**INFORME PRÁCTICA 2**



**Antonio Fernández Martín**

**Cristian Emanuel Anei**

**Juan Francisco Carrión Molina**

**Markel Alvarez Martinez**

**Pablo Alvarez Garcia**

# 1. Explicación y análisis detallado del laboratorio o escenario de análisis forense

Hemos realizado un análisis de los metadatos de unos ficheros dados por el profesor y otros que hemos buscado por nuestra cuenta. El objetivo es obtener un hash y los metadatos como evidencia digital. La tarea se ha realizado con el equipo personal (Windows 10) debido a las clases online. El software empleado ha sido **FOCA**, **Metashield** y **7-Zip** para conseguir los hashes.

# 2. Explicación detallada de las acciones realizadas en las fases

**Evaluar**

Vamos a evaluar los metadatos almacenados en los archivos que encontramos a través de FOCA. Una vez tengamos esa información podemos observar los datos y ver que información sensible que no debería mostrarse encontramos.

**Adquirir**

Para adquirir los documentos se pone la URL de una página web en el buscador de FOCA de manera que esta herramienta pueda explorar la web.

**Analizar**

UCM\_Deporte Estudiantes y Resto Grupo A.doc:

sistema operativo y software

UCM\_SolicitudTarjetaaDeportes.doc:

La información sensible de este documento sería el e-mail sistema operativo, usuario y version del software

Análisis forense FOCA1.docx: e-mail, username, subject confidencial, nivel de acceso.

Análisis forense FOCA2.docx: no tiene metadatos relevantes.

Análisis forense FOCA3.docx: e-mail,username, subject confidencial, nivel de acceso.

Análisis forense FOCA.docx: username, subject confidencial, nivel de acceso.

Análisis forense FOCA?[[1]](#footnote-0).pdf: username, subject confidencial.

BDE\_Becas.pdf: no tiene metadatos.

NOTAINFORMATIVAIGAE\_2010.pdf: no tiene metadatos relevantes.

UCM\_SolicitudTarjetaDeportes.pdf: no tiene metadatos relevantes.

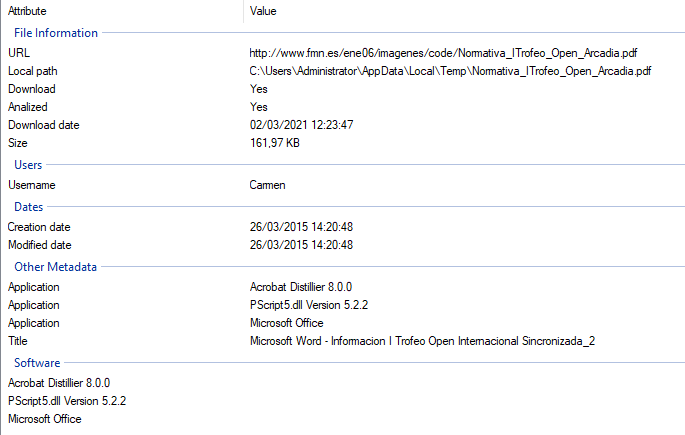
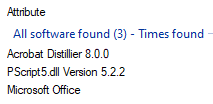
UCM\_SolicitudTarjetaDeportes18años.pdf: no tiene metadatos relevantes.

**Informar**

Se crea el informe con los hallazgos pertinentes para ser entregado al cliente y pueda subsanar el problema. Para generar los hashes usamos la herramienta 7-Zip.

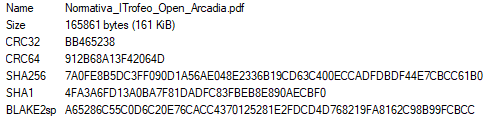
**ANÁLISIS DE ARCHIVOS DE WEBS PÚBLICAS**

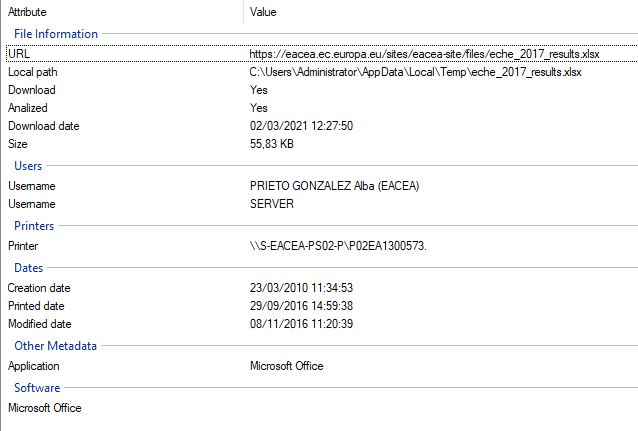
**Archivo 1 pdf colegio:**



La información sensible en este caso sería: el nombre de usuario y los softwares utilizados junto a sus versiones.

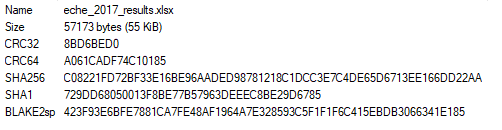
**Hash:**



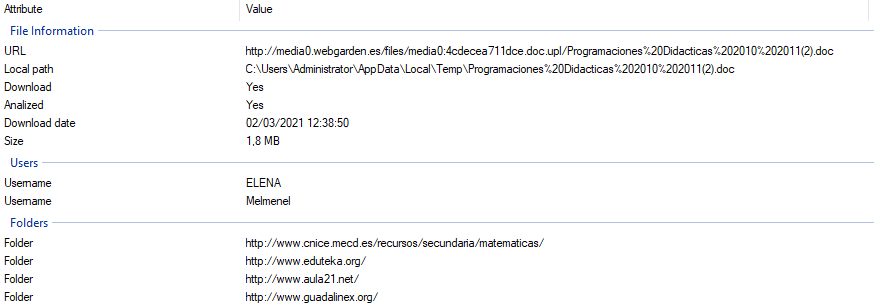
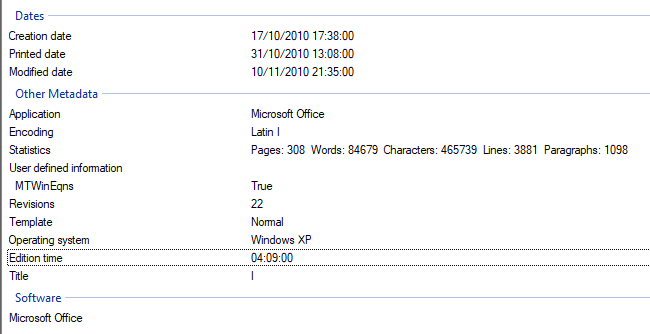
**Archivo 2 renfe xlsx:**

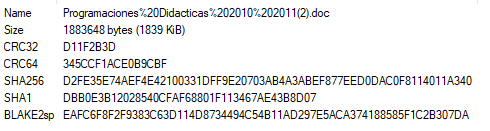
La información sensible en este caso sería: el nombre de usuario, software utilizado y la impresora (printer) utilizada.

Hash:

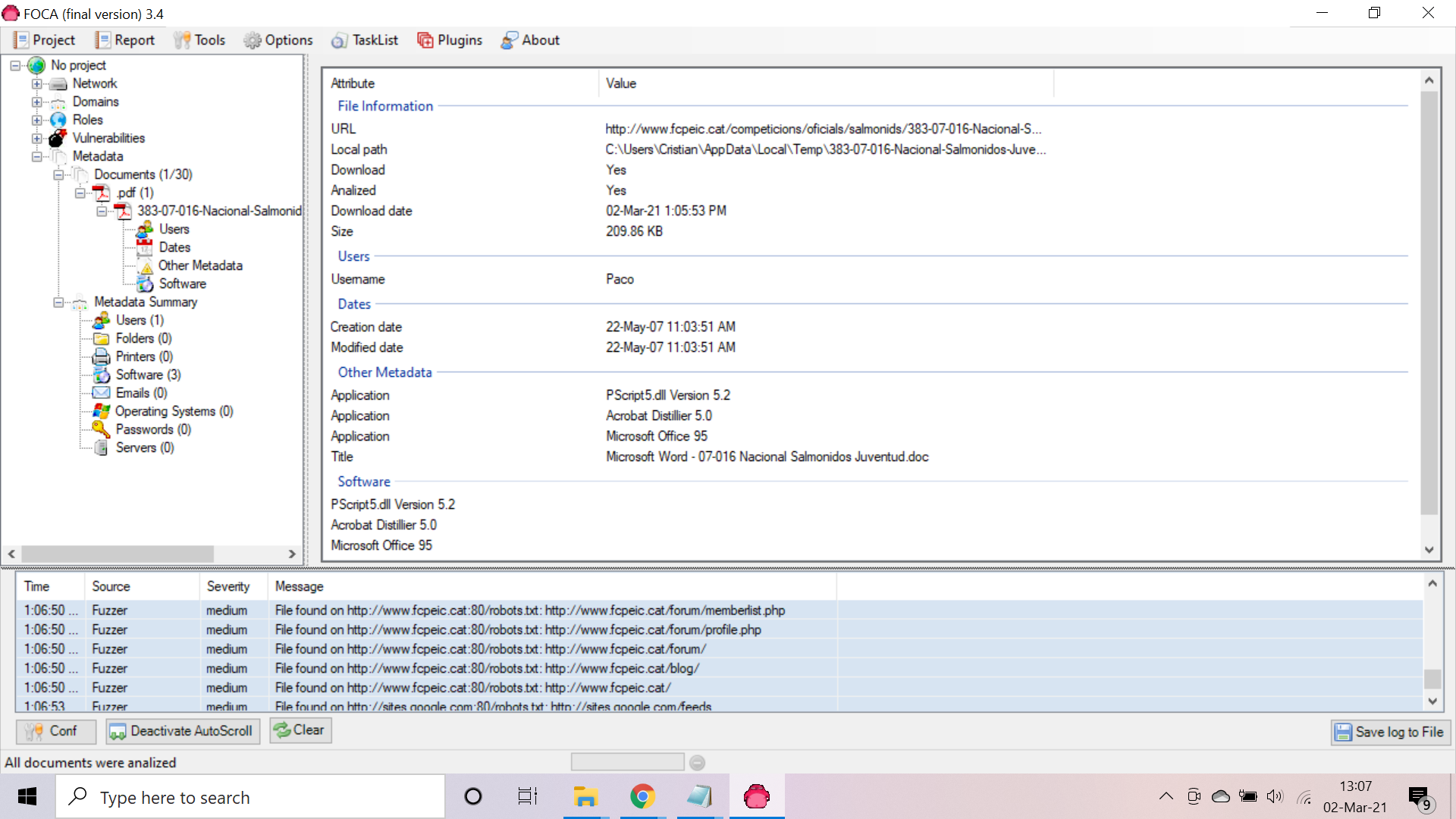


**Archivo 3:**

La información sensible en este caso sería: los nombres de usuario, software utilizado y el sistema operativo.

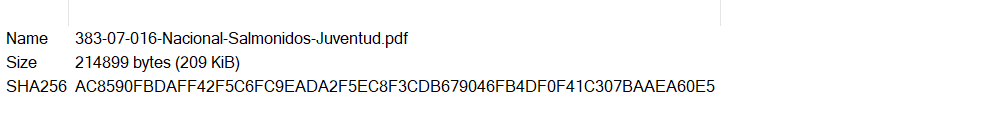
**Hash:**

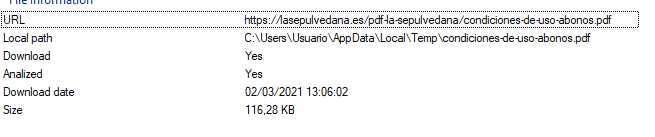
**Archivo 4**



La información sensible reflejada en los metadatos de este archivo serían: el nombre de usuario y el software utilizado junto a sus distintas versiones.

**Hash**

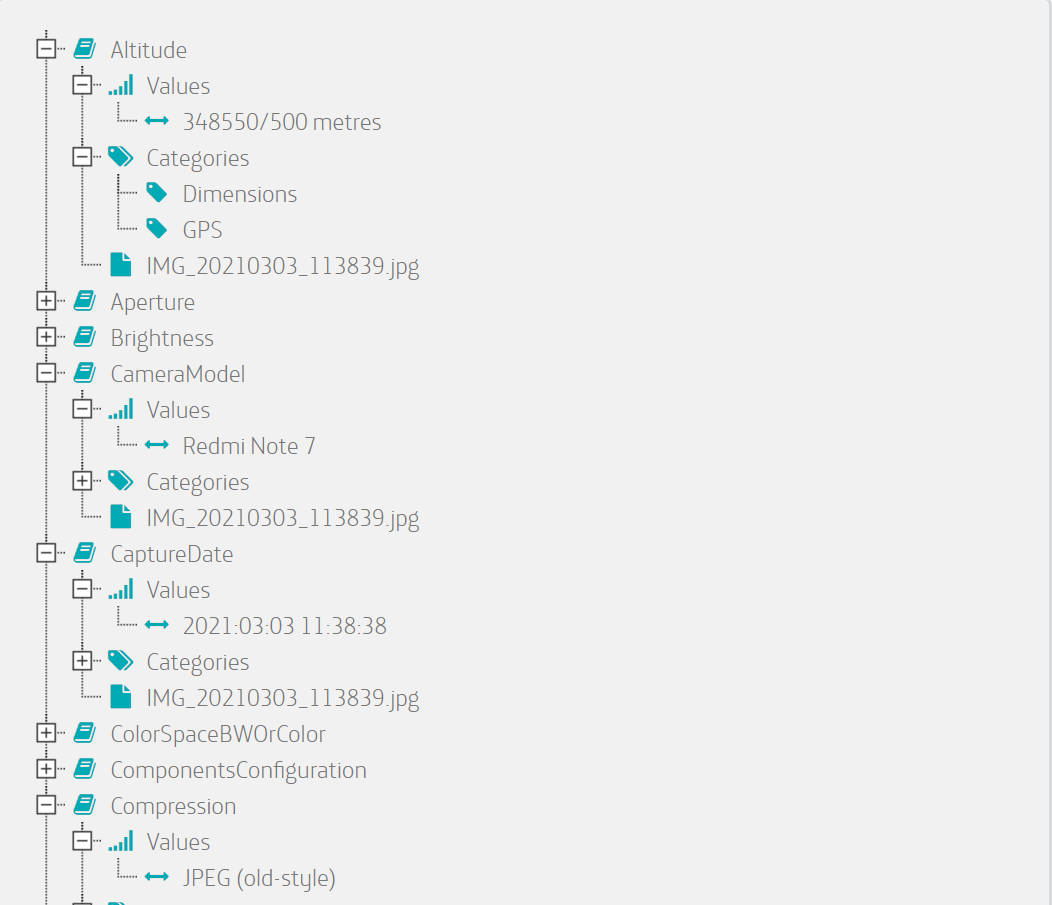
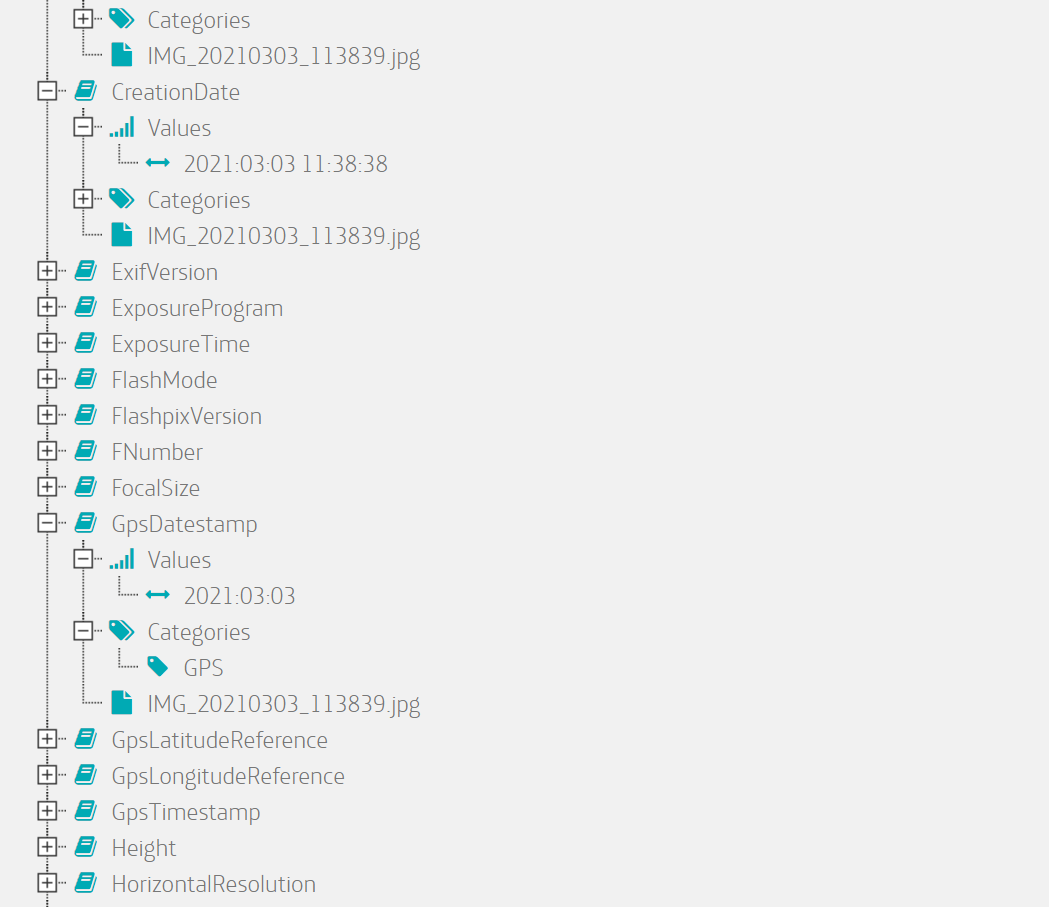


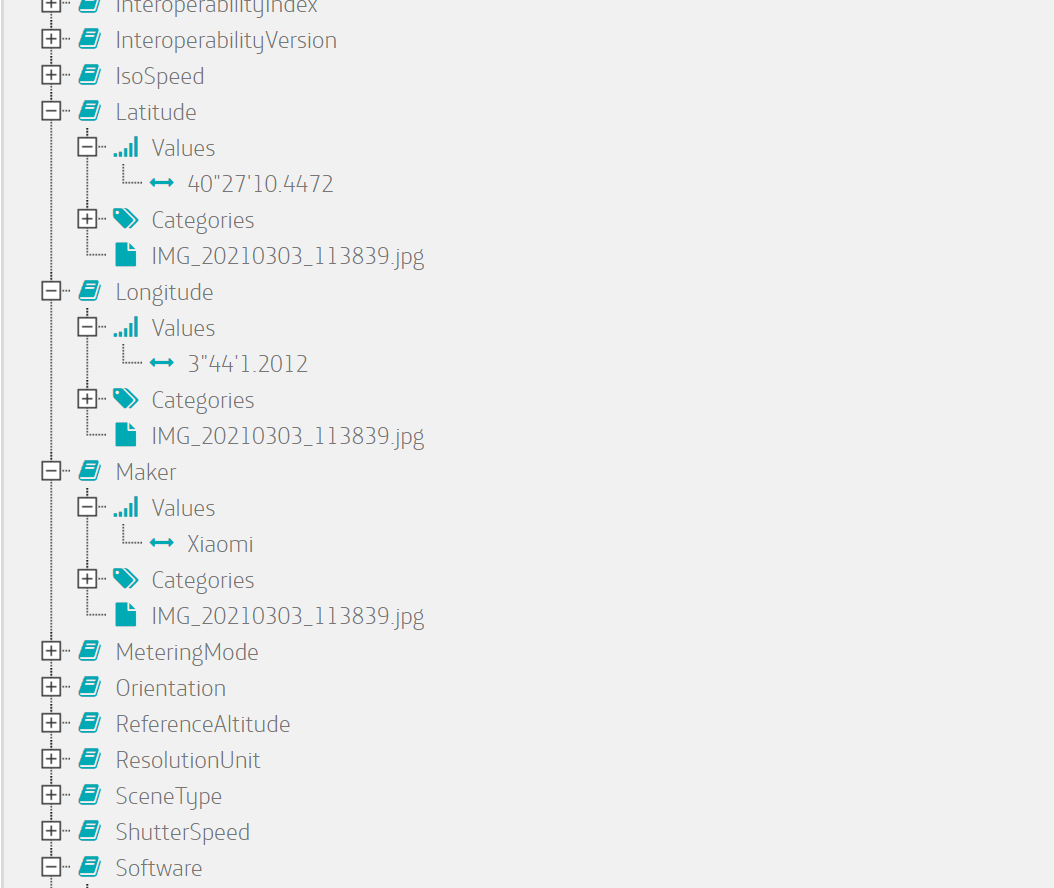
**Archivo 5 Sepulvedana:**

En este caso por ejemplo no habría información sensible ni confidencial.

Hash

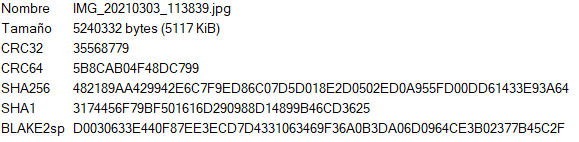


**Archivo 6 Foto (IMG\_20210303\_113839.jpg) con Metashield:**

****

En este caso hemos obtenido una foto de la facultad, y con la herramienta Metashield hemos podido encontrar información sensible como el modelo del dispositivo con el que se ha hecho la foto (xiaomi redmi note 7), la ubicación GPS desde donde se ha hecho la foto (que efectivamente es la ubicación de la facultad), cuando se ha hecho la foto, entre otras cosas.

**Hashes**

****

1. ? Significa cualquier carácter. Esto está puesto porque hay otro archivos con el mismo nombre y que solo cambia un dígito y que tienen los mismos metadatos. [↑](#footnote-ref-0)