

LA INFORMÁTICA FORENSE Y LA BANCA

DOCUMENTO DE TRABAJO

BOGOTÁ, ABRIL DE 2004

CONTENIDO

INTRODUCCIÓN.....	3
1. GENERALIDADES.....	4
1.1 PRINCIPIOS PARA EL MANEJO, RECOLECCIÓN Y RECUPERACIÓN DE EVIDENCIA DIGITAL ...	4
2 CASO HIPOTÉTICO: CANCELACIÓN FRAUDULENTE DE UN CREDITO	5
2.1 PASOS PARA EL ESTUDIO DEL CASO DE INVESTIGACIÓN FORENSE	6
2.1.1 CONOCIMIENTO GENERAL Y LEVANTAMIENTO DE INFORMACIÓN.....	6
2.1.2 RECOLECCIÓN DE EVIDENCIA.....	6
2.1.3 ANÁLISIS DE LA EVIDENCIA	7
2.1.4 PRESENTACIÓN DE LOS HECHOS	8
2.1.5 GENERACIÓN DE INFORME.....	9
2.2 CONCLUSIONES.....	9
3 DIFICULTADES QUE SE LE PODRIAN PRESENTAR AL INVESTIGADOR FORENSE:.....	10
4 VALORES AGREGADOS DE LA INFORMATICA FORENSE	11
5 HERRAMIENTAS DE INFORMACIÓN FORENSE	12
5.1 HERRAMIENTAS PARA LA RECOLECCIÓN DE EVIDENCIA.[1].....	13
5.2 HERRAMIENTAS PARA EL MONITOREO Y/O CONTROL DE COMPUTADORES [1]:.....	17
5.3 HERRAMIENTAS DE MARCADO DE DOCUMENTOS:	18
5.4 HERRAMIENTAS DE HARDWARE:	18
6 REFERENCIAS	18

INTRODUCCIÓN

El tema de la **Informática Forense** fue expuesto en el Boletín de Seguridad Informática de septiembre de 2003 publicado por la Asociación Bancaria, el cual se define como la aplicación de técnicas y herramientas de hardware y software orientados a analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

En dicho boletín se menciona la variedad de aplicaciones de la informática forense dado el creciente uso de la tecnología en la operación cotidiana de las empresas de los diversos sectores, entre ellos por su supuesto, el financiero.

Por lo anterior y teniendo presente aspectos ya mencionados en el boletín, tales como: principios para el manejo, recolección y recuperación de evidencia digital, herramientas para la investigación forense, pasos para el estudio forense y las dificultades que podría tener el investigador forense, en este documento trataremos lo que podría ser en la práctica una investigación forense de un caso en el sector financiero tomando como ejemplo una transacción típica de la operación bancaria.

1. GENERALIDADES.

En la investigación forense existe una gran debilidad: frente a la evidencia documental, la evidencia digital es frágil, dado que la copia de un documento almacenado en un archivo es idéntica al original. Asimismo, existe el riesgo potencial de realizar copias no autorizadas del archivo original sin que quede evidencia de dicha acción. Por lo anterior, en este tipo de investigaciones se deben cumplir con los principios que citamos a continuación:

Principios para el manejo, recolección y recuperación de evidencia digital.

- a. Durante el proceso de recolección de evidencia digital, la evidencia no debe sufrir ningún cambio.
- b. Cuando se requiere que una persona tenga acceso a evidencia digital original, dicha persona debe ser un profesional forense.
- c. Toda actividad referente a la recolección, el acceso, el almacenamiento o la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para revisión.
- d. Mientras la evidencia digital esté en poder de un individuo, éste será totalmente responsable de las acciones tomadas con la misma.
- e. Cualquier entidad que sea responsable de recolectar, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.
- f. Durante todo el proceso de recolección de evidencia digital, debe haber testigos que certifiquen los procedimientos efectuados.
- g. En cuanto al proceso de recuperación, se debe cumplir como mínimo con 4 aspectos fundamentales: capacidad para brindar confianza en cuanto a la integridad de la evidencia, uso de un lenguaje sencillo, aplicabilidad a toda la evidencia forense y ser consistente con todos los sistemas legales.

En lo referente a las **herramientas para la investigación forense** (ver Herramientas de la Información Forense), existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas. Existen para la recolección de evidencia (las de mayor importancia en la computación forense), para el monitoreo o control de computadores, para el marcado de documentos y de hardware (dispositivos físicos para la recolección de evidencia).

Ahora, toda investigación forense en términos generales involucra como mínimo para su desarrollo **cuatro pasos** que enunciamos a continuación y explicamos con mayor detalle en secciones posteriores:

- a. Preparación y conocimiento general.
- b. Recolección y manipulación.
- c. Inspección y análisis de la evidencia.
- d. Reconstrucción de los hechos.

Finalmente, en cuanto las **dificultades** que podría tener el investigador forense, se relacionan con factores como su habilidad, experiencia, carencia de herramientas especializadas, deficientes o inexistentes rastros de auditoría o resistencia por parte de algunos funcionarios de la entidad para la entrega o dar acceso a la información de la entidad (en la exposición del caso, se presenta de manera práctica esta problemática)

2 CASO HIPOTÉTICO: CANCELACIÓN FRAUDULENTO DE UN CREDITO

En términos generales, todas las entidades financieras ofrecen dentro de sus servicios productos de captaciones (depósitos) y colocaciones (crédito) y para cada una de ellas implementan transacciones mediante las cuales los clientes y el banco afectan dichos productos. Para este ejemplo tomaremos el producto colocaciones en donde de manera irregular se realiza una transacción de cancelación (pago total) de un crédito y el caso hipotético planteado sería el siguiente:

En una entidad financiera “X”, existen indicios que se está planeando o que se estarían realizando transacciones fraudulentas de cancelación de créditos. A continuación se presenta, lo que podría ser la secuencia de actividades para llevar a cabo la investigación forense

2.1 PASOS PARA EL ESTUDIO DEL CASO DE INVESTIGACIÓN FORENSE

2.1.1 Conocimiento general y levantamiento de información

Ante tal situación lo primero que debe conocer el investigador son los aspectos básicos del ambiente informático de la entidad, esto es: los canales (oficinas, centros operativos, Internet, audiorespuesta, puntos de autoservicio, otros) desde los cuales es posible realizar transacciones de pago a créditos, plataforma del sistema sobre la cual se procesa el crédito, controles de acceso para la autenticación de los usuarios ante dicho sistema, rastro o pistas de auditoría de los accesos al sistema y su respectivo respaldo y los procedimientos para el control de cambios a los programas.

2.1.2 Recolección de evidencia

Luego que se cuenta con la información del ambiente informático de la entidad y con miras a delimitar el sitio desde el cual se realizaron o realizarían las transacciones fraudulentas, se analizan los diferentes puntos desde los cuales es posible realizar transacciones de pago a créditos pudiendo llegar al siguiente resultado:

Las transacciones que se realizan por medios como Internet, audio respuesta o punto de autoservicio, requieren de claves asignadas a los clientes y dichas operaciones son con cargo a cuenta. Por estos canales sería menos probable la realización fraudulenta de transacciones ya que existiría la clave del cliente, prematrícula de obligaciones (créditos) y cuentas; además que habrían límites en

los montos diarios, lo cual dificultaría la cancelación total de un crédito, que es el caso en estudio.

Quedan entonces por analizar el canal oficinas y los centros operativos. En las oficinas sería el canal más común de donde se originarían transacciones de cancelación de créditos, los cuales cruzan con efectivo, cheque o cargo a cuenta. Al realizarse una transacción fraudulenta desde este canal lo más probable es que se detectara en el cuadro diario, ya sea, por su cuantía y por el tipo de pago con el que se realizaría.

Se detecta que en los centros operativos cuentan con opciones de acceso al sistema para la cancelación de créditos. Estos accesos se pueden usar para la realización de ajustes contables que bien podrían prestarse para realizar cancelaciones de carácter fraudulento y no ser detectadas oportunamente.

En este punto ya el investigador forense orientará su investigación al centro operativo y deberá realizar el siguiente levantamiento de información:

- Identificar los usuarios con acceso a la opción de cancelación de créditos.
- Por cada usuario extraer las transacciones de cancelación de crédito realizadas (pago total del crédito). En este caso tener en cuenta aspectos tales como: periodo a analizar (meses atrás) y montos (cancelaciones de créditos superiores a un valor determinado). Lo anterior con miras a agilizar el análisis, ya que en caso de no encontrar transacciones sospechosas se ampliaría el rango de búsqueda y se disminuirían los valores.

2.1.3 Análisis de la evidencia

Para el caso que nos ocupa, supongamos que encontramos una cancelación total de un préstamo por un valor importante (varios millones de pesos). Se revisan los

logs de auditoría y se determina fecha, hora y usuario que efectuó la transacción verificando que efectivamente lo realizó un funcionario del centro operativo. Sin embargo, para corroborar si la transacción se originó o no inicialmente en una oficina y que la transacción en el centro operativo podría obedecer a algún tipo de ajuste, se solicita y analizan los logs de la oficina sin encontrar evidencia alguna de dicha transacción, lo que evidencia que se está ante un fraude.

Se revisa el microcomputador del funcionario implicado y no se encuentra información relacionada con el crédito en mención o de otros sobre los cuales pudieran parecer sospechosos. Toda la información allí contenida, está relacionada con las actividades que por su labor normal realiza.

2.1.4 Presentación de los hechos

Una vez analizada y organizada la evidencia, el investigador pone en conocimiento de los hechos a la entidad (contacta al área de seguridad bancaria, auditoría de sistemas y área jurídica), se coordina la citación al funcionario implicado, se entrevista y se le muestran las pruebas obtenidas del sistema. Inicialmente el funcionario podría manifestar desconocer la realización de la transacción fraudulenta argumentando que ese día no se encontraba laborando y que era posible le hayan conocido su clave de acceso (aunque esto no lo eximiría de su responsabilidad), pero se le desvirtúa su argumento mostrándole el registro de entrada al sitio de trabajo (ingreso con tarjeta) y además cuando se estableció comunicación con el dueño del crédito afectado, éste mencionó que dicho funcionario lo había contactado y que por una suma muy inferior al valor del crédito el funcionario le realizaría el pago total (cancelación).

Ante las evidencias, al funcionario no le queda más que aceptar su culpabilidad y en ese momento se le solicita relatar los hechos y que deje constancia por escrito de

los mismos (esto en ocasiones podría no darse ya que el funcionario podría negarse y solicitar la presencia de un abogado para que lo asesore)

2.1.5 Generación de informe

Luego de contar con la evidencia necesaria y en lo posible con la confesión escrita del funcionario, el investigador forense deberá elaborar un informe para la entidad (seguridad bancaria, área jurídica, recursos humanos, etc.) donde se detallen claramente los hechos de manera cronológica y el análisis de la evidencia encontrada con los soportes que incriminan al funcionario.

Con la anterior información, la entidad podrá retirar por justa causa al funcionario y pondrá el caso a disposición de la unidad de Delitos Informáticos del DAS, para su respectivo trámite.

2.2 CONCLUSIONES

Para el éxito de una investigación forense ya sea que se busque el procesamiento judicial del implicado o una compensación por los daños causados y tomando como base el ejemplo citado con anterioridad, el investigador debe tener presente lo siguiente:

- La investigación no puede limitarse solamente al microcomputador desde donde se efectuó la transacción fraudulenta. Si bien los discos duros de los microcomputadores son una fuente importante de información, en una investigación a fondo de un incidente informático se requiere que el investigador determine fechas, horas de ingreso y actividades realizadas en los diferentes sistemas, información que no se encuentra en el microcomputador del sospechoso.
- Se debe tener un conocimiento básico de la arquitectura tecnológica del sistema de Información de la entidad.
- Conocer los canales y el flujo del proceso de las operaciones motivo de la investigación.

- Manejo cuidadoso de la evidencia, de tal forma que se garantice que esta no sufra ningún cambio.
- Conocer los diferentes rastros de auditoría que dejan las transacciones y tener habilidad para analizarlos.
- La entidad debe tener políticas mediante las cuales los empleados tengan claros que los elementos informáticos son del banco y que por consiguiente está en libertad de inspeccionarlos en cualquier momento.

Por ultimo, aquí presentamos solo una de las numerosas situaciones en la que la informática forense es útil en nuestro medio. La razón como ya lo vimos, era no limitar el análisis a los aspectos puramente técnicos, sino todos los procedimientos y en general el medio ambiente técnico y operativo en el que se presenta un evento. Otra situación que constituye un riesgo para las entidades financieras es el riesgo de revelación no autorizada o fuga de información, pues las herramientas de informática forense permiten reconstruir muchas de las actividades que haya ejecutado un usuario en su computador personal, lo que incluye copia en diferentes medios y borrado de archivos. Así pues, se podría hacer una larga lista de aplicaciones en el sector financiero, pero el propósito es más dejar unas bases y generar inquietudes que permitan avanzar en el tema.

3 DIFICULTADES QUE SE LE PODRIAN PRESENTAR AL INVESTIGADOR FORENSE:

- No contar con los registros de auditoría. Esto puede suceder, porque el aplicativo no los tiene implementados o si los tiene, están desactivados (la entidad podría justificar que los logs están degradando la máquina).
- Registros incompletos o no claros de las pistas de auditoría. Esto ocurre porque solo se graban algunos campos para no cargar el sistema o no existen descripciones detalladas de los logs.
- No se realiza un buen levantamiento de información de la arquitectura del sistema y se dificulta determinar la forma y quién realizó la transacción fraudulenta.
- Poca habilidad en el manejo de las herramientas.

- Resistencia por parte de los funcionarios para suministrar información porque no les agrada ser investigados o porque podrían estar relacionados con el ilícito.
- Restricción de acceso a la información de la entidad. Si se cuenta con el conocimiento y las herramientas necesarias, los funcionarios de seguridad informática y/o auditoría de sistemas de la entidad podrían adelantar la investigación forense y no habría mayor dificultad en el acceso a la información; pero si se requiere que por la especialización del tema lo realice un tercero, éste investigador deberá trabajar de manera estrecha con las áreas de seguridad bancaria, jurídica y la auditoría de sistemas.

4 VALORES AGREGADOS DE LA INFORMATICA FORENSE

Si bien se menciona que la informática forense es una de las herramientas que se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial, el resultado de una investigación forense también puede determinar oportunidades de mejoramiento en los controles de los procesos de la entidad, ya que el caso investigado pudo haberse facilitado por algunas debilidades de control.

Siguiendo con el caso de ejemplo trabajado, las siguientes serían algunas medidas de control a implementar:

- Revisar, evaluar y reducir al mínimo necesario el número de funcionarios con acceso a transacciones de cancelación de créditos en el centro operativo.
- Implementar la doble intervención (supervisión) en la realización de las transacciones de cancelación de crédito.
- Segregación de funciones entre los funcionarios que realizan los ajustes al sistema y los que realizan el cuadro contable.
- Monitoreo periódico de las transacciones de cancelación de créditos.
- Clarificar y detallar la funciones de las personas que laboran en el centro operativo.
- Reiterar a los funcionarios las normas sobre el manejo de las claves de acceso al sistema.

5 HERRAMIENTAS DE INFORMACIÓN FORENSE

En los últimos dos años se ha disparado el número de herramientas para computación forense, es posible encontrar desde las más sencillas y económicas, como programas de menos de US\$300,00 cuyas prestaciones habitualmente son muy limitadas, hasta herramientas muy sofisticadas que incluyen tanto software como dispositivos de hardware. Otra situación que se ha venido presentando es el uso de herramientas tradicionales como los utilitarios.

Con esa amplia gama de alternativas, si está pensando en adquirir una herramienta para computación forense, es necesario tener claro primero que todo el objetivo que persigue, pues existen varios tipos básicos de herramientas, no todos los productos sirven para todo, algunos están diseñados para tareas muy específicas y más aún, diseñados para trabajar sobre ambientes muy específicos, como determinado sistema operativo.

Siendo la recolección de evidencia una de las tareas más críticas, donde asegurar la integridad de esta es fundamental, es necesario establecer ese nivel de integridad esperado, pues algunas herramientas no permiten asegurar que la evidencia recogida corresponda exactamente a la original. Igual de importante es que durante la recolección de la evidencia se mantenga inalterada la escena del “crimen”

Son todas estas consideraciones que se deben tener en cuenta a la hora de seleccionar una herramienta para este tipo de actividad, claro, además de las normales en cualquier caso de adquisición de tecnología, como presupuesto, soporte, capacitación, idoneidad del proveedor, etc. De hecho una de las alternativas que siempre se deberá evaluar es si incurrir en una inversión de este tipo a la que muy seguramente se tendrá que adicionarle el valor de la capacitación que en algunos casos puede superar el costo mismo del producto, o, contratar una firma especializada para esta tarea, que generalmente cuentan no con una sino con varias herramientas.

En esta parte se presenta una clasificación que agrupa en cuatro los tipos de herramientas de computación forense, se hace mención a algunos productos sin pretender en ningún momento dar una calificación, de igual manera la omisión de alguno no significa desaprobación.

5.1 Herramientas para la recolección de evidencia.[1]

Las herramientas para la recolección de evidencia representan el tipo de herramienta más importante en la computación forense, porque su centro de acción está en el que para muchos es el punto central. Su uso es necesario por varias razones:

- Gran volumen de datos que almacenan los computadores actuales.
- Variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- Necesidad de recopilar la información de una manera exacta, que permita verificar que la copia es fiel y además mantener inalterada la escena del delito.
- Limitaciones de tiempo para analizar toda la información.
- Volatilidad de la información almacenada en los computadores, alta vulnerabilidad al borrado, con una sola información se pueden eliminar hasta varios gigabytes.
- Empleo de mecanismos de encriptación, o de contraseñas.
- Diferentes medios de almacenamiento, como discos duros, CDs y cintas.

Por esto mismo, las herramientas de recolección de evidencia deben reunir características que permitan manejar estos aspectos, pero además incluir facilidades para el análisis. A continuación se presentan las principales facilidades de recolección y análisis que se esperaría de una buena herramienta, para lo cual se siguió como guía las que ofrecen EnCase de Guidance Software y la familia de productos Image Master de Law Enforcement & Comp. Forensic:

- Dispositivos que permitan copiado a una alta velocidad y de diferentes medios, claro, limitado eso si por el medio original de los datos, esto brindando diferentes tipos de dispositivos como cables paralelos, seriales, USB, etc.
- Asegurar un copiado sin pérdida de datos y que corresponde a una copia fiel.
- Copia comprimida de discos origen para facilitar el manejo y conservación de grandes volúmenes de información. Muy practico además cuando se deben manejar investigaciones de varias computadoras o varios casos a la vez.
- Búsqueda y análisis de múltiples partes de archivos adquiridos. Debe permitir la búsqueda y análisis de múltiples partes de la evidencia en forma paralela en diferentes medios como discos duros, discos extraíbles, discos “zip” CDs y otros.
- Capacidad de almacenamiento en varios medios: También es necesario poder almacenar la información recabada en diferentes medios, como discos duros IDE o SCSI, drives ZIP, y Jazz. Uno de los medios ideales son los CD-ROM pues contribuyen a mantener intacta la integridad forense de los archivos.
- Variables de ordenamiento y búsqueda: debe permitir el ordenamiento y búsqueda de los archivos de la evidencia de acuerdo con 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, extensiones y propiedades.
- Capacidad para visualización de archivos en diferentes formatos, además de galerías de archivos gráficos.
- Capacidad para representar en forma gráfica estructuras de datos, archivos, volúmenes, directorios, árboles, organización y en general tópicos de interés que faciliten el trabajo de análisis.
- Búsqueda automática y análisis de archivos de tipo Zip, Cab, Rar, Arj y en general formatos comprimidos, así como archivos adjuntos de correos electrónicos.
- Identificación y análisis de firmas de archivos, es decir aquellos bytes que generalmente se encuentran al comienzo de un archivo y están directamente relacionadas con el tipo de este y por consiguiente con su extensión. Con la capacidad de análisis de firmas es posible detectar si un archivo fue renombrado, pues el solo cambio de su extensión para hacerlo aparecer de otro tipo, no genera cambios en su firma.

- Análisis electrónico del rastro de intervención. Facilidades para recuperar de manera eficiente y no invasiva información crítica como sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento
- Soporte de múltiples sistemas de archivo. Una herramienta de recopilación de evidencia debe estar en capacidad de recuperar información de diversos sistemas de archivos; DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVDR. Esta es la limitación de algunas herramientas, pues está diseñadas para un número limitado de sistemas de archivos o es necesario adquirir módulos aparte, lo que incrementa su costo.
- Captura y manejo automático de cualquier sistema operativo: reconocimiento automático del sistema operativo origen, haciendo cero invasiva la extracción de la información y asegurando la más alta fidelidad.
- Vista de archivos y otros datos en el espacio unallocated: Una buena herramienta deberá proveer facilidades para tener una vista del disco duro de origen, de los archivos borrados y todos los datos en el espacio unallocated, el espacio ocupado por el archivo dentro del cluster, archivos Swap y Print Spooler, todo esto de manera gráfica.
- Recuperación de passwords: en muchas ocasiones la información recuperada puede estar protegida con passwords por lo que será necesario descifrarlos. Generalmente esta facilidad no viene incluida en estas herramientas, se deben comprar a parte.
- Herramientas de gestión; por último una herramienta debería incluir facilidades de gestión para el manejo mismo de los expedientes y reportes de las investigaciones.

A continuación se relacionan algunas herramientas de este tipo, aunque no necesariamente reúnen todas las características mencionadas en este documento:

- ByteBack - Tech Assist, Inc: Copia de discos duros de cualquier formato, transferencia a otros medios internos o externos, sistema de análisis binario para recuperación no destructiva de particiones y sectores de arranque tipo FAT y NTFS (NT) búsqueda binaria, md5 hash integrado, solución multi ambiente, acceso directo, diagnóstico de superficie, control de bajo nivel de hardware. Disponible versión de prueba en www.toolsthatwork.com

- The AccessData Forensic Toolkit: reconocimiento de 270 formatos, explorador gráfico, generación de logs y reportes de casos, recuperación de passwords, indexación por texto, búsqueda avanzada de imágenes JPEG y texto de internet, patrones binarios para búsqueda, recuperación automática de de archivos y particiones borradas, creación personalizada de filtros de archivos, sistemas de archivo soportados NTFS, NTFS compressed, FAT 12/16/32, y Linux ext2 & ext3, análisis de archivos de correo electrónico y Zip, identificación de firmas de archivos de sistemas operativos estándar y programas de archivos.
- Data Recovery Kit - LC Techonogy: Suite compuesta por Filerecovery for windows, Filerecovery professional, y Photorecovery.
- Maresware - Mares and Company Computer Forensics consiste en un conjunto de programas para investigación de registros de computador, Incluye herramientas para respuesta a incidentes y ataques, descubrimiento de secretos y evidencia computacional, documentación de los procedimientos, preparación de reportes de hallazgos y de documentos para uso legal. Data Analysis: Programa para la extracción, validación y análisis de datos de diferentes fuentes.
- Paraben Forensic Toll - Paraben Computer Forensic Software: Herramienta de computación forense diseñada para PDAs y PC Pockets.
- SafeBack - New Technologies Inc: Permite hacer copias espejo de archivos de backups o de discos duros completos, para creación de evidencia en sistemas de computador basados en Intel, transferencia de información a otros medios y preservación de evidencia.

Existen otros productos tradicionales cuyo objetivo primordial no es la computación forense, pero por incluir herramientas para la recuperación de archivos, en ocasiones pueden ser útiles, aunque la integridad de la evidencia recabada a través de estas herramientas podría estar mas expuesta y su valor probatorio podría ser menor que el de evidencias obtenidas a través de herramientas altamente especializadas que garantizan la veracidad de la evidencia. Ejemplo típico de herramientas no propiamente forenses es Norton Systemworks y Norton Utilities.

5.2 Herramientas para el monitoreo y/o control de computadores [1]:

Si se requiere conocer el uso de los computadores es necesario contar con herramientas que los monitoreen para recolectar información. Existen herramientas que permiten recolectar desde las pulsaciones de teclado hasta imágenes de las pantallas que son visualizadas por los usuarios y otras donde las máquinas son controladas remotamente. 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. Estas herramientas pueden ser útiles cuando se quiere comprobar actividad sospechosa ya que guardan 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 otras que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.

Es importante tener en cuenta que herramientas de este tipo han llegado a ser usadas con fines fraudulentos (captura de claves de los clientes en cafés Internet u otros sitios públicos). Se han detectado instalaciones remotas de sencillos programas que registran toda la actividad del usuario en el teclado, esta es almacenada en un archivo que es obtenido de forma remota por el perpetrador. El uso de estas herramientas debe estar plenamente autorizada y un investigador no debería tomar el solo la decisión de su uso.

5.3 Herramientas de marcado de documentos:

El objetivo de este tipo de herramientas es el de insertar una marca a la información sensible para poder detectar el robo o tráfico con la misma, si bien no equivale al sistema LoJack de rastreo y localización de vehículos hurtados, si podría compararse con las marcas que se hace a los vehículos. A través de estas herramientas es posible marcar no solo documentos, sino software también.

5.4 Herramientas de Hardware:

El proceso de recolección de evidencia debe ser lo menos invasivo posible con el objeto de no modificar la información. Esto ha dado origen al desarrollo de herramientas que incluyen dispositivos como conectores, unidades de grabación, etc. Es el caso de herramientas como DIBS "Portable Evidence Recovery Unit" y una serie de herramientas de Intelligent Computer Solutions; LinkMASSter Forensic Soft Case, LinkMASSter Forensic Hard Case, Image MASSter Solo 2 Forensic Kit With Hard Case.

Asimismo, debido a la vulnerabilidad de la copia y modificación de los documentos almacenados en archivos magnéticos, los investigadores deben revisar con frecuencia que sus copias son exactas a las del disco del sospechoso y para esto utilizan varias tecnologías como checksums o Hash MD5.

6 REFERENCIAS .

[1] INFORMÁTICA FORENSE: GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS

Autores : Óscar López, Haver Amaya, Ricardo León; Coautora : Beatriz Acosta; Universidad de Los Andes, Bogotá, Colombia.

[2] <http://www.securitymanagement.com/library/001348.html>

[3] <http://www.virusprot.com/Col12.html>

