Revista Electrónica Humanidades, Tecnología y Ciencia, del Instituto Politécnico Nacional

ISSN 2007-1957

LOCALIZACIÓN GEOGRÁFICA DE PERSONAS UTILIZANDO TÉCNICAS DE COMPUTACIÓN FORENSE

Israel Rivera Zárate
Instituto Politécnico Nacional-CIDETEC
irivera@ipn.mx

Miguel Hernández Bolaños
Instituto Politécnico Nacional-CIDETEC
mbolanos@ipn.mx

Patricia Pérez Romero
Instituto Politécnico Nacional-CIDETEC
promerop@ipn.mx

Resumen

El presente trabajo propone realizar el análisis de datos que contiene un archivo, en este caso fotografías, cada vez que se crea un archivo, este contiene un conjunto de datos llamados Metadatos. Estos proporcionan información específica sobre un archivo, por ejemplo; tipo de extensión, fecha de creación, fecha de modificación, propietario, tamaño que ocupa en almacenamiento, entre otros atributos. Por lo tanto, a las fotografías tomadas desde algún dispositivo móvil (gadget, smartphone), se realizará un análisis para determinar qué tipo de metadatos se necesitan para poder realizar una geolocalización sobre la fotografía, para saber cuándo y dónde fue tomada. Para posteriormente se realice un sistema que automatice el análisis de este tipo de información. También se realizará el análisis de metadatos a redes sociales tales como Twitter, Facebook, Instagram, WhatsApp, Snapchat. Ya que las redes sociales han tenido en los últimos años una gran trascendencia.

Palabras clave: Geolocalización, computación forense, fotografías, metadatos, redes sociales.

La idea de este trabajo nace de la gran importancia que están cobrando en los últimos años las técnicas de cómputo forense. Técnicas que, aunque no son recientes (los primeros estudios datan en los años 90) han podido llevarse a cabo gracias a las diversas situaciones que se han presentado últimamente alrededor de la evolución de la tecnología.

ISSN 2007-1957

Haciendo un poco de historia con la aparición de la computadora, la vida del ser humano se ha vuelto dependiente, a tal grado que surge la una necesidad tecnológica para su uso cotidiano, para comunicarnos, para elaborar trabajos, para entretenernos, resguardar información, análisis financieros, simulaciones espaciales, cálculos matemáticos, incluso sistemas de información que hacen dependiente a toda una nación. (Alonso, 2016).

La información que generamos se ha vuelto un tema de gran relevancia, ya que ésta tiene un valor relativo para cada persona, que comprende desde fotografías, canciones, documentos escolares, hasta documentación clasificada de empresas privadas, instituciones e incluso gubernamentales.

1. Computación Forense

Según el FBI (Acrónimo de Federal Bureau of Investigation), la informática o computación forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. (Castro, 2015). La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia.

Aproximadamente desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Dentro del ámbito forense encontramos varias definiciones:

• Computación forense (computer forensics) que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos. (Donohue, 2016).

• Forensia en redes (network forensics). Es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que, entendiendo las operaciones de las redes de computadoras, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disjuntos y aleatorios, que, en equipos particulares, es poco frecuente. (Giovanni Zuccardi, 2016).

• Forensia digital (digital forensics). Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo? y ¿por qué?) de eventos que podrían catalogarse como

ISSN 2007-1957

incidentes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática. (Google, 2017).

El cómputo forense tiene 3 objetivos:
1) La compensación de los daños causados por los criminales o intrusos, 2) La persecución y procesamiento judicial de los criminales y 3) La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

El Cómputo Forense nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense. (Harvey, 2003).

2. Desarrollo

Equipo empleado:

• Laptop Dell Inspiron 15R Intel Core i7, 16 GB de RAM y Disco Duro de 1 TB.

• Microsoft SQL Server 2016 Express.

• Microsoft Visual Studio 2017 Beta.

Primeramente, se necesitó tomar varias fotografías de diferentes dispositivos, como Laptop, Teléfono celular, de un gadget en este caso un Ipod, se descargaron algunas fotografías de la web y algunas de redes sociales para su posterior análisis.

El SQL Server 2016, se va a necesitar un motor de base de datos para alojar la información de los análisis, así como también realizar el diseño de una base de datos para que exista una integridad en la información. Asimismo, se trabajó con Visual Studio 2017, para ello se necesitó un lenguaje de programación para la automatización del sistema, ya que estamos utilizando SQL Server 2016; por conveniencias de lenguaje vamos a necesitar lenguaje C#.

Se realizó el Diagrama de entidad relación de la base de datos para su implementación en el SQL Server, ver figura 1.

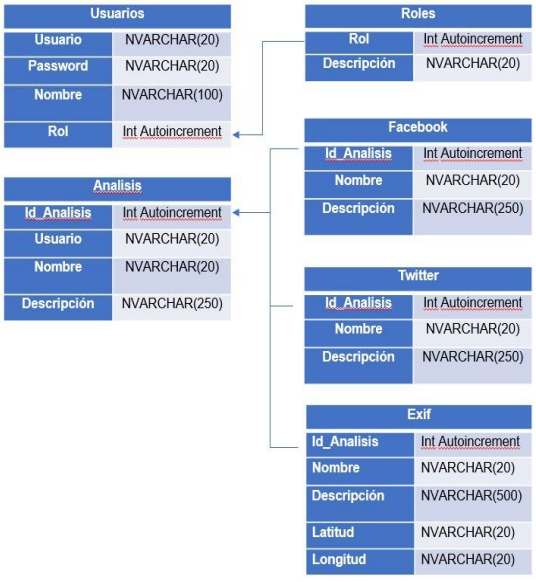


Figura 1. Diagrama de entidad relación de la base de datos

La primera fotografía que se analizó se muestra en la figura 2 y en la figura 3 se

ISSN 2007-1957

observan los metadatos arrojados por el sistema.

Figura 2. Fotografía de la persona a localizar

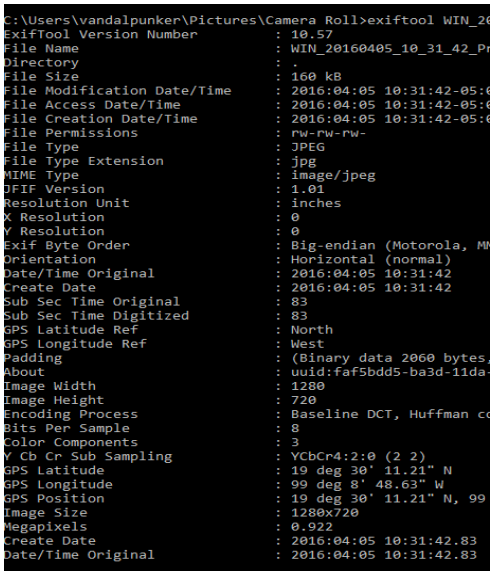


Figura 3. Metadatos arrojados por el sistema

Pero para fines prácticos de la elaboración de este artículo, trabajaremos de la siguiente manera: Realizamos un HASH de la fotografía a analizar para corroborar la integridad de la información y trabajamos con la copia de la fotografía con la herramienta EXIF, para no utilizar la original ya que como comprobamos el archivo original contiene la evidencia que nosotros queremos analizar.

Para ver más evidente este ejemplo realizamos el análisis de metadatos; para ello, se utilizó la herramienta EXIFtool, y desde la consola de Windows escribimos el siguiente comando "EXIFtool WIN_20160405_10_31_42_Pro.jpg" presionamos enter.

Cabe mencionar que el sistema permite tener dentro de ese conjunto de datos el nombre del archivo, que en este caso se llama "WIN_20160405_10_31_42_Pro" la extensión de archivo "JPG", la ruta del archivo "C:\Users\vandalpunker\Pictures\Camera Roll", el tamaño de la Imagen "160KB", la Fecha de creación, modificación y acceso de este archivo "martes, 5 de abril de 2016, 10:31:42 a. m.". Permisos de lectura y escritura, y viene la Latitud y Longitud que son los metadatos que nos interesan.

Ahora bien, extraemos en este caso para la información de la Geolocalización de la fotografía los metadatos siguientes:

- Latitud 19 deg 30' 11.21" N.

- Longitud99 deg 8' 48.63" W.

- Position: 19 deg 30' 11.21" N, 99 deg 8' 48.63" W.

ISSN 2007-1957

Como se sabe, con los mapas y los sistemas de localización geográficos se puede determinar la ubicación de un punto usando dos sistemas de notación: grados sexagesimales o grados decimales. En este caso usamos de la herramienta de Google Maps para la geolocalización la fotografía tenemos que insertar los metadatos en grados decimales. Si la tenemos en el sistema tradicional de grados, minutos y segundos es necesario convertirla previamente. Por lo que por medio del algoritmo de cambio de Grados a decimales nos quedó lo siguiente:

- Latitud 19.5031139.
- Longitud -99.14684166666667.

La figura 4 muestra la posición geográfica en donde se ubica a la persona (foto 1), a través de Google Maps.

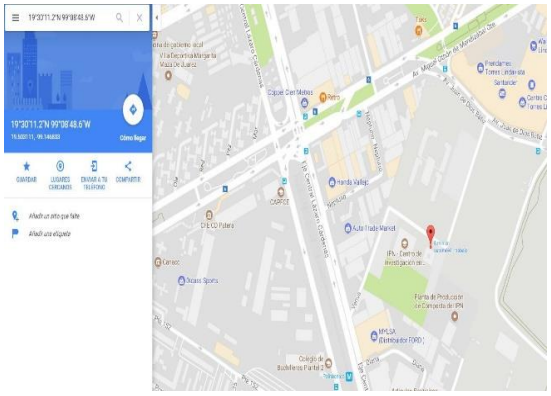
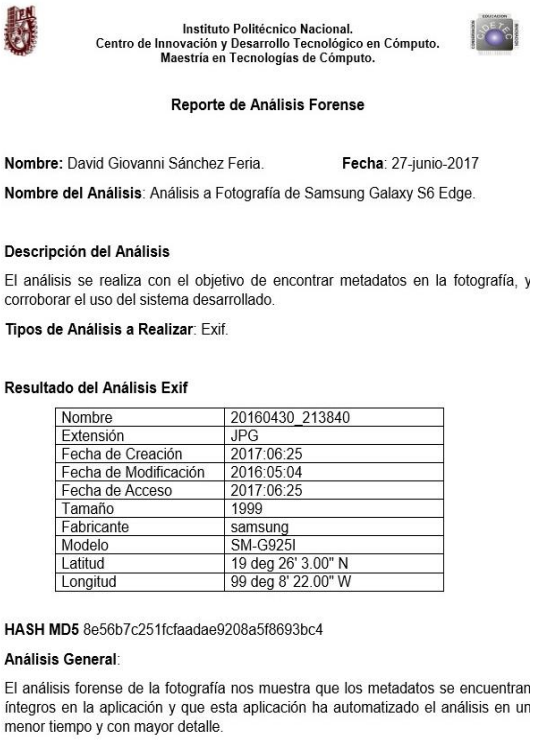


Figura 4. Posición geográfica fotografía 1

La salida del *software* implementado se muestra en la figura 5: Reporte de análisis forense.



Instituto Politécnico Nacional.
Centro de Innovación y Desarrollo Tecnológico en Cómputo.
Maestría en Tecnologías de Cómputo.

Reporte de Análisis Forense

Nombre: David Giovanni Sánchez Feria. **Fecha**: 27-junio-2017

Nombre del Análisis: Análisis a Fotografía de Samsung Galaxy S6 Edge.

Descripción del Análisis

El análisis se realiza con el objetivo de encontrar metadatos en la fotografía, y corroborar el uso del sistema desarrollado.

Tipos de Análisis a Realizar: Exif.

Resultado del Análisis Exif

Nombre	20160430_213840
Extensión	JPG
Fecha de Creación	2017:06:25
Fecha de Modificación	2016:05:04
Fecha de Acceso	2017:06:25
Tamaño	1999
Fabricante	samsung
Modelo	SM-G925I
Latitud	19 deg 26' 3.00" N
Longitud	99 deg 8' 22.00" W

HASH MD5 8e56b7c251fcfaadae9208a5f8693bc4

Análisis General:

El análisis forense de la fotografía nos muestra que los metadatos se encuentran íntegros en la aplicación y que esta aplicación ha automatizado el análisis en un menor tiempo y con mayor detalle.

Figura 5. Reporte de análisis forense

3. Pruebas y resultados

A) Imagen desde Smartphone

Realizamos el siguiente análisis con otra fotografía (ver figura 6), esta vez fue tomada de un teléfono Samsung Galaxy S6 Edge.

Se observa que esta fotografía contiene más metadatos, esto debido al modelo reciente del dispositivo, la versión de EXIF, y principalmente que es un dispositivo diseñado para tomar fotografías.

ISSN 2007-1957

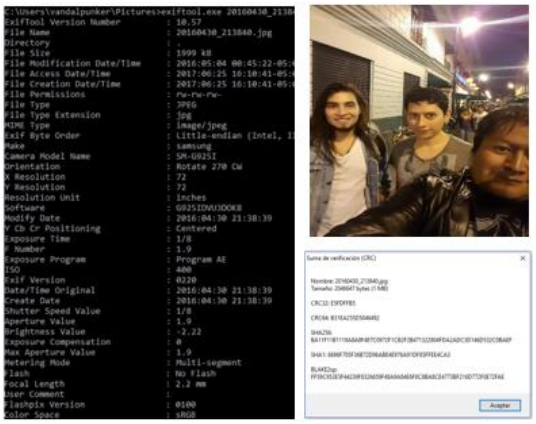


Figura 6. Fotografía 2 y sus metadatos

Sobre el análisis de metadatos tenemos el nombre que en este caso es: "20160430_213840.jpg", su tamaño que es "1999 KB", la fecha de modificación "2016:05:04 00:45:22-05:00", la fecha de creación "2017:06:25 16:10:41-05:00", y la fecha de acceso "2017:06:25 16:10:41-05:00" estas varían debido a que, al copiarlas del dispositivo a la PC, el metadato se sobrescribe por lo que en la fotografía anterior y en las consideraciones teóricas mencionamos de cómo se debe realizar un análisis forense, Tipo de Archivo "JPEG", en este casi si nos menciona el fabricante "samsung", modelo de la cámara del teléfono "SM-G925I", si la fotografía fue tomada con flash "No Flash", y más datos sobre la fotografía como color, bits, que para nuestro análisis no ocupamos.

Extrajimos las coordenadas GPS del análisis de metadatos para ingresarlas a Google Maps, ver figura 7.

- GPS Altitude: 2238 m Above Sea Level.
- GPS Date/Time: 2016:05:01 02:38:38Z.
- GPS Latitude: 19 deg 26' 3.00" N.
- GPS Longitude: 99 deg 8' 22.00" W.
- GPS Position: 19 deg 26' 3.00" N, 99 deg 8' 22.00" W.
- Latitude 19.4341667.
- Longitude -99.13944444444445.

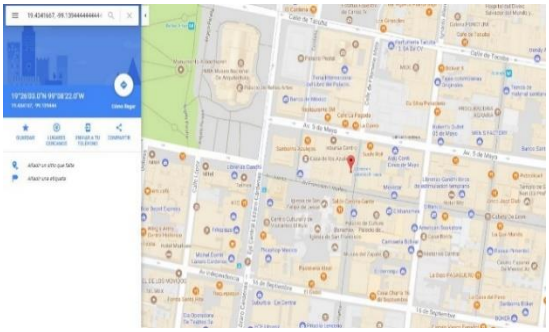


Figura 7. Posición geográfica fotografía 2

B) Imagen en Internet

Ahora realizamos el análisis a una imagen de internet, para utilizar una búsqueda indexada a través de Google, cabe señalar que nos interesa que la imagen contenga los metadatos de geolocalización por lo que realizamos la siguiente hipótesis.

"Suponiendo que la mayoría de los usuarios que navegan en internet tienen al menos un teléfono móvil o un gadget, y que este probablemente lo tienen vinculado para respaldar su información a través de la nube. Entonces podemos decir que si hacemos una búsqueda indexada sobre un directorio donde se almacenan las fotografías cabe una gran posibilidad de que encontremos un directorio de un teléfono lleno de fotografías para llevar a cabo esta búsqueda".

Entonces realizamos una búsqueda indexada con las siguientes palabras claves con la finalidad de encontrar directorios en Google de teléfonos, las palabras que

ISSN 2007-1957

utilizaremos serán “DCIM”, “Camera”, “Android”, “IPhone”,” Windows phone”,” JPG”.

Para realizar una búsqueda indexada se escribe en el navegador el siguiente comando “index of Iphone jpg”. Se consultan índices para decidir qué resultados de búsqueda son los más relevantes y mostrarlos. Cabe mencionar que esta metodología de la búsqueda indexada es con fines académicos y no para fines de lucro o morbo.

Por lo que los autores no nos hacemos responsables si esta metodología se implementa de manera incorrecta o insana. Regresando a la búsqueda le dimos clic a la primera página de Google para realizar el análisis de una fotografía tomada al azar. Seleccionamos la fotografía con nombre “lissabon 004”. En este caso omitimos el HASH, ya que no tenemos alguna referencia para asegurar la integridad de la fotografía. Cabe aclarar que no podemos difuminar a la fotografía para ocultar la identidad de la persona de la fotografía ya que esto haría que los metadatos se alteraran, ver figura 8.

Figura 8. Fotografía 3 y sus metadatos

En la figura 9 se observa la posición geográfica de la persona (foto 3) buscada a través de Google Maps.

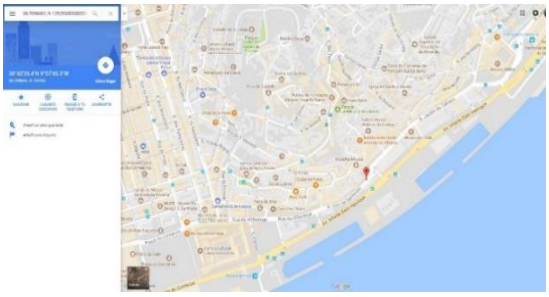


Figura 9. Posición geográfica fotografía 3

Ahora bien, revisamos el análisis y nos mostró lo siguiente. El nombre de la imagen es “lissabon 004.JPG”, La fecha de creación, acceso y modificación contiene esta fecha “2017:06:25 18:17:17-05:00” esto es porque el archivo fue descargado de internet. Podemos ver que la extensión del archivo es “JPEG”, Marca “Apple”, Modelo “iPhone 6”, Fecha Original tomada “2015:04:01 15:49:47”, GPS Latitude: 38 deg 42' 35.41" GPS Longitude: 9 deg 7' 45.32" W.

4. Conclusiones

Podemos concluir que la seguridad informática es una ciencia que va sumando importancia en la actualidad, gracias a la evolución del hombre y su entorno, ya que esto conlleva al estudio de otra de sus ramas como es la Informática forense, como vimos esta se encarga de identificar, preservar o adquirir, analizar y presentar de los resultados. Con la finalidad de dar solución a un delito o a un problema en particular, en este caso el problema que se propuse era el de encontrar personas a través de un análisis forense, el cual cumplió con sus objetivos, ya que con

ISSN 2007-1957

diferentes herramientas se logró localizar a unas personas a través de sus fotografías y publicaciones de sus redes sociales, cabe señalar que el objetivo de esta tesis es académico y es muy importante tomar en cuenta medidas de prevención de integridad de la información ya que estas metodologías se pueden prestar para usos indebidos, por lo que las siguientes sugerencias se proponen como una política de integridad de la información que generamos:

1. Desactivar la geolocalización en el teléfono celular, gadget y en cualquier dispositivo,
2. Revisar la privacidad de las redes sociales donde se está registrado con la finalidad de volver un perfil privado, y no aceptar personas desconocidas dentro de la red social.

5. Referencias

Alonso, C. (2016). Pentesting con FOCA. España: Eleven Paths.

Castro, J. M. (12 de Junio de 2015). Portal Mundos. Obtenido de Portal Mundos: http://www.portalmundos.com/mundoinformatica/comunicaciones/estenografia.htm.

Donohue, B. (30 de Junio de 2016). kaspersky Lab. Obtenido de: kaspersky Lab: https://blog.kaspersky.com.mx/que-es-un-hash-y-como-funciona/2806/.

Geocreepy. (2012). Geocreepy. Obtenido de: http://www.geocreepy.com/.

Giovanni Zuccardi, J. D. (2016). Pontificia Universidad Javeriana. Obtenido de: Pontificia Universidad Javeriana: http://pegasus.javeriana.edu.co/portal/.

Google. (20 de Junio de 2017). Support Google. Obtenido de: https://support.google.com/webmasters/answer/70897?hl=es.

Harvey, P. (2003). EXIFtool by Phil Harvey. Obtenido de: http://owl.phy.queensu.ca/~phil/EXIFtool/.