METODOLOGÍA DE ANÁLISIS FORENSE DE IMAGEN DIGITAL

Aguirre Gallardo Emilse
Universidad Autónoma "Juan Misael Saracho"
Facultad de Ciencia Integradas del Gran Chaco
Yacuiba –Bolivia
emilseaguirre.2012@gmail.com

RESUMEN

En la actualidad, en el mundo se ha encontrado una controversia referente a la validez de las imágenes digitales en diversos tipos de procesos, el hecho se fundamenta en la supuesta facilidad con la que se puede alterar este tipo de imágenes, gracias a la nueva tecnología, una cosa es quitarse años con una aplicación y otra muy diferente es realizar fotomontajes para ocultar la verdad o dañar la integridad física de las personas.

Son muchos los casos donde las fotografías son las causas que han llevado a la cárcel a alguna persona o las han salvado, o han hecho ver al mundo que algo existe, en casi el 80% de los juicios penales presentan pruebas de fotografías o videos como evidencia.

En este sentido, se desarrolla una metodología orientada al análisis forense de imágenes digitales para mejorar el proceso de investigación de Fuerza Especial de Lucha contra la Violencia (FELCV) en la resolución y esclarecimiento de casos donde se ve involucrada una imagen o fotografía como prueba como evidencia en un proceso judicial, cuyo objetivo es de confirmar la fuente y autenticidad de la misma.

Este trabajo de investigación hace una revisión de varias metodologías para definir una nueva adaptada al proceso que debe seguir una imagen para ser presentada como prueba documental en un proceso judicial.

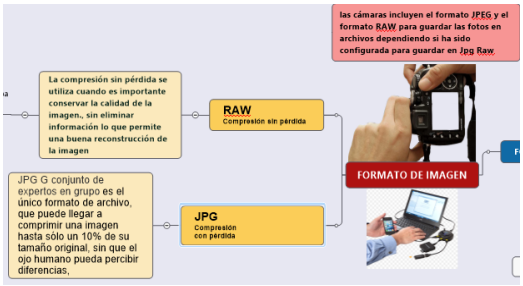
Palabras Clave

Montaje, fotosensible, informática forense, autenticidad.

1. ANÁLISIS FORENSE DE IMÁGENES DIGITALES

El análisis forense es una de las múltiples facetas del perito informático, el objetivo de este tipo de análisis es la de garantizar y determinar el origen fuente y autenticidad de una imagen digital que pretende utilizarse como evidencia en una investigación de carácter legal.

1.2. Formatos y compresión de imágenes digitales



Fuente: Elaboración propia
Figura: 1. Compresión de JPG Y RAW

La compresión de datos es la reducción del volumen de datos para representar una determinada información, intentando que esta reducción de tamaño no afecte al contenido, No obstante, la reducción de datos puede afectar o no a la calidad de la información.

Compresión sin pérdida: los datos antes y después de comprimirlos son iguales, lo cual implica más tiempo de proceso

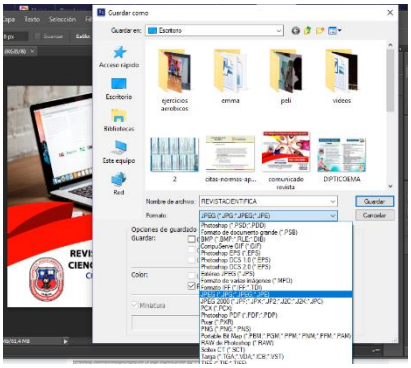
Compresión con pérdida: puede eliminar datos para disminuir aún más el tamaño, con lo que reduce la calidad. Una vez realizada la compresión, no se puede obtener la señal original, aunque sí una aproximación cuya semejanza con la original dependerá del tipo de compresión. (López, 2018)

1.2.1. La profundidad de color

Cada pixel (punto) de la imagen tiene codificado un color, para ello se usan un número determinado de bits, cuanta más profundidad de color más bits y por tanto más tamaño de archivo para una imagen con una determinada resolución. Así una codificación de color de 8 bits requerirá el doble de espacio de almacenamiento que una codificación de 16. (López, 2011)

1.2.2. Formatos de Imágenes

Existen multitud de formatos para comprimir las imágenes digitales RAW, JPG (o JPEG), GIF y PNG, pero nos centraremos en los formatos que utilizaremos en el desarrollo del trabajo de investigación: RAW, JPG (o JPEG), Por ejemplo el formato RAW es muy frecuente en las cámaras digitales profesionales para cambiar su tamaño, resolución o formato hay que emplear un editor de imágenes, como Photoshop, GIMP o Paint.NET. (López, 2018)



Fuente: Elaboración propia
Figura: 2. Formato de una imagen

- **Formato RAW** (en inglés crudo)

El formato RAW solo se encuentra disponible en cámaras digitales sofisticadas, indicadas para fotógrafos profesionales. Este formato ofrece la máxima calidad ya que contiene los píxeles en bruto tal y como se han adquirido.

Los datos del archivo RAW no han sufrido ninguna clase de compresión, lo que hace que este archivo mantenga el máximo detalle de la imagen. El peso del archivo ocupa mucho espacio, no se puede imprimir ni visualizar directamente, precisa del tratamiento informático y realizar conversión para que se pueda utilizar.

- **Formato JPEG (Joint Photographic Experts Group)**

Soporta 16,7 millones de colores (24 bits) y es el más empleado y adecuado para las fotografías. Usa compresión con pérdidas es el único formato de archivo, que puede llegar a comprimir una imagen hasta sólo un 10% de su tamaño original, sin que el ojo humano pueda percibir diferencias. (Perdomo, 2018)

1.3. ¿Qué son los metadatos?

Los Metadatos son información adicional sobre los datos con estos metadatos podemos demostrar que cierta persona es dueña de un archivo, también podemos obtener los nombres de los usuarios que crearon el archivo datos propios de los documentos, no de su contenido, en el caso de las imágenes, por ejemplo, la fecha y la hora en la que han sido tomadas, con qué cámara o teléfono, ubicación geográfica, calidad, tamaño, etc.
Exif un estándar creado para guardar metadatos en imágenes digitales, los datos EXIF contienen información propia de la imagen en donde son incrustados como fichero en la imagen digital por lo que en cierto modo se podrá saber los datos del dispositivo el dónde fue tomada la imagen. (Moya, 2017)

1.3.1. Herramientas para ver los metadatos

Fuente: Elaboración propia
Figura: 3. Herramientas para ver metadatos de una imagen

Existen muchas herramientas para ver los metadatos y análisis de montajes que se estudiaron para el desarrollo de la metodología, de las cuales se recomiendan las más adecuada y completas para este tipo de análisis.

- **ExifTool (Herramienta Exif)**

ExifTool también está disponible como un ejecutable independiente de Windows y un paquete MacOS. Se trata de un programa que permite consultar los metadatos que contiene un archivo; hay dos formas de realización por comando y también tiene interfaz gráfica.

- Forensically

Forensically es una herramienta web pensada específicamente para la detección de alteraciones en una fotografía.

Su lista de funciones permite ver retoques digitales en cualquier imagen que se suba a esta página, cuenta con la lupa, detección de la función clonar de Photoshop, análisis de ruido, acceso a los metadatos y a las etiquetas de geolocalización.

- **FotoForensics**

FotoForensics busca aspectos retocados de una imagen que subas en formato JPEG o RAW o de la que conozcas su enlace online es más sencillo que Forensically. Se limita a mostrar los metadatos, analizar el ruido de la imagen y la compresión JPEG.

Las imágenes que suban son públicas y puedes compartir el resultado del análisis a través de Twitter, Facebook, Google, Pinterest o Reddit. Una manera rápida y práctica de desenmascarar imágenes falsas y compartir el resultado con otros internautas.

1.4. Detección de manipulaciones: fotomontajes, áreas “clonadas” y demás ajustes.

Uno de los aspectos que más suele interesar a la hora de hacer un análisis forense de una imagen es detectar manipulaciones dentro de la escena, es decir, si hay elementos añadidos o retirados de la misma, que no corresponden con el momento de la toma.

Para ello hoy en día se puede realizar diferentes análisis que puedan aportar evidencias.

“Para el análisis pericial se toma como premisa el establecimiento de la relación inequívoca de los 3 elementos fundamentales del delito, el hecho o el crimen: atacante, víctima y escena del hecho”. (Rosales, 2017).

1.5. Perito informático en Bolivia

Para definir la selección del perito se debe tomar en cuenta primero el ordenamiento legal:

NCPP Artículo 204º.- (Pericia). Se ordenará una pericia cuando para descubrir o valorar un elemento de prueba sean necesarios conocimientos especializados en alguna ciencia, arte o técnica.

Sin embargo, dada la naturaleza del proceso o investigación y su semejanza con juegos estratégicos o ajedrez se debe tomar en cuenta lo que normalmente se conoce como “el pedigrí del perito” o en otros términos la solvencia profesional que precede al profesional que prestara juramento.

NCPP Artículo 205º.- (Peritos). Serán designados peritos quienes, según reglamentación estatal, acrediten idoneidad en la materia. Si la ciencia, técnica o arte no está reglamentada o si no es posible contar con un perito en el lugar del proceso, se designará a una persona de idoneidad manifiesta.

Las reglas de este Título regirán para los traductores e intérpretes.

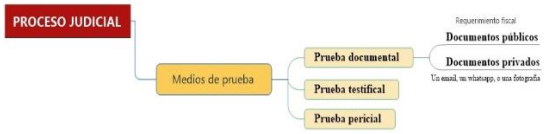
En Bolivia no tenemos definido los criterios para seleccionar un perito informático sin embargo se practica aplicar los siguientes:

- Profesional de licenciatura o ingeniería de sistemas.
- Colegiado en la Sociedad de Ingenieros o Colegios de Informáticos legalmente reconocidos.
- Especializado en temas de seguridad por cuanto es lo más cercano a los trabajos periciales como formación reconocida. Sin embargo, desde el año 2006 se ha instaurado en Bolivia el programa de entrenamiento profesional FCA – Forensic Computer Advisor que pretende establecer la formación básica para esta actividad.
- Trayectoria profesional mínima de 5 años.

Dada la conformación de equipos en las partes querellante y querellado, se debe tomar en cuenta la figura del consultor técnico.

Las atribuciones de este último están definidas legalmente en el Art. 207 c.p.p.:

1.6. Fotografía como Medios de prueba en procesos judiciales



Fuente: Elaboración propia
Figura: 4. **Medios de Pruebas**

En los procesos judiciales, de manera resumida, pueden existir tres medios de prueba diferentes.

Prueba documental Arts. 216-220 NCPP: La formada por los documentos aportados durante el proceso. Tantos documentos públicos como privados.

- **Documentos públicos:** que son los autorizados por notario, las resoluciones judiciales, las certificaciones de los registradores, y los expedidos por los funcionarios en el ámbito de sus funciones, y con arreglo a las leyes. Estos documentos sirven como medio de prueba plena en un juicio sobre el hecho de que tratan, su fecha y la identidad de las personas que intervienen.
- **Documentos privados**, que son todos los demás, y que producirán efectos en un juicio si no son impugnados por la parte a la que perjudiquen. En otro caso será necesario utilizar cualquier medio de prueba que permita valorar su autenticidad por el tribunal.

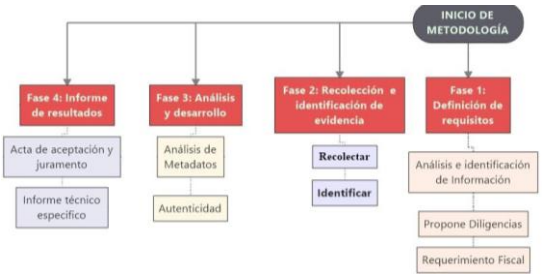
Un email, un whatsapp, o una fotografía, es un documento, 'medios de prueba', sin embargo, los tribunales, califican estos mensajes como documentos privados.

Prueba testifical Arts. 193-215 NCPP (Arts. 350 y 355): Firmada por el interrogatorio a las partes y testigos.

Prueba pericial Arts. 204-215 NCPP (Art. 349): Que la forman los dictámenes elaborados por los peritos.

2. METODOLOGÍA PARA EL ANÁLISIS FORENSE DE IMAGEN DIGITAL

La metodología propuesta se divide en 4 etapas las cuales se muestran a continuación.



Fuente: Elaboración propia
Figura: 5. Metodología Propuesta

Tabla 1: **Metodologías estudiadas.**

METODOLOGIA	PASOS
Metodología para un análisis forense	Asegurar la escena Identificar y recolectar las evidencias Preservar las evidencias Analizar las evidencias obtenidas Redactar informes sobre los resultados
Metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador	Definición de los requisitos para el inicio de la investigación. Identificación de dispositivos y evidencia digital, recolección de información volátil. Extracción de la información volátil, empaquetado y transporte de dispositivos e información extraída. Copias bit a bit de medios de almacenamiento, verificación de integridad y recuperación de imágenes ocultas y eliminadas. Identificación, detección de contenido oculto. Recolección de fichas para sustentar la cadena de custodia y creación de informes técnico y ejecutivo.
Análisis informático forense para la recopilación confiable de datos y evidencias digitales	***Fase De Identificación*** Solicitud Forense Asegurar La Escena Identificar Las Evidencias Prioridades Del Administrador Tipo De Dispositivo Modo De Almacenamiento ***Fase De Recopilación*** ***Fase de Preservación*** Copias De La Evidencia Cadena De Custodia ***Fase De Análisis*** Preparación Para El Análisis Pasos Para Realizar un Análisis de Datos Forense ***Fase De Documentación Y Presentación De Las Pruebas*** Utilización De Formularios De Registro Del Incidente.
Aplicación de la técnica error level análisis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles	levantamiento de mapa de procesos Análisis de la información Aplicabilidad de la técnica ELA

Fuente: Elaboración propia

A continuación, se describe las etapas de la metodología propuesta.

2.1. Fase 1: Definición de requisitos

Fuente: Elaboración propia

Figura: 6. Fase 1 Definición de requisitos

Como primer paso se hace un análisis e identificación de la información que se requiera, para esto se formula la pregunta:

¿Qué necesito y para qué lo necesito? se determina si se requiere acción policial etc.

Se **propone diligencias** en calidad de pruebas de descargo señalando que solicitud se requiere de acuerdo al caso.

- **Propone diligencias**

- solicitudes de pericia informática
- secuestro de evidencia (celular)
- orden de allanamiento requisa y secuestro
- Consentimiento libre de la persona afectada para el registro y extracción de evidencia.

Los peritos forenses deberán recibir una solicitud de investigación y deberán realizar el estudio científico bajo la dirección de la Fiscalía mediante un memorial

Estos peritos forenses deberán tener el perfil que se norma en Bolivia como se menciona anteriormente en el Nuevo código de procesamiento penal en Bolivia.
"NCPP Artículo 205" donde se define qué características debe tener un perito de acuerdo a eso propone diligencias mediante un memorial al fiscal. Ejemplo anexo1

Señor Fiscal de Materia III de la ciudad de Yacuiba
(Fernando Valverde Sebastián)

Propone diligencias en calidad de prueba de descargo.-
Otrosies.-

Juan Pérez, de Generales conocida dentro del proceso que sigue en mi contra la señora **Rosa** por la presunta comisión del delito de agresión física y psicológica, interno 174/2018, ante Ud. Con el debido respeto expongo y pido

Solicito SE DESIGNE como perito informatico al señor, GUSTAVO PADILLA, mayor de edad, hábil por ley, casado, Informatico, con domicilio en calle independencia y avaroa 2 **CI:** 5045295 tj para que:

Se realice un estudio técnico en el teléfono celular marca Samsung color blanco táctil, en fecha 02/01/2018 al 04/01/2018 para la verificación de existencia de archivos de imágenes con IMEI: 1223654789 y posterior copiado de las mismas para brindar un inrome del las imágenes analizadas.

Amparado en lo establecido por el art. 306 del C.P.P, a efecto de contar con prueba pertinente y licita que demuestre que mi persona no cometió el delito del que se me acusa.

Otrosí.- Determinaciones en la secretaria de su digno despacho

Otrosí 2.- Solicito fotocopias legalizada del resultado de la pericia del análisis forense de imagen realizada.

Yacuiba 20 de octubre 2018

Fuente: Elaboración propia

Figura: 7. Propone Diligencias

- **Requerimiento fiscal es la respuesta del fiscal a lo solicitado en la diligencia**

De acuerdo a los resultados de la investigación inicial, el requerimiento fiscal puede tener distintas finalidades. Por ejemplo, puede contener una petición de instrucción también puede pedir la desestimación de la denuncia, querella o de informe de la policía, la aplicación de un criterio de oportunidad, etc.
Ejemplo un requerimiento fiscal para solicitud de un perito informático para el análisis de evidencia.

2.2 Fase 2: Recolección e identificación de evidencia

Esta fase se ejecuta de forma previa al proceso de análisis y consiste en recolectar los elementos físicos que se van a analizar y las evidencias que se buscaran en cada uno de los elementos analizados

- Recolectar el dispositivo que contiene las imágenes para analizar de acuerdo a requerimiento fiscal

Puntos a tomar en cuenta:

- Tomar las debidas protecciones físicas.
- Etiquetar con un número único a cada uno de los dispositivos incautados.
- Fotografiar la evidencia de los dispositivos físicos a analizar
- Fotografiar la preservación de la evidencia.

Para evitar ataques e impugnación a las imágenes digitales sugerimos a los expertos no hacer cambios a las imágenes originales ni ajustes sino recomendamos el hacerlo sobre duplicados digitales de las imágenes tomadas para preservar la imagen original como una especie de negativo o de prueba de certeza de la fidelidad de la imagen tomada en el sitio del suceso o lugar de los hechos.

El formulario para el registro de objetos físicos y archivo digital (imágenes) se muestra a continuación, donde se especifican características de los dispositivos e imágenes, se deberán adjuntar fotografías tomadas en el paso anterior.

FORMULARIO DE RECOLECCION E IDENTIFICACION DE EVIDENCIAS

FASE 2

Nº CASO:
12 de Agosto de 201 8
YACUIBA

NOMBRE DE PERITO FORENCE: Ronal Ivar Rodriguez Solis **CI:** 4569871
PROFESION: Ingeniero Informático **ESPECIALIDAD:** En seguridad informática
DOMICILIO: XXX **NACIONALIDAD:** Boliviano **DNI:** 45454
FECHA Y HORA DE INFORME EMITIDO: 12/08/2018
NATURALEZA DEL HECHO: ANALISIS FORENCE DE VERIFICACION DE AUTENTICIDAD Y FUENTE DE IMAGEN DIGITAL

TIPO DE EVIDENCIA: Fotografias del Celular "MARCA SAMSUNG GALAXI S-4 DE COLOR AZUL"

NOMBRE DEL ARCHIVOS: DSC_0109, DSC_0107, DSC_0111, DSC_0112, DSC_0120

FORMATO DE ARCHIVOS: Archivo JPG (.jpg)

FECHA Y HORA DE CREACIÓN DE EVIDENCIA: 09 de Agosto de 2018

UBICACIÓN DEL MEDIO ALMACENADO:

C:\Users\Portatil 3\Documents\easo ds15894\copia de seguridad

CONTIENE: 9 archivos, 0 carpetas

TAMAÑO: 653 KB (669,620 bytes)

TAMAÑO DE COPIA DE RESPALDO: 556 KB (569,967 bytes)

FORMATO DE COPIA DE RESPALDO: Imagen comprimida en Zip

PERSONA AL QUE PERTENCE LA EVIDENCIA:

Fuente: Elaboración propia
Figura: 8. Formulario de recolección de evidencias

2.3 Fase 3: Análisis y desarrollo

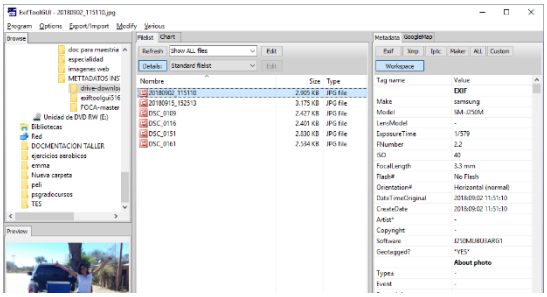
La elección de una correcta herramienta es de gran importancia en esta fase pues debemos tener en mente la preservación de la confiabilidad, con lo que estaremos asegurando la correcta aplicación de la cadena de custodia.

Lo más recomendables es realizar el proceso de análisis con una herramienta y confirmarla con otra, ya que existen software que devuelven resultados por medio de porcentajes, entonces esta comprobación asegura los resultados que obtengamos.

En esta fase se tiene en cuenta que en el análisis forense de imágenes digitales no hay una técnica mágica que permita obtener una conclusión categórica y que, en la mayoría de los escenarios, será necesario aplicar más de una y cruzar los resultados con información geográfica, personal, etc.

2.3.1 Metadatos con Exiftol

La primera técnica de análisis es por metadatos, en la cual se extraen los datos de marca y modelo del objeto de estudio, mismos que son comparados con la información de una imagen de referencia. Se recomienda el programa ExifToolGUI Interfaz Modo Grafica y confirmar con modo comando para Windows.



Fuente: Elaboración propia captura de pantalla.

Figura: 9. Interfaz ExifTool grafica en Windows

Para verificación de la autenticidad de la imagen se recomienda Forensically y FotoForensics

Datos de localización

Marca de tiempo: 2018: 09: 02 11: 51: 10-04: 00

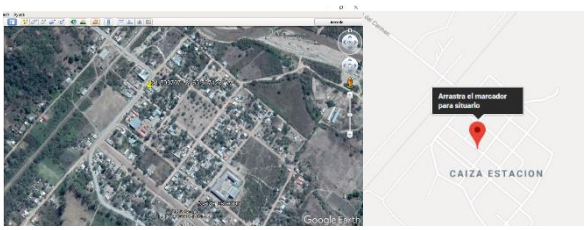
Fecha y Hora: 02 /sep./2018 horas 11:51

Lugar de donde se sacó la foto: Caiza Estación a 30 minutos de Yacuiba

Modo de cámara: SM-J250M

Fabricante de cámara: Samsung

Ubicación grafica de google earth de acuerdo a coordenadas arrojadas por el programa.



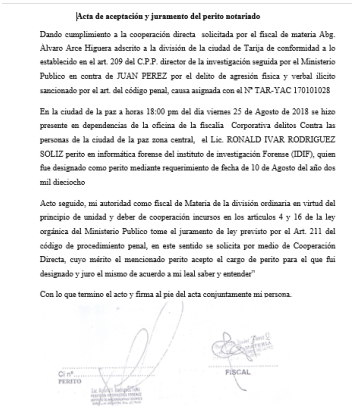
Fuente: Elaboración propia captura del programa
Figura: 10. Interfaz Ubicación geográfica

El siguiente paso es identificar la validez de una imagen para esto se recomienda el programa anteriormente descrito.

2.3.2 Fase 4: Informe de resultados

La última fase del procedimiento consiste en la generación de acta y un informe técnico sobre los resultados de lo que se analizó de acuerdo a requerimiento del fiscal, a partir del procedimiento operativo estándar.

- Acta de aceptación y juramento del perito notariado
- Informe técnico específico.



|Acta de aceptación y juramento del perito notariado

Dando cumplimiento a la cooperación directa solicitada por el fiscal de materia Abg. Alvaro Arce Higuera adscrito a la división de la ciudad de Tarija de conformidad a lo establecido en el art. 209 del C.P.P. director de la investigación seguida por el Ministerio Publico en contra de JUAN PEREZ por el delito de agresión física y verbal ilicito sancionado por el art. del código penal, causa asignada con el Nº TAR-YAC 170101028

En la ciudad de la paz a horas 18:00 pm del dia viernes 25 de Agosto de 2018 se hizo presente en dependencias de la oficina de la fiscalia Corporativa delitos Contra las personas de la ciudad de la paz zona central, el Lic. RONALD IVAR RODRIGUEZ SOLIZ perito en informática forense del instituto de investigación Forense (IDIF), quien fue designado como perito mediante requerimiento de fecha de 10 de Agosto del año dos mil dieciocho

Acto seguido, mi autoridad como fiscal de Materia de la división ordinaria en virtud del principio de unidad y deber de cooperación incursos en los articulos 4 y 16 de la ley orgánica del Ministerio Publico tome el juramento de ley previsto por el Art. 211 del código de procedimiento penal, en este sentido se solicita por medio de Cooperación Directa, cuyo mérito el mencionado perito acepto el cargo de perito para el que fue designado y juro el mismo de acuerdo a mi leal saber y entender"

Con lo que termino el acto y firma al pie del acta conjuntamente mi persona.

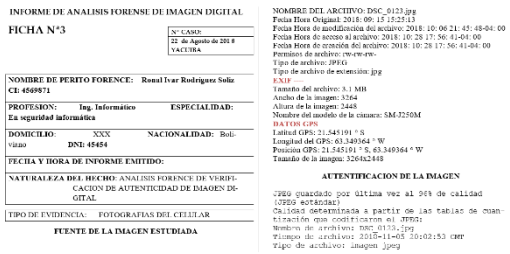
PERITO

FISCAL

Fuente: Elaboración propia

Figura: 11. Acta notariada del perito informático

- Informe técnico específico perito



INFORME DE ANALISIS FORENSE DE IMAGEN DIGITAL

FICHA Nº3

Nº CASO:	22 de Agosto de 201 8 YACUIBA

NOMBRE DE PERITO FORENCE: Ronal Ivar Rodriguez Soliz
CI: 4569871

PROFESION: Ing. Informático **ESPECIALIDAD:** En seguridad informática

DOMICILIO: XXX **NACIONALIDAD:** Bolivino **DNI: 45454**

FECHA Y HORA DE INFORME EMITIDO:

NATURALEZA DEL HECHO: ANALISIS FORENCE DE VERIFICACION DE AUTENTICIDAD DE IMAGEN DIGITAL

TIPO DE EVIDENCIA: FOTOGRAFIAS DEL CELULAR

FUENTE DE LA IMAGEN ESTUDIADA

NOMBRE DEL ARCHIVO: DSC_0123.jpg
Fecha Hora Original: 2018: 09: 15 15:25:13
Fecha Hora de modificación del archivo: 2018: 10: 06 21: 45: 48-04: 00
Fecha Hora de acceso al archivo: 2018: 10: 28 17: 56: 41-04: 00
Fecha Hora de creación del archivo: 2018: 10: 28 17: 56: 41-04: 00
Permisos de archivo: rw-rw-rw-
Tipo de archivo: JPEG
Tipo de archivo de extensión: jpg
EXIF
Tamaño del archivo: 3.1 MB
Ancho de la imagen: 3264
Altura de la imagen: 2448
Nombre del modelo de la cámara: SM-J250M
BATCH GPS
Latitud GPS: 21.545191 ° S
Longitud del GPS: 63.340364 ° W
Posición GPS: 21.545191 ° S, 63.340364 ° W
Tamaño de la imagen: 3264x2448

AUTENTIFICACION DE LA IMAGEN

JPEG guardado por última vez al 96% de calidad (JPEG estándar)
Calidad determinada a partir de las tablas de cuantización que codificaron el JFIF:
Nombre de archivo: DSC_0115.jpg
Tiempo de archivo: 2018-11-05 20:02:53 CET
Tipo de archivo: imagen jpeg

Fuente: Elaboración propia

Figura: 12. Informe técnico del perito informático

3. CONCLUSIONES

Los procesos judiciales, los Abogados, Jueces y en fin las justicias deben permitir que la tecnología permee rápidamente para ayudar a acércanos a la verdad verdadera. Cerrar a los avances tecnológicos es permitir que el Derecho vaya varios años detrás de las ciencias.

La informática forense es de gran manera una de las ayudas que tiene la ley con respecto a la identificación de fotografías truncadas o verdaderas, gracias a ella se puede ver la autenticidad y fuente.

Se recomienda no centrarse en una sola herramienta, si no en varias para comprobar resultados ya que dichas técnicas no están exentas de arrojar falsos positivos, recomendamos realizar el proceso de análisis con una herramienta y confirmarla con otra, ya que existen software que devuelven resultados por medio de porcentajes, entonces esta comprobación asegura los resultados que obtengamos.

Para evitar ataques e impugnación a las imágenes digitales sugerimos a los expertos no hacer el análisis en las imágenes originales ni ajustes sino recomendamos el hacerlo sobre duplicados, para preservar la imagen original como una especie de negativo.

4. BIBLIOGRAFÍA

Guido Rosales. (2011, agosto 21). La informática forense trabaja en Bolivia con tecnología propia. Recuperado 26 de septiembre de 2018, de http://eju.tv/2011/08/la-informtica-forense-trabaja-en-bolivia-con-tecnologa-propia/

Vedia, J. E. P. (2016). El derecho y las tecnologías de la información y comunicación.

Carla Hannover.(2016, 03).Delitos informáticos carecen de atención oportuna y capaz - Diario Página Siete. Recuperado 14 de octubre de 2018, de https://www.paginasiete.bo/sociedad/2016/3/13/delitos-informaticos-carecen-atencion-oportuna-capaz-89688.html

Moya, E. (2017, octubre 8). 7 herramientas para consultar metadatos de .jpg online (Exif) - Magic Words of Intelligence. Recuperado 29 de septiembre de 2018, de https://inteligenciacomunicacionononline.blogspot.com/2015/06/7-herramientas-para-consultar-metadatos.html

Perdomo, S. (2018, febrero 6). Tipos de formatos de imagen digital | Deusto Formación. Recuperado 3 de diciembre de 2018, de https://www.deustoformacion.com/blog/diseno-produccion-audiovisual/tipos-formatos-imagen-digital

Rosales, G. (2017, septiembre 19). Informática forense - Método de las 6Rs. Recuperado 6 de octubre de 2018, de https://yanapti.com/index.php/2017/09/19/informatica-forense-metodo-las-6rs/

Rosales, G. (2017, septiembre 19). Informática forense Método de las 6Rs. Recuperado 6 de octubre de 2018, de https://yanapti.com/index.php/2017/09/19/informatica-forense-metodo-las-6rs/

Berto López. (2018, noviembre 7). Los formatos más importantes para fotos e imágenes digitales. Recuperado 11 de noviembre de 2018, de https://www.ciudadano2cero.com/formatos-imagenes-fotos/

7 útiles herramientas para detectar imágenes falsas. (2018, septiembre 26). Recuperado 26 de septiembre de 2018, de https://www.diariolasamericas.com/tecnologia/7-utiles-herramientas-detectar-imagenes-falsas-n4119324