Seguridad en Redes y Telecomunicaciones

Grado en Criminología

Curso 2017-18

Guía de Prácticas

Práctica 2.- Identidad digital y privacidad
Sesión 5. Filtrado de correo y limpieza de metadatos

Objetivo: Hoy veremos:

- Cómo instalar un cliente de correo y ajustar el filtro anti-spam.
- Comprender que son los metadatos de los archivos, cómo afectan a la privacidad y cómo podemos eliminarlos (limpiarlos).

1.- Clientes de correo y filtros antispam

Para leer y gestionar de una forma segura el correo electrónico, podemos usar un programa cliente de correo. Vamos a configurar una aplicación multiplataforma (podemos instalarla en Windows, Linux y Mac) muy extendida **thunderbird**[1].

Si bien el sistema Windows del aula de prácticas ya tiene instalado *thunderbird*, esta versión es antigua y algo más compleja de configurar. Por ello, vamos a descargar una versión reciente de Internet e instalarla, que no tiene ningún paso complejo.

Para configurarla solo necesitamos de entrada una cuenta de correo electrónico (ugr, gmail, etc.) y los nombres de los servidores de de correo entrante y saliente. En el caso de la UGR estos se denominan `correo.ugr.es`. La UGR tiene un manual de configuración de diferentes clientes de correo, entre los que se encuentra thunderbird, podemos verlo en la dirección https://csirc.ugr.es/informatica/correoelectronico/Acceso/TutorialesConfiguracion/Alumnos/MozillaThunderbird.html. La nuevas versiones de *thunderbird* permiten una configuración más simple.

Los pasos detallados de la instalación de *thunderbird* podemos verlos en https://info.securityinabox.org/es/thunderbird_principal, con especial interés en los ajuste de configuración de la seguridad (https://info.securityinabox.org/es/thunderbird_seguridad). Si bien la configuración por defecto lo incluye, el elemento más importante desde el punto de vista de seguridad es el *protocolo SSL* (*Secure Socket Layer*) que posibilita el intercambio cifrado de correo entre el cliente y el servidor de forma que aunque se intercepte un correo éste no podrá ser leído por el atacante.

Ya hemos comentado que un problema de seguridad con el correo proviene del *spam*. Si bien, los servidores de correo electrónico incorporan filtros de correo basura, es posible que ciertos correos basura pasen estos filtros y lleguen a nuestra dirección. Por ello, los clientes de correo permiten gestionar el *spam*. En el siguiente enlace, y el indicado más arriba, podemos ver como se configura el mecanismo *anti-spam* que incorpora *thunderbird*, https://support.mozilla.org/es/kb/thunderbird-y-el-correo-basura. La versiones actuales tienen un *filtro anti-spam adaptativo*, de esta forma no solo filtra el correo spam, sino que aquel correo sospechoso se muestra al usuario y se le pregunta si es

1 https://www.mozilla.org/es-ES/thunderbird/

spam para que adaptar el filtro. De esta forma, si nos llega spam que ha pasado por el filtro podemos ir mejorando el filtro para correos posteriores.

También puede ver cómo configurar el filtro en la dirección: https://ayuda.guebs.com/como-crear-filtro-de-correo-en-mozilla-thunderbird/.

Ejercicio 1.- Descargar e instalar la última versión de `thunderbird` utilizando bien vuestra cuenta de correo de la ugr u otra (tened presente que los datos que deis se borraran al reiniciar el computador nuevamente, por lo que no hay peligro de que sean accesible posteriormente. Si aún así no os fiais, podéis desinstalar la aplicación antes de finalizar). Un vez operativo el cliente de correo:
a) Verificar que esta utilizando un protocolo cifrado: SSL/TLS o STARTTLS para el correo entrante/saliente.
b) Verificar el estado del filtro anti-spam, y si no esta activo, configurarlo para que lo este.
c) Que otras medidas relativa a la seguridad/privacidad nos permite controlar el cliente.

2.- Limpieza de metadatos

Como vimos en el Tema 1, en todos los sistemas operativos se mantiene ligado a cada documento un conjunto de datos asociados que describen dicho documento y que denominamos *atributos* o *metadatos*. Estos metadatos indican, por ejemplo, cuando se a creado el documento, quién lo ha creado, cuando, etc. En el caso de fotografías, además se recogen las características de la cámara y cómo se ha tomado. Si además, se ha realizado con un móvil, si puede incluso recoger la ubicación a través de las coordenadas GPS.

Si estos documentos junto con sus metadatos se publican si más en Internet, estamos exponiendo nuestra privacidad y somos más vulnerable a sufrir diferentes tipos de ataques. Por ejemplo, si publicamos un foto en la red social tal cual se almacena, estamos publicando donde se tomo y la hora, con lo cual un delincuente puede ubicarnos y saber si estamos o no en casa. Además, los metadatos tienen interés en la informática forense, puesto que se pueden utilizar como evidencias.

Por ello, antes de hacer públicos documentos personales/empresariales debemos asegurarnos de limpiar aquellos metadatos que no queramos mostrar. De hecho, esto esta recogido en el Apartado 5.7.6 del Esquema Nacional de Ciberseguridad (https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/3286-actualizacion-del-esquema-nacional-de-seguridad-en-la-administracion-electronica.html) que establece:

> *"**5.7.6 Limpieza de documentos***
> *En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.*
> *Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información. El incumplimiento de esta medida puede perjudicar:*
> *a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.*
> *b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.*
> *c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer."*

- **Limpieza de metadatos con la herramienta de Windows**

En Windows, ya se contempla esta funcionalidad y el propio sistema operativo nos permite eliminar metadatos de los documentos. Para ello, seleccionamos un documento (imagen, .doc, etc.), y con el botón derecho del ratón seleccionar “Propiedades”. En la ventana que aparece, seleccionamos la pestaña “Detalles” como aparece en la figura:

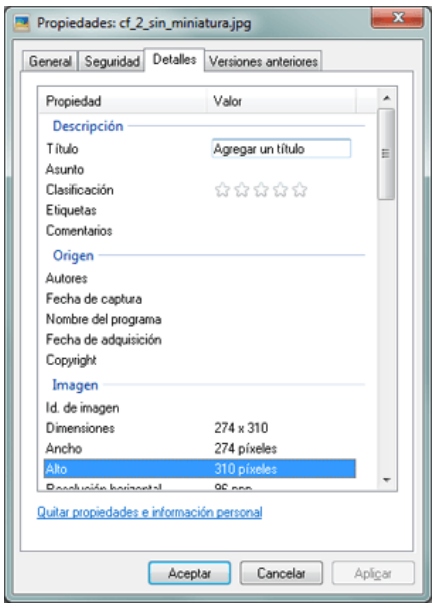

Figura .- Ventana de propiedades de una archivo.

Como podemos ver, aparece un enlace a “Quitar propiedades e información personal” hacia el final de la ventana. Seleccionando este enlace, podemos eliminar los metadatos que deseemos o hacer una copia de lo que vamos a eliminar. Una vez eliminados los metadatos, será más seguro desde el punto de vista de la privacidad publicar el documento.

Otras muchas aplicaciones también nos permiten controlar/ver los metadatos que se incrustan en los documentos, como ocurre con Adobe en documentos .pdf, o en programas de edición de fotografía o multimedia.

Dejamos para una práctica posterior el uso de herramientas destinadas a extraer metadatos de documentos y grupos de documentos, como pueden ser FOCA (http://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml).

> **Ejercicio 2.-** Selecciona un par de documentos de dos tipos, por ejemplo, un documento de word y una imagen, y muestra los metadatos de los mismos. También indica el proceso para limpiar los metadatos de los mismo.

- **Limpieza de metadatos con `exiftool`**

Una herramienta que permiten un control más fino sobre los metadatos es **`exiftool`**[2]. Esta herramienta esta construida para ser utilizada en la consola de órdenes, por lo que además utilizaremos una interfaz gráfica para la herramienta **`exiftoolgui`**[3] (aunque esta en inglés, la

2 https://sno.phy.queensu.ca/~phil/exiftool/.
3 http://u88.n24.queensu.ca/~bogdan/.

interfaz es sencilla). Ambas herramientas están disponibles en https://lsi.ugr.es/jagomez/srt/p2s5.

Su instalación es sencilla, descargamos y descomprimimos los archivos que hay en la carpeta: **exiftool-10.65.zip** y **exiftoolgui516.zip**. La única precaución es que al descomprimir `exiftool-10.65.zip` nos genera un archivo ejecutable denominado `exiftool(-k).exe` que debemos renombrar a `exiftool.exe` y mover a la misma carpeta donde hayamos extraído `exiftoolgui`.

El aspecto de la interfaz gráfica se muestra en la Figura . En el panel de la izquierda podemos navegar por el sistema de archivo para seleccionar una carpeta. En el panel central tenemos los archivos de la carpeta seleccionada y una vez seleccionado el archivo deseado, el panel de la derecha nos muestra los metadatos asociados.

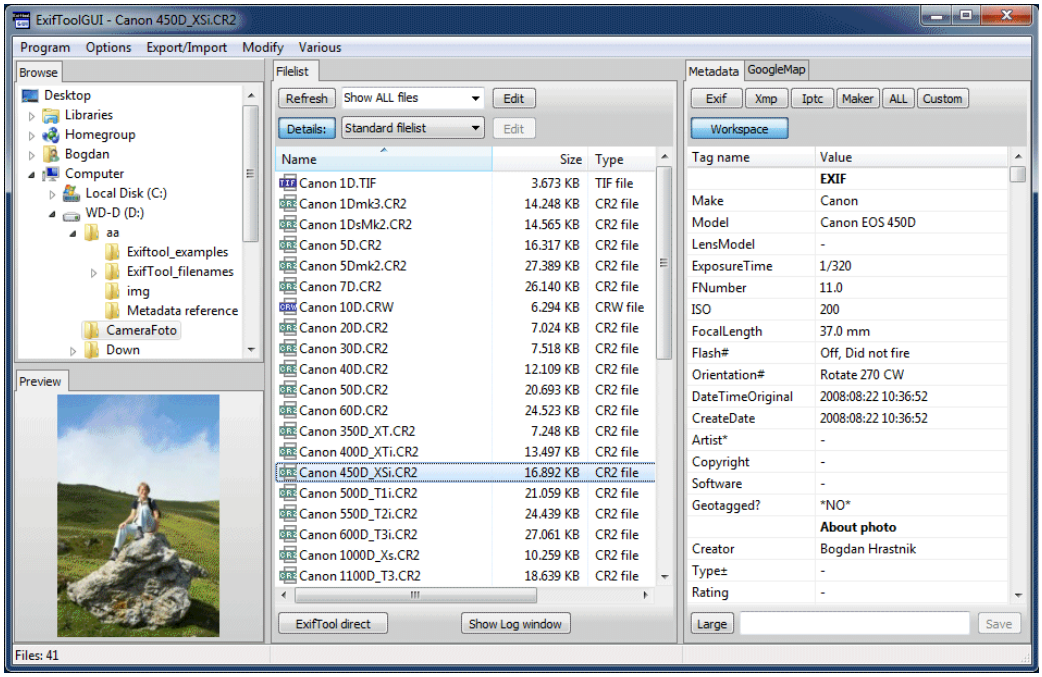

Figura .- Ventana de la interfaz gráfica de `exiftool`.

La herramienta permite diferentes opciones, pero nos vamos a centra en la del borrado de metadatos, disponible en la opción de menú "Modify→Remove". Una vez seleccionada, nos muestra una ventana que nos permite seleccionar los metadatos a eliminar. Hay que tener presente que dependiendo del formato de la imagen podría ser posible que no se eliminen. Otra opción que podemos tomar es modificarlos.

Ejercicio 3:
a) Instala las herramientas y analizar los metadatos de diferentes imágenes descargadas de Internet para ver si tienen o no metadatos asociados.
b) En http://lsi.ugr.es/jagomez/p2s5/ hay una imagen *Ejercicio3.jpg* con metadatos asociados. Analízala e indica la información que se puede extraer de ella.