INFORMÁTICA FORENSE. RETO DEL SIGLO XXI

Estepa Santos Carlos Eduardo, Durán Roa Javier Alejando
cienegsan, javi276@gmail.com
Universidad Piloto de Colombia

***Resumen* – Hoy día la tecnología avanza de una manera acelerada y con ello las personas ahora pueden acceder a muchas fuentes de información, realizar transacciones electrónicas desde cualquier parte del mundo, interactuar con otras personas de cualquier parte del globo, viajar en corto tiempo a cualquier destino. Sin embargo, esta interacción con la tecnología genera que la información de las personas resida en una gran cantidad de dispositivos electrónicos (computadores, tablets, smartphones, smartcards, etc.) siendo vulnerable a ser almacenada sin restricciones y a ser utilizada de manera indiscriminada para diversos fines, no estrictamente éticos ni comerciales.**

Es ahí donde la informática forense toma relevancia. Los ingenieros forenses, con este avance tecnológico, deben estar a la par con herramientas, técnicas y procedimientos que permitan enfrentar los diferentes retos planteados por el avance y el dinamismo de la tecnología de cara a la sociedad.

***Índice de términos* – bios, dos, esata, ext1, ext2, ext3, ext4, fat, fat16, fat32, forense, grub, hash, hfs, hpfs, ide, lilo, mbr, mólex, ntfs, sata, uefi**

I. INTRODUCCIÓN

El trabajo de un ingeniero forense requiere la observancia de muchos elementos para poder sustentar su actividad ante la sociedad y las autoridades. Su meta, mantener incólume la evidencia digital recolectada. Para ello, el ingeniero forense a través del seguimiento de una serie de procedimientos rigurosamente establecidos por la comunidad científica y apoyándose en el uso de herramientas, técnicas y tecnología debe recolectar toda la información posible para lograr explicar, sin lugar a dudas, un hecho o situación específica que involucre el uso de la tecnología.

Dentro de los elementos importantes que el ingeniero forense debe observar se encuentran las leyes. Nunca, el actuar de un ingeniero forense puede transgredir los derechos o libertadores de una persona.

Adicionalmente, los procedimientos realizados por el ingeniero forense deben estar soportados en manuales, técnica extraída de la experiencia y literatura (manuales de procedimientos, formatos, etc.) aceptada dentro de la comunidad científica que permita demostrar que no hubo vicio alguno en la obtención de la evidencia.

Finalmente, las herramientas son los medios a través de los cuales el ingeniero forense se apoya en la tecnología para permitirle, haciendo uso de las técnicas aprobadas por la comunidad científica y la experticia, realizar su trabajo y extraer de forma inequívoca la información sin alterarla.

II. LEYES

El avance de la tecnología le ha dado a la humanidad muchas herramientas que facilitan su modo de vida pero así mismo los delincuentes han encontrado en este notable desarrollo un nicho propicio para cometer delitos y es un campo cuya regulación y doctrina legal se ha desarrollado lentamente pero con rigor. Nuestro país ha sido pionero en la legislación de crímenes a través del uso de la tecnología y a continuación se presentará la transcripción de las normas más relevantes en nuestro país a fin de presentar un breve marco legal con el que se ha regulado en parte, la creciente ola de delincuencia cibernética.

A. *Ley 527 de 1999:*

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [1].

B. *Ley Estatutaria 1266 de 2008:*

Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones [2].

C. *Ley 1273 de 2009:*

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [3].

D. *Ley 1581 de 2012:*

Por la cual se dictan disposiciones generales para la protección de datos personales [4].

E. *Decreto 1377 de 2013:*

Por el cual se reglamenta parcialmente la Ley 1581 de 2012 [5].

> *"Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas"*

III. SOFTWARE

A. *Sistemas Operativos*

Los sistemas operativos son la razón de ser de cualquier sistema de información. Sin él, las aplicaciones no tendrían un ambiente en el cual ejecutarse y realizar las diversas tareas para las que fueron creadas.

Para el ejercicio de la informática forense es de suma importancia conocer la estructura de cada sistema operativo pues facilitará el trabajo de recolección de evidencia.

Cada sistema operativo tiene características distintivas y muy importantes que determinarán la forma en la cual se debe recolectar la evidencia. Dentro de estas características se encuentran forma y tipo de arranque del sistema operativo (bios, uefi, mbr, grub, lilo), estructura del sistema de archivos (fat, fat[16, 32], ntfs, ext[1, 2, 3, 4], dos, hpfs, hfs, estructura de directorios, esquemas de autenticación y seguridad, conjunto de instrucciones, interrupciones, manejo de memoria, manejo de discos, sistema de registro de eventos, forma de ejecución de aplicaciones, extensiones de archivos, librerías, administración de hardware y la gestión de procesos entre muchos otros que permiten que un usuario pueda realizar cualquier tarea.

Pero estos programas (sistemas operativos) por más robustos que sean deben ser construidos para ser utilizados por los usuarios quienes dentro de su desarrollo normal del conocimiento e inherente a la práctica de una profesión y/o trabajo encuentran formas de usarlos de forma irregular contra otros sistemas de información para afectar compañías y/o personas a través de la explotación de sus vulnerabilidad pues ningún sistema es del todo seguro.

Es por ello que también la práctica de la informática forense exige que existan herramientas, diseñadas para cada entorno de sistema operativo, las cuales ofrezcan la posibilidad de recolectar evidencia del uso de estos sistemas informáticos.

Incluso, existen distribuciones de sistemas operativos (generalmente basados en Linux) los cuales cuentan con múltiples herramientas para hacer análisis de evidencia recolectada de otros sistemas operativos. Estas herramientas cada vez son más potentes, portables y compatibles con las tecnologías emergentes.

B. *EnCase®:*

Guidance Software es reconocida en todo el mundo como una empresa líder en soluciones de investigación digital. La plataforma de EnCase® brinda la base para que las organizaciones gubernamentales y empresariales y las

organizaciones encargadas del cumplimiento de la ley lleven a cabo investigaciones informáticas exhaustivas y eficaces de cualquier tipo, como robo de propiedad intelectual, respuesta a incidentes, auditoría de cumplimiento y respuesta a solicitudes de medios de prueba de fuentes electrónicas, y, al mismo tiempo, puedan mantener la integridad forense de los datos[6].

C. *AccessData® FTK® Imager:*

FTK es una plataforma de investigaciones digitales aprobada por tribunales, que está diseñada para ser veloz, analítica y contar con escalabilidad de clase empresarial. Conocido por su interfaz intuitiva, el análisis de correo electrónico, las vistas personalizadas de datos y su estabilidad, FTK establece el marco para una expansión sin problemas, por lo que su solución de informática forense puede crecer de acuerdo a las necesidades de su organización [7].

D. *Tableau Imager:*

Aplicación desarrollada para la generación de imágenes lógicas y físicas de discos la cual trabaja en complemento con los bloqueadores de escritura.

E. *PassMark® OsForensics:*

Es una herramienta bastante versátil, diseñada para Microsoft Windows®, que permite administrar un caso y la cual incluye funcionalidades útiles sobre la evidencia tales como indexación, extracción de la actividad reciente del equipo, visor de memoria, visor del registro del sistema operativo, explorador de archivos, extracción de contraseñas, creación y comparación de firmas, verificación y creación de hash, creación de copias forenses y otras más que hacen de esta herramienta una opción robusta a la hora de crear, gestionar y administrar evidencia digital.

IV. TECNOLOGÍA

A. *Los bloqueadores de escritura por hardware:*

Durante el proceso de adquisición de información de los dispositivos de almacenamiento de los equipos informáticos se requiere garantizar que el contenedor del cual se obtendrán los archivos para su análisis no se contamine al momento de correr las aplicaciones o de ejecutar los procedimientos necesarios y por ello se debe disponer de herramientas que no permitan sea alterada la información pues al momento de conectarse a un sistema informático se escriben datos en el dispositivo. Este proceso es propio de todos los sistemas operativos y permite que se pueda tener acceso a él.

Por lo tanto, los bloqueadores de escritura por hardware son dispositivos electrónicos que garantizan se pueda conectar un disco duro o cualquier otra unidad de almacenamiento al equipo desde el cual se obtendrá la información. Este componente permite tener acceso exclusivamente de lectura al dispositivo que se analiza, garantizando que no se escribirán datos de ningún tipo y evitando que se modifique la estructura de directorios y archivos y adicionalmente, que se realicen cambios en los metadatos de la información.

De esta manera se pueden realizar copias a modo de imagen del dispositivo que se analiza para su posterior análisis.

B. *Los clonadores de discos:*

Dispositivo a través del cual se conectan las unidades de almacenamiento y se obtienen imágenes completas idénticas para su posterior estudio y análisis de la información.

Esta imagen luego se analizará por separado en un laboratorio y con el uso de herramientas especializadas que extraerán la información y los metadatos que se requieren.

C. *Los maletines forenses:*

Para el trabajo forense se necesita un conjunto de herramientas tanto de hardware como de software que permitan extraer la evidencia facilitando el tratamiento y la gestión de los dispositivos y/o equipos informáticos de forma práctica.

Es así como estas herramientas se agrupan en un maletín y a continuación se listan algunos de los elementos mínimos de hardware con los que cuenta:

- Conector IDE
- Conector eSATA

- Bus de datos IDE
- Bus de datos eSATA
- Conector mólex
- Cargador de energía
- Cable de poder
- Disco duro
- Bloqueador de escritura por hardware

Para complementar la tarea de recolección de evidencia y gestionar el hardware se cuenta con herramientas de software que permiten realizar variadas tareas. Algunos de esas herramientas son:

- Tableau Imager ®
- AccessData FTK Imager®
- Deft-extra 3.0 – Windows Forensics Toolkit

V. INGENIERÍA SOCIAL

Una de las prácticas que más difusión ha tenido a la hora de obtener datos confidenciales es la ingeniería social. Esta "actividad" le permite a un atacante obtener información personal y empresarial de tipo privilegiada y/o confidencial sin utilizar ningún tipo de fuerza ni herramienta, tan solo el conocimiento de las personas es suficiente pues se ven persuadidas a características o rasgos notables como:

- Autoridad
- Carisma
- Reciprocidad
- Validación social

El objetivo de la ingeniería social es básicamente ganar acceso a sistemas informáticos y redes de computadores con el fin de sabotear información privilegiada a través de las personas que trabajan dentro de las corporaciones.

Muchas empresas actualmente son blanco de este tipo de ataques pues la información que almacenan y manejan dentro del desarrollo de su objeto social es muy valiosa para diversos fines, es información vital para los negocios y por ello empresas como las telefónicas, gubernamentales, militares y financieras se ven inmersas en estos ataques de manera constante y persistente en el tiempo.

La ingeniería social se vale de varias técnicas para lograr acceso a la información de las personas y las corporaciones, técnicas y herramientas tan sencillas como:

- El teléfono
- Internet
- Intranet
- Sitio de trabajo
- La Basura

Con las herramientas y técnicas anteriores los delincuentes logran obtener información de datos personales, manuales, extractos, contactos, números de teléfono, acceso a lugares no autorizados, etc., siendo esta información muy valiosa y que no debería estar expuesta por falta de gestión del riesgo.

Pero este tipo de ataques se pueden evitar tomando precauciones sencillas como:

- Ser cauteloso con las personas a las que se les brinda ayuda
- Verificar siempre con quién se habla al momento de revelar información confidencial
- Corroborar siempre la información de las personas que ofrecen soporte técnico. Deben estar plenamente identificadas
- No aceptar intimidaciones por teléfono
- Estar atento a las personas extrañas que se encuentran en los sitios de trabajo
- No participar de ninguna cadena de correos o promociones a través de internet o intranet

La práctica de la ingeniería social es un modo bastante conocido y utilizado por los delincuentes debido a que el eslabón más débil en la cadena de la seguridad de la información es siempre el usuario. Si se es cauteloso con la información que se maneja, los delincuentes no tendrán oportunidad alguna. Debe existir un plan de capacitación permanente y un programa de concientización y gestión documental que permita establecer procedimientos claros y precisos para el manejo de la información dentro de las compañías, esto reducirá notablemente la exposición a los ataques.

VI. CONCLUSIONES

El rápido desarrollo de la tecnología y de sistemas de información cada vez más complejos ha instado a los profesionales de TIC a estar más preparados, a contar con herramientas más robustas y a diseñar técnicas y procedimientos más flexibles pero que permitan enfrentar las amenazas que conlleva este avance tan acelerado dentro de una sociedad orientada al conocimiento.

Hoy día ya no se requieren conocimientos avanzados para vulnerar sistemas o poner en peligro la información pues los intereses de las personas son motivados por el ego, la superación personal y, en el peor de los casos, el dinero.

La sociedad ha exigido vehementemente a la justicia que interceda y defienda los derechos que se han ido perdiendo con el desarrollo de la tecnología y su aprovechamiento de manera indebida para vulnerar la información y es por ello que el sistema judicial del país ha dictado un conjunto de leyes orientadas a la protección de los datos, su tratamiento y finalmente, a las personas.

Por otro lado, las herramientas forenses se van mejorando con cada ataque, con cada incidente de seguridad queda una lección y eso abarca también la especialización cada vez más intensiva y la convergencia del conocimiento para tratar de enfrentar, por parte de los peritos informáticos, a las constantes y crecientes amenazas.

Todos estos elementos constituyen el gran reto para la informática forense pues hay que entrenar a los peritos en la convergencia de muchas ramas técnicas del conocimiento para sobrellevar el gran volumen de nacientes ataques y/o vulnerabilidades de los sistemas de información.

REFERENCIAS

[1] Ley 527 de 1999 Nivel Nacional. Diaro Oficial 43.673 del 21 de Agosto de 1999. Fecha de expedición 18 de Agosto de 1999. Fecha de Entrada en Vigencia 21 de Agosto de 1999.

[2] Ley 1266 de 2008 Nivel Nacional. Diario Oficial 47.219 de Diciembre 31 de 2008. Fecha de expedición 31 de Diciembre de 2008. Fecha de Entrada en Vigencia 31 de Diciembre de 2008.

[3] Ley 1273 de 2009 Nivel Nacional. Diario Oficial 47.223 de Enero 5 de 2009. Fecha de expedición 5 de Enero de 2009. Fecha de Entrada en Vigencia 5 de Enero de 2009.

[4] Ley 1581 de 2012 Nivel Nacional. Diario Oficial 48.587 de 18 de Octubre de 2012. Fecha de expedición 17 de Octubre de 2012. Fecha de Entrada en Vigencia 17 de Octubre de 2012.

[5] Decreto 1377 de 2013 Nivel Nacional. Diario Oficial 48.834 del 27 de junio de 2013. Fecha de expedición 27 de Junio de 2013. Fecha de Entrada en Vigencia 27 de Junio de 2013.

[6] (Handbook style) *EnCase® Enterprise para empresas*, Guidance Software, 2009, pp. 6. [Online]. Disponible: https://www.encase.com/resources/Pages/doclib/Spanish-Library/EnCase-Enterprise-for-Corporations-Spanish.aspx

[7] AccessData. *Forensic Toolkit® (FTK®), "Reconocido alrededor del Mundo como el Estandar en Software de Informática Forense"*. [Online]. Disponible: http://www.accessdata.com/es/productos/soluciones-forenses/ftk