Informática Forense en Colombia

Computer Forensics in Colombia

Computação Forense Na Colômbia

Luisa Fernanda Castillo Saavedra[1], John A. Bohada[2]
Grupo de investigación MUISCA, Facultad de Ingeniería, Especialización en Seguridad de la Información, Fundación Universitaria Juan de Castellanos, Tunja, Colombia
[1]luisa.fda.castillo@gmail.com, [2]jbohada@jdc.edu.co

Recibido / Received: 21/08/2015 – Aceptado / Accepted: 12/10/2015

Resumen

Hoy en día, la información electrónica se ha convertido en el activo más importante para la sociedad, lo que obliga a las personas a utilizar diferentes medios para guardarla, procesarla y asegurarla, evitando de esta forma un robo de información o un ataque informático. Lastimosamente, así como surgen medios o herramientas a favor de la información, también existen las herramientas en contra de la misma, los cuales permiten alterarla, eliminarla o robarla según el objetivo del ataque informático, violando por completo los principios generales de la información (confidencialidad, disponibilidad e integridad). Es allí, donde aparece la informática forense, que se encarga de identificar y analizar la evidencia de un delito informático o prevenirlo si aún no ha sucedido. Lo que la sociedad no se imagina es que con la evolución de las tecnologías, y teniendo en cuenta que actualmente todo se maneja mediante dispositivos electrónicos, los delitos informáticos van en aumento y serán más comunes de lo que ahora son en Colombia, por tal razón, con este artículo se quiere mostrar la importancia de la informática forense, sus herramientas, procesos y cómo en Colombia se está aplicando mediante un caso real.

Palabras clave: Informática Forense, Delito Informático, Código Malicioso, Seguridad de la Información, Seguridad de Datos.

Abstract

Today, electronic information has become the most important asset for society, forcing people to use different means for storing, processing and secure, thus preventing theft of information or a computer attack. Unfortunately, as well as means or tools for information emerge, there are also tools against it, which allow altering it, delete or steal according to the purpose of the hacker attack, violating completely the general principles of information (confidentiality availability and integrity). It is there where computer forensics takes care of identifying and analyzing the evidence of computer crime or prevent it, if it has not happened yet. What society cannot imagine is that with the evolution of technology, and considering that currently everything is handled through electronic devices, computer crimes are increasing and are more common

than they are now in Colombia, for this reason with this article is intended to show the importance of computer forensics, its tools, processes and how in Colombia is being implemented by a real case.

Keywords: Forensic Computing, Cybercrime, Malware, Information Security, Data Security.

Resumo

Hoje, a informação electrónica tornou-se o ativo mais importante para a sociedade, forçando as pessoas a usar diferentes meios para armazenamento, processamento e seguro, impedindo assim, o roubo de informação ou de um ataque de computador. Infelizmente, assim como surgem meios ou ferramentas para cuidar a informação, há também ferramentas contra ela, que permitem alterar, excluir ou roubar dependendo da finalidade do hacker, violando completamente os princípios gerais da informação (confidencialidade disponibilidade e integridade). É ali onde computação forense aparece que é responsável por identificar e analisar as provas do crime de computador ou impedi-lo se ele não aconteceu ainda. O que a sociedade não pode imaginar é que, com a evolução da tecnologia, e considerando que, atualmente, tudo é tratado através de dispositivos electrónicos, crimes informáticos estão a aumentar e são mais comuns do que são agora na Colômbia, por esta razão este artigo é para mostrar a importância da computação forense, suas ferramentas, processos e como na Colômbia está sendo implementado por um caso real.

Palavras-chave: Computação Forense, Crime Cibernético, malware, segurança da informação, segurança de dados.

I. Introducción

Hoy en día, y gracias a la evolución de las tecnologías y a las grandes ventajas del internet, la información se puede salvaguardar en diferentes sitios o dispositivos electrónicos con el fin de procesarla según la necesidad de quien la posea, haciendo más fácil y ágil su portabilidad y manipulación.

En la actualidad, la mayoría de las personas ya realizan sus actividades del diario vivir por medio del internet y con ayuda de dispositivos electrónicos; dichas actividades pueden ser: consulta de cualquier tipo de información, envío y recepción de e-mail, transferencias electrónicas, compras de artículos, medicamentos, videoconferencias desde cualquier lugar del mundo, descargar películas, videos, etc. Es decir, la tecnología y el internet le han hecho la vida más fácil a las personas, pero al mismo tiempo abre puertas para los delitos informáticos o actos que estén en contra de la ley o que no se deberían realizar, pues así como el internet ayuda con las tareas o actividades del diario vivir, también por este mismo medio o por los dispositivos electrónicos, se puede obtener la información de una forma incorrecta o ilegal para darle un uso inadecuado que puede afectar directamente a la persona o entidad que la poseía.

Colombia no se queda atrás de estos delitos informáticos, pues cada día se presenta una suplantación de identidad o *phishing*, el cual ya no es solo con entidades bancarias, suplantación de páginas financieras o plataformas de compras o pagos en línea, extorsión o –la más común– envio de correos con código malicioso, el cual le deja las puertas abiertas al delincuente informático en el momento que abre el correo electrónico, etc. , dejando como causa principal la forma inadecuada del manejo de información, y la seguridad de la misma [1].

Es aquí donde se debe hacer uso la informática forense, la cual es una ciencia que se encarga de realizar el estudio de la escena del crimen en el dispositivo electrónico o la red sobre la cual se cometió el delito informático, con el fin de identificar, recolectar y analizar todo tipo de pruebas digitales, que ayuden a resolver el caso, o a prevenir casos futuros [2].

Por tal razón, el objetivo de esta investigación es conocer más acerca de la informática forense y cómo se ha venido implementando en Colombia, sus he-

rramientas y procesos, buscando que las personas y las empresas estén enteradas del uso de esta ciencia, y sepan en qué casos les puede ser útil para investigar un delito informático (acto que va en contra de la ley o acto que esté en contra de la normatividad de una empresa), a través de los especialistas forenses.

II. Informática Forense

La informática forense (IF) puede tener varios conceptos, pero al analizar cada uno de ellos, todos están enlazados al mismo significado, algunos de estos conceptos son:

Según el FBI (Oficina Federal de Investigación de los Estados Unidos): "La informática forense fue creada para atender las necesidades específicas y articuladas de aplicación de la ley para hacer la mayor parte de esta nueva forma de pruebas electrónicas. Informática forense es la ciencia de adquirir, preservar, recuperar y presentar los datos que han sido procesados electrónicamente y almacenados en soportes informáticos" [2].

Según la IFC (Informática Forense Colombiana), la informática forense se define "Como la disciplina que combina elementos de derecho y ciencias de la computación para recopilar y analizar datos de los sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que es admisible como pruebas en un tribunal de justicia" [3].

Si se unieran los dos conceptos, se tendría que la IF es una disciplina auxiliar de la justicia, que ayuda a neutralizar o prevenir los ataques de delincuentes informáticos, con la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica, las cuales permiten identificar, preservar y analizar datos que han sido procesados electrónicamente, con el fin de obtener evidencias o pruebas de un delito informático (competencia desleal, robo) o conductas irregulares dentro de algún proceso, y así presentar la evidencia ante un tribunal o como defensa en alguna situación en el que esté involucrada la persona o entidad. Todo esto mediante el uso de técnicas, principios y herramientas forenses. También se usa para probar que se han cometido actos deshonestos. Algunos de los ámbitos en los que se pueden presentar los delitos informáticos o conductas irregulares, que ameritan una investigación forense son: mercantil, laboral, judicial, educativo, financiero, entre otros [4].

Algunos de los objetivos que se plantea la IF, son los siguientes:

- Prevenir y detectar vulnerabilidades de seguridad con el fin de corregirlas oportunamente, ya que en ocasiones las empresas contratan IF como manera preventiva y así anticiparse al posible problema.
- Identificar las fuentes del delito informático, o del crimen cibernético (como también es llamado).
- Recoger diferentes tipos de evidencias de la forma más adecuada, haciendo uso de las técnicas, herramientas y metodologías según el caso.
- Analizar las evidencias encontradas una y otra vez, si no existe evidencia no se puede probar nada.

"Es muy importante tener en cuenta, a la hora de realizar una investigación forense, que la acumulación de evidencia le da peso a las investigaciones**"** [5].

A. Herramientas de la Informática Forense

Para determinar el estado de un sistema después de que sus medidas de seguridad han sido vulneradas, es decir, después de que se intentó o se cometió un delito informático, la informática forense utiliza las herramientas necesarias (según el caso que se esté investigando) para buscar y analizar evidencia que permitan identificar los mecanismos o técnicas que se utilizaron para acceder al sistema de una forma inadecuada, un ejemplo de estas herramientas es el que se muestra en la Tabla 1:

TABLA 1. HERRAMIENTAS DE LA IF

TIPO	HERRAMIENTA
H. de Disco y Captura de Datos	Recovers–Historian 1. 4; NTFS Recovery – recuva – Pandora Recovery; Visores de archivos; Open Freely.
H. Análisis de Registro	Regripper-registry decoder; MUI Cacheview; Recon Registro
H. Análisis de correo electrónico	FTK (Forensic Toolkit); Eindeuting.
H. Forenses de Red	Wireshar; Xplico
H. de Dispositivos Móviles	Oxígeno Suite Forens; XRY
H. de Adquisición y Análisis de Memoria	Responder CE; Volatility
H. de Recuperación de Contraseñas	Ntpwedit – ntpasswp; Mail PassView.
H. de Análisis de Malware	Microsoft Process Monitor; EsetSys Inspector; Firebug.

Fuente: Los autores, 2014.

1) Herramientas de Disco y de Captura de Datos: estas herramientas permiten proteger o reparar el disco duro mediante limpiezas, optimización de espacio, verificación de la integridad del sistema lógico, etc. , con el fin de mejorar el rendimiento del disco. También permiten recuperar y capturar información de un disco que, por alguna razón, se perdió o se borró, dicha información puede ser imágenes, videos, textos, etc. Otro de sus usos es obtener imágenes de los discos que se van a analizar [7]. Algunas de estas herramientas son:

- Recovers – Historian 1. 4: esta herramienta se encarga de recuperar las URL de acceso a sitios web y ficheros correspondientes, que en algún momento fueron eliminados [8], [9].

- NTFS Recovery–recuva - Pandora Recovery: recupera la mayor parte de información de un disco formateado o los archivos eliminados del dispositivo electrónico, por medio de un análisis que se inicia en el momento de ejecutar la herramienta que depende de los parámetros de búsqueda seleccionados por el usuario [10], [11].

- Open Freely: permite realizar la visualización y edición de un archivo en cualquier formato y brinda las características técnicas del archivo [12].

- Visores de archivos - Free File Opener – Universal Viewer – Free Opener: esta herramienta brinda la opción de visualizar diferentes formatos de archivos, tales como imágenes, texto, música, video audio [13].

- X-Ways Forense - ImDisk -OSFMount - FTK Imager: estas herramientas permiten obtener una o varias imágenes de un disco duro.

2) Herramientas de Análisis de Registro: estas herramientas permiten obtener todos los datos relacionados a los registros que se generan en los computadores cuando se tiene instalado sistema operativo Windows, y cuando se instalan cualquier tipo de programas, algunos de estos registros son: usuarios del sistema, permisos de acceso, ficheros ejecutados, información del sistema, dirección IP configurada en la red, información de las aplicaciones instalas y en ejecución, etc., algunas de estas herramientas son:

- Regripper – registry decoder: estas herramientas permiten realizar la extracción y correlación de la información de los registros, mostrando al final un listado detallado de dicha información [14].

- MUI Cacheview: permite al usuario visualizar y corregir la información relacionada al nombre de las aplicaciones que se están ejecutando [15].

- Recon Registro: esta herramienta es muy popular, ya que permite obtener información de los registros del sistema que se han eliminado sin importar el tiempo que haya transcurrido [16].

3) Herramientas Análisis de Correo Electrónico: en la actualidad, el correo electrónico es el medio más usado para cometer un delito informático (insultos, amenazas, estafas, ejecución de código malicioso para tener pleno acceso al PC), debido a esto existen herramientas que son capaces de buscar correos electrónicos eliminados o alterados y reconstruirlos hasta obtener el original y así conseguir una evidencia válida para presentar ante un juez relacionada a su creación, el momento en que se envió, el remitente, etc., además, algo que no es muy conocido por las personas es que el correo electrónico en los encabezados tiene información oculta, que permite su reconstrucción. Ejemplo de estas herramientas tenemos [1], [17]:

- FTK (Forensic Toolkit): herramienta de uso comercial, soporta servidores de correo electrónico, tales como Outlook (PST), Outlook Expres (DBX), Netscape, Yahoo, Eudora, Hotmail, MSN [18].

- Eindeuting: esta herramienta es open source y soporta servidores de correo electrónico, tales como Outlook (PST), Outlook Expres (DBX).

4) Herramientas Forenses de Red: el propósito de estas herramientas en una investigación forense es encontrar patrones anómalos, malware, conexiones sospechosas o identificar ataques, basadas en el tráfico de datos. Algunas de estas herramientas son [19]:

- Wireshark: permite capturar paquetes de la red, analizando conexión y detectando posibles problemas en la transmisión de paquetes, y presentando el resultado del análisis mediante una interfaz gráfica [20].

- Xplico: extrae todo el contenido de datos de una red, como por ejemplo información de correo electrónico como protocolos, todos los contenidos HTTP, información de llamadas VoIP, entre otras [21].

5) Herramientas de Análisis de Dispositivos Móviles: teniendo en cuenta el avance de las Tecnologías de la Información (TI), los dispositivos móviles se encuentran dentro de la lista de escenas del crimen de un delito informático, dado que estos dispositivos ya brindan los mismos servicios que un PC de escritorio, el cual se puede utilizar como medio para realizar o cometer un delito informático, debido a esto existen herramientas que permiten realizar un análisis detallado al dispositivo móvil en busca de evidencia útil para la investigación, algunas de estas herramientas son:

- Oxígeno Suite Forense: obtiene todo tipo de información eliminada, dañada o manipulada (registro de llamadas hechas o recibidas, mensajes de texto, correos electrónicos, contactos, documentos) [22].

- XRY: fue diseñada para recuperar todo tipo de información que se encuentre en el dispositivo móvil, así como las características del mismo, viene con un dispositivo para hardware y para software [23].

6) Herramientas de Adquisición y Análisis de Memoria: permite obtener, o como su misma palabra lo dice, adquirir la información o instrucciones que se almacenan en la memoria RAM (Memoria de Acceso Aleatorio) para realizar un análisis de ella en busca de evidencia, como por ejemplo programas que fueron utilizados o documentos que fueron alterados, etc.

- Responder CE: esta herramienta permite capturar la memoria RAM, para su posterior análisis.

- Volatility: esta herramienta se encarga de realizarle un seguimiento a los procesos indicados por el especialista forense, con el fin de extraer información útil para su posterior análisis [24].

7) Herramientas de Recuperación de Contraseñas: es muy común que en una investigación forense, para obtener evidencias, sea necesario ingresar a correos, computadores, programas, documentos, sitios web, entre otros, que solicitan contraseñas para su ingreso, en estos casos existen herramientas cuya función es la de obtener cualquier tipo de contraseña y así ingresar y extraer la información a investigar [25]. Algunas de estas herramientas son:

- Ntpwedit - ntpasswp: sobrescriben la contraseña de un usuario o un administrador, y así poder iniciar sesión con la información editada, estas herramientas son limitadas, ya que solo aplican para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8).

- Mail PassView: recupera contraseñas de cuentas de correos electrónicos.

8) Herramientas de Análisis de Malware: un malware es un código malicioso o un código no autorizado, que ingresa al sistema por diferentes medios a causar daños a un usuario o a una organización, en estos casos es donde se debe realizar un análisis de malware que permite identificar cuál es la pieza del sistema o de la red que se encuentra infectada, y así entender cómo funciona y luego buscar cómo derrotarlo o eliminarlo. A continuación, se mencionan algunas herramientas que son muy utilices a la hora de realizar un análisis de malware [26], [27].

- Microsoft Process Monitor: esta herramienta permite identificar si se han realizado acciones maliciosas en los registros, en el sistema de archivos o en las conexiones de red [28].

- EsetSys Inspector: el objetivo de esta herramienta es guardar la información del estado del sistema antes y después de la ejecución de un código malicioso, con el fin de identificar los cambios que se pudieron realizar en el sistema [29].

- Firebug: permite realizar el análisis de aplicaciones web, mostrando el código que la compone, identificando de esta forma el código malicioso que haya sido ejecutado sobre ella.

B. Procedimientos en la Informática Forense

Para realizar las investigaciones forenses, los peritos deben realizar una serie de procedimientos que ayudan a que las investigaciones realizadas en la escena del crimen y las pruebas que de esta se obtengan, tengan el valor necesario ante un tribunal, dichos procesos son [30]:

- Esterilidad de los medios informáticos de trabajo: antes de iniciar cualquier actividad relacionada a la investigación forense, es necesario que los medios informáticos utilizados estén esterilizados y certificados para su uso, por ejemplo verificar que no hayan sido expuestos a variaciones magnéticas, láser o similares, pues estas clases de exposiciones pueden conllevar a una contaminación de la evidencia.

- Adquisición: una investigación forense no se realiza directamente sobre la escena del crimen informático, para esto es necesario sacar una copia exacta de la información digital (imágenes de discos, USB, CD) o del dispositivo a ser investigado (Disco Duro) en los medios informáticos esterilizados con anterioridad. Estas copias de la escena del crimen son muy importantes, ya que después de terminar todo el proceso que el perito informático debe aplicar, se procede a realizar la investigación y obtención de evidencia a partir de la copia, pues la escena original del crimen jamás puede ser alterada y así mismo se debe presentar al juez.

- Validación y preservación de los datos adquiridos: con el fin de identificar si la copia de la escena del crimen es idéntica a la original, los peritos informáticos deben realizar una serie de verificaciones a partir de cálculos matemáticos o procesos de algoritmos que permitan establecer la completitud de la información traspasada a la copia, un ejemplo de este proceso de verificación es por medio de un algoritmo calcular un código único para toda la información original, dicho código está encriptado y no se puede reversar, por tal razón, al calcular el código de las copias obtenidas de la original tiene que ser igual, de no ser así significa que la copia no es exacta y se sacó incorrectamente, este proceso se efectúa con el fin de no alterar en nada la escena del crimen original, salvaguardando la evidencia del delito informativo para presentarla ante un juez.

- Análisis y descubrimiento de evidencia: una vez terminada la verificación de las copias, se procede a realizar la investigación, análisis y levantamiento de evidencia forense que se pueda utilizar como prueba ante un juez. Dicho análi-

sis se puede realizar por diferentes niveles, que pueden ser:

a. Archivos borrados, archivos creados, accedidos o modificados dentro de determinado rango de fechas.

b. Verificar los tipos de archivos que tengan un formato en especial y que se hubieran alterado.

c. Imágenes, videos, mensajes de correo electrónico, navegación en internet.

d. Buscar en diferentes niveles palabras clave, tales como un número telefónico, el nombre de una ciudad o una empresa, correos electrónicos utilizados con más frecuencia, etc.

Una vez terminado dicho análisis, los peritos informáticos pueden obtener un patrón de comportamiento del usuario investigado, en relación a: creación, modificación, borrado de mensajes, actividad en un correo electrónico, contacto frecuente con determinadas personas o visitas a lugares específicos. Es importante aclarar que, una escena del crimen se puede alterar muy fácilmente si este proceso no se realiza adecuadamente, ya que con el simple hecho de prender un equipo, arrancar un disco duro, abrir un archivo, etc. , ya se puede estar comprometiendo la evidencia.

- Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados: el perito informático es el encargado de que los procesos y herramientas utilizados para la investigación sean los correctos, y en el caso de las herramientas sean las adecuadas según versiones, licencias o actualizaciones, esto con el fin de garantizar que la investigación se realiza correctamente y los resultados obtenidos sean documentados claramente, explicando paso a paso qué se realizó y por qué se realizó, qué herramientas se utilizaron y, sobre todo, documentar muy bien el resultado obtenido en cada parte de la investigación, de tal manera que cualquier persona externa pueda revisar y validar la información; o también, si en determinado caso es realizado un segundo estudio, el perito asignado, haciendo uso de las herramientas y procesos documentados, obtenga los mismos resultados. Este proceso es muy importante en el caso en el que el juez tenga dudas de la validez de la investigación, pues si todo el proceso fue verificado y documentado correctamente toda la evidencia es válida, pero si se incurrió en alguno, la evidencia puede ser desechada.

- Informe: el perito informático, una vez termine la investigación, debe presentar un informe escrito en un lenguaje técnico y de una forma ordenada, en él debe describir detalladamente el proceso realizado y los resultados obtenidos, este informe debe ir con copia en un CD.

III. Aplicación de la Informática Forense: Caso Real Colombiano

En Colombia se han presentado varios casos en los que ha sido necesario utilizar las herramientas y metodologías de la informática forense para obtener información de vital importancia para Colombia, para un caso legal o por un delito informático, uno de los casos más sonados es el de Raúl Reyes.

A. Caso Raúl Reyes

El caso de Raúl Reyes, uno de los líderes de las Fuerzas Armadas Revolucionarias de Colombia, es uno de los ejemplos más sonados de la importancia de la informática forense en Colombia, como se escuchó en las noticias, en el lugar en el que fue abatido se encontraron varios dispositivos electrónicos (3 computadores portátiles, 2 discos duros portables y 3 memorias USB), de los cuales algunos quedaron en mal estado a causa de la operación realizada por las fuerzas militares; sin embargo, esto no era ningún impedimento para que, con el uso de las herramientas y procesos de la informática forense, se obtuviera información útil de dichos dispositivos [31]-[33].

Es muy importante mencionar que, a pesar de que Colombia contaba con los especialistas en infor-

mática forense y las herramientas necesarias para la investigación, por la complejidad del caso, fue necesaria la ayuda de la INTERPOL, esto con el fin de garantizar la investigación. Sin más preámbulos, para el caso de los dispositivos electrónicos de Raúl Reyes, según investigaciones realizadas en diferentes fuentes de internet, algunos de los procesos y metodologías utilizadas fueron:

- Inventario: lo primero que hizo el grupo de investigadores fue realizar un inventario detallado de los dispositivos electrónicos que les habían sido confiados, dentro de este inventario se encontraban fotos de cada uno de los dispositivos, y una descripción detallada de las características de fábrica de cada uno de estos [33].

- Imágenes de los dispositivos: los investigadores forenses sacaron copias exactas de los discos duros de los 3 computadores y los 2 discos duros portables y copias de los datos alojados en las 3 memorias USB, a este proceso se le conoce como IMAGING que significa obtención de imágenes forenses de datos, ya que con estas copias exactas de los dispositivos electrónicos es realmente sobre las que se realiza la investigación, y así no se alteran los originales. Durante esta etapa del análisis, se sacaron 2 copias exactas de cada uno de los dispositivos. Estas copias se tienen que sacar con los dispositivos apagados y no se debe acceder directamente, ya que al encenderlos se pueden estar alterando los últimos registros generados y, si se accede directamente el proceso de validación de las pruebas, ya no tendrá el mismo significado ante un tribunal. Para realizar este proceso en cualquier investigación forense, se podrían utilizar herramientas, tales como: X-Ways Forense - ImDisk - OSFMount - FTK Imager [31]-[33].

- Extracción de información: los investigadores forenses trabajan sobre una de las copias generadas y utilizan las herramientas necesarias para obtener información relacionada a documentos, correos, imágenes, videos, páginas web, etc., que están o estaban alojados en cada uno de los dispositivos electrónicos. En este proceso, los investigadores tardaron alrededor de 3 días. Es importante mencionar que, algunos archivos estaban cifrados, pero lo que aún es más sorprendente para los investigadores es que el disco duro de Raúl Reyes no lo estaba (según fuentes de ENTER 2. 0) [1], lo que hizo menos compleja la extracción de la información, y obtención de resultados en corto tiempo; para los archivos que se encontraban cifrados, fue necesario el uso de herramientas de obtención de contraseñas.

- Verificación de tipo de acceso: los investigadores dela INTERPOL debían descartar la manipulación de la información por parte de las autoridades que realizaron el levantamiento de los dispositivos de la zona en la que se realizó el operativo, para esto se utilizaron herramientas que permiten obtener la información relacionada a la marca del tiempo de los documentos (fecha en la que se creó, se modificó, o se accedió por última vez), y así identificar si en el transcurso del tiempo en el que se encontraron los dispositivos y la fecha en la que se entregaron a la INTERPOL se había realizado algún tipo de manipulación [33].

- Indexar datos: los investigadores indexaron todos los datos, facilitando de esta forma búsquedas de documentos importantes para la investigación por palabras claves. En este proceso, se tardaron más o menos una semana, debido a la cantidad de archivos que se habían encontrado [32], [33].

- Durante la investigación forense, se realizaron varios procesos como la verificación de autenticidad de los datos encontrados (documentos, imágenes, videos).

Como se muestra anteriormente, la informática forense fue muy importante en la investigación realizada a los dispositivos encontrados pertenecientes a Raúl Reyes, ya que gracias a sus herramientas, metodologías y procesos, se pudo extraer datos, imágenes, videos significativos para Colombia. Cabe resaltar que, en el informe revelado por la INTERPOL, no se muestran las herramientas utilizadas durante la investigación, la razón es por la complejidad del caso que se está investigando. El resultado detallado se encuentra en el Informe forense de la

Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia.

IV. Conclusiones

La informática forense es una ciencia que permite realizar una investigación sobre un delito informático, y obtener las evidencias necesarias válidas ante un juzgado, las cuales ayudarán a juzgar a las personas responsables.

Es muy importante que las personas sepan que los peritos de informática forense son los únicos autorizados para realizar las investigaciones de los delitos informáticos, ya que para obtener las evidencias es necesario aplicar los procesos definidos, y utilizar las herramientas correctas para la investigación, y de la misma forma manipular la evidencia correctamente para que esta sea válida.

Además de ser una ciencia de investigación de delitos informáticos, la informática forense también ayuda a las grandes empresas a identificar si están expuestas a alguna amenaza cibernética, obligándolas a utilizar nuevas herramientas y procesos de seguridad, con el fin de mitigar dichos riesgos.

Es importante que no solo las empresas, sino también las personas del común, conozcan la importancia de la Informática Forense en la actualidad, para que sepan cómo actuar ante un delito informático y qué herramientas utilizar para mejorar la seguridad de la información y lograr reducir el riesgo de los delitos informáticos.

Un delito informático jamás se podrá evitar en un 100%, pues las tecnologías de la Información están en constante evolución, lo que sí se puede es reducir o mitigar, con ayuda de auditorías de seguridad de la información, investigaciones de informática forense, o herramientas y metodologías de seguridad de la información.

Es muy importante identificar los procesos forenses que se van a aplicar durante una investigación cibernética, pues de acuerdo al orden y la forma como se realicen, se garantizan mejores resultados.

Referencias

[1] Organización de los Estados Americanos, Habilidades de Análisis Forense Informático. [Online]. Available: http://www.oas.org/juridico/english/cyb_mex_forense.pdf

[2] G. Zuccardi, and J. D. Gutiérrez, Informática Forense. [Online]. Available: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0. 6.pdf

[3] Informática Forense, Informática Forense en Colombia. [Online]. Available: http://www.Informatica forense.com.co/index.php/joomla-overview

[4] Informática Forense, Informática forense como una disciplina. [Online]. Available: http://www.in formaticaforense.com.co/index.php/joomla-overview/informatica-forense-como-una-disciplina

[5] J. Pages, Conferencia: "Informática Forense y Seguridad". [Online]. Available: https://www.youtube.com/watch?v=UhumXfZedM0

[6] L. E. González, 21 herramientas más populares de informática forense. [Online]. Available: https://prezi.com/kcoki3kq5ws-j/21-herramientas-mas-populares-de-informatica-forense/

[7] Conexión Inversa, Forensics Power Tools (Listado de herramientas forenses). [Online]. Available: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de. html

[8] Gaijin, Historian. [Online]. Available: http: //www.gaijin.at/en/dlhistorian.php

[9] ¡TARINGA!, 10 Herramientas que usa el FBI para el análisis de la PC. [Online]. Available: http://www.taringa.net/posts/

info/2048400/10-Herramientas-que-usa-el-FBI-para-el-analisis-de-la-PC. html

[10] Tecnologyc, Recuva para recuperar archivos borrados. [Online]. Available: http://tecnologyc.com/recuva-para-recuperar-archivos-borrados/

[11] Pandora Recovery, Pandora Recovery Tool. [Online]. Available: http://www.pandorarecovery.com/local/es/

[12] Filesee, Open Freely. [Online]. Available: http://www.filesee.com/

[13] Freefileopener, FreeFileOpen. [Online]. Available: http://www.freefileopener.com/

[14] National Institute of Justice, Digital evidence analysis: Windows registry decoder. [Online]. Available: http://www.nij.gov/topics/forensics/evidence/digital/analysis/pages/windows-registry.aspx

[15] Forensic artifacts, Regitry: MUICache. [Online]. Available: http://forensicartifacts.com/2010/08/registry-muicache/

[16] Arsenal Recon, Registry Recon. [Online]. Available: http://www.arsenalrecon. com/apps/recon/

[17] Conexión Inversa, Forense en correos electrónicos. [Online]. Available: http://conexioninversa.blogspot.com/2008/11/forense-en-correo-electrnicos-outlook. html

[18] Instrasoft, Forensic Toolkit, Intrasoft soluciones para emprendedores. [Online]. Available: http://www.intrasoftpanama.com/index.php?option=com_content&view=article&id=17&Itemid=11

[19] Seguridad y Redes, Análisis de Red con Wireshark – Interpretando los Datos. [Online]. Available: https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/

[20] Welive Security, Uso de filtros en WireSahrk para detectar actividad maliciosa. [Online]. Available: http://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/

[21] S. Hernando, Xplico una herramienta de análisis forense de tráfico de red. [Online]. Available: http://www.sahw.com/wp/archivos/2009/09/01/xplico-una-herramienta-de-analisis-forense-de-trafico-de-red/

[22] Inovtec consultoría y soluciones HI-TEC, OxygenForensic. [Online]. Available: http://www.inovtec.com.mx/oxygen-forensic/

[23] MSAB, Que es XRY, Introducción a la tecnología forense móvil y extracciones de teléfonos móviles. [Online]. Available: https://www.msab.com/download/product_sheets/spanish_product_sheets/XRY_What-is-XRY_ES.pdf

[24] Conexión inversa, Forensics con volatility. [Online]. Available: http://conexioninversa.blogspot.com/2009/02/forensics-con-volatility.html

[25] Caminogeek, Lista de herramientas de recuperación de contraseña: Windows – Navegadores. [Online]. Available: http://www.caminogeek.com/lista-de-herramientas-de-recuperacion-de-contrasena-windows-navegadores/

[26] P. Ramos, Herramientas para el análisis dinámico de malware. [Online]. 2011. Available: http://www.welivesecurity.com/la-es/2011/12/22/herramientas-analisis-dinamico-malware/

[27] Hard2Bit, Análisis de malware: enfoque y caso práctico, Seguridad informática. [Online]. Available: https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/

[28] Softonic, Microsoft Process Monitor. [Online]. Available: http://microsoft-process-monitor. softonic.com/

[29] Eset-la, EsetSysInspector. [Online]. Available: http: //www.eset-la. com/download/sysinspector

[30] Seguridad informática garcia-s, Seguridad Informática. [Online]. Available: http://seguridadinforma ticagarcia-s.wikispaces.com/Procedimientos+de+Informatica+Forense

[31] Buenastareas, Ensayo investigación forense Raúl Reyes. [Online]. Available: http://www.buenastareas.com/ensayos/Ensayo-Investigacion-Forense-Raul-Reyes/4232425.html

[32] El Universal, Informe forense de interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia, publicado por OIPC-INTERPOL. [Online]. 2008. Available: http://images.eluniversal.com//2008/05/15/infointerpol.pdf

[33] Forensica digital, Interpol y el caso de Raúl Reyes. [Online]. Available: http://myslide.es/docume nts/forensica-digital-interpol-y-farc.html

[34] F. Fabri, Cómo ser un detective informático. [Online]. Available: http://articulos.softonic.com/informatica-forense

[35] SlideChare, Laboratorios con herramientas de computación forense. [Online]. Available: http://es.slideshare.net/miriam1785/herramientas-de-computacion-forense

[36] Enter 2. 0, Los detectives de la era digital. [Online]. Available: http://e.eltiempo.com/media/produccion/especialReyes/pdf/especialDesencriptacionENTER.pdf

[37] Fundación Criminalística Forense Colombiana, La prueba grafológica y la participación del perito grafo técnico en el caso de alias 'Raúl Reyes'. [Online]. Available: http://www.criminalisticaforense.com/notiforensescolombia.html

[38] C. Pérez García, En Colombia se investigan los delitos informáticos. [Online]. Available: http://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html

[39] V. H. Mora Mendoza, Así funciona la informática forense en Colombia. [Online]. Available: http://www.eluniversal.com.co/tecnologia/asi-funciona-la-informatica-forense-en-colombia-134018

[40] A. Salazar, El reto para los expertos forenses en sistemas digitales de la interpol y los supuestos computadores de Raúl Reyes. [Online]. Available: http://www.aporrea.org/actualidad/a56963.html

[41] Norton, Norton Cybercrime Report. [Online]. 2012. Available: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[42] Software libre, El software libre y la informática forense. [Online]. Available: http://software-libre-if.blogspot.com/p/herramientas-para-el-analisis-de. html

[43] M. López Delgado, Análisis Forense Digital. [Online]. Available: http://software-libre-if.

blogspot.com/p/herramientas-para-el-analisis-de.html

[44] J. J. Cano, Introducción a la informática forense. [Online]. Available: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[45] L. Martínez Rodríguez, Buenas prácticas forenses: Casos prácticos iOS y Linux. [Online]. 2013. Available: https://www.youtube.com/watch?v=cU9myrfUsT0

[46] E. Hidalgo, PhotoRec, recupera archivos borrados en cualquier soporte. [Online]. Available: http://linuxzone.es/2012/01/17/photorec-recupera-archivos-borrados-en-cualquier-soporte/

[47] Live View. [Online]. Available: http://liveview. sourceforge.net/

[48] Softonic, Disk Investigator. [Online]. Available: http://disk-investigator.softonic. com/

[49] J. M. López, Visores de archive para abrir cualquier formato. [Online]. Available: http://hipertextual.com/archivo/2013/06/visores-de-archivos-universales/