Metadatos, (in) seguridad y fotografías digitales

1 Introducción

La fotografía digital se ha popularizado sobre todo debido a la inclusión de las micro-cámaras de los teléfonos inteligentes y la interacción de los usuarios con **Redes Sociales** (RRSS).

Hacer una foto y copiarla de forma inmediata en la Red de forma pública o privada desvela numerosos datos privados de forma imprevista por los usuarios.

Detrás de la imagen existen **metadatos** asociados, que se generan tanto en el captador de imagen (foto y/o video) como en el dispositivo que alberga el sensor, por el teléfono móvil:

datos de exposición de la foto, tamaño en pixeles y dimensiones exactas, modo de exposición, tipo de iluminación, balance de color, modelo de lente,, localización de la foto (**GPS**) incluida la altitud, distancia del sujeto principal, tipo de escena, audio asociado, caras identificables y posteriormente etiquetable (**tags**), copyright de la imagen, propietario del teléfono, fecha y hora exactas de la toma … modelo del teléfono, correo electrónico, identificador del usuario, a veces una imagen en miniatura, etc.

2 In-Seguridad de los Metadatos

Al entregar la foto al mundo de las RRSS nos desprendemos de la fotografía como elemento de valor documental y renunciamos inconscientemente a cualquier autoría intelectual o artística pues es un documento electrónico fácilmente editable.

El seguimiento del rastro de la foto es técnicamente imposible ya que los únicos términos de búsqueda que podrían ayudar en la trazabilidad están en los metadatos de la imagen, no en la imagen en sí. Teniendo en cuenta lo mencionado antes, cualquiera puede cambiar los metadatos poniendo por ejemplo su identificador personal y suplantar la “propiedad” del autor de la foto.

Otra alteración que interviene en **el significado de la fotografía** es su edición gráfica, añadiendo o eliminando contenido por medio de potentes editores como Photoshop, lo cual lleva a interpretaciones diferentes de la toma inicial.

La edición con fines artísticos es no solo aceptable sino deseable, pero si el objeto de la foto es aportar un valor documental, cualquier alteración es inaceptable.

La publicación de una foto en RRSS puede iniciarse desde el teléfono móvil o tableta, pero el origen de la foto con sus metadatos puede ser muy diversos: cámara del teléfono (anterior para los “selfies”, posterior para los paisajes o entorno callejero), aplicación “fotos” del terminal, o programas de edición como **Photoshop, Snapseed, Enlight, Pixelmator** … Si se utilizan cámaras compactas o profesionales, éstas aportan sus propios editores para post-procesar las fotos o videos.

Cada programa que interviene en el post-procesado de la foto, aunque sea solamente para añadir un filtro de viveza de color, de recorte, o de inclusión de una marca de texto, o de agua, modifica los metadatos originales. Existen apps para ver los metadatos del fichero de imagen como por ejemplo **Exif, exif photo viewer, Photo Investigator, Metadata viewer**, y que también permiten reescribir fecha, GPS, nombre de la foto o autor sin ninguna limitación.

Las **marcas de agua** son textos sobreescritos sobre los pixeles de la imagen. Pueden ser visibles, cuando el autor quiere dejar su copyright no solo en los metadatos sino también en la imagen que se va a publicar. Con diferente propósito las marcas de agua pueden ser invisibles, denominándose marcas de **esteganografía**. Es una forma poco conocida de trasmitir información subliminal, que solo podrán detectar y leer ciertos programas específicos. No es una forma segura de trasmitir información secreta pero se ha usado con ese propósito sobretodo en guiones de cine.

La mayoría de los terminales móviles permiten acceder a las imágenes en formatos abiertos como **jpeg, mpeg**, etc. En este formato no hay mecanismos de integridad de las fotos, debido a ello, publicar una foto es regalarla para cualquier uso, fraudulento o no.

Algunos pocos dispositivos y cámaras profesionales permiten acceder a los ficheros nativos generados por el sensor de imagen, que se denominan de forma genérica "**ficheros en bruto** (raw)" y que cada fabricante específica a su libre albedrío. En este caso sí pueden existir mecanismos de integridad de los metadatos originales, aquellos creados en el mismo instante de la captura. Este aspecto es relevante cuando se va a utilizar la fotografía (video) para dejar **evidencias forenses** de un hecho.

Todo fichero de tipo RAW tiene un mecanismo de integridad de su contenido que permite verificar siempre si los metadatos han sido modificados o no. Gracias a este mecanismo las agencias de información saben si la foto es la original o ha sido modificada aunque sea levemente. Un recorte del tamaño de la imagen podría ocultar un elemento esencial para interpretar la foto, o alterar la fecha del suceso y la altitud de la toma podrían cambiar completamente la noticia.

3 Recomendaciones

En primer lugar hay que reflexionar sobre la utilidad de la publicación de la fotografía.

Si se trata de una publicación personal e intrascendente es recomendable borrar cualquier metadato usando una de las aplicaciones gratuitas de borrado de metadatos. Es la mejor forma de dejar el menor rastro posible, no de la foto en sí, sino de nuestros datos, que podrían ser utilizados en contra nuestra.

Si el fin es profesional, la recomendación va en sentido contrario hay que marcar lo mejor posible los metadatos que deseamos que permanezcan, para que puedan ser trazados hasta su origen, ya que lo que deseamos es que nuestra propiedad artística, intelectual o documental sea detectada en caso de entrar en conflicto. Se deben utilizar varias técnicas marcado para que el esfuerzo de borrado o modificación desanime a los posibles suplantadores.

Si la finalidad es forense, la fotografía o el video no deberían publicarse en RRSS, aunque todos sabemos que por algún extraño mecanismo siempre se producen “filtraciones”. En este caso se deberá trabajar solamente en formato RAW, y archivar la imagen en varios volúmenes protegidos de forma segura según la normativa aplicable a la entidad que realiza la investigación forense.

Manuel Jacinto Martínez Álvarez

Consultor Seguridad GCR

Áudea Seguridad de la Información