INFORMÁTICA FORENSE “LA NUEVA TECNOLOGÍA EN BUSCA DE DELINCUENTES”

Javier Augusto Castillo Salazar
e-mail: jacsmania@hotmail.com

RESUMEN: *Este artículo da un vistazo general acerca de la informática forense, su característica y su definición. Además muestra la importancia que tiene en la actualidad y que debe ser puesta en práctica de manera efectiva, en conjunto con el apoyo que recibe de las herramientas tecnológicas y la regulación jurídica.*

ABSTRACT: *This article gives an overview about computer forensics, their property and their definition. It also shows the importance of today and should be implemented effectively, together with the support it receives from the technological tools and legal regulation.*

PALABRAS CLAVE: Informática forense, Vulnerabilidad, evidencia digital, Atacante (Hackers).

1 INTRODUCCIÓN

La Informática Forense en la actualidad está adquiriendo una gran importancia dentro del área de los sistemas y/o electrónico, debido al aumento en crecimiento de información día a día y el uso que se le da a esta. Dicha información se desarrolla en espacios ya sean por internet o en el extenso uso de las computadoras por parte de las compañías.
Es por eso que cuando se realiza un crimen, la mayor parte de la información queda almacenada en forma digital, esto conlleva a que las computadoras guardan la información de forma tal que no pueda ser recolectada o usada como prueba. Es de aquí que surge el estudio de la computación forense o Informática Forense, como una ciencia relativamente nueva.

La informática forense acompañada de procedimientos y regulaciones jurídicas pueden ayudar a resolver grandes delitos o crímenes apoyándose en el método de la recolección, análisis, y validación de todo tipo de pruebas digitales.

2 DESARROLLO

2.1 INFORMÁTICA FORENSE

Si comienza a recibir mensajes de textos amenazadores, si sus datos del computador han sido alterados, si la información de alta importancia ha sido borrada, si a través de un programa mediante la línea ADSL se está compartiendo información de la empresa, puede estar siendo una de las tantas víctimas en el delito informático.

La cifra de delitos informáticos en el país va en aumento. Tanto que Colombia es, actualmente, el tercer país en Latinoamérica donde más se comenten. Se calculan que 187 denuncias mensuales son interpuestas por fraude a diferentes bancos. **[1]**

Según la Asociación Colombiana de Ingenieros de Sistemas, Acis, en Colombia la cifra de delitos por este caso ha aumentado de un 36% a un 56% en menos de dos años por falta de cuidado. **[2]**

Actualmente la tecnología está avanzando a pasos agigantados, y con ella la forma en que gran parte del mundo opera. Ahora toda la información es almacenada en los ordenadores de manera automática, a diferencia de épocas anteriores en donde dicha información era almacenada de manera manual, en papel y en cajas fuertes. Esto ha conllevado a ciertos tipos de ventajas y desventajas.

Las ventajas han crecido de manera evidente y mejorando; rapidez en la recolección y análisis, alta disponibilidad, mayor facilidad en el manejo de la información, entre otras. Sin embargo las desventajas y riesgos en los que se incurren no son tan obvios y no son tenidos en cuenta, dejándose pasar por un lado y dejando allí huecos denominados *Vulnerabilidades en la seguridad de la información*. Entre estos, la vulnerabilidad de la información al ser borrada o modificada, la fácil replicación de la información, la explotación de la información por vulnerabilidades de un sistema, o la vulnerabilidad de un integrante de la misma empresa.

Figura 1. [3] Seguridad de la Información.

Con todo el riesgo que se corre al manejar la información debemos de tener una manera de protegernos y de proteger a las personas de las que mantenemos la información. Para poder garantizar la confidencialidad, integridad y disponibilidad de la

información, garantizar las políticas de seguridad, la protección de la información y las tecnologías que facilitan la gestión de la información surge lo que es llamado la *Informática Forense*.

La Informática Forense abarca cuatro partes fundamentales que son:

1. La identificación de evidencia digita.
2. Preservación de la evidencia digital.
3. El análisis de la evidencia digital.
4. La presentación de la evidencia digital.

Definimos la Informática Forense 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.

En muchas ocasiones los atacantes inexpertos dejan rastros el cual son muy fáciles de identificar y analizar llevando a una rápida y fácil detección, de igual forma a medida que los conocimientos de los atacantes aumentan, se extienden proporcionalmente el nivel de sofisticación de los ataques. Esto revela que las organizaciones y jefes de los departamentos de sistemas y de seguridad, hoy en día no se están enfrentando a personas inexpertas que solo quieren llamar la atención, sino que se están enfrentando a gente inquieta con sed de ir más allá de lo que cualquier programa o guía de computación les pueda aportar, llevando así a un análisis mucho más complejo y demorado, utilizando un sin-número de herramientas para poder obtener la información y/o llegar al atacante.

¿Pero qué tan demorado puede ser el reunir las suficientes pistas que den con el autor o autores del o los ataques?

Es una pregunta algo complicada de responder, debido a que como mencionamos anteriormente, hay atacantes con conocimientos muy avanzados, que utilizan o se camuflan mediante herramientas avanzadas como enmascarar direcciones IP reales, correos electrónicos, ingeniería social, entre otros, el cual limitan las investigaciones y efectividad de las misma, demorando así la recolección de pistas el cual pueden llevar hasta años en solo esta labor.

Los forenses despliegan toda su pericia en el sitio donde se originó el crimen donde hay una computadora. Dicho equipo es tratado como otra escena del delito, nadie puede mover o tocar la computadora ya que esto conlleva a contaminar la evidencia o en el peor de los casos a desproteger y perder la información que hay en la computadora, ya que solo basta con mover un dispositivo de almacenamiento, una cámara, apagar o encender el equipo para que las pruebas se contaminen. Todo esto lleva un sin-número de pasos a seguir de manera cuidadosa y profesional, tal como se haría con un cadáver, nadie puede moverlo ni tocarlo, lo primero que se tiene que hacer es acordonar el lugar, después se debe observar que tipo de conexiones tiene la máquina. Se procede a filmar y fotografiar todo el entorno e incluso se llega a medir la distancia entre los diferentes dispositivos. Las herramientas forenses que se utilizan en materia de cómputo para dar con los atacantes, se han desarrollado con el paso del tiempo, ayudándonos así en cuestiones de velocidad e identificar lo que pasó realmente en el sistema. De allí el personal que labore en la Informática Forense debe poseer altos conocimientos tanto técnicos como prácticos, conocer las herramientas de uso, de igual forma estar actualizado en las vulnerabilidades que salen tanto en los Sistemas Operativos como en el Hardware, no deben emprender un examen más allá de su nivel de conocimiento y habilidad, hasta que sean debidamente capacitados, por ende deben buscar la ayuda de personal más experimentado y con conocimientos en el tema, sobre todo de los denominados Hackers, tal y como sucede en diferentes países del mundo que reclutan Hackers con el fin de contrarrestar e identificar las vulnerabilidades y atacantes.

Un procedimiento clave para una revisión exhausta es la realización de una copia en imagen. No la copia habitual de copiar y pegar documentos, ya que así no se registran archivos a fondo y borrados. Se trata de un duplicado exacto del disco duro que se investiga. Hay que tener en cuenta que no solo se analizan discos duros, sino todo dispositivo de almacenamiento de información tales como, Memorias USB, tarjetas flash, discos floppy, ópticos y discos (CD, DVD, Blu-ray)

Luego de identificar qué tipo de ataque se realizó, aparecen un tipo de preguntas que deben ser resueltas:

- ¿Cuándo se realizó el ataque?
- ¿Cómo se realizó el ataque?
- ¿Que se utilizó para hacer el ataque?
- ¿Hubo fuga de información en el ataque?
- ¿El ataque se realizó fuera de la red, o fue un ataque interno?

Imagen 1. [4] Informática Forense.

Todos estos procedimientos son claves y primordiales en una investigación

2.2 CIENCIA FORENSE Y PRINCIPIO DE TRANSFERENCIA DE LOCARD

La ciencia Forense nos proporciona las técnicas y principios facilitando la investigación de un delito criminal, cualquier principio o técnica que se aplica para recuperar, identificar, reconstruir, recuperar y analizar la evidencia se denomina Ciencia Forense.

Un forense aporta su conocimiento y entrenamiento para ayudar a los investigadores a reconstruir un crimen y encontrar pistas creando hipótesis sobre lo ocurrido. Esto conlleva a un sinfín de posibilidades sobre lo que pudo ocurrir disponiendo de tan solo una información limitada.
Un principio fundamental en la ciencia forense es el Principio de Transferencia o Intercambio de Locard. Dicho principio tiene plena validez en el ámbito informático y las evidencias electrónicas.

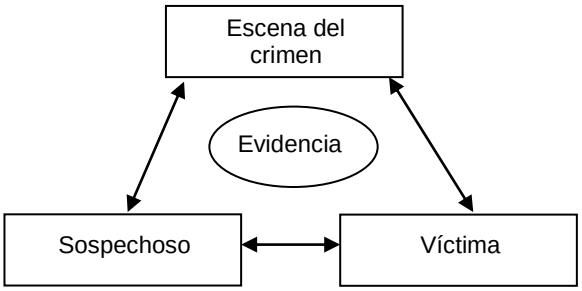

Figura 2. [5] Principio de Transferencia de Locard.

Este principio nos define fundamentalmente:

- Cualquier objeto que entra en la escena de crimen deja un rastro ya sea en la escena, en la victima y viceversa.

En términos reales, si yo piso la escena del crimen dejare algo mío, ya sea pelo, sudor, huellas, etc., pero también me llevare algo conmigo cuando abandone la escena, ya sea barro, fibra, olor, etc.

En la ciencia forense hay varios tipos de evidencias físicas:

- Evidencia transitoria.
- Evidencia curso o patrón.
- Evidencia condicional.
- Evidencia transferida.

En esta última evidencia (Transferidas) se dividen dos tipos:

- Transferencia por rastro: sangre, pelo, semen, etc.
- Transferencia por huella: de zapato, dactilares, etc.

Brevemente, la ciencia forense nos facilita las herramientas, métodos y técnicas que pueden ser usados para analizar una evidencia digital y usar dicha evidencia para reconstruir lo que ocurrió durante la realización del crimen, a la víctima y a la escena del crimen.

2.2.1 MANIPULACIÓN DE LA EVIDENCIA DIGITAL

Es importante tener presente los siguientes requisitos que se deben cumplir en la manipulación de la evidencia digital:

- Mantener y controlar la integridad del medio original.
- Hacer uso de medios forenses estériles.
- Las copias de los datos obtenidas, deben estar correctamente marcadas
- Siempre que la evidencia digital este en poder de algún individuo, este será el responsable de todas las acciones tomadas, mientras esté en su poder.
- Cuando sea necesario que una persona tenga acceso a evidencia forense, esa persona debe ser profesional en forense.

2.3 HERRAMIENTAS DE INFORMÁTICA FORENSE

En la actualidad se cuenta con un sin-número de herramientas forense tanto gratis como de pago, esto con el fin de encontrar imágenes, textos, archivos borrados, registro de conversaciones, historiales web, contraseñas y todos aquellos archivos que permiten rastrear la actividad de una persona en un ordenador. Por supuesto muchas de estas utilidades también sirven para rescatar información propia.
A continuación se enumeran algunas de las herramientas según su función:

Herramientas de Cómputo Forense:

- Sleuth Kit.
- Py-Flag.
- Dumpzilla.
- Netcat.
- NTFS-Tools.
- Md5deep.
- Helix.

Herramientas para análisis de discos duros:

- Accesdata Forensic Toolkit (FTK).
- Kit electrónico de transferencia de datos.

Herramientas para el análisis de correos electrónicos:

- Paraben.
- AccesData Forensic Toolkit (FTK).

Herramientas para el análisis de redes:

- SilentRunner – Acces Data.
- E-Detective – Decision Computer Group.

2.4 CONSEJOS ÚTILES A SEGUIR

Ya sea como persona, o bien sea como empresa, es muy importante seguir algunos consejos que nos pueden ayudar y evitar el ser víctimas de fraudes, sabotajes y robos, productos de medios informáticos y tecnológicos.
La informática forense nos brinda un sin-número de consejos para ser puestos en práctica:

- No prestar su computador a personas desconocidas, puede ser objeto para que le instalen programas espías.
- En ningún caso recibir ni compartir información en archivos adjuntos de dudosa precedencia.
- Si recibe un correo electrónico de origen desconocido bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloggers, etc.) de igual forma evitar ejecutar los links de dudosa procedencia que sean recibidos al correo.
- Cambie los passwords de sus computadoras y pines de tarjetas con cierta frecuencia.
- No revele información por correo, tales como contraseñas, nombre de usuarios o números de tarjeta.
- Ignore todos aquellos correos electrónicos conocidos como SPAM.
- Mantenga instalada las últimas actualizaciones de su sistema.
- Siempre que navegue por internet, busque la imagen de un candado amarillo en la parte superior izquierda. Esta imagen junto a la línea HTTPS al inicio de la barra de dirección le da la seguridad de que usted se encuentra navegando por un sitio seguro y protegido.

Seguir estos consejos, entre muchos otros, no significa que se estará libre de ser víctima de fraude o de un delito informático, sin embargo nos ayudara sustancialmente a mejorar la seguridad de su sitio Web, computadora y a cuidar la valiosa información que es alojada allí.

Para una buena aplicación preventiva de la informática forense es necesario establecer y que se cumplan políticas de seguridad para los usuarios y administradores de los sistemas, realizar auditorías continuas en los sistemas y mantener actualizados nuestros softwares.
Para la parte reactiva de la informática forense se necesita el uso programas tales para la detección de intrusos, antivirus actualizados, logs de sistemas de información, firewalls, entre otros.

Para que todo el análisis e investigación en la informática forense sea exitoso, es necesario que se tenga una regulación jurídica que penalice a los atacantes descubiertos y que sean sentenciados por los delitos cometidos según la ley, de manera que los delitos que se comenten no queden impunes.

Imagen 2. [6] Regulación Jurídica.

2.5 CONSIDERACIONES INMEDIATAS PARA LA AUDITORÍA DE LA SEGURIDAD

Las normas que se deben tener en cuenta para elaborar la evaluación de la seguridad se menciona a continuación:

- Uso del computador.
- Cantidad y tipo de información.
- Sistema de acceso.
- Medios de control.
- Instalaciones.
- Control de residuos.
- Establecer las áreas y grados de riesgo.

Para tener un impacto positivo dentro del resguardo de los datos y la seguridad integral dentro de una institución se debe llevar a cabo:

- Definir políticas de seguridad.
- Organizar y dividir las responsabilidades.
- Planificación de programas de desastres y sus pruebas.
- Política de destrucción de basura, copias, fotocopias, etc.

3 CONCLUSIONES

Ante el análisis presentado podemos concluir que actualmente la seguridad en la información y su integridad en la confidencialidad no depende de la máquina, no depende del software, sino enteramente del usuario y de cómo sea tratada la información.

Las metodologías mencionadas durante el análisis, las herramientas y técnicas aplicadas pueden ser comunes en otro tipo de ámbitos, pero aquí y en conjunto ayudan a explicar hechos ocurridos a diario.

Las herramientas que se utilizan en Informática Forense son muy variadas, grades, costosas, gratis, comerciales, sencillas. Pero al final un buen forense debe saber que herramienta necesita para el caso específico e interpretar adecuadamente los resultados que arroja.

Actualmente estamos inmersos en un mundo digital, como usuarios estamos en la obligación de informarnos que tan sensible es que se viole el derecho a la privacidad y a la seguridad en la información que se extrae y se ingresa a un determinado sistema.

4 REFERENCIAS

1 Informática Forense, *“Que es la Informática Forense”*, Disponible: http://www.informaticaforense.com.co/index.php/joomla-overview

2 Cifras de delitos informáticos
Disponible:
[1] http://mattica.com/en-colombia-las-cifras-de-delitos-informaticos-van-en-aumento/
[2]http://www.atlas.com.co/sia/public/index.php/articulo/3388/print

3 Los sectores más propensos a ataques cibernéticos
Disponible:
http://colombiadigital.net/actualidad/noticias/item/7062-los-sectores-mas-propensos-a-ataques-ciberneticos.html

4 *NORSE* Mapa de ataques cibernéticos en tiempo real.
Disponible: http://map.ipviking.com/

5 Herramientas de cómputo forense. Wikipedia
Disponible:
http://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Herramientas_de_C.C3.B3mputo_Forense

6 *Análisis Forense Digital*, Lopez Delgado Miguel, Junio del 2007, CRIPORED

7 Seguridad de la Información (Figura 1.)
Disponible:
[3]http://cursohispano.com/conceptos-basicos-en-seguridad-de-la-informacion/

8 Principio de Transferencia de Locard (Figura 2.)
Disponible:
[5] http://www.notinueve.com.mx/que-es-la-ciencia-forense-computacional/

9 Informática Forense (Imagen 1.)
Disponible:
[4] http://www.fotosdigitalesgratis.com/galeriafotos/8494/auditoria_analisis_forense_digital_informatica_forense

10 Regulación Jurídica (Imagen 2.)
Disponible:
[6]http://kasner.kiev.ua/peredova-tehnologija-torgivli-majbutnogo/