Informática forense y sus beneficios

Guerrero Paiva Américo
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
CONSULT_AME@hotmail.com

RESUMEN

El presente trabajo de investigación mostrará sobre las generalidades, importancia herramientas y beneficios que conlleva el conocimiento de la informática forense, desde una perspectiva general, marcando un hito que haga del lector una persona que indague a mayor detalle este mundo que si bien está en estructuración de sus normas y criterios, está siendo de gran utilidad en la recuperación de evidencias para casos judiciales.

Palabras Clave

Importancia, herramientas, evidencia, pericial, legal, comunicación.

1. INTRODUCCIÓN

El proceso de recopilación de evidencias de eventos posee 3 componentes esenciales: técnico que contribuye en la búsqueda de indicios y bitácoras de auditoría, pericial en que el Perito examina y transforma la evidencia en medios de prueba y finalmente fase Legal y de comunicación, en que el asesor legal denunciará el delito apoyado en el informe pericial.

Los Investigadores criminalisticos necesitan recopilar evidencias en procesos judiciales penales, civiles y laborales o sanciones disciplinarias al interior de la empresa, recopilar bitacoras e indicios, observando procedimientos forenses, con expertos en la metodología forense, utilizando herramientas técnicas, conectores y hardware de apoyo forense, utilizando software legal y certificado para el trabajo forense informático, de acuerdo a las normas legales del país en que se realiza el estudio, finalmente se recomienda respaldar en modo seguro usando contraseñas y criptografía, según se observa en las RFC 3.227 y RFC 2.196, relativas a la guia para la recolección de evidencia.

En la actualidad, se está trabajando en la estandarización de los procedimientos forenses informáticos, a fin de alinearlos y facilitar la comunicación y trabajo cooperativo entre otros organismos de investigación y laboratorios criminalísticos.

2. SU IMPORTANCIA

El proceso forense, el apoyo pericial y las herramientas forenses informáticas garantizan que la identificación, obtención y análisis forense no alterará la evidencia, permitiendo a la empresa poder avanzar en la identificación del crimen informático y ubicar responsables, permitiendo dar inicio a la formalización legal de los hechos a través de denuncia o querella en lo Penal, Civil o Laboral, con la certeza que la evidencia permanece inalterable y con el apoyo de un informe forense informático que avala en una exposición y análisis técnico los dichos legales conforme a derecho.

En el marco de su importancia podemos citar los campos de incidencia de la informática forense.

Prosecución Criminal. Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

Litigación Civil. Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

Investigación de Seguros. La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

Temas corporativos. Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

Mantenimiento de la ley. La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Los investigadores de la computación forense usan gran cantidad de técnicas para descubrir evidencia, incluyendo herramientas de software que automatizan y aceleran el análisis computacional.

La evidencia computacional es única, cuando se la compara con otras formas de “evidencia documental”. A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

3. HERRAMIENTAS DE INVESTIGACIÓN FORENSE

En la actualidad existen cientos de herramientas, las cuales se pueden clasificar en cuatro grupos principales.

3.1. Herramientas para la Recolección de Evidencia

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

1. La gran cantidad de datos que pueden estar almacenados en un computador.

2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.

3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.

4. Limitaciones de tiempo para analizar toda la información.

5. Facilidad para borrar archivos de computadores.

6. Mecanismos de encripción, o de contraseñas.

A continuación haremos una descripción somera de tales herramientas.

EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc. (http://www.guidancesoftware.com), permite asistir al especialista forense durante el análisis de un crimen digital.

Se escogió mostrar esta herramienta por tratarse del software líder en el mercado, el producto más ampliamente difundido y de mayor uso en el campo del análisis forense.

Diferente capacidad de Almacenamiento. Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.

Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo. EnCase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

Análisis Compuesto del Documento. EnCase permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el slack interno y los datos del espacio unallocated.

Búsqueda Automática y Análisis de archivos de tipo Zip y Attachments de E-Mail.

Firmas de archivos, Identificación y Análisis. La mayoría de las graficas y de los archivos de texto comunes contiene una pequeña cantidad de bytes en el comienzo del sector los cuales constituyen una firma del archivo. EnCase verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que unos sospechosos hayan escondido un archivo o simplemente lo haya renombrado, EnCase detecta automáticamente la identidad del archivo, e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle.

También muestra el Slack File con un color rojo después de terminar el espacio ocupado por el archivo dentro del cluster, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos Swap y Print Spooler son mostrados con sus estampillas de datos para ordenar y revisar.

Visualizador Integrado de imágenes con Galería. EnCase ofrece una vista completamente integrada que localiza automáticamente, extrae y despliega muchos archivos de imágenes como .gif y .jpg del disco. Seleccionando la "Vista de Galería" se despliega muchos formatos de imágenes conocidas, incluyendo imágenes eliminadas, en el caso de una vista pequeña. El examinador puede después escoger las imágenes relevantes al caso e inmediatamente integrar todas las imágenes en el reporte de EnCase. No es necesario ver los archivos gráficos usando software de terceros, a menos que el formato de archivo no sea muy conocido y todavía no sea soportado por EnCase.

EnCase es un software costoso, y en Estados Unidos se presentan de esta manera:

- Gobierno y Educación US$1,995
- Sector Privado US$2,495

Actualmente EnCase se encuentra en su versión 3.0.

3.2. Herramientas para el Monitoreo y/o Control de Computadores

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como key loggers o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.

“KeyLogger” es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se

quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por e-mail. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen dos versiones. la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas.

3.3. Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

3.4. Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como DIBS "Portable Evidence Recovery Unit".

4. DIFICULTADES DEL INVESTIGADOR FORENSE

El investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes:

1. Carencia de software especializado para buscar la información en varios computadores.

2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.

3. Será difícil encontrar toda la información valiosa.

4. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.

5. Los errores cometidos pueden costar caro para la persona o la organización que representa.

6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.

7. Falta de experiencia para mostrar, reportar y documentar un incidente computacional.

8. Dificultad para conducir la investigación de manera objetiva.

9. Dificultad para hacer correctamente una entrevista con las personas involucradas.

10. Reglamentación que puede causar problemas legales a la persona.

5. CONCLUSIONES

Los resultados que podemos compartir mediante este artículo es de mostrar una panorámica muy general de los beneficios de la computación forense, discutiendo algunos temas muchas veces ignorados como en que áreas inciden, así como una clasificación general de las herramientas a disposición del investigador forense, en particular del famoso EnCase.

Bajo la especialidad a la que se dedica un estudio informático forense se tiene varios truncamientos por los cuales no se pueden realizar con exactitud y plenitud su desarrollo en el mundo puesto que la tecnología esta de lado por las personas que viven el los países tercermundistas, pretendiendo dar una visión amplia de la naciente ciencia de la computación forense. En trabajos posteriores se podría mirar con mayor detenimiento alguno de los temas tocados, pero por el momento invitamos al lector que desee profundizar más sobre el tema consultando la bibliografía de referencia.

6. REFERENCIAS

Las siguientes direcciones electrónicas fueron consultadas entre el 2 y el 5 de julio de 2001.

[1]http://www.forensics-intl.com/art12.html

[2]http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

[3]http://www.ioce.org/ioceprinc.shtml

[4]http://www.forensics-intl.com/def6.html

[5]http://www.forensics-intl.com/def7.html

[6]http://www.forensics-intl.com/def8.html

[7]http://www.forensics-intl.com/def3.html

[8]http://www.encase.com/html/how_encase_works.html

[9]http://www.keylogger.com/

[10]http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm Janet Reno, U.S. Attorney General, Oct 28, 1996