Grado en Ingeniería Informática

Departamento de Ingeniería Informática

Seguridad en los Sistemas Informáticos

Práctica 3.4: Análisis de metadatos con FOCA

Autores:
Juan Boubeta Puig,
Manuel Lara Romera y
David Ureba Moreno

Fecha:
29 de octubre de 2019

Índice

Índice de figuras

1. Objetivo

El objetivo de esta práctica es conocer la famosa herramienta FOCA y aprender a usarla para analizar los metadatos [2].

2. Conocimientos previos

A continuación, se describen los conocimientos previos que han de conocerse para llevar a cabo esta práctica:

Metadatos Se denominan metadatos a la información extra existente sobre un archivo que describe características de ese archivo o fichero. Un ejemplo sería la metainformación relativa a una fotografía digital: cuando esta se toma se almacenan datos sobre la cámara, el flash, el obturador e incluso la geolocalización.

3. Herramientas necesarias

Para la correcta realización de la práctica usaremos la herramienta FOCA, la cual tendremos que instalar.

FOCA funciona en Windows de manera nativa y en Linux / OS X haciendo uso de Wine.

3.1. Instalación de FOCA en Windows

En primer lugar, tendremos que acceder a la página web oficial de FOCA (`https://www.elevenpaths.com/es/labstools/foca-2/index.html`) y descargar la herramienta.

Como podemos ver en la Figura 1, si hacemos clic donde se indica "pincha aquí", se nos descargará un archivo llamado *FocaPro.zip*. Entonces descomprimimos el contenido de dicho archivo en el sitio donde queramos almacenar la herramienta, ya que es un ejecutable portable y no requiere de instalación en el equipo.

Una vez realizado el paso anterior, accedemos a la carpeta *bin/* y, dentro de esta carpeta, ejecutaremos *FOCA.exe*, que será la herramienta con la que vamos a trabajar a lo largo de esta práctica.

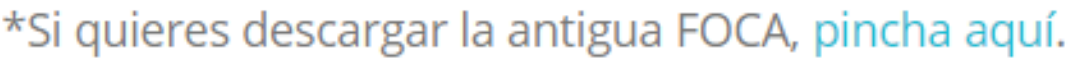

Figura 1: Descarga de la herramienta FOCA.

Nota: es posible descargarse la última versión disponible de FOCA desde GitHub: `https://github.com/ElevenPaths/FOCA/releases` En este caso, para que FOCA pueda ejecutarse correctamente, será necesario descargar e instalar también SQL Server 2017 Express Edition.

3.2. Instalación de FOCA en Linux

También podemos instalar FOCA en Linux en una máquina externa, a partir de los pasos descritos en el tutorial publicado en [1].

Conviene destacar que para usuarios de distribuciones Linux debemos usar una aplicación conocida como *PlayOnLinux* que nos ayudará a instalarlo. Se puede encontrar en casi todos los centros de software de las distintas distribuciones.

4. Desarrollo de la práctica

Para la realización de la práctica investigaremos sobre el uso de FOCA, el análisis de metadatos y el análisis de archivos sobre un sitio web. FOCA usa técnicas de *gathering* y *hacking* con buscadores para obtener información sobre sitios webs.

5. Análisis de archivos locales

Lo primero que haremos, una vez instalada la herramienta, será ejecutarla. Cuando se nos abra veremos una pantalla como la que apreciamos en la Figura 2. Abrimos nuestro explorador de archivos, seleccionamos algún grupo de archivos que queramos analizar, y los arrastramos a la ventana de FOCA.

Una vez hecho esto, desplegaremos en la barra de la izquierda el menú *metadata* y, dentro de este, *documents*, lo que nos mostrará los archivos añadidos. Los seleccionamos todos y hacemos clic derecho y pulsamos en *extract all metadata*, devolviéndonos un resultado como el que podemos ver en la Figura 3.

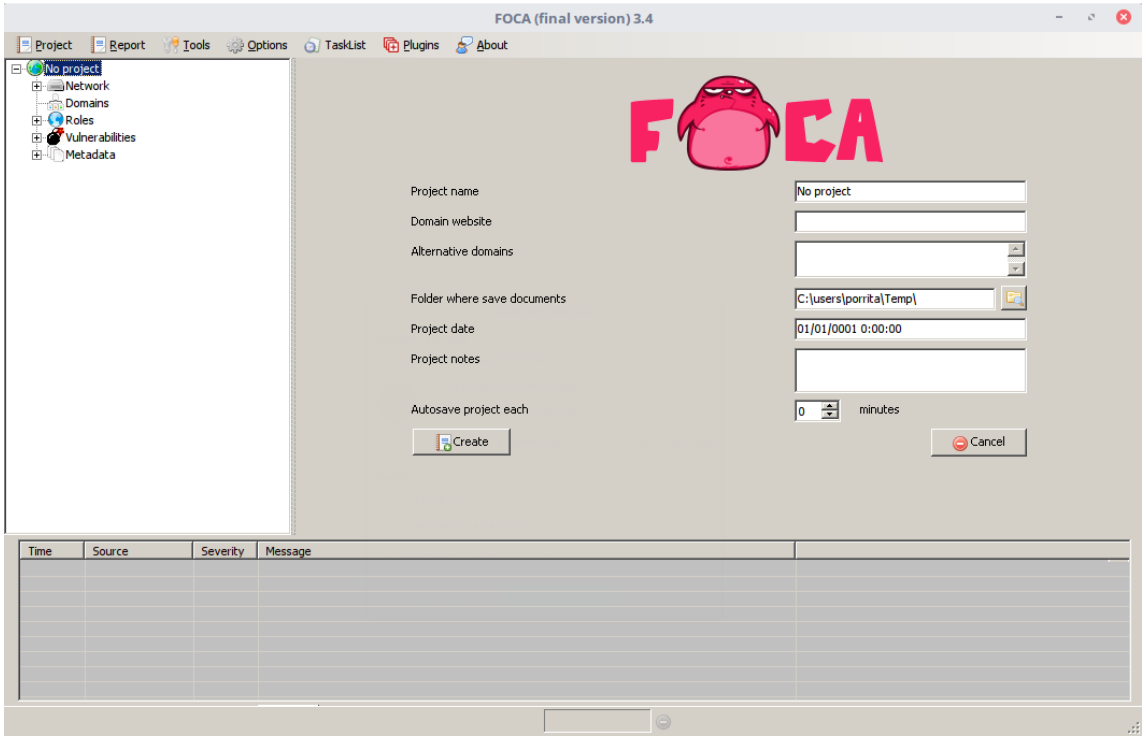

Figura 2: Ventana principal de FOCA.

Si entre los archivos que hemos añadido hay diversos tipos, veremos los resultados por categorías de archivos. Si hemos añadido alguna imagen, en sus metadatos podremos ver toda la información relacionada con la manera en que se tomó la fotografía y los valores de los parámetros de la cámara.

5.1. Ejercicio 1

Haciendo uso de los ficheros contenidos en *METADATA_FOCA.zip*, contesta a las siguientes preguntas:

- ¿Qué datos específicos podemos observar en *metadata summary*?
- ¿Qué utilidad podemos deducir que tiene el analizar localmente los metadatos de archivos de nuestro sistema?

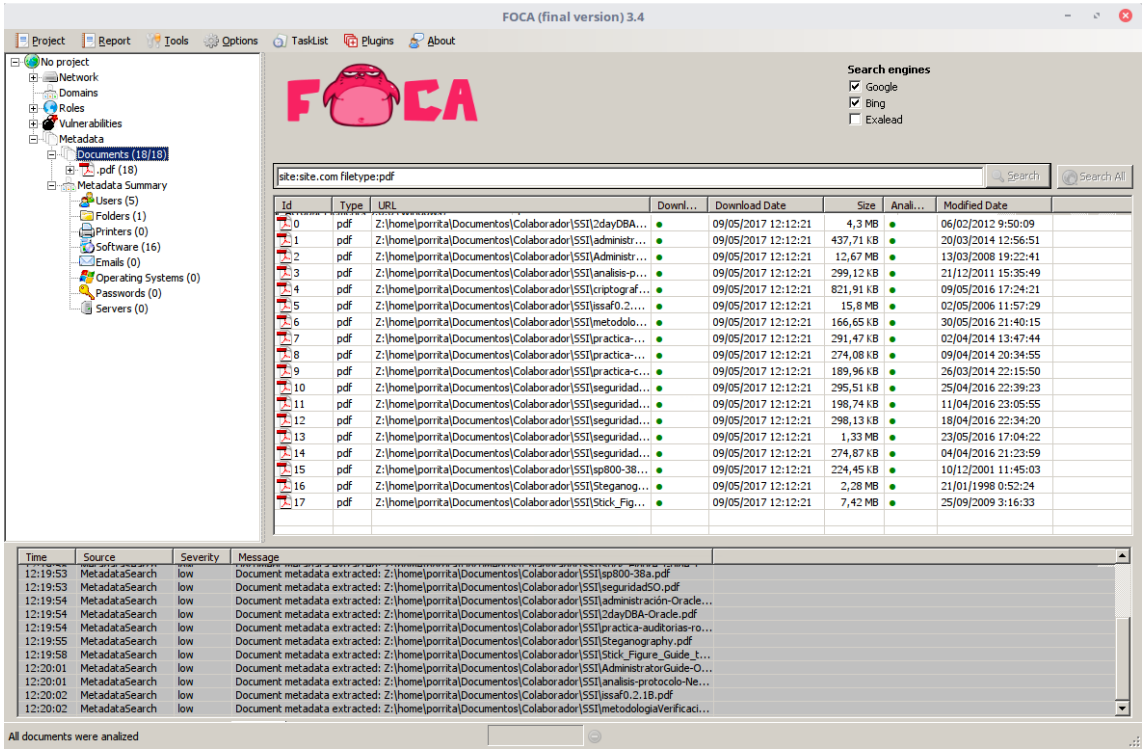

Figura 3: Resultado del análisis de metadatos de documentos locales con FOCA.

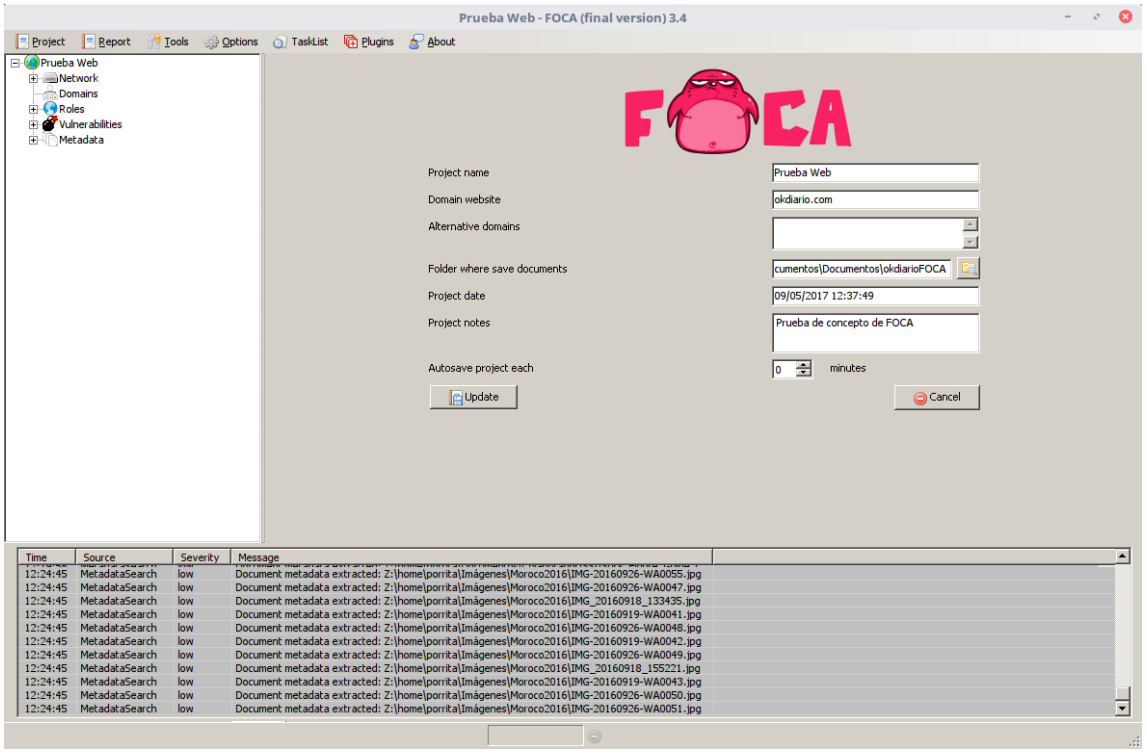

Figura 4: Creación de nuevo proyecto en FOCA.

6. Análisis de metadatos de una web con FOCA

Para realizar el análisis de metadatos de una web, lo primero que necesitamos es crear un proyecto. Para ello, vamos al menú *Project*, opción *New Project* y hacemos clic en ella, lo que nos llevará a una pantalla como la que vemos en la Figura 4.

Entonces, rellenamos los campos que nos piden y seleccionamos un directorio donde se guardarán los archivos descargados. Una vez hecho esto, nos saldrá una ventana similar a la Figura 5; en la que podemos ver, arriba a la derecha, una lista de extensiones con la que indicaremos el tipo de archivo a buscar. Una vez establecido esto, pulsamos en el botón *Search all* y empezará a trabajar.

Tras llevar a cabo estos pasos, podemos observar que ha realizado una búsqueda de archivos relacionados con la web, mostrándonos todos tal y como vemos en la Figura 6.

A continuación, nos descargaremos todos los archivos haciendo clic derecho sobre uno cualquiera y pulsamos *Download All*. Al finalizar la descarga, tendremos en el directorio que hemos indicado anteriormente todos los archivos descargados para

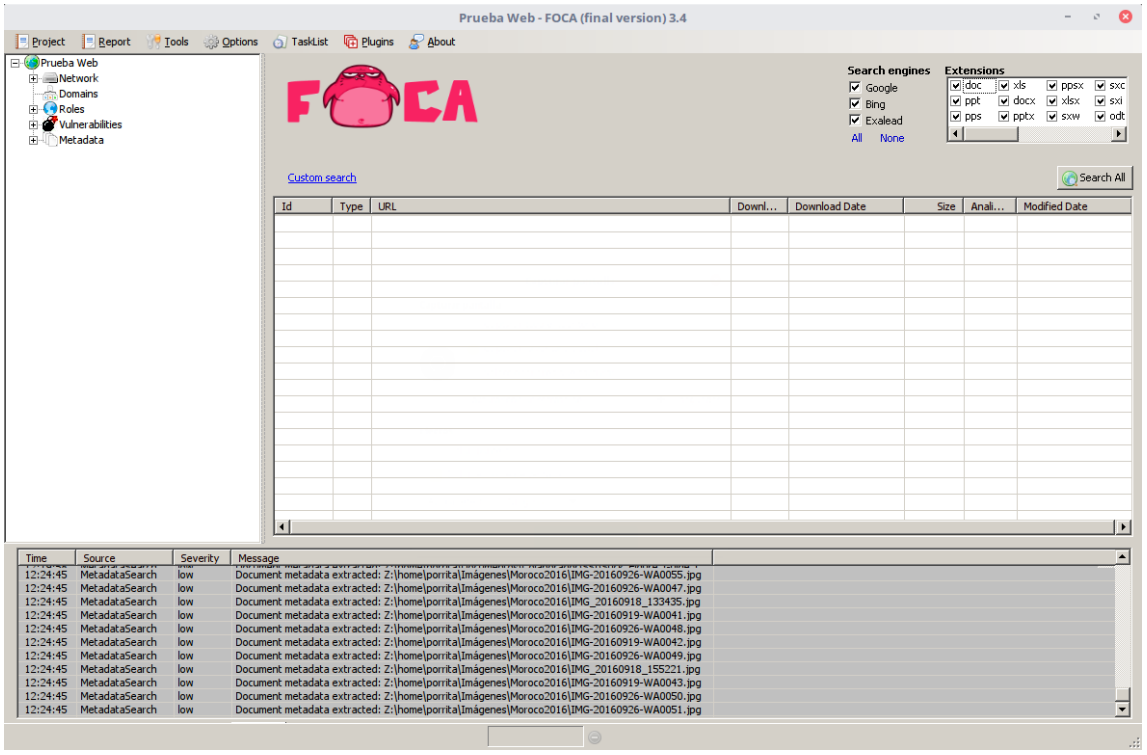

Figura 5: Selección de archivos a buscar en el proyecto de FOCA.

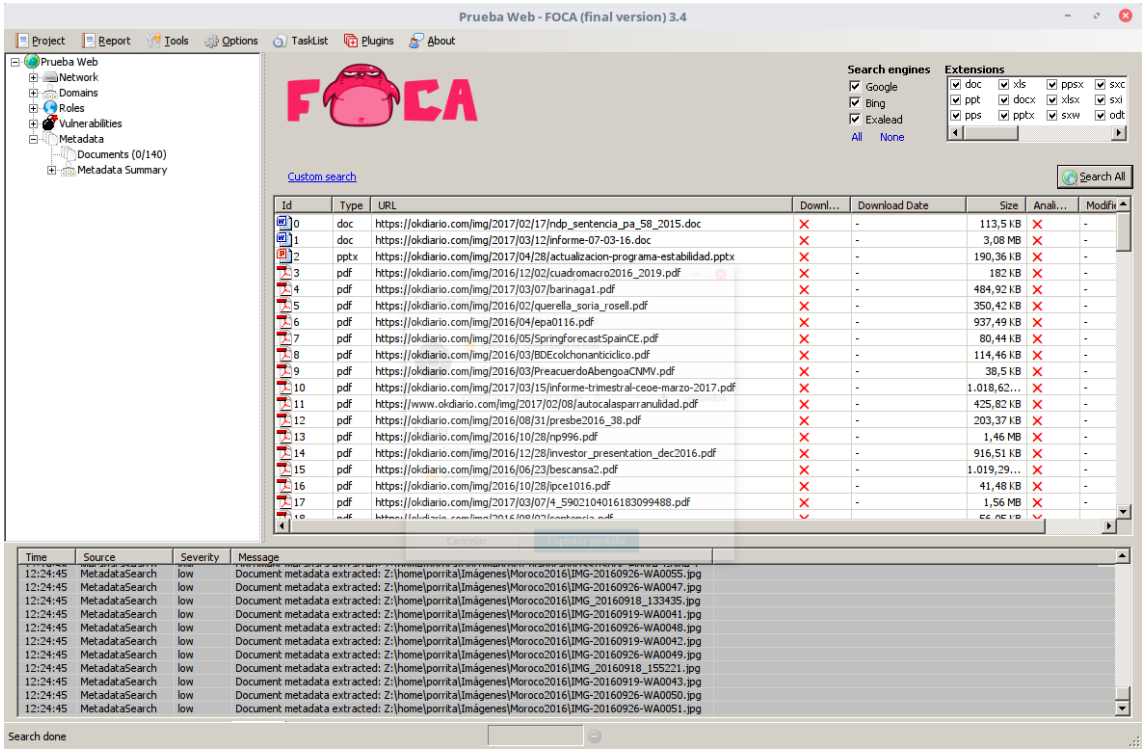

Figura 6: Resultado de búsqueda realizada con FOCA sobre un sitio web.

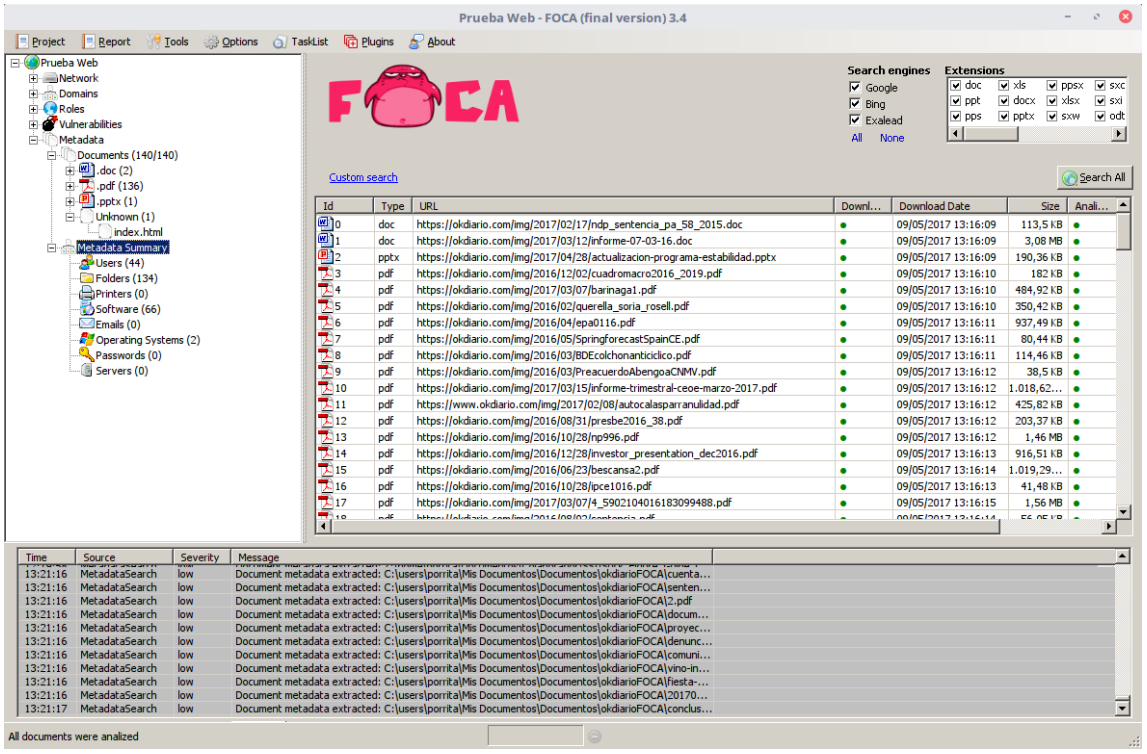

Figura 7: Extracción de metadatos sobre una web con FOCA.

poder visualizar su contenido. Puesto que lo que más nos interesa es su metainformación, seleccionaremos todos los archivos, hacemos clic derecho y pulsamos en *Extract all metadata*. Nuevamente nos aparecerá la pestaña *Metadata Summary* repleta de información jugosa que podemos pasar a analizar y observar, tal y como vemos en la Figura 7.

Nota: algunas páginas web podrían no devolver resultados en la herramienta FOCA. En ese caso, se recomienda usar otra página web.

6.1. Ejercicio 2

Contesta a las siguientes preguntas:

- Elige 3 sitios web cualesquiera para realizar el proceso de análisis con FOCA.
- ¿Qué información específica podemos obtener del menú *Metadata Summary* para cada sitio web?
- ¿Qué utilidad, desde el punto de vista de la seguridad, proporciona el resultado que nos muestra esta aplicación?
- ¿Qué utilidad, desde el punto de vista malicioso, proporciona el resultado que nos muestra esta aplicación?

Referencias

[1] *Instalando FOCA en Linux. ¿Acaso creías que solo corría en Windows?* `https://1bytegris.blogspot.com.es/2016/08/instalando-foca-en-linux-acaso-creias.html`. [Última consulta: 2019-03-05].

[2] Chema Alonso: *Pentesting con FOCA*. 0xWORD, 2ª edición, 2017, ISBN 978-84-616-6319-4.