***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

26/3/2021

Trabajo 3

FOCA

Diseño y Administración de Sistemas y Redes

Contenido

[1. Introducción 2](#_Toc68681142)

[1.1. ¿Qué es FOCA? 2](#_Toc68681143)

[1.2. Técnicas 3](#_Toc68681144)

[2. Instalación de FOCA 4](#_Toc68681145)

[3. ¿Qué son los Metadatos? 5](#_Toc68681146)

[3.1 Metadatos en la Informática 6](#_Toc68681147)

[3.1.1. Como ver los metadatos de forma manual 7](#_Toc68681148)

[4. Análisis con FOCA: DNS Spoofing 8](#_Toc68681149)

[5. Análisis con FOCA: Metadatos de un documento 9](#_Toc68681150)

[5.1. Análisis de Metadatos de una imagen 10](#_Toc68681151)

[5.2. Análisis de metadatos de un documento Word 12](#_Toc68681152)

[5.3. Análisis de un dominio Web (marca.com) 14](#_Toc68681153)

[5.3.1. Configuración de Motor de Busqueda personalizado 14](#_Toc68681154)

[5.3.2. Busqueda de los metadatos 15](#_Toc68681155)

[5.3.3. Análisis de los metadatos 18](#_Toc68681156)

[5.4. Análisis de un dominio Web (ubu.es) 20](#_Toc68681157)

[6. Casos que tienen que ver con los metadatos: Tony Blair y el informe Chilcot 24](#_Toc68681158)

[7. Buenas practicas para evitar problemas con los metadatos 25](#_Toc68681159)

[8. Conclusiones 26](#_Toc68681160)

[9. Bibliografía 27](#_Toc68681161)

# Introducción

## 1.1. ¿Qué es FOCA?

Como diría uno de sus autores, (Alonso, s.f.) FOCA es una herramienta para ayudar en la recolección de ficheros publicados en websites, la extracción de metadatos y el análisis de estos.

Esta herramienta fue creada por el equipo de Eleven Paths, sección de ciberseguridad de telefónica. Si vamos a su página web (Eleven Paths, s.f.), nos dan una breve descripción de esta herramienta. Nos dicen que FOCA (Fingerprinting Organizations with Collected Archives) es una **herramienta** usada para **encontrar metadatos e información escondida en los documentos que escanea**. Estos documentos pueden estar en páginas web, o los podemos analizar nosotros desde nuestro equipo.

Estos documentos se buscan usando tres posibles motores de búsqueda (Google, Bing y DuckDuckGo). Todos los resultados obtenidos por estos motores de búsqueda se juntan, obteniendo una gran variedad de documentos. También se pueden añadir archivos locales para extraer la información EXIF de imágenes, (esta es la información que tienen las imágenes tomadas con cámaras digitales) y también se hace un análisis completo de la información descubierta gracias a la URL antes de descargar los archivos.

Con todos los datos extraídos de los archivos, FOCA va emparejando información con la intención de identificar que documentos han sido creados por el mismo equipo y que servidores y clientes podemos inferir de ellos.

## 1.2. Técnicas

En su página web (Eleven Paths, s.f.) también nos explican las técnicas usadas para llevar a cabo las tareas que hemos visto antes:

* **Busqueda en la Web:** Busca hosts y dominios comunicados con las URLs asociadas al dominio principal. Cada link se analiza por separado para extraer de nuevos hosts y dominios.
* **Busqueda por DNS:** Cada domino se comprueba para verificar cuales son los nombres de host configurados en los servidores NS, MX y SPF, para conseguir nuevos nombres de hosts y de dominio.
* **Resolución IP:** Cada nombre de host se resuelve por DNS para obtener su dirección IP asociada. Para realizar esta tarea lo más preciso posible, el análisis se hace usando el DNS interno a la organización.
* **Escáner PTR:** Para detectar más servers en el mismo segmento que una determinada dirección IP.
* **Bing IP:** Para cada IP que se ha descubierto, se buscan nuevos nombres de dominio asociados con esa IP.
* **Nombres Comunes:** Es un módulo diseñado para llevar a cabo ataques de diccionario contra el DNS. Usa un documento de texto que contienen nombres comunes de host como ftp, pc01, pc02, intranet, extranet, internal, test, etc.
* **Predicción DNS:** Cuando se descubre un nombre de una máquina, se utiliza esta técnica si se sospecha que el resto de los nombres de las maquinas pueden seguir un patrón.
* **Robtex:** El servicio Robtex es un servicio de internet para analizar direcciones IP y nombres de dominio. FOCA usa este servicio para intentar descubrir nuevos dominios buscando la información disponible en Robtex.

# 2. Instalación de FOCA

En este apartado vamos a cubrir la instalación de la herramienta FOCA paso a paso.

He decidido cubrir este paso, ya que no es tan simple como ejecutar un instalador y listo. Al ser FOCA un programa de **código abierto**, el programa viene sin compilar, por lo que veremos qué pasos seguir para su instalación. Para ello, haremos uso de su [repositorio en GitHub](https://github.com/ElevenPaths/FOCA) (GitHub FOCA, s.f.)

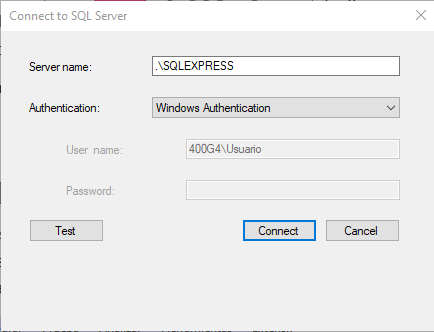
Primero descargaremos el repositorio en formato ZIP.

Para compilarlo, lo abriremos con el visual studio, dando doble click en el archivo de la solución.



Una vez se nos abra el proyecto, podremos hacer cualquier cambio en el código. En nuestro caso esto no va a ser necesario, por lo que compilaremos la solución desde la pestaña Compilar.





Aviso que nos saldrá si no tenemos instalado SQL Express

FOCA necesita una conexión a un **servidor SQL,** por lo que será lo primero que nos pida. Para ello, deberemos tener instalado el programa **SQL Express**.

Una vez lo tengamos instalado, podremos acceder ya a la pantalla principal de FOCA.

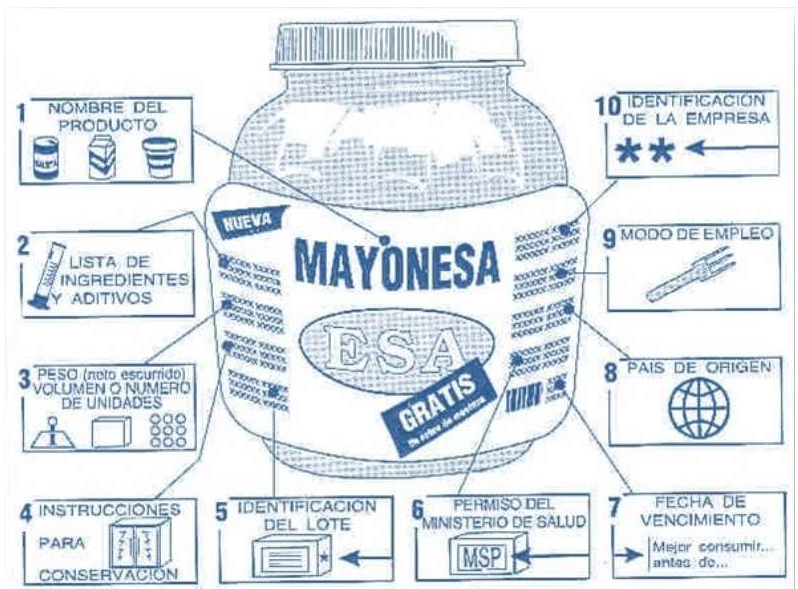
# 3. ¿Qué son los Metadatos?

Hemos mencionado que la principal utilidad de la herramienta FOCA es la extracción de metadatos de dominios web (y archivos), por lo que antes de comenzar a utilizar esta herramienta debemos tener claro lo que son.

Para empezar, debemos tener en cuenta que los metadatos no es un termino exclusivo del mundo de la informática, sino que se aplica a muchos más ámbitos.

Por ejemplo, una buena definición la encontramos en la Infraestructura de Datos Espaciales del Gobierno de Perú (Gob. de Perú), que nos dice que son **“datos acerca de los datos”** y sirven para suministrar información sobre los datos producidos. Los metadatos consisten en información que caracteriza datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos.

Podríamos pensar en los metadatos como, por ejemplo, toda la información que nos viene en la etiqueta de un alimento. Nos dice donde se originó, como se creó, que contiene, cuánto cuesta, etc.



## 3.1 Metadatos en la Informática

Si ya nos cerramos al ámbito de la informática, podemos concretar un poco lo que son los metadatos que nos conciernen para esta práctica. Para entenderlos mejor, tomaremos como ejemplo la explicación de Yúbal Fernandez (Fernandez, 2018).

Los archivos que generamos en el ordenador con diferentes programas tienen **datos concretos**, que son **los que introducimos**, pero también hay otra serie de datos que describen otras características sobre el contexto del archivo, unos **metadatos** de los que por defecto **no se tiene control directo**. Por ejemplo, si creamos un archivo de Windows con Word u otra herramienta podemos escribir en él todo lo que queramos, pero luego la aplicación generará una serie de metadatos para ese archivo. En ellos describirá aspectos como la fecha en la que fue creado, la aplicación exacta que utilizaste o la fecha en la que hiciste una última modificación del contenido.

En el caso de archivos multimedia, como fotos y videos encontraremos también información que va desde las características de la foto como la velocidad ISO o tiempo de exposición hasta otros datos más personales, como el fabricante o modelo de la cámara o smartphone desde el que se sacó la foto.

En ambos casos son metadatos que **se general automáticamente** para describir el contenido de los datos del archivo, de ahí la descripción de "datos sobre datos".

Estos datos a priori pueden parecer que no son muy útiles, a parte de como curiosidad, pero **diferentes servicios y redes sociales también los utilizan** para categorizar y organizar el contenido que subes a ellos, pudiendo establecer la fecha exacta cuando se creó el archivo, la localización u otras características.

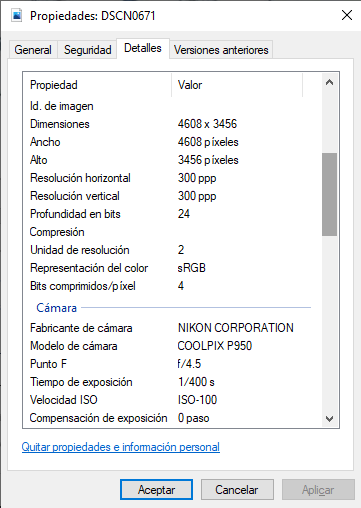
### 3.1.1. Como ver los metadatos de forma manual

En este apartado veremos como ver los metadatos de cualquier archivo de forma manual (esto es, sin herramientas de terceros), en un sistema operativo Windows. En nuestro caso, comprobaremos los metadatos que se guardan en una fotografía realizada por una cámara.

Para ello, lo primero que tenemos que hacer es dar click derecho en el archivo, y acceder a las **propiedades**.



Después, seleccionamos, dentro de las pestañas superiores, la pestaña “**Detalles**”. Aquí podremos ver toda la información almacenada sobre nuestra fotografía.



Podemos observar que vienen muchos datos tecnicos sobre la foto, así como el nombre y las especificaciones de la cámara, y los parámetros que tenia cuando se tomó la fotografía. Aunque no se vea en la captura, también nos informa de la fecha y hora cuando se realizó, entre otros parámetros.

La herramienta FOCA hace uso de estos datos para poder realizar un análisis complejo sobre la infraestructura o la red detrás de una página web.

Si queremos **eliminar estos metadatos**, en la parte inferior de la ventana tenemos una opción que nos deja “Quitar propiedades e información personal”.

# 4. Análisis con FOCA: DNS Spoofing

Aunque no es una de las funciones principales de FOCA, es una función bastante interesante. Debido a que no su función principal, únicamente explicaremos lo que hace esta característica, pero no se entrara en un ejemplo práctico.

La idea de esta característica es simple, aprovechar si una empresa, a través de su dominio web, usa un DNS propio, para introducirse y ver las resoluciones de este DNS.

Dicho con otras palabras, podemos aprovecharnos si una empresa tiene un DNS propio para **tener un log en tiempo real de todas las páginas web a las que están accediendo**.

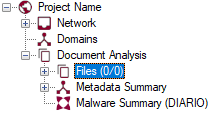
Esto es un potencial riesgo, ya que si se sabe a qué paginas acceden nuestros trabajadores, a que horas, y con qué frecuencia, se podría preparar un ataque “personalizado” a nuestra empresa bastante complejo.

# 5. Análisis con FOCA: Metadatos de un documento

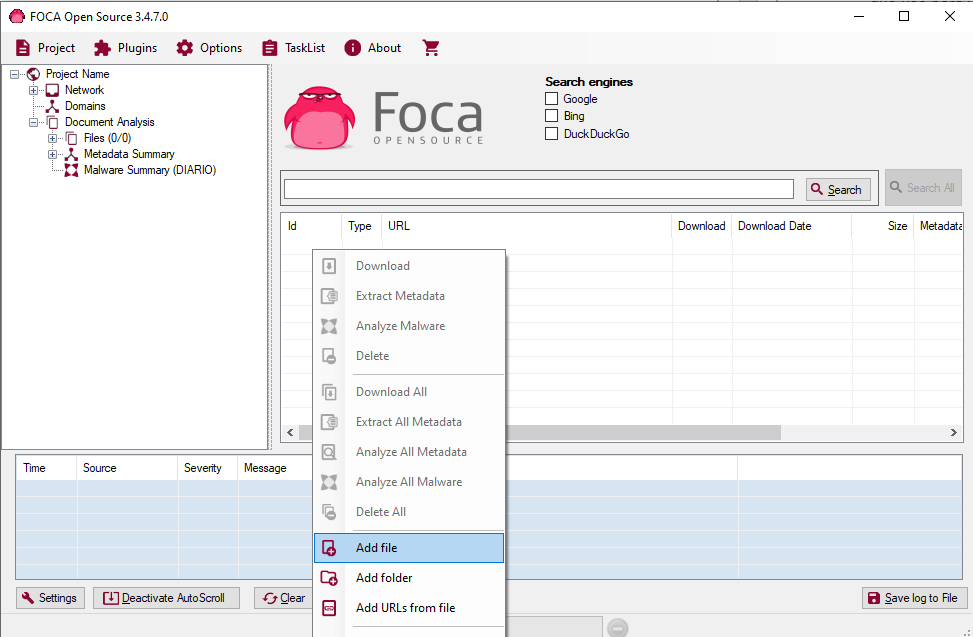
En este apartado veremos, paso a paso, como analizar los metadatos de un documento con la herramienta foca, y aprenderemos a interpretar los resultados.

Lo primero que tenemos que hacer es abrir FOCA, y **subir el archivo que queramos analizar**. Por poder hacer una comparativa, utilizaré la misma imagen que use para ver los metadatos de forma manual.

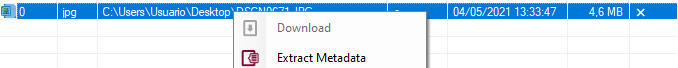
Para ello primero tenemos que ir, en el menú de la izquierda, a la pestaña **Files**, dentro de **Document Analysis**.



Para agregar archivos a FOCA podemos o bien arrastrarlos, o bien dando click derecho a la lista de archivos (en un principio vacía), y seleccionar agregar archivo.



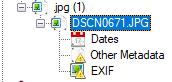
Una vez hayamos subido el archivo, daremos click derecho sobre él y seleccionaremos “**Extract Metadata**”



Una vez hecho esto, nos añadirá la información sacada al “**Metadata Summary**”, que es un apartado donde se va registrando todos los datos que se van sacando de todos los archivos. Esto es muy útil cuando se analizan muchos archivos de una misma pagina web, por ejemplo, como veremos más adelante

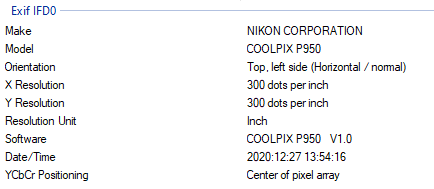
## 5.1. Análisis de Metadatos de una imagen

Si lo que queremos es ver los datos extraídos de nuestra imagen, daremos click sobre la imagen en el menú de la izquierda.

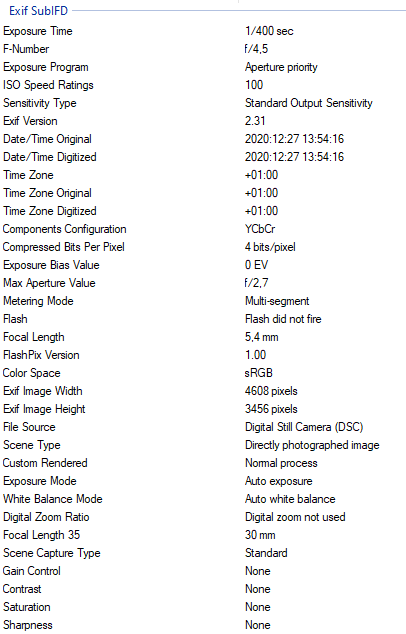


Como podemos observar, ha extraído diferentes metadatos: **Fechas, EXIF,** y **otros metadatos**.

Lo que realmente nos interesa de una imagen es la información EXIF, que vimos a continuación, por lo que vamos a analizar por encima, mediante capturas, lo que hemos conseguido extraer.

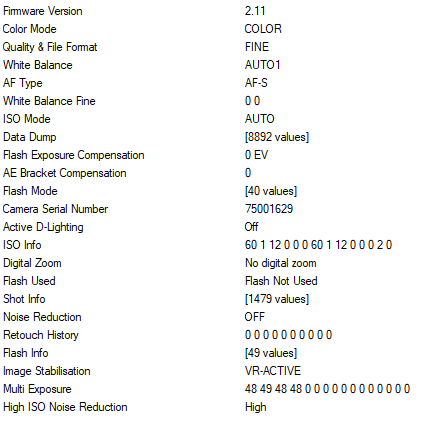


En el primer apartado podemos ver, como apartados importantes, la marca y modelo de la cámara, y fecha de toma de la fotografía.



En el segundo apartado podemos ver datos mas interesantes, como los parámetros de la cámara a la hora de tomar la imagen. Algunos de estos so la **exposición**, el **tiempo de ISO**, o la **apertura**. También podemos ver detalles como si se había usado **flash**, o los parámetros para el color.

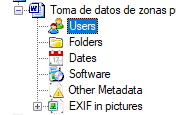
En el ultimo apartado podemos ver parámetros propios de Nikon, como su **versión de firmware**, el **color de la cámara**, o su **número de serie**.



Dependiendo con que dispositivo se haya sacado la foto, se pueden extraer más o menos datos EXIF. Por ejemplo, si la fotografía se hubiera tomado con un IPhone, podríamos **saber las coordenadas de la fotografía**, ya que los IPhone tienen esta función por defecto activada.

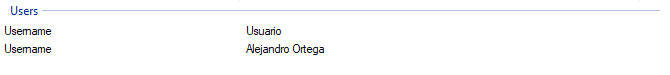
## 5.2. Análisis de metadatos de un documento Word

En este apartado analizaremos un documento de Microsoft Word, para ver por encima que diferencias en cuanto a extracción de metadatos conseguimos con respecto a una foto.

Para ello utilizaremos el segundo trabajo de esta misma asignatura, correspondiente a la toma de videos en vías públicas.

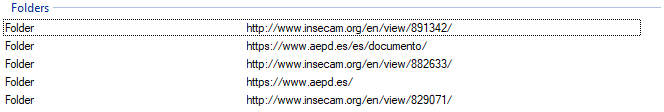
Los pasos para cargar el archivo y extraer los datos son los mismos, por lo que nos saltaremos la explicación e iremos directamente al resultado.

Como podemos observar, la primera categoría que vemos es la de los **usuarios** que han trabajado.

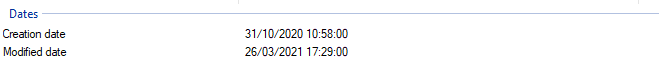


En este caso, podemos observar como trabaje en el Word con dos usuarios diferentes. Al ser yo el autor de este archivo, puedo dar fe de que así fue, ya que trabaje en este archivo desde dos usuarios diferentes.

En **folders** podemos observar también links que aparecen en el documento.



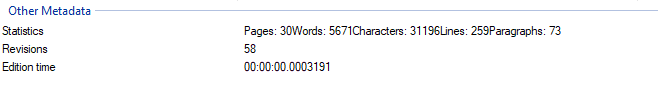
Tenemos también un apartado de **fechas**, donde aparecen la fecha de creación y de última modificación.

****

En el apartado de **software** vemos con que programa ha sido creado, que en nuestro caso es Microsoft Word



En el apartado de **otros metadatos**, podemos ver información relevante al archivo, como el número de páginas, de caracteres, etc.



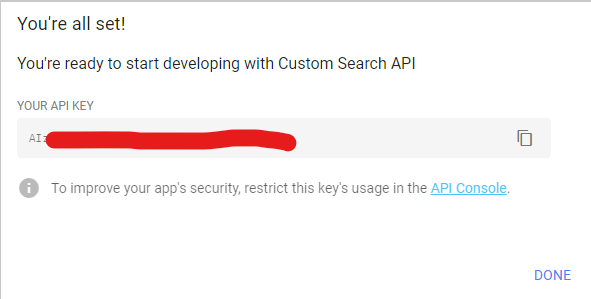
Por último, también hay un apartado para ver los **metadatos EXIF** de las imágenes del archivo.

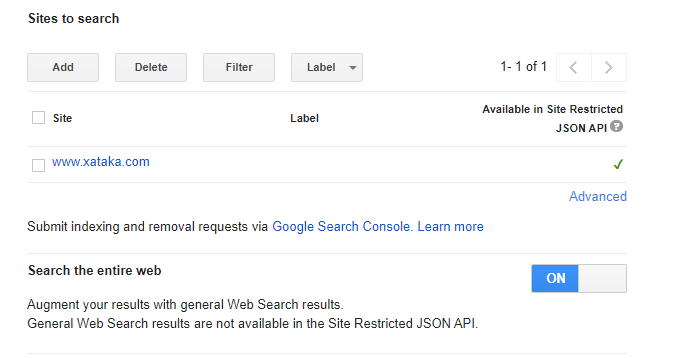
## 5.3. Análisis de un dominio Web (marca.com)

En este apartado usaremos FOCA para uno de los propósitos para los que se creó, y en uno de los que más destaca: el análisis de metadatos de un dominio web.

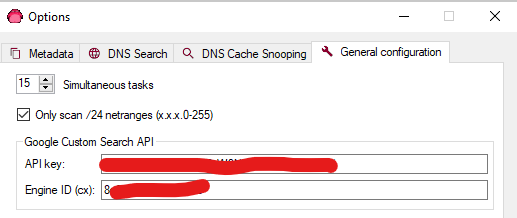
### 5.3.1. Configuración de Motor de Busqueda personalizado

Como hemos visto anteriormente, FOCA se basa en realizar continuadas consultas a un dominio web, para encontrar sus documentos y descargarlos. Sin embargo, esta pagina web puede **confundir las búsquedas de FOCA con un ataque DoS**. Para esto, tendremos que configurar FOCA para que use el **API de Búsquedas de Google**. En su página de GitHub (Bezares, s.f.) nos explican cómo conseguir una key de desarrollador de Google para poder usar esta api.

Para ello nos tenemos que dar de alta en su pagina de desarrolladores de Google, ir al producto “**Custom Search JSON Api**”**,** y darle al botón “get a key”. Seguiremos los pasos, y nos darán la key.

A continuación hay que modificar los parámetros de nuestro nuevo motor de búsqueda en <https://cse.google.com/create/new?refresh=1>, por lo que seguiremos los pasos de la issue del GitHub de foca referenciada anteriormente, seleccionando la pagina web que queremos buscar y el parámetro “Search the entire Website”.

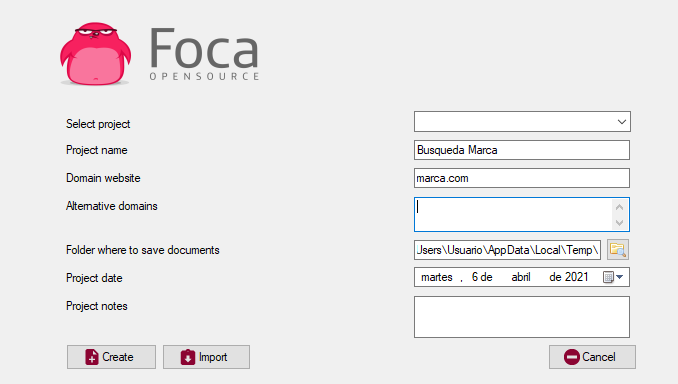
Por último, **configuraremos FOCA para que use esta API de motor de búsqueda**. Para ello iremos a foca, y a la pestaña ajustes.



Le daremos a guardar, y ya tendremos configurado FOCA para que busque con nuestro motor de búsqueda.

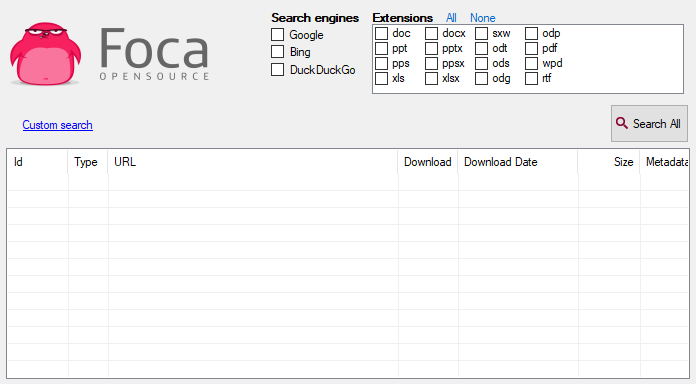
### 5.3.2. Busqueda de los metadatos

A continuación veremos cómo realizar este escaneo y análisis, y una vez obtenidos los resultados, los interpretaremos. Para nuestro ejemplo, usare la web de marca.com. Lo primero de todo es crear un nuevo proyecto desde la pestaña “**Project Name**”**.** Los primeros pasos son rellenar todos los campos con el nombre del proyecto, el dominio web que queremos analizar, y la carpeta donde queramos que se almacenen los archivos descargados.

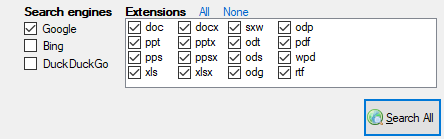


En nuestro caso no introduciremos ningún dominio alternativo, ni ninguna anotación. Además, dejaremos la carpeta predeterminada para guardar los archivos descargados. Esta es una carpeta temporal, con lo que, al apagar el equipo, se borraran todos los documentos que hay en ella.

A continuación le daremos a **crear**, y nos llevara a la “pagina principal” del proyecto, como podemos ver a continuación.



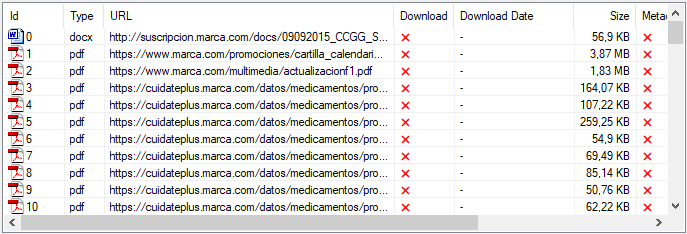
Lo que nos interesa ahora es el cuadro superior. En el podemos marcar **que** **tipos de archivos queremos descargar**, y **con que buscadores indexarlos**. En nuestro caso, y lo que se suele hacer generalmente, es **seleccionarlo todo**; es decir, buscaremos todos los archivos posibles, pero solo con Google, que es el que hemos configurado previamente.



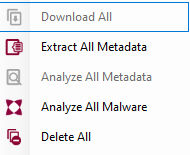
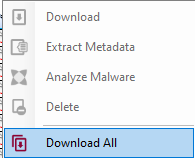
Una vez seleccionados, le daremos a buscar todo, y comenzará la búsqueda y descarga de los archivos.



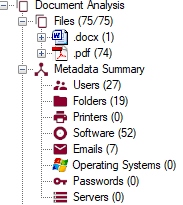
Como podemos observar en el log, ha encontrado 75 archivos diferentes, que nos aparecerán en la ventana del proyecto:



A continuación hay que **descargarlos todos**, dándole a “download all”, y posteriormente, **extraer sus metadatos**.



También se recomienda analizar el malware que puedan tener los documentos antes de hacer nada con ellos. Este malware se analiza con la herramienta DIARIO. Una vez analizado, procederemos a la extracción de los metadatos.

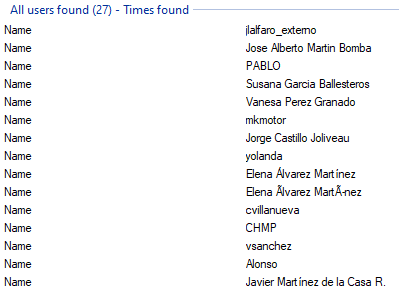
Una vez extraídos, podemos observar que se nos han creado varios desplegables en el menú de la izquierda, por lo que vamos a analizar.

### 5.3.3. Análisis de los metadatos

Este análisis no es muy diferente del hecho con archivos individuales, pero vamos a indagar un poco en que tipo de datos hemos conseguido.

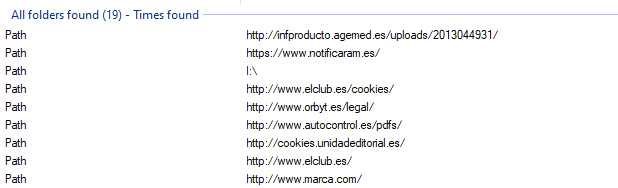
**Usuarios**

Podemos empezar con los usuarios que ha encontrado. La herramienta ha conseguido sacar 27 personas que han trabajado en estos documentos, algunos de los cuales se ven a continuación.



Esto es útil para saber, por ejemplo, que tipo de personas trabajan en esta empresa, y podemos interpretar que tienen acceso a lo que se cuelga a la web, por lo que con otras herramientas podríamos investigarles un poco más, con el objetivo de sacar más información suya, o contraseñas.

**Ficheros**



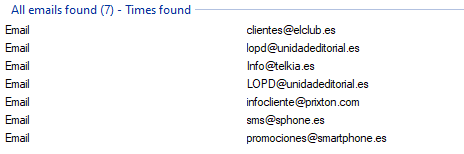
En este apartado podemos observar, dentro de la pagina web, que subdominios o ficheros están relacionados con ella, para poder hacer a posteriori una búsqueda más profunda si queremos.

**Software**



Dentro del software, podemos ver una larga lista de programas que se usan dentro de esta empresa. Esto nos puede ser útil a la hora de buscar vulnerabilidades, ya que si sabemos si alguno de esos programas tiene algún fallo, podremos explotarlo. También nos podría servir, por ejemplo, si queremos introducir algún tipo de virus, ya que sabemos con que trabajan, y eso nos facilita el trabajo porque sabemos con que tipo de programa abrirán nuestros archivos, por ejemplo.

**Emails**

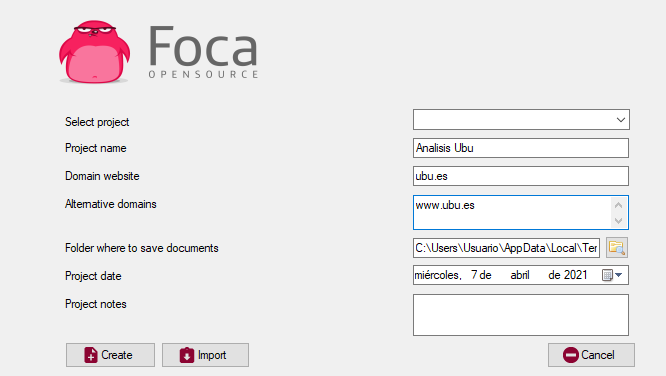


Lo ultimo que hemos conseguido sacar son una lista de emails que había por la página web, aunque en este caso son todo emails públicos, por lo que no hemos podido sacar más información de valor.

Podríamos haber sacado más información de valor, como **servidores**, **impresoras**, **sistemas operativos** o incluso **contraseñas** pero en este caso no ha sido posible.

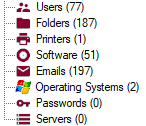
Por último, nos deja también ver los metadatos de cada fichero descargado por individual, como hicimos en apartados anteriores. Esto es útil si queremos saber, por ejemplo, la fecha en concreto en que se han ido creando, o información EXIF de las imágenes.

## 5.4. Análisis de un dominio Web (ubu.es)

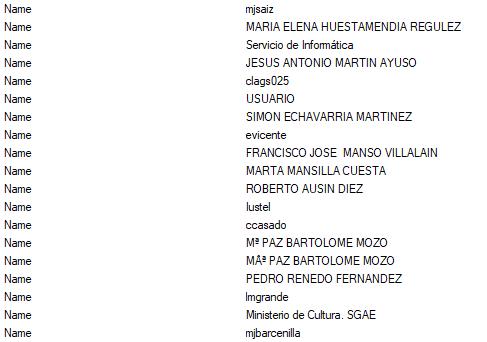


En este caso, a modo de curiosidad, escanearemos la página web de la ubu, para comprobar a ver que podemos encontrar.



Como podemos observar, se han encontrado 104 ficheros, por lo que procederemos a descargarlos, extraer sus metadatos, y analizarlos.

En cuanto a los **usuarios**, podemos ver que hemos sacado 77 usuarios, entre los que se distinguen una peligrosa cantidad de nombres propios.



Esto es peligroso, ya que, si conocemos que estas personas tienen acceso a subir documentos a la pagina principal de la ubu, podrían ser un potencial blanco de ataques.

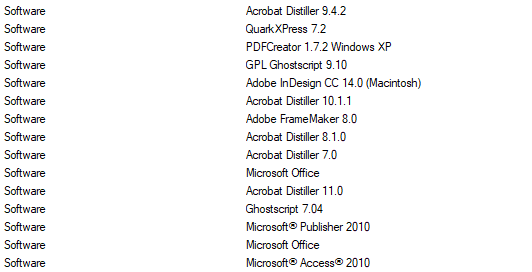
Pasamos a las **carpetas**, de las cuales se han detectado 187, aunque de un vistazo general podemos observar que la mayoría son únicamente direcciones web de donde se toman referencias:



Es curioso, porque también encontramos una **impresora**, que, sin más datos, puede ser una de las que se usan para imprimir los documentos en la universidad.



Dentro del **software**, donde encontramos 51 diferentes, podemos ver los programas con los que se han creado los documentos, aunque son los típicos de ofimática.



Mirando los **sistemas operativos** que aparecen, podemos ver que en la gestión de la página web de la universidad se usa Windows XP (lo cual sabemos que, por su antigüedad, podría ser bastante vulnerable).



Lo **Peligroso** viene a la hora de ver los **correos** donde, a parte de un par de correos de gestión de la universidad, podemos ver mas de 150 correos de alumnos.

Esto, aunque no sea ilegal, es una mala práctica, que luego veremos cómo solucionar.

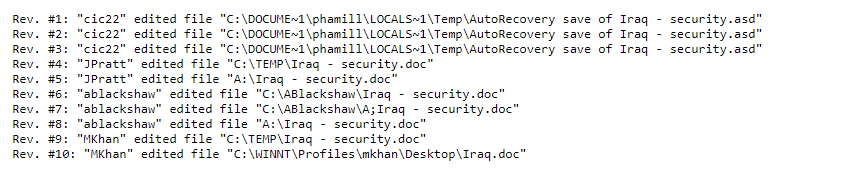
# 6. Casos que tienen que ver con los metadatos: Tony Blair y el informe Chilcot

En este apartado veremos un caso en los que los metadatos han jugado un papel importante, para ver lo útiles (o peligrosos) que pueden llegar a ser los metadatos.

En torno a 2009, Tony Blair, primer ministro del Reino Unido entre 1997 y 2007, creo un documento en la guerra con Iraq.

Cuando lo entrego al presidente de Reino Unido, este le preguntó que si el, o su gabinete, había modificado este documento, lo cual Anthony Blair respondía siempre que no.

Sin embargo, a la hora de analizar los metadatos de este documento, que era un Word normal y corriente, se encontró que en verdad sí que había sido modificado por multitud de personas, lo que supuso un gran escándalo.

Aunque el documento original es bastante difícil de encontrar, podemos ver un registro de los metadatos de edición (Microsoft Word Bytes, s.f.), en el que podemos ver cuantas personas lo editaron.

Esto es porque por aquel entonces, Microsoft Word guardaba un log de las ultimas 10 modificaciones de un fichero. Como podemos observar, hay hasta cuatro personas que editaron el documento antes de que Tony Blair se lo presentara al presidente de Reino Unido:

* **P. Hamill**
* **J. Pratt**
* **A. Blackshaw**
* **M. Khan**

# 7. Buenas practicas para evitar problemas con los metadatos

En palabras de uno de los autores de FOCA, Chema Alonso, una de las mejores prácticas, de cara a proteger nuestra empresa, asociación, entidad, etc. frente a ataques, es **deshacernos de los metadatos** para disminuir la facilidad con la que se nos puede efectuar un ataque informático.

Una de las maneras que hay para hacerlo es **eliminando los metadatos manualmente antes de subir un documento a la web**. Podemos eliminarlos como vimos en el apartado de sacar los metadatos automáticamente, o con las herramientas que nos proporcionan algunos programas.

Por ejemplo, Word tiene implementado un modo para eliminar los metadatos, mediante el inspector de documento.

Otra herramienta, mas orientada a nivel empresarial, es **metashield** (Eleven Paths, s.f.), creada por el grupo de eleven Paths, se trata de un programa que corre en el servidor web y que, cuando se sube un nuevo documento (ya sea a la página web, por correo, etc.), antes de estar disponible al público, pasa por metashield, y este le borra todos los metadatos.

# 8. Conclusiones

En mi opinión, este ha sido uno de los trabajos mas interesantes que he realizado.

No solo me ha enseñado lo que son los metadatos, algo bastante curioso e interesante ya de por sí, sino que he aprendido también a analizarlos, ya sea de documentos individuales, o de grandes páginas web.

Me parece que esto va a ser bastante útil, ya sea para el resto de los trabajos de la asignatura, como para mi futuro laboral, ya que me gustaría orientarme en algo que tenga que ver con la seguridad.

También me ha obligado a indagar en maneras de protegerme de estos posibles ataques, y a medida que iba realizando el trabajo y viendo la cantidad de datos que podía recabar, se me han ido ocurriendo maneras de aprovechar estos datos (tanto para buenas como para malas prácticas).

# 9. Bibliografía

(s.f.). Obtenido de https://www.blacknetworkhacking.com/2014/04/metadatosen-el-documento-de-tony-blair.html

Alonso, C. (s.f.). *Un Informatico en el Lado del Mal*. Obtenido de https://www.elladodelmal.com/2009/04/foca-manual-de-usuario-i-de iv.html

Bezares, M. (s.f.). *github.com*. Obtenido de https://github.com/ElevenPaths/FOCA/wiki/How-to-set-up-Google-API-search

Eleven Paths. (s.f.). Obtenido de https://www.elevenpaths.com/es/productos-servicios/data-protection/data-lossprevention/metashield

Eleven Paths. (s.f.). *Eleven Paths*. Obtenido de https://www.elevenpaths.com/innovation-labs/technologies/foca

Fernandez, Y. (17 de Septiembre de 2018). *Xatak*. Obtenido de https://www.xataka.com/basics/que-metadatos-archivo-que-informacion-muestran-como-se-borran

*GitHub FOCA*. (s.f.). Obtenido de https://github.com/ElevenPaths/FOCA

Gob. de Perú. (s.f.). *Gobierno de Perú.* Obtenido de https://geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos

Microsoft Word Bytes. (s.f.). Obtenido de http://dfir.com.br/wp-content/uploads/2014/02/blair.htm