**Ciberseguridad en SCI - Demos**

**3.- Equipos expuestos en internet**

INDICE

**3.- Equipos expuestos en Internet.**

***Demo 1 - Shodan***

***Demo 2 - Censys***

***Demo 3 - Webserver abierto***

***Demo 4 - Google Dorks***

***Demo 5 - Búsquedas DNS***. **DNSDumpster**

***Demo 6 - FOCA*. Metadatos**

**Demo1- Shodan **

**Shodan** es un motor de búsqueda que sirve para encontrar dispositivos escaneados conectados a internet. Este buscador se vale del escaneo de puertos, realizado por miles de usuarios, cuyos resultados se almacenan en sus servidores para que otros puedan consultarlos.

En este caso se utilizará para localizar PLCs expuestos en internet pero con la misma mecánica de búsqueda se pueden localizar cámaras IP , dispositivos IOT, bases de datos….

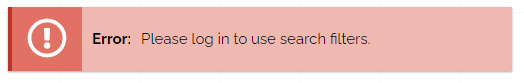
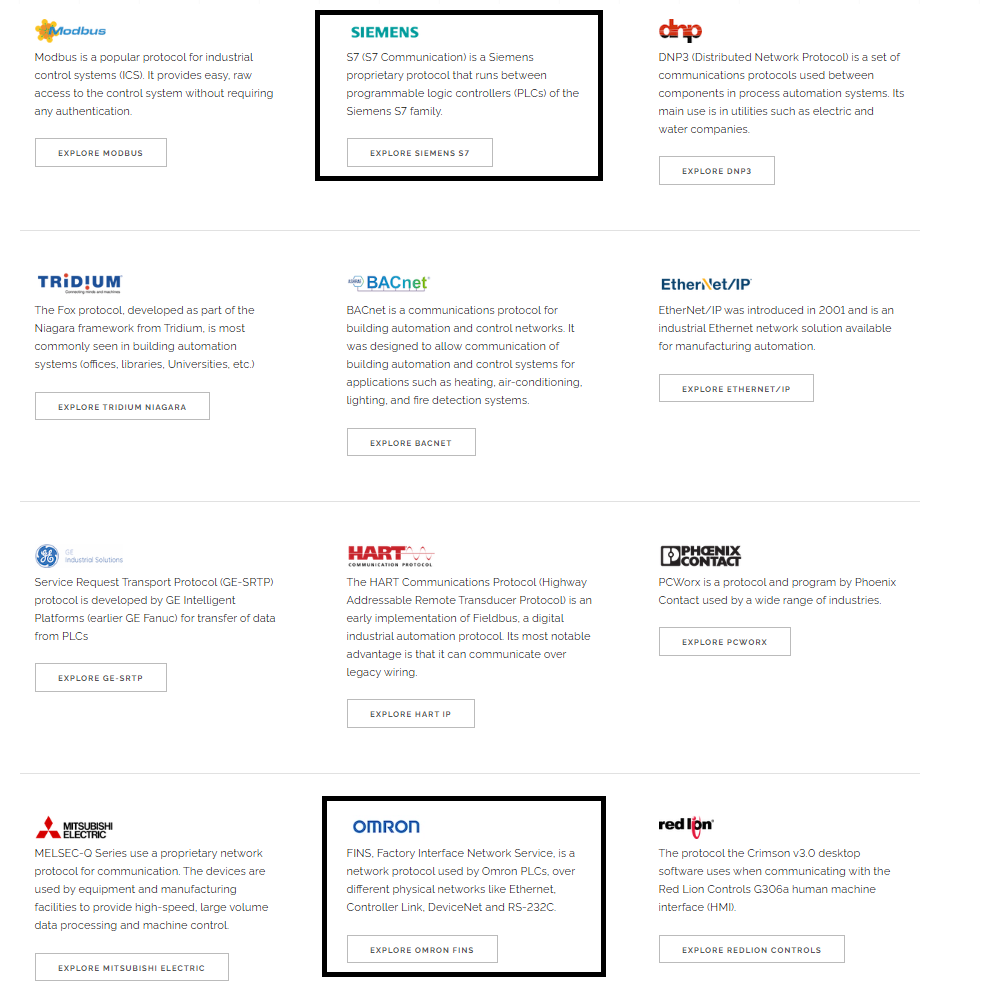
<https://www.shodan.io/>

Para localizar dispositivos industriales iremos a **Explore** y **Sistemas de control industrial**

****



Nos muestra diferentes fabricantes. En este caso nos centraremos en Siemens y Omron que son los más utilizados en nuestros entornos educativos.





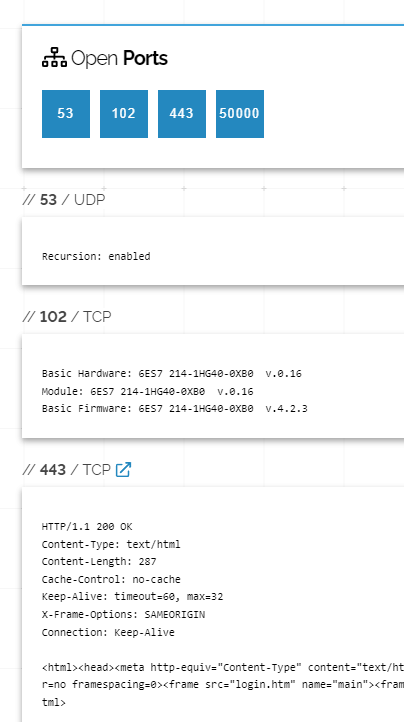
Requiere que nos logeemos. Podemos utilizar nuestro usuario Google.

Al seleccionar el sistema Omron ya nos identifica el puerto que utiliza para comunicarse port:9600. Podemos filtrar por país y ciudad.Nos muestra un listado de PLC expuesto al exterior y con varios puertos abierto, entre ellos el 9600 de Omron.En principio es un PLC que ha sido identificado como accesible (respondería a un ping) pues tiene el puerto 9600 abierto al exterior. En el ejemplo muestra el puerto 8080 abierto. La dirección [http://IPdelPLC:8080](http://ipdelplc:8080) nos mostraría un webserver.

**port:9600 response code country:"ES" city:"xxxxxxxxx"**

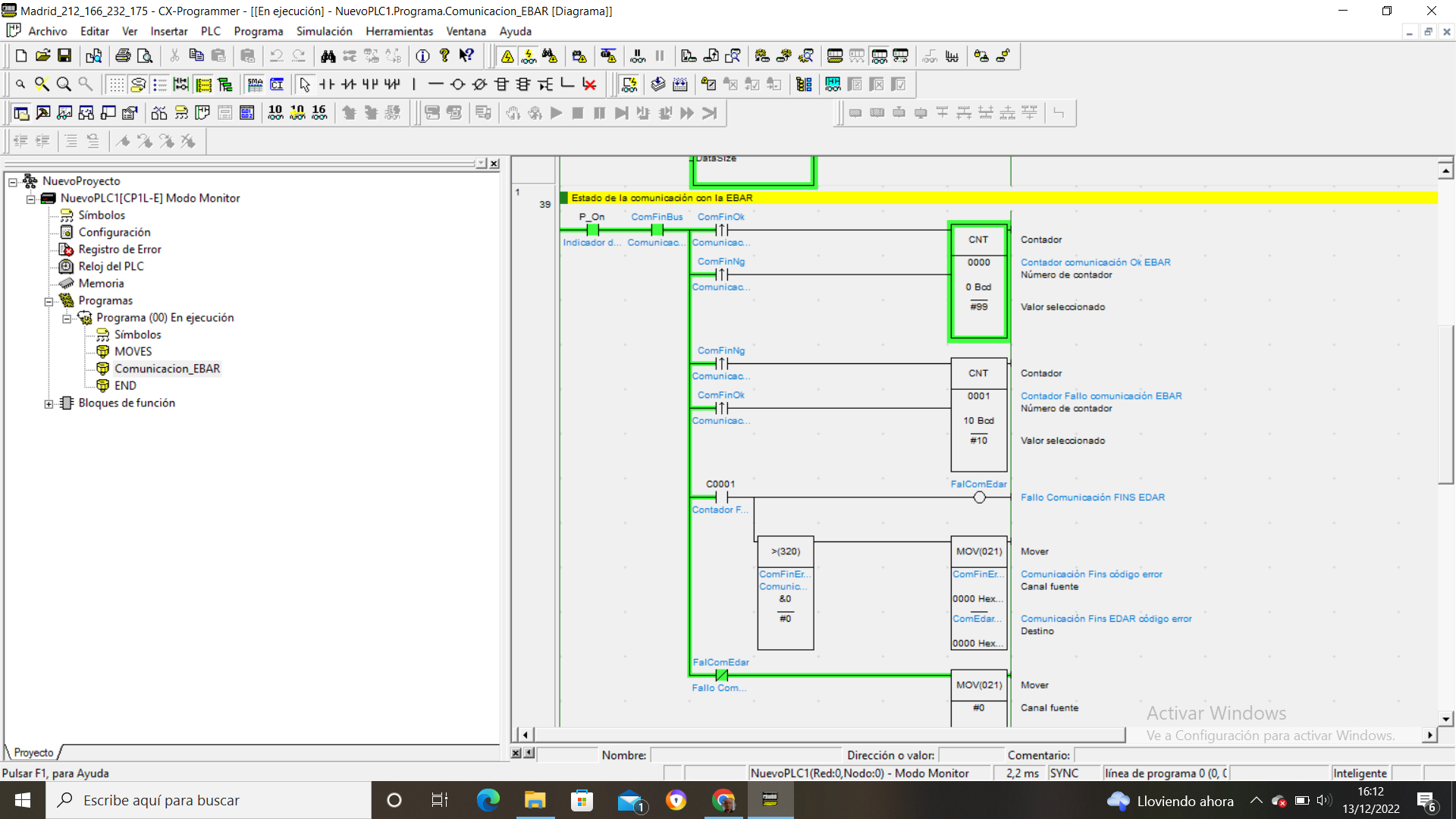
****

De manera similar podemos localizar un PLC Siemens. En este caso el puerto a buscar es **port:102 country:"ES".** Nos devuelve un listado ordenado por país y con las características de dicho dispositivos.Modelo CPU, puertos, servicios web… En el ejemplo además del puerto Siemens específico port 102, nos muestra un puerto 443 que se utiliza para https. Eso quiere decir que con [https://IPdelPLC](https://ipdel) nos mostraría el webserver.



Si se acierta con el PLC adecuado podemos conectarnos a él y tener el control sobre el mismo. Estableciendo conexión online podemos forzar variables, salidas, escribir en memoria, ponerlo en stop y cargarle un nuevo programa.

**ATENCIÓN!!! Esta es una actividad peligrosa que puede alterar el comportamiento de PLC y ocasionar daños en el sistema que controla. Estamos accediendo de manera directa a un PLC privado.**



Se pueden hacer búsquedas más elaboradas conociendo los filtros adecuados.:

EJ: IPs de servidores de Donosti que usen Apache Tomcat:

country:es product:tomcat city:"Donostia / San Sebastián"

Una manera más sencilla es utilizar los **Shodan Query** que ya están creados y clasificados.

Shodan Query exemples en <https://www.shodan.io/search/examples>

Colección de Querys ya creadas

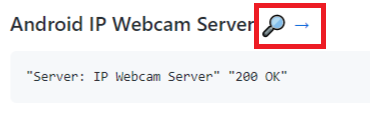
<https://github.com/jakejarvis/awesome-shodan-queries>

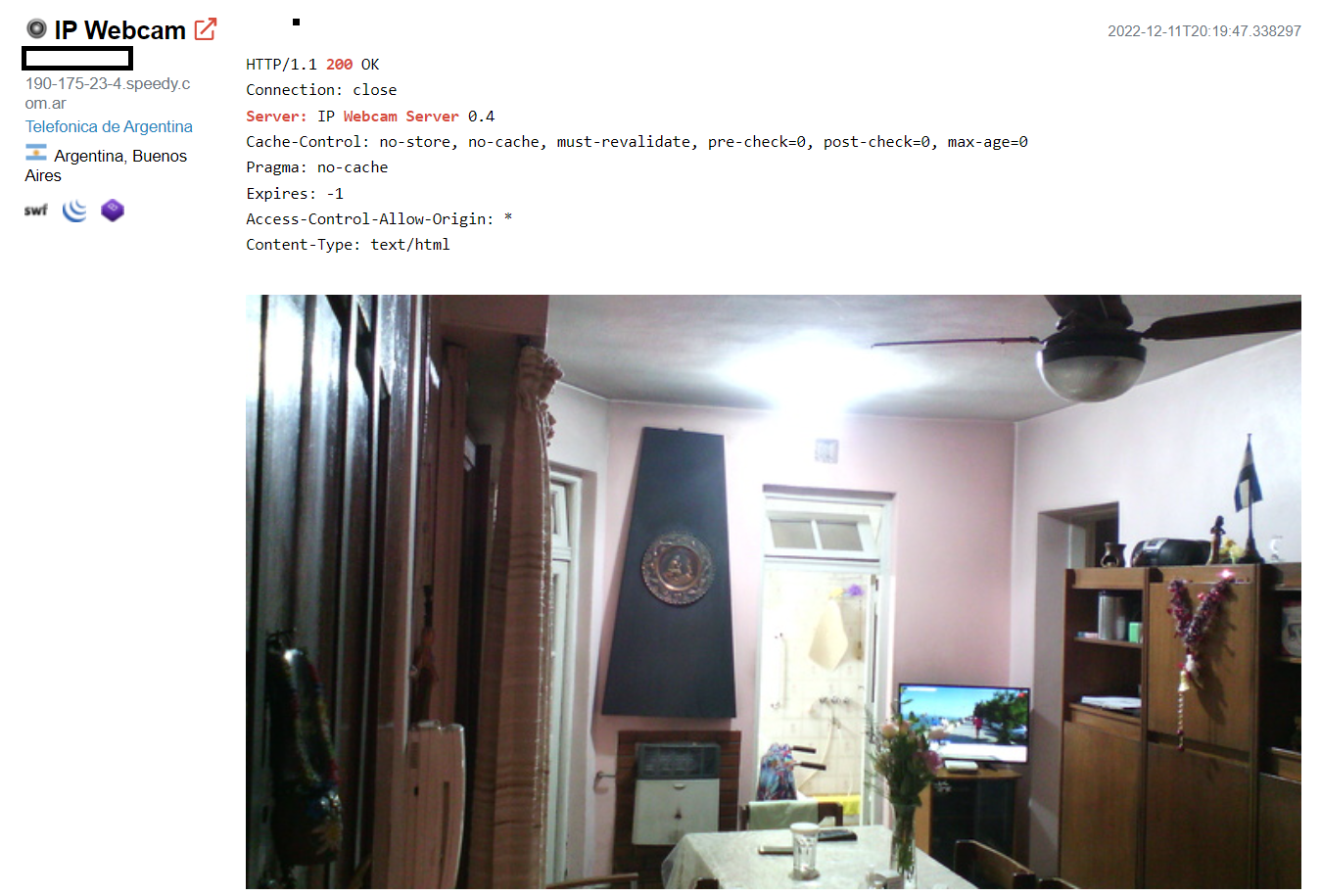


Un ejemplo de Industrial Control System. Búsqueda de dispositivos de control de cámaras de tráfico.



Otro ejemplo es acceder a webcams





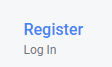
**Demo 2 - Censys**

El buscador de dispositivos industriales e IOT más conocido es Shodan pero hay

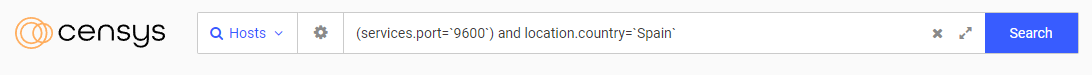
otros que realizan funciones parecidas. Zoom Eye, Ivre, Thingful y Censys.

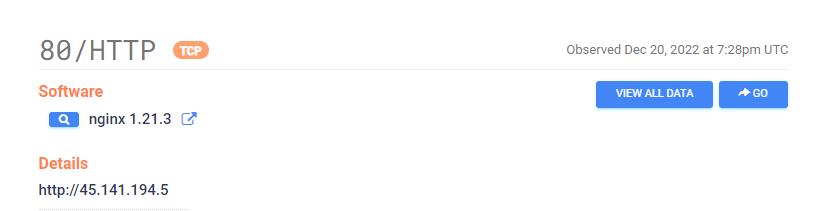
<https://censys.io/>



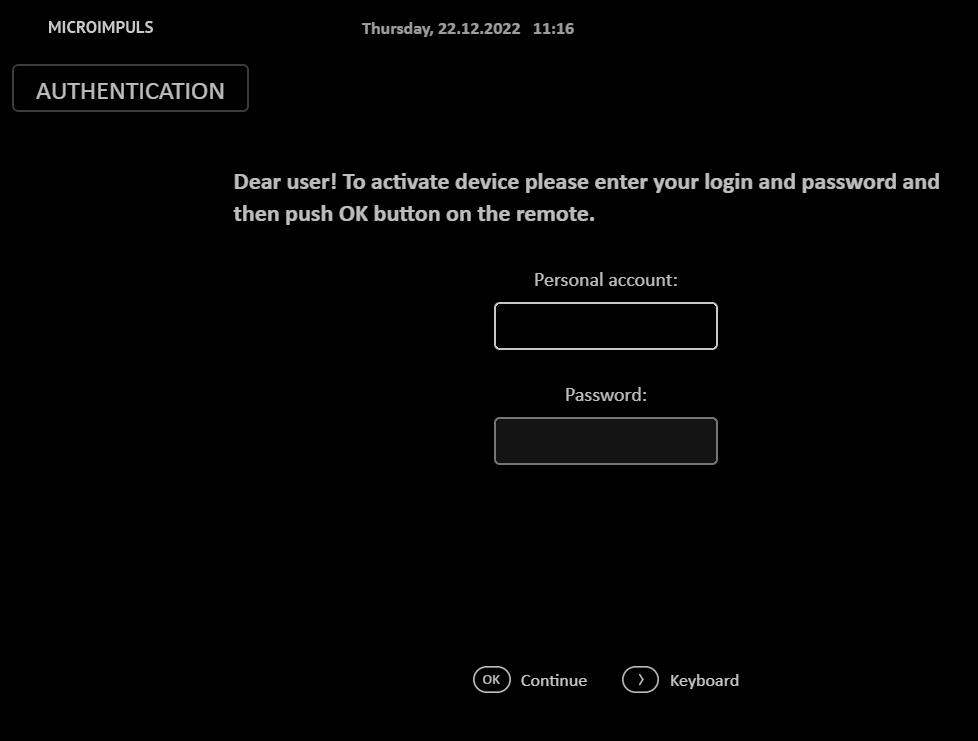
**** Registrarse , acceder y clicamos en 

Podemos filtrar por puerto , ciudad, fabricante… o combinar filtros





Por ejemplo filtramos dispositivos que tienen el puerto 80 abierto y están ubicados en España, Una vez localizado el dispositivo podemos intentar acceder vía web.

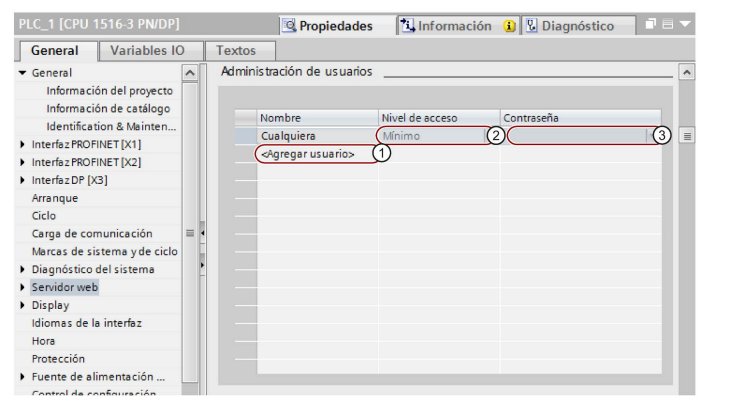


**Demo 3 - Webserver abierto **

Cuando abrimos el webserver de los plc Siemens estamos mostrando al exterior una página web interna que tiene el plc. Esto puede ser práctico en algunos casos en los que el operario necesite visualizar algún parámetro desde una aplicación web ya sea desde el navegador de un pc , una tablet o el smartphone sin necesidad de usar el software específico de Siemens Tia Portal.

Desde el momento que abrimos el web server estamos abriendo un puerto , ya sea el http (80) o el https (443) con el consiguiente peligro. Hay que tener muy en cuenta los permisos que otorgamos a los usuarios.

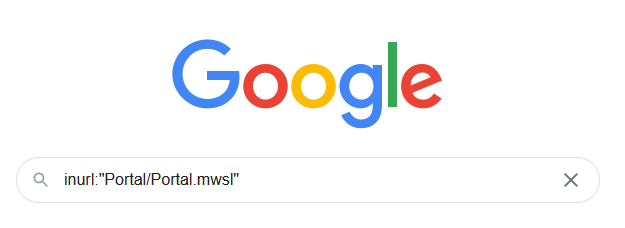




Poniendo la IP del plc en el navegador accederemos al servicio web. Hay que usar http o https según se ha configurado.



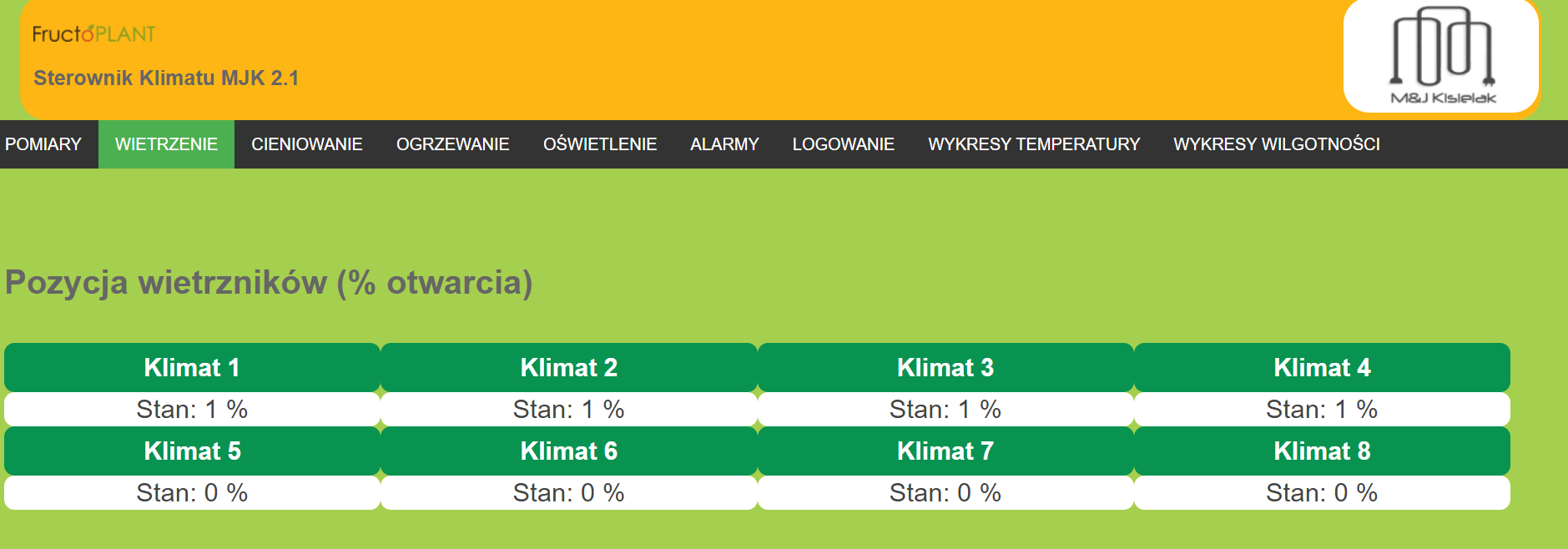
El problema está en que al activar el servidor web estamos habilitando la página de inicio del mismo que normalmente es del formato **Portal.mwsl** . Una simple búsqueda en el google nos localiza páginas que cumplen ese criterio, es decir, tienen el web server activo. **inurl:”Portal/Portal.mwsl”**



Podemos acceder a información que el web server muestra sobre la CPU, modelo, IP..en algunos casos acceder a visualizar el estado de las variables, o escribir en ellas, visualizar la página de inicio con información del proceso.







Resumiendo, si es necesario habilitar el webserver del plc utilizar un protocolo https y verificar los permisos de acceso de los usuarios.

**Demo 4 - Google Dorks **

Aunque no está directamente relacionado con el ámbito industrial se menciona como herramienta de búsqueda de información de la organización que puede ser confidencial. Se expondrá por lo tanto la mecánica de uso pero sin profundizar en ella.

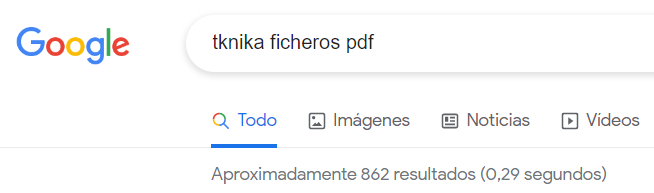
Los **Google Dorks**, también conocidos como [**Google Hacking**](https://es.wikipedia.org/wiki/Google_Hacking), son combinaciones de operadores de búsqueda que se utilizan para extraer información valiosa desde Google. El término tiene un origen despectivo, debido a que *dork* significa «idiota» y se denomina *googledork* a una persona inepta.

En términos más simples, un Google Dork es una búsqueda avanzada, la cual admite una serie de parámetros para realizar búsquedas en Google y obtener resultados concretos o información más relevante para el usuario.

Estos son ejemplos de información sensible que se puede encontrar mediante los Google Dorks:

* Nombre de usuario y contraseñas.
* Imágenes y videos.
* URLs privadas.
* Documentos sensibles.
* Detalles de cuentas bancarias.
* Listas de correos electrónicos.
* Sitios web vulnerables.
* Páginas de inicio de sesión de administrador.
* Directorios de copias de seguridad.
* Y mucho más.

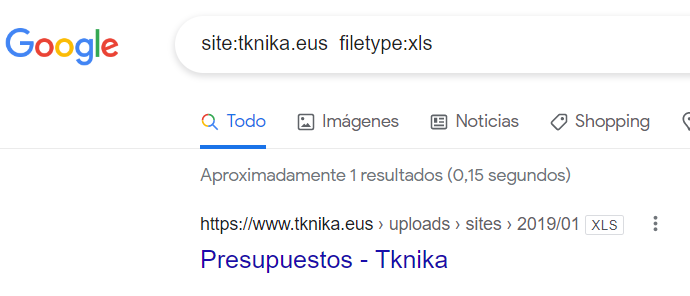
Ejemplo: Buscar todos los ficheros pdf relacionados con un dominio en concreto.Si hacemos una búsqueda normal obtenemos resultados de todo tipo en los que aparece el concepto pdf..



En cambio si utilizamos búsquedas avanzadas obtenemos unos resultado más fiables. Se reduce el número de resultados y todos nos devuelven un fichero pdf.



Se pueden buscar ficheros de diferente tipo, hasta encontrar alguno que pueda tener una información más confidencial.



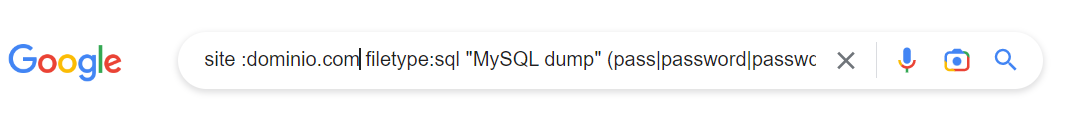
Otros ejemplos:

site:uned.es filetype:sql

site:uned.es filetype:txt

filetype:sql "MySQL dump" (pass|password|passwd|pwd)

site: dominio filetype:sql "MySQL dump" (pass|password|passwd|pwd)

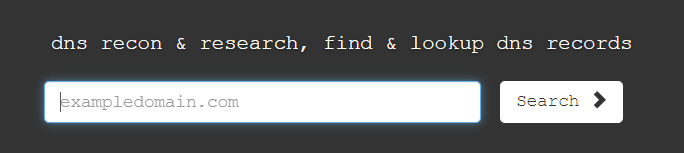


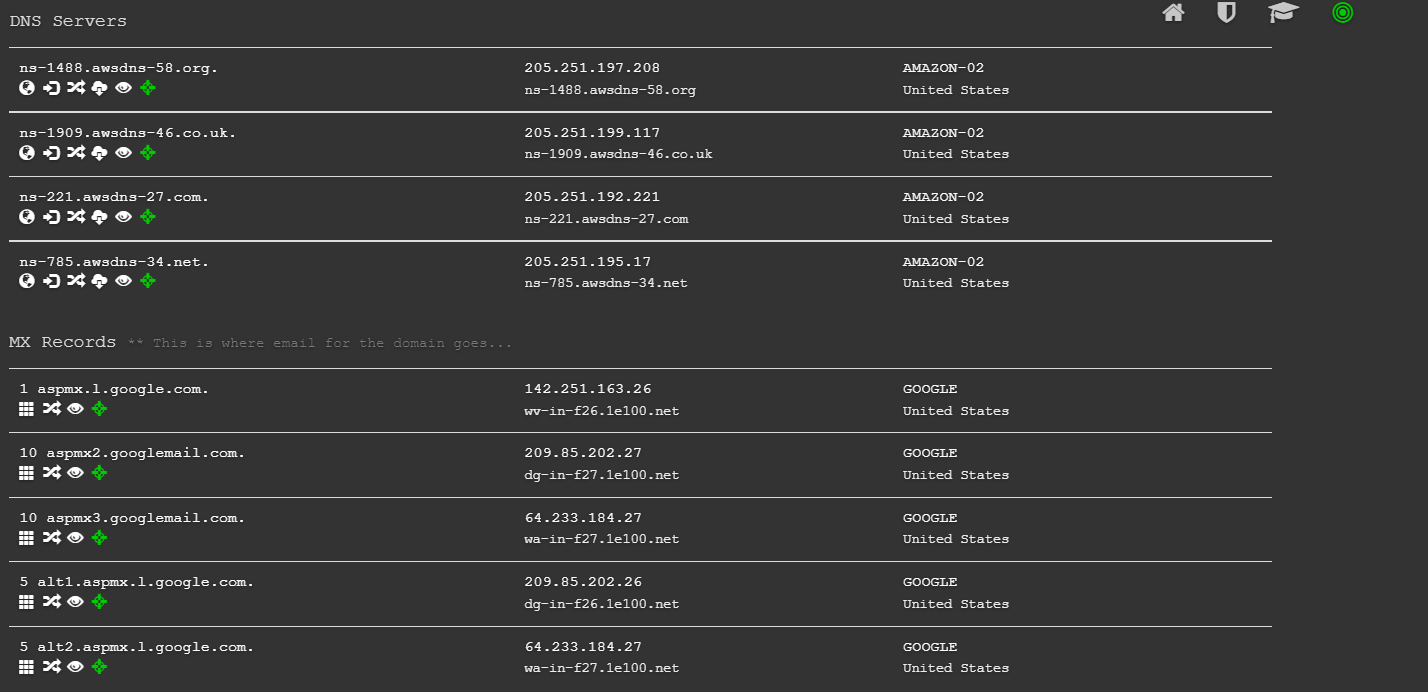
Banco de Dorks: <https://www.exploit-db.com/>

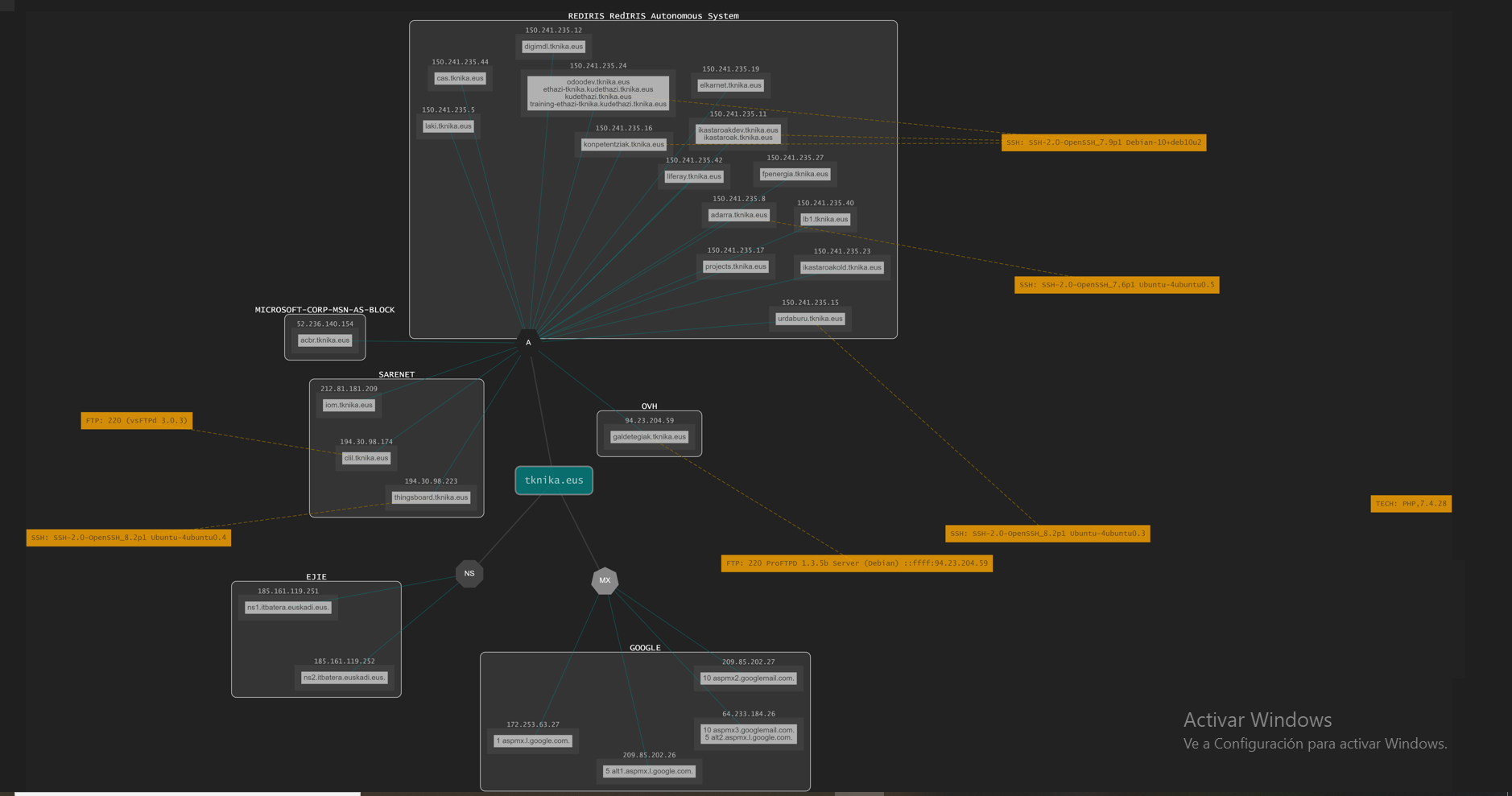
**Demo 5 - Búsquedas DNS **

**DNSdumpster** es una herramienta totalmente gratuita diseñada para facilitarnos el análisis de cualquier dominio y poder obtener en segundos todo tipo de información relacionada con este. <https://dnsdumpster.com/>

Nos muestra las máquinas que tiene relacionadas ese dominio,, servidores de correo y servidores varios y dibuja un esquema de la red con los equipos y los servicios.





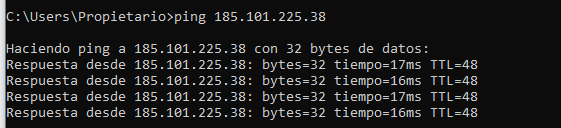


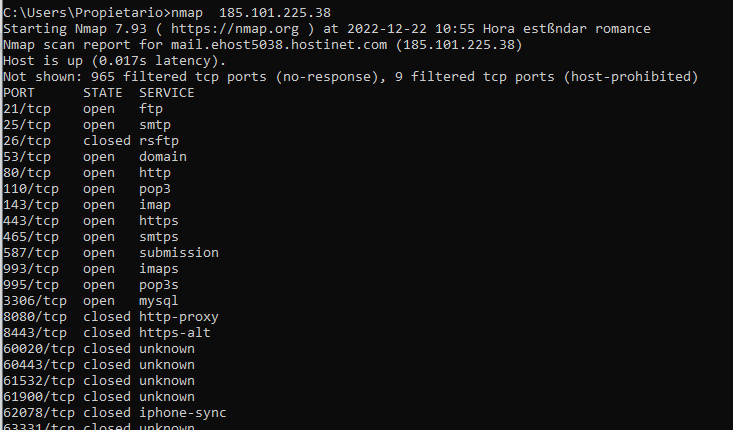
Nos aparece un esquema con los servidores mostrados al exterior y servicios que ofrecen.

Es posible hacerle un ping e incluso preguntarle qué puertos tiene abiertos (Se verá nmap más adelante).

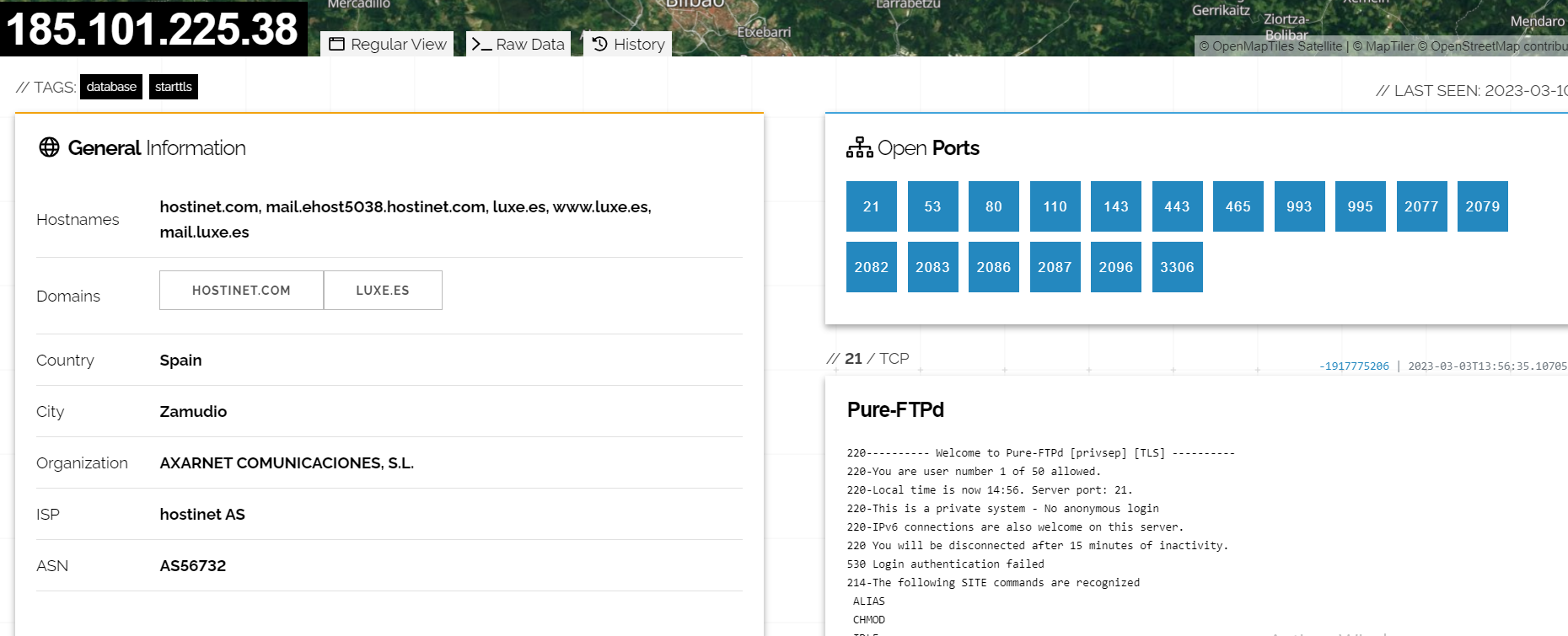
**ATENCIÓN!! Realizar nmap contra servidores externos puede ser intrusivo**





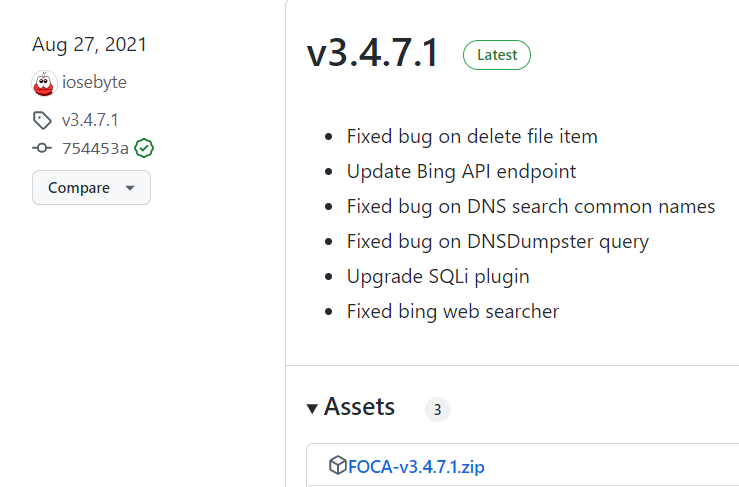


Otra posibilidad es utilizar Shodan para ver la información de los puertos asociados a esa IP



**Demo 6 - FOCA Metadatos **

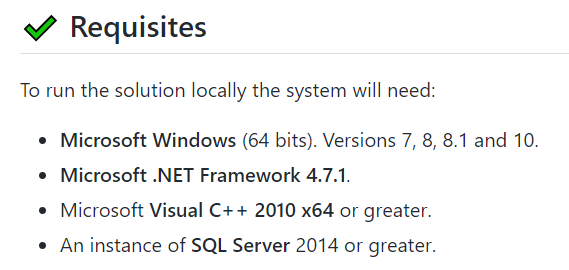
**FOCA** es un software de código abierto con el que podremos extraer los metadatos de cualquier tipo de documento (documentos de texto, imágenes, vídeos, etc.). podemos descargarlo desde <https://github.com/ElevenPaths/FOCA/releases>



Descargar y descomprimir el fichero. Dentro de la carpeta descomprimida hay un ejecutable ( no necesita instalación)

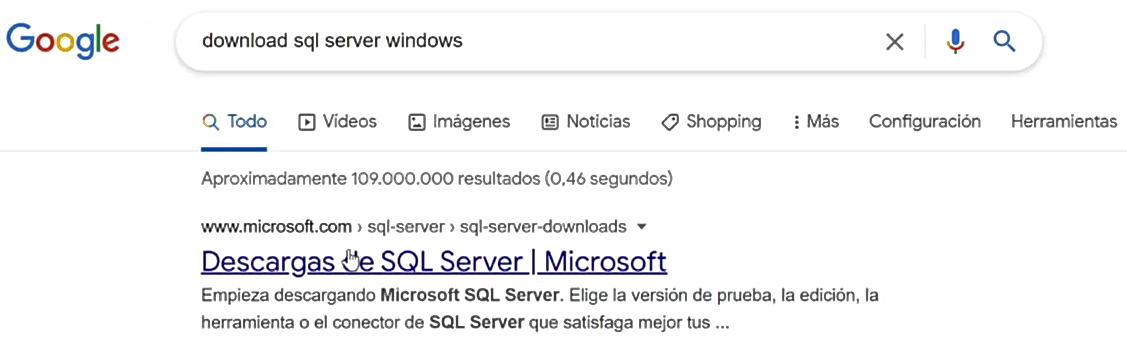


Al abrirlo por primera vez da un error, pues necesita varios programas para su funcionamiento. 



Seguramente tengamos que instalar SQL Server

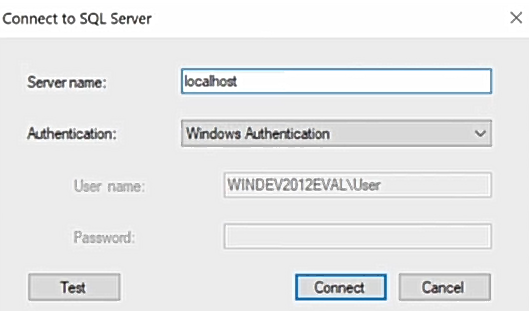
**download sql server windows**



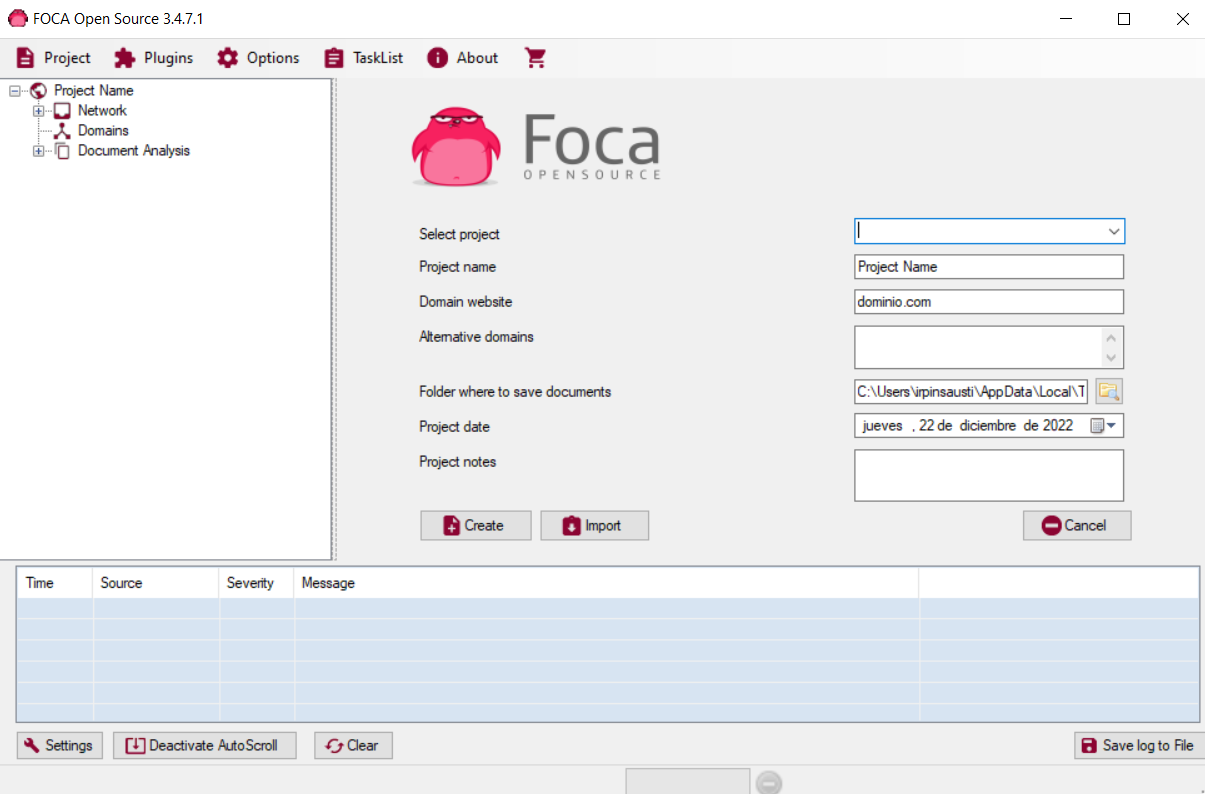
Utilizamos la versión para desarrolladores. La descargamos y la instalamos.



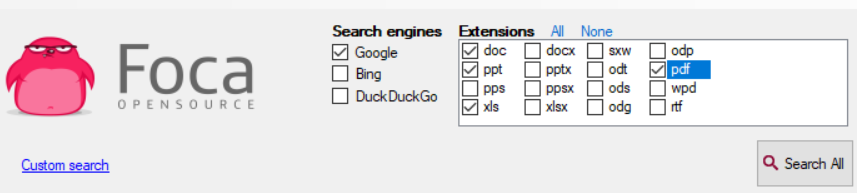
Una vez instalado SQL la primera vez dará un error porque no encuentra la base de datos. Le indicamos localhost

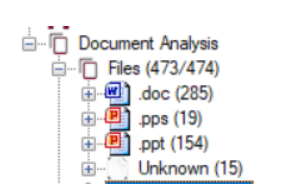


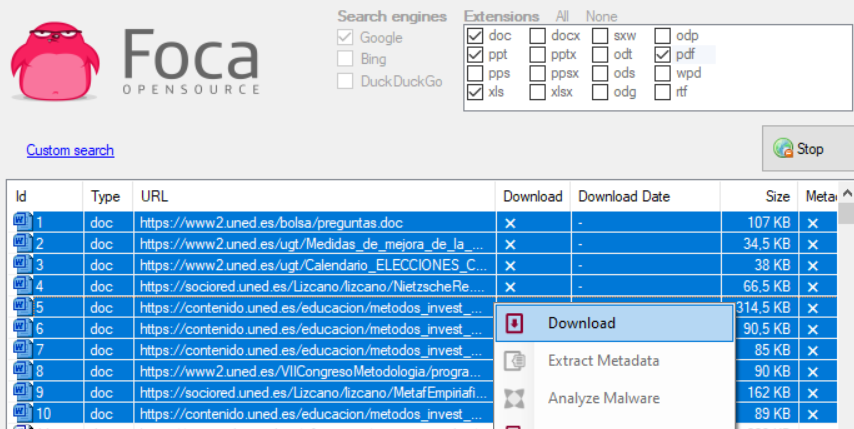
Una vez abierta la aplicación podemos extraer metadatos de ficheros individuales o algo más interesante de dominios completos.Ponemos el nombre del dominio y el dominio y creamos el proyecto.



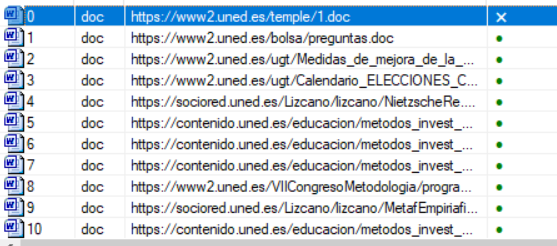
Seleccionamos los tipos de ficheros que queremos buscar y el buscador a utilizar y pulsamos en búsqueda.



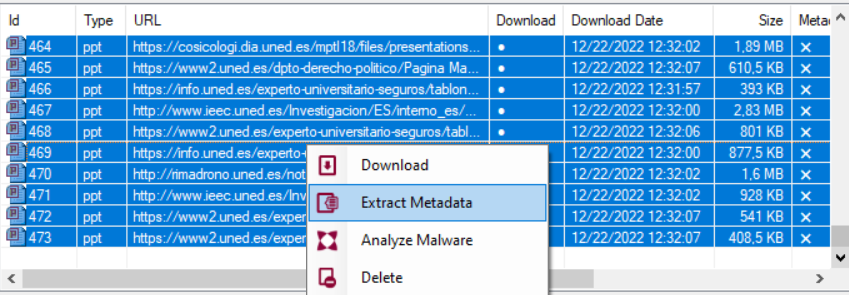
Una vez ha localizado los archivos ,pulsamos botón derecho y los descargamos.

****

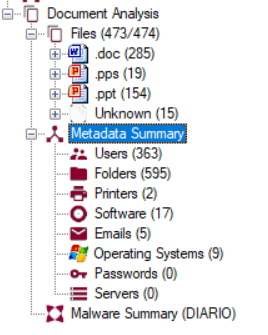
Según se van descargando el indicador de download se pone en verde



Una vez se han descargado los seleccionamos y con el botón derecho le damos a extraer metadatos



Tras finalizar el proceso podemos ver , que en el ejemplo, ha localizado 363 nombres de usuario, 595 carpetas, 2 impresoras , ha identificado 17 softwares diferentes para la creación de los archivos y 5 email de la organización .



Esta información respecto a la organización puede ser utilizada para realizar algún ataque más sofisticado.