Pasos a seguir para la recolección de evidencias

Mayta Cosme Marybel
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
lebyram_111@hotmail.com

RESUMEN

En este trabajo trataremos los pasos necesarios que un experto forense debe realizar para efectuar la recolección de evidencias y las recomendaciones que urge los cuidados necesarios para evitar cualquier tipo de pérdida por mínima que sea.

Palabras Clave

Recolección, evidencia, dispositivos electrónicos, perito informático.

1. INTRODUCCIÓN

El proceso de investigar dispositivos electrónicos o computadora es para descubrir y analizar información que se encuentran en estos, puede encontrarse de forma suprimida, u ocultada aun así sirve como evidencia en un asunto legal. Es Igualmente provechosa cuando se han perdido accidentalmente datos debido a fallas.

Conforme ha pasado el tiempo la tecnología informática se ha ido convirtiendo rápidamente en un instrumento universal, y así siendo utilizado tanto para vulnerar las normas como para perseguir a quien las vulnera. Incluso en delitos para cuya comisión no se ha utilizado ninguna herramienta informática, en ocasiones se pueden encontrar evidencias informáticas que pueden resultar vitales.

La Informatica Forense es aplicada en la recolección de evidencia digital para casos de delitos informáticos y las utiliza para demostrar algún tipo de delito en caso de que existiera, tambien para otro tipo de crimenes usando técnicas y tecnologías avanzadas. Un experto en informática forense utilizaría algunas de estas técnicas para descubrir evidencia de un dispositivo de almacenaje electrónico. Los datos pueden estar en cualquier clase de dispositivo informático como discos duros, cintas de respaldo, computadores portatiles, memorias extraibles, archivos y correos electronicos.

La ocupación del Perito Informático es la valoración de dichas evidencias, este perito dará como resultado el informe o dictamen pericial, que a su vez se constituye las evidencias recogidas como pruebas, llegado el momento del juicio. Sin embargo, la labor del perito no es fácil y no suele comenzar con las evidencias en la mano listas para ser estudiadas. Todas las fases del trabajo del Perito son importantes, y mucho más delicada es la fase de obtención de evidencias. En la informática todo lo que se hace deja algún tipo de huella, como decía el principio de intercambio de Locard que se puede resumir en que “cada contacto deja un rastro”. Este hecho es una gran ventaja para el investigador, también implica una gran dificultad y requiere la máxima profesionalidad y cuidado. Cualquier mal paso en la identificación y recogida de evidencias puede alterar la información obtenida, y con ello invalidar todo el trabajo.

Los pasos fundamentales al momento de aplicar informática forense son: identificación, recogida de evidencias, Registro de actuaciones, identificación del tipo de evidencia. Todos estos deben cumplir con ciertos requisitos para tener valor probatorio y no quedarse sólo como indicio. Mucho del valor probatorio de la evidencia digital recae en los pentavalores de la seguridad: confidencialidad, disponibilidad, autenticidad, integridad y no repudio.

2. COMENZANDO CON LA IDENTIFICACIÓN

El primer paso para realizar el proceso de recolección de la evidencia forense es la identificación. Generalmente el objeto de estudio de la informática forense son únicamente los ordenadores, y específicamente los datos que se encuentran en ellos. En realidad puede encontrarse información muy útil en muchos dispositivos: CDs, memorias de todo tipo, MP3, teléfonos móviles, PDAs, tarjetas SIM, routers y otros elementos de red, impresoras, fotocopiadoras, faxes, bandas magnéticas, cintas de audio/video, etc.

El mayor aliado de un Perito Informático son los logs o registros de eventos. Tenemos los logs del Sistema Operativo, los de muchos programas, los Spools de las impresoras, los ficheros de paginación, los ficheros temporales, las cookies del navegador, los volcados de errores (memory dumps), incluso la papelera de reciclaje… y eso sólo en un ordenador. Pero muchos otros dispositivos tienen un sistema operativo más o menos complejo, con su propios logs, etc. En general, cualquier dispositivo informatico que tenga memoria contiene rastros de información que haya pasado por él aunque ya haya sido eliminado no se debe descartar esa información.

La cantidad de información a recolectar puede ser enorme. Hay que identificar lo que puede ser relevante y admisible. Siempre es recomendable recoger en exceso que quedarse cortos.

Una vez que identificamos los dispositivos en los que

Figura 1. Computadores como evidencia o portadores de evidencia

podríamos encontrar información útil, el tipo de información, y el formato en el que podría estar almacenada, es fundamental lo que hacernos con las herramientas adecuadas para recuperarla.

Se debe decidir también el orden en el que se va a recoger las evidencias, es recomendable seguir el orden de volatilidad de las mismas. Primero tenemos que asegurar las que puedan ser más volátiles, como puede ser todo aquello que esté en la memoria del equipo, caché, estadísticas, etc. Si el equipo está encendido hay mucha información que se perderá en cuanto se apague. Pero también habrá mucha información que se irá corrompiendo con el tiempo que el equipo permanezca encendido. Esta es la primera de muchas decisiones difíciles que se pueden presentar en el proceso.

A continuación nos encontramos con otro problema fundamental en esta parte del trabajo. Idealmente no deberíamos estudiar la información directamente en su ubicación original. Aunque no siempre es posible o rentable, debemos trabajar sobre copias forenses de la información. Entendemos por copia forense aquella en cuya realización se cumplen dos objetivos fundamentales para la validez del estudio:

1. El origen de la información no ha sido alterado en el proceso de copia o clonación.

2. El resultado es, en los términos que interesan en cada caso, una copia exacta de la evidencia.

Cuanto más sutil sea el rastro a seguir, o mayores hayan sido los esfuerzos por encubrirlo, más esmero será necesario dedicar en este momento, pues cualquier corrupción de los datos puede dar lugar a que la evidencia se pierda o aparezcan "falsos positivos".

Evidentemente, el destino de la copia debe estar previamente vacío. Y un formateo no es suficiente. En el caso del clonado de una memoria o un disco, la mejor forma de asegurarse es que el destino sea una memoria o un disco nuevos. Y si se trata de un tema delicado, lo mejor es sacarlo de su paquete ante testigos. También puede ser útil en este momento realizar más de una copia, pues más adelante podríamos no tener esa oportunidad.

Las herramientas utilizadas para el clonado también son importantes. Se debe buscar siempre herramientas que impidan la escritura en los medios originales (lectores de tarjetas con la escritura deshabilitada, bloqueadores de buses, etc). También debemos seleccionar herramientas que hagan una copia completa bit a bit, es decir, al más bajo nivel posible.

4. REGISTRO DE ACTUACIONES

Durante todo el proceso pericial, no solamente en la fase de recogida de evidencias, hay que llevar un registro completo de todos los pasos que damos. Si además podemos tener testigos, grabaciones, fotos, videos… mejor. No hay nada peor que llegar a la vista y no poder explicar alguna de nuestras conclusiones porque alguno de los pasos que nos llevaron a ella no está documentado. Es importante tomar nota de todo: fechas y horas, personas presentes, cómo nos encontramos todo, lo que hacemos, por qué lo hacemos, cómo y con qué lo hacemos.

5. IDENTIFICACIÓN DEL TIPO DE EVIDENCIA

Para continuar con el laboratorio se hace necesario identificar el tipo de evidencia analizar. Pues aún no se tiene información sobre la misma (bien podría tratarse de una imagen de disco, partición u otro tipo de imagen).

Para este propósito bastará, con analizar los primeros bytes de la imagen con un editor hexadecimal.

Además se debe ver el procedimiento para determinar el Sistema Operativo de la imágen a analizar.

Para ello se verá un caso con la solución para Análisis Forense conocida como (Interfaz gráfico para).

 es un conjunto de herramientas en línea de comandos, desarrolladas en y que permiten llevar a cabo Análisis Forenses a sistemas computacionales. Ambas herramientas (The Sleuth Kit y su interfaz web Autopsy) son de libre uso y libre distribución.

Al igual que para las tareas de y existe una distribución favorita conocida como , para las labores relacionadas con la Informática Forense existe otra favorita bajo el nombre de , la cual incluye un completo Set de utilidades que nos facilitan la vida para este tipo de trabajos.

Cabe aclarar que está no es la única manera de identificar el Sistema Operativo, pues en varias publicaciones se puede ver

diferentes métodos.

El artículo tiene un breve resumen de los detalles, sin embargo se debe considerar otras opciones de clonacion, phishing, pharming e incluso manipulacion informatica en los mismos bancos o en su defecto en los administradores de tarjetas. Las opciones son varias y se han dado casos en todas partes del mundo. Por otro lado no es suficiente que los bancos se deslinden de la responsabilidad culpando al cliente por no cuidar su tarjeta y su PIN. Vemos que esa es la opcion mas comoda tanto para las entidades financieras como para las entidades de regulacion. Las medidas son minimas, las campañas de concientizacion igualmente. Esperamos que la Ley actue de manera mas objetiva.

Para finalizar comentamos una guía de prácticas que pueden resultar útiles para la recolección de evidencias.

El objetivo de esta fase en el ciclo de vida de administración de la evidencia digital es

localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales (aquellos disponibles y asegurados en las máquinas o dispositivos) no han sido

alterados. Para ello el estándar establece algunos elementos a considerar como:

- Establecer buenas prácticas y estándares para recolección de evidencia digital
- Preparar las evidencias para ser utilizadas en la actualidad y en tiempo futuro
- Mantener y verificar la cadena de custodia
- Respetar y validar las regulaciones y normativas alrededor de la recolección de la evidencia digital
- Desarrollar criterios para establecer la relevancia o no de la evidencia recolectada.

Prácticas recomendadas son:

1. Establecer un criterio de recolección de evidencia digital según su volatibilidad:

de la más volátil a la menos volátil.

- Registros de memoria, memoria cache
- Tablas de enrutamiento, cache de arp, estadísticas del funcionamiento del sistema operacional.
- Archivos temporales
- Almacenamiento en diskettes, memorias USB, CD, DVD.
- Registro remoto de las actividades de la aplicación y monitoreo del tráfico de los datos
- Configuración física de dispositivos y topología de red.
- Manuales y registros disponibles de los dispositivos y software bajo estudio.

2. Documentar todas las actividades que el profesional a cargo de la recolección ha efectuado durante el proceso de tal manera que se pueda auditar el proceso en sí

mismo y se cuente con la evidencia de este proceso.

3. Asegurar el área dónde ocurrió el siniestro, con el fin de custodiar el área o escena

del delito y así fortalecer la cadena de custodia y recolección de la evidencia.

4. Registrar en medio fotográfico o video la escena del posible ilícito, detallando los

elementos informáticos allí involucrados.

5. Levantar un mapa o diagrama de conexiones de los elementos informáticos

involucrados, los cuales deberán ser parte del reporte del levantamiento de

información en la escena del posible ilícito.

6. CONCLUSIONES

Al cabo de este trabajo llegamos a la conclusión que la informática forense debe regirse bajo un fundamento sistemático riguroso para proceder de manera tal que la recolección de evidencias tengan el efecto deseado para respaldar una conjetura que podría significar ganar un caso judicial o perderlo.

7. REFERENCIAS

[1]http://www.sticc.com/articulos/ver.aspx?Id=35

[2]http://labs.dragonjar.org/informatica-forense-identificacion-del-tipo-de-evidencia

[3]http://www.edicionesespeciales.elmercurio.co Catalina Correia C.

[4]http://gecti.uniandes.edu.co/docs/buenas%20practica%20evidencia%20digital%20jcano.pdf "Buenas prácticas en la administración de evidencia digital"