado herramientas de vanguardia y técnicas de exploración pasiva para extraer información oculta en la vastedad digital de su ciberespacio. Este proceso ha revelado tanto fortalezas como áreas de mejora en la seguridad y la gestión de la información de la universidad.

Una reflexión crítica sobre los hallazgos revela que, si bien las herramientas utilizadas han demostrado ser efectivas para recopilar información sobre la infraestructura y la presencia en línea de la universidad, también han resaltado algunas vulnerabilidades potenciales. Por ejemplo, el descubrimiento de subdominios adicionales mediante Anubis señala posibles puntos de entrada para ataques externos si no se gestionan adecuadamente. Del mismo modo, el análisis de metadatos con Spiderfoot puede haber revelado información sensible que podría ser explotada si no se protege adecuadamente.

Es recomendable que la Universidad Alfonso X "El Sabio" tome medidas proactivas para abordar las vulnerabilidades identificadas durante la expedición. Esto podría incluir la implementación de medidas de seguridad adicionales para proteger los subdominios descubiertos, así como la revisión de los procedimientos de gestión de la información para garantizar que los metadatos no sensibles estén debidamente protegidos. Además, se recomienda una evaluación continua de la postura de seguridad de la universidad, así como la formación del personal en prácticas seguras de ciberseguridad para mitigar cualquier riesgo potencial.