Anomalías en el Seguimiento de Exif en el Análisis Forense de Metadatos de Imágenes de Móviles

Ana Lucila Sandoval Orozco[1], David Manuel Arenas González[1], Luis Javier García Villalba[1], Julio César Hernández Castro[2]

[1] Grupo de Análisis, Seguridad y Sistemas (GASS), Departamento. de Ingeniería del Software e Inteligencia Artificial
Facultad de Informática, Despacho 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid
Email: {asandoval, darenas, javiergv}@fdi.ucm.es

[2] School of Computing, Buckingham Building, Lion Terrace, Portsmouth University
Portsmouth PO1 3HE, Reino Unido
Email: Julio.Hernandez-Castro@port.ac.uk

***Resumen*—Hoy en día el número de cámaras fotográficas integradas en dispositivos móviles crece a un ritmo imparable, haciendo necesario el uso de técnicas de análisis forense específicas para las imágenes generadas por este tipo de dispositivos, dada la singularidad de los mismos. La mayoría de estos dispositivos insertan metadatos Exif en el proceso de adquisición de la imagen y aun siendo estos fácilmente vulnerables a distintos tipos de modificaciones, son de gran ayuda para una gran variedad de técnicas de análisis forense. Teniendo todo esto en cuenta, se estima necesario la existencia de herramientas eficaces y robustas, que permitan la extracción de los metadatos de una forma veraz y consistente. Igualmente esta extracción de metadatos no debe manipular en ningún momento la imagen y requiere tener en cuenta posibles violaciones de la especificación Exif, tanto en la inserción de los metadatos en el proceso de adquisición de la imagen por parte de los fabricantes, como por parte de cualquier modificación, ya sea malintencionada o no. En este artículo se muestran anomalías en el seguimiento de la especificación Exif, lo que puede producir graves problemas en la extracción de los metadatos de las imágenes por medio de aplicaciones, así como problemas de interoperabilidad entre distintos dispositivos. Asimismo, se muestran anomalías en el funcionamiento de diversas herramientas forenses.**

I. Introducción

Actualmente, el número de cámaras integradas en dispositivos móviles supera a las cámaras digitales tradicionales (DSCs). Existen razones para ver que esta extensión de las cámaras fotográficas en dispositivos móviles son beneficiosas para las distintas situaciones en las que se requiere una prueba gráfica de un hecho (pruebas de delitos, privación de la libertad de prensa, etc.). Dadas las características técnicas particulares de este tipo de dispositivos, se necesitan herramientas de análisis forense específicas, no siendo válidas las herramientas que tratan imágenes de forma general o las generadas por otro tipo de dispositivos (DSCs, escáneres, etc.). Este trabajo está estructurado en 8 secciones, siendo la primera de ellas la presente introducción. La sección II realiza un estado del arte del análisis forense para imágenes generadas por dispositivos móviles haciendo un compendio de las principales técnicas utilizadas. En la sección III se realiza una descripción de los principales sistemas de metadatos en imágenes dando una especial importancia al estándar Exif que se detalla en la sección IV por su alto grado de utilización en imágenes generadas por dispositivos móviles. En la sección V se realiza un análisis binario de los metadatos de imágenes reales de varios teléfonos móviles. Este estudio permite una comprensión más a fondo del estándar Exif, así como examinar el cumplimiento de la especificación Exif por parte del los fabricantes. En la sección VI se describen algunos de los casos de violaciones encontrados en el seguimiento de la especificación Exif. En la sección VII se realiza un estudio comparativo de herramientas de análisis forense enfocadas al análisis de metadatos para evaluar la fiabilidad de la información Exif con inconsistencias en el seguimiento del estándar. Por último en la sección VIII se presentan las conclusiones y el trabajo futuro.

II. Técnicas de Análisis Forense de Imágenes

El área del análisis forense de imágenes puede dividirse en dos grandes ramas: autenticidad de las imágenes y la identificación de la fuente de creación de la imagen [1]. Con respecto a la primera de las ramas, nos referimos a determinar si una imagen no ha sufrido ningún procesamiento posterior al de su creación, es decir que no haya sido manipulada. La segunda de las ramas apunta a la identificación de la fuente de creación de la imagen. Las técnicas de esta rama se fundamentan en el estudio de las características del proceso de adquisición del dispositivo concreto y de la tecnología utilizada.

Aun teniendo en cuenta estas dos grandes ramas no se puede dejar pasar por alto la información de los metadatos que los dispositivos introducen en el proceso de adquisición de la fotografía. Suponiendo la veracidad de los datos contenidos en la imagen, es decir, que no se hayan dado manipulaciones mal intencionadas a posteriori, dependiendo de cada fabricante y dispositivo se arroja en una diversidad de formatos, una información útil para el analista forense (localización GPS, fuente de la foto, características técnicas de la imagen, etc.). Las

Tabla I
ESQUEMA GENERAL CON MARCADORES DE UNA IMAGEN JPEG

SOI	**Marcador (1 a n)**				**SOS**			**Datos Imagen**	**EOI**
FFD8	FF	No. de Marca (1 byte)	Tamaño de los Datos (2 bytes)	Datos (n bytes)	FFDA	Tamaño de los Datos (2 bytes)	Datos (n bytes)	Datos (n bytes)	FFD9

técnicas basadas en metadatos son las más sencillas, aunque dependen en gran medida de los datos que el fabricante decida insertar como metadatos en la imagen en el momento de la toma. Asimismo, este método es el más vulnerable a posibles cambios malintencionados por terceros. Aún así una vez que se pueda comprobar por distintos métodos o situaciones que no ha habido ningún tipo de manipulación externa, el análisis de la gran cantidad de metadatos que, actualmente como norma general insertan los fabricantes, puede ser de gran ayuda para las funciones del analista forense. Existe una gran variedad de trabajos que hacen referencia a los distintos tipos de metadatos en las imágenes con fines de búsquedas y clasificación [4] [5] [6]. Concretamente, para identificación de fuente de la cámara la especificación más seguida por la mayoría de los fabricantes, Exif, cuenta con dos etiquetas concretas "Make", para la marca y "Model" para el modelo. En ninguna de las versiones de la especificación Exif (hasta la versión 2.3) es obligatorio la existencia de estos dos campos. Asimismo si se incluyen pueden aparecer con valores vacíos indicando de esta forma que los valores son desconocidos.

III. METADATOS EN IMÁGENES

Los metadatos habitualmente son denominados "datos sobre los datos", es decir información de interés que complementa el contenido principal de un documento digital. Los metadatos pueden llegar a ser una potente ayuda para la organización y búsqueda a lo largo de librerías de imágenes.

Las imágenes digitales son almacenadas en una gran variedad de formatos como TIFF, JPEG, PSD o RAW entre otros. Cada formato de imagen tiene distintas reglas de cómo los distintos formatos de metadatos son almacenados junto al propio archivo que contiene la imagen. Algunos de los distintos contenedores de metadatos para los distintos formatos son: IFDs Exif/TIFF, Adobe XMP e IPTC-IIM. Cada uno de estos contenedores de metadatos tiene un formato propio que indica las propiedades de los metadatos que son almacenadas, el orden y su codificación en el contenedor. En cada contenedor suele haber una subdivisión con criterios semánticos. Estos grupos semánticos se dividen a su vez en propiedades de metadatos individuales. Cada propiedad tiene asociada unos tipos de datos específicos como pueden ser cadenas de caracteres, números o vectores. Algunas propiedades como la orientación de la imagen no son comunes a los distintos contenedores estándar, en cambio otras, como las cadenas de *copyright* pueden ser almacenadas por varios contenedores con similar información pero posiblemente con una semántica o estructura sutilmente distinta. La complejidad estructural descrita anteriormente ocasiona problemas en el uso eficiente y efectivo de los metadatos. Estos problemas causan en los usuarios frustración y desconfianza sobre los distintos sistemas de metadatos, ya que lo que se busca es la interoperabilidad entre los distintos productos y servicios de imagen digital. Conscientes de estos problemas los fabricantes invierten gran cantidad de recursos para resolverlos. Tanto es así que existen grupos de fabricantes como el *Metadata Working Group* con el objetivo de mitigar o erradicar los problemas anteriormente descritos. Este grupo está formado por empresas como Apple, Adobe, Canon, Microsoft, Nokia y Sony. Incluso con la existencia de este grupo, los problemas no se resuelven por completo, dada la inmensa variedad de fabricantes existentes. Cabe destacar que este hecho no implica la inutilidad del uso de metadatos en imágenes, ya que actualmente se puede asegurar que son imprescindibles e inseparables en una imagen digital.

IV. ESPECIFICACIÓN EXIF

El formato Exif (Exchangeable Image File Format) define un conjunto de etiquetas TIFF (Tagged Image File Format) para describir imágenes fotográficas. La especificación usa los formatos de archivos existentes como JPEG [7] y TIFF Rev. 6.0 a los que se agrega etiquetas específicas de metadatos. No está soportado en JPEG 2000 o PNG. Existen distintas versiones de la especificación de Exif. Cada dispositivo soporta una versión que incluye a todas las anteriores. La versión Exif utilizada es una etiqueta más en los metadatos. La última versión de la especificación es la 2.3 de abril de 2010 [8].

Dado que el formato más utilizado en cámaras digitales, y concretamente en dispositivos móviles, es JPEG, a continuación se describen los elementos y estructuras de datos que utiliza JPEG/Exif.

Todos los archivos JPEG comienzan con el valor binario 0xFFD8 (SOI - *Start Of Image*) y terminan con 0xFFD9 (EOI - *End Of Image*). SOI y EOI son marcadores que no tienen datos posteriores a diferencia de los otros restantes que tienen una estructura fija y datos asociados.

En el formato JPEG la marca 0xFFDA (SOS - *Start of stream*), indica el inicio de los datos propiamente dichos de la imagen, cuyo fin se limita con la marca EOI. Por tanto un esquema general con la posibilidad de *n* marcadores para una imagen JPEG se presenta en la Tabla I.

Los marcadores o segmentos obligatorios en un archivo JPEG/Exif son: SOI, APP1 (*Application Marker Segment 1*), DQT (*Define Quantization Table*), DHT (*Define Huffman Table*), SOF (*Start of Frame*), SOS y EOI. Además es obligatorio que estén los datos comprimidos de la imagen propiamente dicha. La información Exif es albergada en el segmento APP1. Existe un conjunto de segmentos APPn no utilizados por Exif que pueden ser empleados por los fabricantes para almacenar

Tabla II
ANÁLISIS DE ETIQUETAS DEL 0TH IFD

Móvil	Entradas *0th IFD*	Etiqueta	Tipo	No. de Elementos	Offset
Samsung Galaxy S	0x0E010200140000009E000000	Image Description (0x010E)	ASCII (0x0002)	20 (0x00000014)	158 bytes (0x0000009E)
	0x0F01020014000000B2000000	Make (0x010F)	ASCII (0x0002)	20 (0x00000014)	178 bytes (0x000000B2)
Sony Ericsson W580i	0x0F0102000E00000086000000	Make (0x010F)	ASCII (0x0002)	13 (0x0000000E)	134 bytes (0x00000086)
	0x1001020006000000A6000000	Model (0x0110)	ASCII (0x0002)	6 (0x00000006)	166 bytes (0x000000A6)

cualquier otro tipo información manteniendo la compatibilidad con Exif. Exif utiliza el marcador APP1, para evitar conflictos con el marcador APP0 del formato JFIF. Tras el tamaño del segmento APP1, se encuentra la cadena "Exif" en caracteres ASCII ('0x45786966') seguida de 2 bytes '0x00' lo cual indica que ese archivo sigue la especificación Exif. Exif utiliza la estructura TIFF para almacenar los datos en forma de tuplas (etiquetas) característica-valor. Estas etiquetas se almacenan como entradas de un directorio en una estructura de orden superior denominada IFD (*Image File Directory*). La estructura TIFF se compone de 2 IFDs, el 0th IFD y el 1st IFD. El 0th IFD contiene información sobre la propia imagen y el 1st IFD se utiliza para almacenar todo lo relacionado con la imagen thumbnail (imagen en miniatura).

V. ANÁLISIS BINARIO DE LA ESPECIFICACIÓN EXIF EN IMÁGENES DE DISPOSITIVOS MÓVILES

Una vez presentada la especificación Exif, se ha estimado oportuno realizar un análisis a nivel binario de imágenes reales tomadas con dispositivos móviles. Este análisis tiene como objetivos profundizar en el conocimiento de la propia especificación y comprobar si ésta es seguida por los fabricantes. Obviamente dado el alto número de etiquetas que posee Exif y que cada imagen sólo posee un subconjunto de ellos, se han elegido algunas estructuras y etiquetas para el análisis. El análisis ha seguido un orden lógico de estructuras de mayor a menor nivel (estructura general JPEG, cabecera TIFF, marcadores, IFDs y etiquetas concretas).

Para el primer análisis se han seleccionado dos fotografías tomadas desde 2 teléfonos móviles (Samsung Galaxy S y Sony Ericsson W580i). Estas fotografías no han sufrido ningún tipo de proceso posterior a la captura de la imagen en el teléfono móvil. Inicialmente se comprobó que los archivos son JPEG. Analizando a grandes rasgos su estructura general se observa que ambas imágenes comienzan con el valor binario 0xFFD8 (SOI) y terminan con el valor binario 0xFFD9 (EOI). Posteriormente, en la imagen del Samsung Galaxy S puede comprobarse la existencia del marcador APP1 (0xFFE1), seguido de su tamaño 0x288E (alineación "Motorola"), es decir, 10382 bytes de datos (incluidos los 2 bytes que indican la longitud). Por tanto APP1 en este caso comienza en 0x0004 y termina en 0x2892 (este byte no incluido).

Para el caso del Sony Ericsson W580i, igualmente se contempla el marcador APP1 (0xFFE1), seguido del tamaño 0x133D (alineación "Motorola"), es decir, 4925 bytes de datos (incluidos los 2 bytes que indican la longitud). Por tanto APP1 en este caso comienza en 0x0004 y termina en 0x1341 (este byte no incluido). Si se extrae para las dos imágenes el marcador que sigue a APP1 se observan diferentes resultados:

- Samsung Galaxy S: El siguiente marcador (en la dirección 0x2892) es 0xFFDB, el cual según Exif se corresponde con DQT.
- Sony Ericsson W580i: El siguiente marcador (en la dirección 0x1314) es 0xFFC4, el cual según el Exif se corresponde con DHT.

Con estos dos datos anteriores se observa que tras APP1, en imágenes diferentes le siguen marcadores diferentes, lo cual es totalmente permitido por Exif.

Dentro de la estructura del marcador APP1 se encuentran los datos de la cabecera TIFF, donde puede observarse que ambas imágenes siguen la especificación Exif, tienen alineación "Intel" para representar los datos TIFF y un offset de 0x00000008 bytes al primer IFD.

Una vez analizados algunos marcadores, hay que pasar al siguiente nivel, los IFDs. En la imagen del Samsung Galaxy S se va a examinar la estructura de su primer IFD y las dos primeras etiquetas. Tras la cabecera TIFF se encuentran los bytes 0x0C00. Teniendo en cuenta que la alineación es "Intel" éstos bytes indican cuantas entradas tiene el directorio actual, en este caso el *0th IFD*. Por tanto el *0th IFD* tiene 12 entradas: La primera entrada del directorio 0x0E010200140000009E000000 se interpreta como se muestra en la Tabla II.

Para obtener el valor de la etiqueta "Image Description" tenemos que ir al lugar que nos indica el offset debido a que su tamaño es mayor de 4 bytes. Como la longitud es 0x9E con respecto al inicio de la cabecera TIFF, los datos de la etiqueta comienzan en la posición 0xAA. A partir de ese byte hay que contar 20 elementos de tipo ASCII (7-bit ASCII) por lo que el valor de la etiqueta es "SAMSUNG (12 espacios en blanco, 0x00)", terminando en NULL (0x00) como se indica en Exif, ya que cada etiqueta posee una semántica diferente.

Al examinar la siguiente etiqueta del directorio *0th IFD* para el mismo archivo se observa que la segunda entrada del directorio es la 0x0F01020014000000B2000000, cuya interpretación se muestra en la Tabla II.

Para obtener el valor de la etiqueta "Make" se debe ir al lugar que indica el offset. Como la longitud es 0xB2 con respecto al inicio de la cabecera TIFF, los datos de la etiqueta comienzan en la posición 0xBE. A partir de ese byte hay que contar 20 elementos de tipo ASCII, por lo que el valor de la etiqueta es "SAMSUNG (12 espacios en blanco - 0x00)" terminando en NULL (0x00) como se indica en Exif. Como se puede observar en la Tabla II dos etiquetas diferentes "Image Description" y "Make" pueden tener los mismos valores para

Tabla III
ANOMALÍAS EN ETIQUETAS EN *0th IFD*

Móvil	Entradas *0th IFD*	Etiqueta	Tipo	No. de Elementos	Offset
Samsung Galaxy S	0x10010200080000000C6000000	Model (0x0110)	ASCII (0x0002)	8 (0x00000008)	198 bytes (0x000000C6)
Nokia N70	0x04A0020001000000031005202	Related Audio File (0x04A0)	ASCII (0x0002)	1 (0x00000001)	0x31005202
	0x20A0020001000000031909504	Unique Image ID (0xA420)	ASCII (0x0002)	1 (0x00000001)	0x31909504

una misma imagen, eso sí, su información debe ser duplicada para que se siga la especificación Exif.

A continuación se van a analizar los mismos elementos del IFD para la imagen del Sony Ericsson W580i. Tras la cabecera TIFF están los bytes 0x0A00. Teniendo en cuenta que la alineación es "II" ("Intel") éstos bytes 0x0A00 indican cuantas entradas tiene el directorio actual, en este caso el *0th IFD*. Por tanto el 0th IFD tiene 10 entradas. La primera entrada del directorio 0x0F0102000E00000086000000 se interpreta como se muestra en la Tabla II.

Por tanto para obtener el valor de la etiqueta "Make" se debe ir al lugar que indica el offset. Como la longitud es 0x86 con respecto al inicio de la cabecera TIFF, los datos de la etiqueta comienzan en la posición 0x92. A partir de ese byte hay que contar 13 elementos de tipo ASCII por lo que el valor de la etiqueta es "Sony Ericsson0x00" terminando en NULL (0x00) como lo indica la especificación de Exif. Al examinar la siguiente etiqueta del directorio *0th IFD* se observa que la segunda entrada del directorio es 0x10010200060000000A6000000, cuyo significado se muestra en la Tabla II.

Por tanto para obtener el valor de la etiqueta "Model" se debe ir al lugar que indica el offset. Como la longitud es 0xA6 con respecto al inicio de la cabecera TIFF, los datos de la etiqueta comienzan en la posición 0xB2. A partir de ese byte hay que contar 6 elementos de tipo ASCII, por lo que el valor de la etiqueta es "W580i0x00" terminando en NULL (0x00), siguiendo la especificación Exif.

VI. ANOMALÍAS EN METADATOS EXIF

Tras el análisis binario de varias imágenes, se han detectado casos en los que no se sigue la especificación al 100 %, aún indicando en su cabecera lo contrario. A continuación se mostrarán casos en el que el fabricante asegura que su imagen sigue Exif 2.2 y realmente no cumple la especificación. Posteriormente se analizarán dichas anomalías.

En una fotografía tomada con un Samsung Galaxy S, se detecta que una entrada del directorio IFD0 es 0x10010200080000000C6000000, cuyo significado se muestra en la Tabla III.

Por tanto como se observa del offset 0xC6 desde el inicio de la cabecera TIFF apunta a la dirección 0xD2, donde se encuentra el valor de la etiqueta "Model" es "GT-I9000" y tiene longitud 8 como se indicaba en la cabecera. A simple vista todo es correcto, pero siendo estrictos, esta imagen no cumple al 100 % la especificación Exif 2.2, ya que se indica que el tipo es 2 (ASCII terminado en NULL - 0x00) y esta cadena no termina en NULL. Para almacenar "GT-I9000" se necesitan 9 elementos (8 caracteres ASCII + 1 NULL) y no 8 como indica la entrada del directorio.

Dos casos más se presentan en las etiquetas 0xA004 ("Related Audio File") y 0xA420 ("Unique Image ID") de una fotografía de un teléfono móvil Nokia N70, que asegura igualmente seguir la especificación Exif 2.2. Las entradas de las dos etiquetas anteriores y su interpretación se muestran en la Tabla III.

Según la especificación Exif la etiqueta "Related Audio File" es de tipo ASCII y posee 13 elementos, es decir 0x0000000D, pero como se puede observar en la Tabla III realmente almacena 0x00000001, es decir 1 elemento, lo cual viola claramente la especificación, por dos razones. Primero porque la etiqueta "Related Audio File" indica que el tamaño de los datos tiene que ser 13 bytes y segundo porque la especificación Exif indica que el tamaño mínimo de los datos tiene que ser 4 bytes. Al analizar los datos que se almacenan (0x31005202) vemos que el valor es un 1 en ASCII, seguido del valor nulo 0x00, R en ASCII y el valor 0x02 (STX en ASCII).

En el caso de la etiqueta "Unique Image ID", cuya interpretación se muestra en la Tabla III, que según la especificación Exif, es de tipo ASCII y posee 33 elementos, es decir 0x00000021, pero realmente almacena 0x00000001, es decir 1 elemento, lo cual viola claramente la especificación.

Una vez visto que este archivo no sigue la especificación, vemos que el valor de la etiqueta es 0x31909504 y tiene en cuenta 4 bytes, el análisis revela que el quinto byte es el comienzo de otra etiqueta. Este hecho hace que se viole de nuevo la especificación, ya que en el tipo ASCII es obligatorio que termine en nulo (0x00) y en este caso el nulo no aparece en la cadena. Asimismo existe otra violación de la especificación en los datos almacenados cuyo valor en ASCII es "1□□{{EOT}}", ya que los caracteres ASCII son de 7 bits (rango de 0-127, 0x00-0x7F), por lo que los caracteres 0x90 y 0x95 están totalmente fuera de lo que permite la especificación. Estos hechos pueden generar problemas para los programas que extraen la información Exif por la incoherencia entre la especificación y los datos almacenados. Dado que este tipo de casos pueden llegar a ser numerosos, los visores de información Exif deberían tomar un criterio uniforme para la extracción de cadenas ASCII. Existen distintas opciones posibles entre las que destacamos:

1. En casos de violación de la especificación no mostrar los datos e indicar un error en el parseo ya que no se sigue la misma. Esta opción es la más restrictiva, ya que no permite ningún tipo de "licencias" sobre la especificación.
2. Extraer todos los datos del tipo ASCII hasta que se en-

cuentre el primer nulo (0x00). Esta opción puede hacer que se generen errores graves, ya que si las cadenas ASCII no terminan en nulo, se pueden mostrar datos no pertenecientes a la etiqueta. Y en el peor de los casos, puede producir desbordamientos de memoria si en los bytes sucesivos a la etiqueta no existiera el valor nulo.

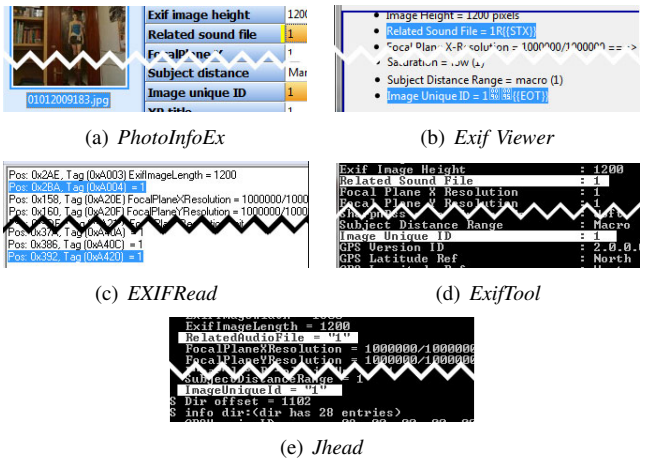
3. Extraer todos los datos teniendo únicamente en cuenta el tamaño indicado en la propia etiqueta. Esta es la opción menos restrictiva, ya que mostraría los caracteres ASCII del tamaño indicado, aunque estos no cumplieran las restricciones de la especificación Exif.
4. Opción mixta entre 2 y 3. Es decir extraer todos los datos teniendo el cuenta el tamaño de los mismos y separando las distintas cadenas teniendo en cuenta el nulo (0x00) como separador.
5. Extraer todos los datos de la etiqueta ignorando el tamaño indicado en el mismo. Es decir si el tamaño es menor o igual a 4 bytes, extraer los cuatro bytes siguientes, y si es mayor de 4 bytes obtener el número de bytes indicados en el tamaño a partir del offset correspondiente. Para el tratamiento de los valores nulos (0x00) se debe escoger entre distintas opciones dentro de este mismo caso, como pueden ser tratarlos como espacios en blanco (lo cual puede generar problemas por hacerlo indistinguible con respecto al caracter ASCII de espacio en blanco), ignorarlos (caracter vacío) o sustituirlos por un caracter especial fuera del rango ASCII válido para Exif (rango de 0-127).

Las opciones 2 a 5 muestran alternativas que permiten la extracción de la información de la imagen a costa de pasar por alto el seguimiento estricto de la especificación Exif.

VII. Anomalías en Herramientas de Análisis Forense de Metadatos Exif

Para analizar los datos mostrados de las etiquetas presentadas en la Tabla III, se utilizaron 5 herramientas enfocadas al análisis de metadatos Exif: *PhotoInfoEx*, *Exif Viewer*, *EXIFRead*, *ExifTool* y *Jhead*. Con respecto a la etiqueta "Related Audio File" de la Tabla III, *Exif Viewer* muestra exactamente "1R{{STX}}", lo cual indica que toma como opción la 5, ya que se ignora el tamaño de los datos de la etiqueta (que en este caso es 1). En este caso se observa que *Exif Viewer* ignora los caracteres nulos (0x00), ya que existen 4 bytes pero sólo muestra los 3 que no son nulos. Teniendo en cuenta que el tamaño mínimo de los datos de una etiqueta es 4 bytes (ya que si es menor se tienen que ocupar los cuatro bytes destinados al campo datos de la etiqueta) la forma de presentar los datos de *PhotoInfoEx*, *EXIFRead*, *ExifTool* y *Jhead* parece ser el mostrar estrictamente el número de elementos que dicta la etiqueta ("1"), es decir, utilizan la opción 3, no visualizando posible información sin inicializar o "basura" (ver figura 1).

Independientemente de la forma de mostrar los datos de los 5 visores Exif mencionados, hay un problema en la creación del archivo por parte del fabricante al no seguir fielmente la especificación. Por tanto, la opción tomada en la interpretación de estas anomalías es relevante y tiene consecuencias en los resultados obtenidos para su posterior análisis forense, ya que las opciones 2, 3 y 4 muestran datos alterados o sesgados sobre etiquetas inválidas que no siguen la especificación.



(a) *PhotoInfoEx* (b) *Exif Viewer*

(c) *EXIFRead* (d) *ExifTool*

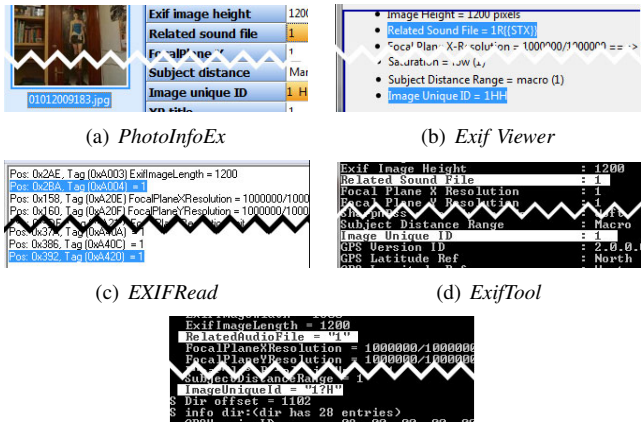
(e) *Jhead*

Figura 1. Herramientas para el análisis de metadatos Exif.

En el caso de la etiqueta "Unique Image ID", las herramientas *PhotoInfoEx*, *EXIFRead*, *Exif Tool* y *Jhead* muestran como valor de la etiqueta un "1" , por lo que muestran los datos hasta el número de elementos que dicta la etiqueta, observando que en este caso se sigue también la opción de análisis sintáctico número 3, por otra parte, *Exif Viewer* muestra "1□□{{EOT}}", es decir cuatro caracteres, mostrando correctamente los valores ASCII que pertenecen al rango válido de la especificación Exif y un "cuadrado" con el valor en hexadecimal del byte en el interior cuando no pertenecen al rango válido (para este caso concreto los valores 90 y 95).

Para poder asegurar en qué caso de los anteriormente expuestos con respecto a los datos ASCII mostrados se encuentran estas 5 herramientas, se va a modificar el archivo con un editor hexadecimal indicando que para la etiqueta "Unique Image ID", el tamaño de los datos a 3 (lo que sigue violando la especificación) y que los datos son '0x31004848', por lo que la etiqueta completa quedaría '0x20A4020003000000031004848'. Tras este cambio se analizan nuevamente los datos de las etiquetas con las 5 herramientas (ver figura 2), observando que *EXIFRead* y *Exif Tool* muestran "1", según la opción 2, *PhotoInfoEx* y *Jhead* muestran "1 H" y "1?H" respectivamente, según la opción 3. Además se comprueba que *PhotoInfoEx* y *Jhead* muestran los nulos (0x00) como el caracter espacio en blanco y el símbolo "?", lo cual causa un grave problema de indistiguibilidad con los caracteres ASCII espacio en blanco y "?" (0x20 y 0x3F) incluidos en el rango válido ASCII para Exif. Es decir, en este caso concreto desde *PhotoInfoEx* y *Jhead* el analista forense no puede distinguir si los datos que almacena la etiqueta son "10x00H" o "10x20H" y "10x3FH". *Exif Viewer* muestra los datos como "1HH", por lo que se puede ratificar de nuevo que muestra los datos de la forma indicada en el caso 5, ignorando el tamaño de los datos de la etiqueta (que en este caso es 3). En este caso se confirma, como era de esperar, que *Exif Viewer* ignora los caracteres nulos (0x00), corroborando los resultados obtenidos anteriormente

en la visualización de la etiqueta “Image Unique ID” por parte de la misma herramienta. Aún así para todos estos casos, es conveniente volver a reseñar que el problema proviene del fabricante que no sigue la especificación Exif.



(a) *PhotoInfoEx* (b) *Exif Viewer*

(c) *EXIFRead* (d) *ExifTool*

(e) *Jhead*

Figura 2. Información una vez editada la etiqueta “Unique Image ID”.

Asimismo, se observa un error crítico en la herramienta *PhotoInfoEx*, que al seguir la opción 3, al hacer “clic” en una etiqueta específica, por ejemplo en la etiqueta “Related Audio File” cuyo valor mostrado es “1”, el valor de la etiqueta pasa a ser “1” automáticamente y simplemente realizar esta acción y no hacer ninguna otra más hace que la herramienta tome ese campo como editado. Al cambiar de fotografía nos indica si queremos guardar los cambios. Al aceptar la modificación de los metadatos de la fotografía, *PhotoInfoEx* no solo modifica el valor de la etiqueta editada sino que modifica todas las etiquetas de los metadatos Exif, por ejemplo, la etiqueta “Image Unique ID” cuyo valor original es “1□□{{EOT}}”, que no fue editada por el analista. Esto puede ser perjudicial para la tarea del análisis forense ya que modifica datos sin autorización atentando así contra la integridad de la evidencia. En la Tabla IV se muestra el MD5 calculado del fichero analizado antes y después de visualizarlo con *PhotoInfoEx*.

Tabla IV
MD5 GENERADO DE FOTOGRAFÍA ANTES Y DESPUÉS DE SER ANALIZADA CON *PhotoInfoEx*

	Datos
Antes	4A07D9094BE9ADE0B719A2BF8AC1218C
Después	785B5670940811F0F58CE9D689FB2BFF

VIII. CONCLUSIONES Y TRABAJO FUTURO

En este artículo se han mostrado tres ejemplos de las anomalías detectadas en etiquetas (“Model”, “Related Audio File” y “Unique Image ID”) tras el análisis binario manual de varias imágenes, pero no han sido las únicas detectadas, ya que se han encontrado más otras etiquetas como “Exif version”, “Meetering Mode”, “Exposure Program”, “DateTimeOriginal”, etc. Por tanto, se puede concluir que muchos de los fabricantes no siguen fielmente las especificaciones Exif, indicando en el propio archivo lo contrario, lo cual puede producir graves problemas en la extracción de los metadatos de las imágenes por medio de aplicaciones, así como problemas de interoperabilidad entre distintos dispositivos. Adicionalmente, se ha evaluado la robustez de 5 herramientas (*PhotoInfoEx*, *Exif Viewer*, *EXIFRead*, *Exif Tool* y *Jhead*) con respecto a la extracción de metadatos que no cumplan la especificación Exif, encontrando que *EXIFRead* y *Exif Tool* extraen los datos de la etiqueta hasta que encuentran un caracter nulo; *PhotoInfoEx* y *Jhead* extraen los datos teniendo en cuenta únicamente el tamaño indicado en la etiqueta identificando los caracteres nulos con los símbolos “espacio en blanco” y “?” respectivamente y *Exif Viewer* muestra la información completa de la etiqueta ignorando los caracteres nulos aunque dicha etiqueta tenga anomalías en el seguimiento de la especificación Exif. Asimismo, se detectó que la herramienta *PhotoInfoEx* con sólo hacer clic sobre una etiqueta modifica todas las etiquetas de los metadatos Exif almacenados en una fotografía, dejando como valor el presentado en pantalla, sin que el analista forense autorice su modificación. Este es un error crítico en una herramienta utilizada para el análisis forense ya que lo que se quiere es garantizar la inviolabilidad de los datos. Por todo lo anterior, en la actualidad estamos trabajando en el desarrollo de una herramienta que solucione los problemas detectados y posea funcionalidades adicionales.

AGRADECIMIENTOS

Los autores agradecen la financiación que les brinda el Subprograma AVANZA COMPETITIVIDAD I+D+I del Ministerio de Industria, Turismo y Comercio (MITyC) a través del Proyecto TSI-020100-2011-165. Asimismo, los autores agradecen la financiación que les brinda el Programa de Cooperación Interuniversitaria de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), Programa PCI-AECID, a través de la Acción Integrada MAEC-AECID MEDITERRÁNEO A1/037528/11.

REFERENCIAS

[1] T. Gloe, M. Kirchner, A. Winkler, R. Böhme, “Can We Trust Digital Image Forensics?”, *in Proceedings of the 15th international Conference on Multimedia (MM’07)*, Augsburg, Bavaria, Germany, September 23-28, pp. 78-86. ACM Press, New York, 2007.

[2] V. Thing, K.-Y. Ng, E. Chang, “Live Memory Forensics of Mobile Phones”, *in Digital Investigation*, Vol 7, pp. S 74-82, 2010.

[3] C. McKay, A. Swaminathan, H. Gou, M. Wu, “Image Acquisition Forensics: Forensic Analysis to Identify Imaging Source”, *in Proceedings of the 2008 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2008)*, pp. 1657-1660, 2008.

[4] M. Boutell, J. Luo, “Photo Classification by Integrating Image Content and Camera Metadata”, *in Proceedings of the 17th International Conference on Pattern Recognition (ICPR ’04)*, Vol. 4, pp. 901-904, 2004.

[5] J. Tesic, “Metadata Practices for Consumer Photos”, en *IEEE Multimedia*, Vol. 12, No. 3, pp.86-92, 2005.

[6] M. Boutell, J. Luo, “Beyond Pixels: Exploiting Camera Metadata for Photo Classification”, en *Pattern Recognition*, Vol. 38 No. 6, pp. 935-946, 2005.

[7] C. Hamilton, C. Cube, “Microsystems. JPEG File Interchange Format”. Version 1.02, September 1, 1992. www.w3.org/Graphics/JPEG/jfif3.pdf.

[8] “Exchangeable Image File for digital still cameras: Exif version 2.3. www.cipa.jp/english/hyoujunka/kikaku/pdf/DC-008-2010_E.pdf.