Cyber Forensics:

Una Perspectiva de Operaciones Militar

Autores: Joseph Giordano (Technical Advisor, AFRL Information Warfare Branch)
Chester Maciag (Program Manager, AFRL Digital Forensics Program)

Visión General:

En este paper se discute algunos de los requerimientos y desafios militares en el contexto del "Cyber Forensics".. Presenta una definición de Cyber Forensics en el contexto militar. Se comenta las capacidades necesarias para el desempeño de análisis forence en un ambiente intercopnectado por una red. Para finalizar se presenta una manera en la cual las tecnologías pueden ser utilizadas en el entorno legal, así como en la industria.

La manera común en que se ve la disciplina de Análisis Forence está relacionada con el mundo legal, en donde la mayor parte del esfuerzo ha sido dedicado al estudio y creación de herramientas que asistan el trabajo de la policia, orientado principalmente al proceso "post-mortem", más que a un análisis en línea.

Mientras que el término "Cyber Forensics" se presenta como relativamente nuevo en el área militar (en Estados Unidos), el término "análisis forence de sistemas computacionales" tiene sus raíces en los primeros días de los sistemas de detección de intrusos. La protección de los sistemas militares requiere de asistencia y análisis en tiempo real ante un ciber ataque, sin el beneficio común de poder poner en cuarentena o retirar el equipo víctima del ataque, como se presenta en el modelo legal. Cabe mencionar que el sistema computacional completo es el objetivo de ataque, y tanto el sistema como sus elementos interconectados son las fuentes primarias de evidencias para una comparación o recontrucción de los eventos ocurridos. Esto requiere de la preservación, recuperación y análisis de la información digital obtenida de un amplio conjunto de dispositivos y aplicaciones de red con el objetivo de detectar y determinar cómo el sistema cayó y realizó las acciones objetivo del adversario. Este mecanismo juega un rol especial en el proceso de toma de decisiones militares, conocido como OODA Loop (Observe, Orient, Decide and Act). La meta de este proceso es entrar en el ciclo OODA del adversario al ir reduciendo de manera continua el tiempo que toma el equipo militar en observar y responder a las acciones del enemigo, logrando sobrepasar las abilidades del enemigo de responder a las acciones propias. Es el proceso de análisis forence lo que dirige la recuperación del sistema luego de ciber ataques, la reacción ante estos. Los militares requieren de un análisis post ataque bajo un rango de tiempo controlado, y si es posible, indicaciones y advertencias anticipadas ante un ciber ataque.

La definición de Análisis Forence militar es:

"La exploración y aplicación de métodos científicamente probados para procesar, interpretar y utilizar evidencia digital con el objeto de":

- Proveer una descripción concluyente de todas las actividades en ciber ataques, con el objetivo de restaurar la información e infraestructura crítica luego de un ataque.
- Correlacionar, interpretar y predecir las acciones del adversario y su impacto en las operaciones militares planeadas.
- Transformar las evidencias digitales en un medio persuasivo disponible y utilizable en un proceso de investigación criminal.

El comandante acargo del problema necesita tener información respecto de lo que está sucediendo para saber quien está atacando antes de tomar cualquier acción que pueda ser vista o tomada como una

violación a algún tratado o acuerdo internacional. El resultado del análisi forense otorga un criterio que puede ser utilizado como justificación de las acciones tomadas por el comandante.

Desafios actuales del Análisis Forense:

Se presenta un conjunto de ítems que representan desafíos del análisis forence de sistemas computacionales:

- No existe un proceso universalmente aceptado en los métodos utilizados para recuperar o interpretar la información digital. Exite un gran número de buenas prácticas, pero estas varían de acuerdo con quienes las utilizan.
- Hay una carencia de estándares para guiar o dirigir el desarrollo de herramientas y tecnología de análisis forense tanto en el área legal como militar.
- Existe una carencia de comunicación y compartición de información entre las comunidades relacionadas con la creación de herramientas y las de desarrollo de tecnologías.
- Las herramientas, tanto comerciales como privadas, ofrecidas están limitadas al análisis post ataque. Esto se debe al modelo legal. Sin embargo, un modelo trans-ataque podría ser aplicado en la construcción de una nueva generación de herramientas tanto para la industria como para el gobierno.
- Las herramientas o conceptos de análisis ofrecidos actualmente no escalan de manera adecuada en ambientes de redes. La mayoria de las herramientas suponen un entorno compuesto por computadores aislados.

Capacidades de Operación Militares Requeridas

Los siguientes requerimientos de capacidades han sido adaptados a partir de la cumbre de Ciberterrorismo en la Universidad de Princeton en 2002.

- Protección de datos: Cuando se encuentra una fuente de información digital candidata, se debe tomar medidas para prevenir que esta información sea destruída.
- Adquisición de Datos: Es la práctica general de transferir datos de un lugar a otro lugar físico en una posición controlada.
- Creación de Imagen: Es la creación de una copia bit a bit de los datos recogidos, con el propósito de proveer una herramienta que pueda ser analizada por un gran número de personas sin temor a corromper las evidencias.
- Extración: Corresponde a la identificación y separación de datos potenicalmente útiles desde el conjunto de datos imagen.
- Interrogación: Es la interrogación de los datos extraídos para determinar si existe indicadores a priori o relaciones entre los datos.
- Normalización: Corresponde al almacenamiento de los datos en un formato o nomenclatura que sea comprensible para los investigadores.
- Análisis: La fusión, correlación, mapeo o timelining de los datos para determinar posibles relaciones al interior de los datos, y desarrollar hopótesis investigativas.
- Reporte: La presentación de los datos analizados en una forma persuasiva y evidente para un investigador o comandante militar.

Un área que representa una gran promesa en el análisis forense en entornos de operaciones militares es “agentes forences inteligentes distribuidos”. Estos agentes serían procesos livianos lanzados desde un agente central o control central cada vez que se detecte un evento sospechoso. Estos agentes podrian recuperar evidencias y luego llevarlas hasta el control central para un análisis posterior mediante otras

herramientas.

Se puede observar la necesidad de un estándar para el desarrollo y prueba de herramientas de análisis forense, se necesita de métricas que establezcan el alcance de una determinada herramienta de software o hardware logra, así como la tasa de error asociada al proceso.

An examination of Digital Forensic Models

Autores:
Mark Reith (Department of Electrical and Computer Engineering)
Clint Carr (Graduate School of Engineering and Management)
Gregg Gunsch (Air Force Institute of Technology)

Este paper explora el desarrollo de procesos forense digitales, se compara y contrasta cuatro metodologías forenses particulares, a partir de las cuales se propone un modelo abstracto de proceso forense. Este modelo intenta superar algunas de las limitaciones de las metodologias estudiadas, con lo que provee las siguientes ventajas: un framework consistente y estandarizado para el desarrollo de herramientas de análisis forense, un mecanismo para aplicar este framework a tecnologías digitales futuras, una metodología generalizada que pueda ser utilizada por miembros judiciales para relatar eventos a observadores no técnicos, y el potencial para incorporar tecnologias no digitales dentro de la abstracción.

La incorporación de los sistemas computacionales como herramienta privada, comercial, educacional, gubernamental y muchas otras facetas de la vida moderna ha mejorado la productividad y eficiencia de estas entidades. De la misma manera, la introducción de los computadores como herramienta criminal ha mejorado las habilidades de los criminales para cometer los delitos o también asistir actividades ilegales o poco éticas. Cabe mencionar que los Ciber crímenes no son necesariamente nuevos, más bien son crímenes clásicos que explotan el poder computacional y el acceso a la información.

Digital Forensics

Digital forensics es una ciencia relativamente nueva, derivada como sinónimo de computer forensics, esta definición ha sido expandida para incluir todos los dispositivos digitales al análisis forense.

Se define Digital Forensics como el uso de métodos científicamente provados y derivados orientados a la preservación, colección, validación, identificación, análisis, interpretación, documentación y presentación de la evidencia derivada desde fuentes digitales con el propósito de facilitar la posterior reconstrucción de los eventos determinados como criminales, o ayudar a anticipar acciones no autorizadas.

Mientras que la computación forense tiende a enfocarse en métodos para la axtracción de evidencia desde una plataforma particular, el análisis forense digital debe ser modelado de manera tal que pueda incluir todo tipo de dispositivos digitales, incluyendo tecnologias digitales futuras. Desafortunadamente no existe un estándar o metodología consistente, sino que un conjunto de procedimientos y herramientas construidos a partir de la experiencia de investigadores y trabajadores del entorno legal y administradores de sistemas. Gary Palmer sugiere que la evolución del análisis forense digital ha nacido desde técnicas y herramientas ad hoc, más que desde la comunidad científica.

Carencia de estandarización del Análisis Forense Digital.

En muchos de los casos de crímenes digitales, el procedimiento utilizado para su estudio no es ni estándar ni consistente. Un gran número de personas han intentado crear directrices rudimentarias durante los últimos años, pero lo que han propuesto se enfoca en los detalles de la tecnología, sin

considerar un proceso generalizado. Respecto de este problema, D. Farmer y W. Venema construyeron su propio conjunto de herramientas forense, denominados The Coroners Tool Kit (TCT), este conjunto de herramientas asisten a los investigadores en el logro de algunos de los pasos del análisis forense, en primera instancia la sistemática búsqueda de evidencias. Mientras que se orienta en la direccion correcta, este conjunto de procedimientos se enfoca en una plataforma determinada, siendo no muy aropiado como modelo de análisis forense digital.

Otro intento por definir un proceso de análisis forense digital es describido por Mandia y Prosise como metodología de respuesta ante un incidente. Esta metodología es comprendida pos los siguientes pasos: preparación pre incidente, detección de incidente, repuesta inicial, formulación de estrategias de respuestas, duplicación, investigación, implementación de medidas de seguridad, monitoreo de la red, recuperación, reporte, y seguimiento. Sin embargo su enfoque es púramente asociado a los crímenes computacionales, no haciendo referencia a procesos de análisis forense de otro tipo de dispositivos digitales como teléfonos celulares, dispositivos periféricos o cualquier otro tipo de dispositivos digitales. La preparación pre incidente corresponde al proceso de preparar las herramientas y el equipamiento necesario, así como el continuo estudio de nuevas tecnologías que puedan ser útiles en el tratamiento de nuevos incidentes.

El Departamento de Justicia de Estados Unidos también intenta describir el proceso de computación forense, pero ha realizado el beneficio de abstraerse de tecnologías específicas. Este conjunto de preocesos incluye las faces de: colección, examinación, análisis y reporte. Este modelo identifica de manera significativa los aspectos centrales del proceso forense y construyendo los pasos para soportarlo, más que caer en los detalles de una tecnología o metodología particular. En resumen, el modelo del DOJ (Department Of Justice) no hace distinción entre los métodos forenses aplicados a computadores o algún otro dispositivos electrónicos. En vez de esto, intenta construir un proceso generalizado que será aplicado a la mayoría de los dispositivos electrónicos. La identificación de potenciales tipos de evidencia y las posibles ubicaciones en diferentes tipos de dispositivos es un buen paso para quienes desean desarrollar un porceso generalizado que puede ser instanciado con una tecnología para producir resultados significativos en una corte.

Finalmente, el DFRW (Digital Forensics Research Workshop) es otro participante significativo en el desarrollo de un proceso forense. El único aspecto de DFRW es que es uno de los primeros consorcios a gran escala dirigidos por la academia más que por el mundo legal. Esto es importante ya que ayudará a definir y enfocar la dirección de la comunidad científica hacia los desafíos del análisis forense digital. DFRW ha trabajado para desarrollar un framework que incluya pasos como: preservación, identificación, colección, examinación, análisis, presentación y decisión. Basada en este modelo la comunidad científica podrá en el futuro desarrollar y definir mejor este modelo.

Modelo Propuesto.

A partir de los modelos antes mencionados, se observa un conjunto de pasos que pueden ser definidos de manera más abstracta para producir un modelo independiente de alguna tecnología o tipo de crimen particular. La base de este modelo es determinar los aspectos clave de los protocolos anteriormente mencionados así como también las ideas de mecanismos forenses tradicionales, en particular el protocolo de una investigación de escena del crimen del FBI. Los componentes claves de este modelo se presentan a continuación:

- **Identificación**: reconocer un incidente mediante indicadores y determinar su tipo. Esto no esta incluido dentro del análisis forense, pero es significativo en los siguientes pasos.
- **Preparación**: preparar las herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo.
- **Estrategia de acercamiento**: formular de manera dinámica una estrategia basada en el impacto sobre la tecnología en cuestión. La idea es obtener el máximo de evidencia minimizando el impacto en la víctima.
- **Preservación**: aislar, asegurar y preservar el estado de la evidencia física y digital. Esto incluye evitar que personas usen los dispositivos digitales, o que algún otro dispositivo electromagnético se use dentro de un determinado radio.
- **Colección**: almacenar la escena física y duplicar las evidencias digitales utilizando procedimientos aceptados y estandarizados.
- **Examinación**: búsqueda sistemática en profundidad de evidencia relacionada con el crimen. Se enfoca en identificar y localizar evidencia potencial, posíblemente dentro de lugares no convencionales. Cosntruir documentación detallada para el análisis.
- **Análisis**: determina la significancia de las evidencias, reconstruye los fragmentos de datos y genera conclusiones basadas en las evidencias encontradas. Un detalle del análisis es que puede no requerir grandes habilidades técnicas para su desarrollo, es por esto que una gran cantidad de personas puede trabajar en esta etapa.
- **Presentación**: resume y provee una explicación de las conclusiones. Se puede escribir en términos legales utilizando una terminología abstracta, la que debe hacer referencia a detalles específicos.
- **Regresar la evidencia**: asegurar que la propiedad física y digital sea retornada a su porpietario, así como determinar cómo y cuál evidencia debe ser removida.

Se puede observar que hasta este punto, el tipo de tecnología digital utilizada puede ser definida de manera abstracta. Esto es importante ya que permite una metodología consistente para tratar con el presente, pasado y futuro de los dispositivos digitales en una formabien comprendida y ampliamente aceptada.

Se puede observar la necesidad de subprocesos para definir las diferentes clases de tecnologias digitales consideradas bajo este modelo.

La ventaja de la abstracción lograda dentro de este modelo es que la mayoria de los dispositivos digitales, sena estos sistemas computacionales, PDA's, cámaras digitales o algún otro dispositivo, contine algún tipo de almacenamiento persistente que puede ser utilizado como evidencia potencial.

A continuación se presenta las ventajas y desventajas de este modelo:

Ventajas:
- Crea un framework consistente y estandarizado para el desarrollo del análisis forense digital.
- Presenta un mecanismo para aplicar el mismo framework a tecnologías digitales futuras.
- Presenta una metodología generalizada que puede ser utilizada por los miembros del entorno judicial para relatar incidentes tecnológicos a observadores no técnicos.
- Identifica la necesidad de herramientas dependientes de tecnologías específicas.
- Presenta unpotencial para identificar e incorporar tecnologías no digitales dentro de la abstracción.

Desventajas:

- Las catogorías pueden estar descritas de manera demasiado genéricas para su uso práctico.
- No se presenta un método simple u obvio para probar la validez del modelo.
- Cada subcategoría agregada al modelo lo hace más complejo de usar.

En conclusión se puede observar que el entorno legal (policías, jueces, etc) se encuentran en una carrera continua, y al parecer perpetua, contra los delincuentes para poder matenerse a un mismo nivel o superarlos. Parte de esta carrera incluye el desarrollo de herramientas que posean la habilidad de buscar de manera sistemática dentro de los diferentes dispositivos digitales potenciales evidencias. Mientras más dispositivos digitales se creen, el desarrollo de herramientas debe aumentar para incluir estos nuevos dispositivos. Otro aspecto de esta carrera consiste en el desarrollo de metodologías de análisis forense que incluyan todos los tipos de investigación de escenas de crímenes digitales. La metodología porpuesta debiese ser aplicable a todo tipo de crimen digital, así como también a tipos de crímenes que aún no se han realizado. Muchos de los métodos son simplemente dependientes de la tecnología, el modelo propuesto intenta introducir mejoras a los modelos hasta el momento existentes mediante la intersección de técnicas comunes, mientras resuelve los problemas de otras, para llegar a un modelo suficientemente general.

Computer Forensics-- We've had an incident, who do we get to investigate?

Autor: Karen Ryder (SANS Institute:http://www.sans.org/rr/whitepapers/incident/)

La computación forense es utilizada en investigaciones relacionadas con incidentes en los que se ven incluidos computadores, en donde el incidente es una intrusión a un determinado sistema, fraude interno, o alguien interno a la organización que no respeta las políticas de seguridad impuestas. Decidir qué método de investigación utilizar corresponde a una decisión de la organización como tal, pudiendo ser este uno de los siguientes tres: Interno, Policial, o por organizaciones particulares. La decisión sobre qué método utilizar debiese estar incluida dentro del plan de respuesta ante incidentes.

Una definición de lo que es Computación Forense:

" ***Computación forense es el proceso de identificar, preservar, analizar y presentar evidencias digitales en una forme que sea legalmente aceptada***." (Rodney McKemmish 1999)

A partir de esta definición se puede observar cuatro componentes:

- Identificar: este proceso corresponde a identificar qué cosas pueden ser evidencias, dónde y cómo está almacenada, qué sistema operativo se está utilizando. A partir de este paso, el investigador puede identificar las metodologías de recuperación de evidencias adecuadas, así como las herramientas a utilizar.
- Preservación: corresponde a preservar la integridad de las evidencias digitales, asegurando que la cadena de custodia no se rompa. Cualquier cambio en la evidencia debe ser documentado.
- Análisis: es el proceso de revisar y examinar los datos.
- Presentación: es el proceso de presentar la evidencia en un formato legalmente aceptable y comprensible. El formato debe ser comprendido por alguien que no posea experiencia computacional, como es el caso de un juez, de lo contrario el esfuerzo impreso en el trabajo no tendrá sentido.

Dentro de lo que es la computación forense se establece un conjunto de reglas que debiesen ser aplicadas a la investigación, estas son:

- Mínima manipulación del original: esto puede ser lo más importante dentro de una investigación forense, se propone que se realice copias a la evidencia y se trabaje sobre estas copias, de esta manera se puede establecer una medida de integridad de la evidencia, evitando alterarla o contaminarla.
- Reportar cada cambio: en ciertas circunstancias hay casos en la evidencia que son inevitables, por ejemplo apagar un computador, lo que podría alterar el estado de la memoria principal, etc. cuando ocurre este tipo de cambios, se debe guardar un reporte de la causa del cambio, la extensión de este, la razón y el responsable de este cambio.
- Cumplir con las reglas de evidencias: existe un conjunto de reglas que se debe seguir en la manipulación de evidencias para asegurar que estas evidencias serán aceptadas en un proceso legal.
- No exceder el conocimiento propio: si la complejidad de la investigación va más allá de las habilidades y conocimiento del investigador, entonces es recomendable solicitar ayuda a alguien con mayor exériencia, o si el tiempo lo permite, adquirir un entrenamiento y conocimientos que permitan manejar el caso.

Las reglas sobre el manejo de evidencias son, nrmalmente, propias y particulares para cada jurisdicción legal, por lo tanto se debe prestar especial atención en el conocimiento de estas. A pesar de ello existe un conjunto de 5 reglas genéricas presentadas por Matthew Braid en su paper "Collecting Evidence after a System Compromise", estas son:

- **Admisible**: es la regla más básica, la evidencia debe poder ser utilizada en una corte o en cualquier otro lugar, el no cumplir con esta regla es equivalente a la no colección de evidencia.
- **Autentica**: si no se puede relacionar la evidencia con el caso, entonces no se puede utilizar para probar algo. Se debe poder demostrar que la evidencia representa información respecto del incidente en alguna forma.
- **Completa**: no es suficiente recolectar evidencia respecto de unoa de las perspectivas del incidente. No solo se debe recolectar evidencias inculpatorias, sino también evidencias exculpatorias, que ayuden a reducir el universo de posibles culpables.
- **Confiable**: tanto las evidencias recolectadas, como el método utilizado para su recolección deben ser confiables y no refutables.
- **Creible**: la evidencia presentada debe ser clara y fácil de comprender por un juez.

Respecto de la cadena de custodia, esta corresponde a una vitácora de las evidencias, vale decir, un documento en el cual se destaque cada paso que ha dado la evidencia en el proceso forense, desde la recolección, el análisis, hasta la presentación de las conclusiones finales del estudio, así como las personas que las han manipulado, indicando fechas, horas y lugares físicos.

Manejo de las evidencias

Es un aspecto miportante en toda investigación forense. Existe procedimientos y políticas estrictas respecto del tratamiento de las evidencias. Todo esto para asegurar que no se rompa la cadena de custodia, y por lo tanto se preserve la integridad de las evidencias.
El manejo de evidencias incluye items como:

- Estar capacitado para determinar que evidencia proviene de que trozo de HW.
- De donde se obtubo tal pieza de HW.
- Proveer almacenamiento seguro de las evidencias, manteniendo un acceso restringido a estas.
- Documentar cada proceso utilizado para extraer información.
- Asegurar que los procesos son reproducibles, y que producirán los mismos resultados.

Las opciones de investigación ante un incidente son normalmente 3:

- Investigación Interna: corresponde a conducir una investigación al interior de la organización, utilizando al personal de IT interno puede ser la opción menos costosa, sin embargo, dependiendo del tipo de incidente, puede ser la menos efectiva.
- Investigación Policial: puede no siempre poseer los recursos para manejar la investigación, y es posible necesitar proveer de evidencias a los investigadores antes de que puedan comenzar con su investigación. Varias organizaciones se presentan opuestas a reportar sus incidentes ante la policia, ya que a veces el costo de la investigación sobrepasa el consto de las consecuencias del incidente.
- Investigación por parte de Especialistas Privados: en el caso de Australia, un gran número de policias se retira y comienzan a trabajar de manera particular, con la ventaja de que conocen sobre las reglas del manejo de evidencias, y poseen experiencia que pueden poner a disposición de sus clientes en el momento que estos la necesiten.

En conclusión se puede ver que dentro del entorno de Australia, existe una falta de procedimientos y métodos estandarizados para dirigir una investigación forense.
En este paper se presenta un problema generalizado en el mundo actual, manejado en base a sistemas computacionales y dispositivos digitales. Se muestra una guía de acción ante la eventualidad de un incidente, así como las alternativas para enfrentarlo, junto con las ventajas y desventajas intrínsecas a cada alternativa.

Análsis Forense de Sistemas Linux

Autor: Juan Manuel Canelada Oset (Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones, Universidad Carlos III de Madrid).

La facilidad de acceso a Internet, así como el desarrollo y avance en el meracado de las tecnologías de la información han cambiado no sólo la forma en que se llevan a cabo los negocios y las actividades comunes, sino que también la forma en que los delincuentes desarrollan sus actividades.

Tanto los computadores commo las redes de computadores pueden verse involucrados en un incidente o crimen informático siendo estos las víctimas del incidento, o bien las herramientas utilizadas para el desarrollo de estos.

Se comprende por Análsis Forense de Sistemas Computacionales a los procesos de extracción, conservación, identificación, documentación, interpretación y presentación de las evidencias digitales de forma que sean legalmete aceptadas en un proceso legal, proporcionando las técnicas y principios que facilitan la investigación del delito.

El inmenso crecimiento de las redes de computadores y sistemas informáticos ha movido al mundo a un entornoen el cual se vive globalmente conectado, pudiéndose mantener conversaciones o negocios con personas en casi cualquier parte del mundo de manera rápida y de bajo costo. Pero, sin embargo, esta accesibilidad digital abre nuevas oportunidades también a los delincuentes, quienes encuentran nuevas formas de delitos, así como herramientas potentes que les permiten desarrollar ahora sus delitos de manera más sencilla y efectiva.

Según la encuesta sobre Seguridad y Crimen Informático del año 2004 publicada por el CSI y el FBI en conjunto, las pérdidas ocasionadas por culpa de ataques informáticos durante el año 2004 ascienden a casi ciento cincuenta millones de dólares.

En el Décimo Congreso de las Naciones Unidas sobre la prevención del Crimen y el tratamiento de los Delincuentes, celebrado en Viena el año 2000, se definieron dos categorías de Crímenes Informáticos, estos son:

- Crimen Informático en Sentido Estricto: Cualquier comportamiento ilegal, dirigido por medio de operaciones electrónicas que tengan como objetivo la seguridad de sistemas informáticos y de los datos que estos procesen.
- Crimen Informático en Sentido Amplio: Cualquier comportamiento ilegal cometido por medio o en relación con un sistema informático o una red, incluyendo crímenes como la posesión ilegal, la oferta y la distribución de información por medio de un sistema informático o de una red.

Respecto de las definiciones anteriores, se puede observar que los computadores y las redes pueden verse involucradas en un delito informático de varias formas:

1.- El computador o la red pueden ser las herramientas utilizadas para cometer el delito.

2.- El computador o la red puden ser los objetivos o víctimas del delito.

3.- El computador o la red pueden ser utilizadasd para propósitos incidentales relacionados con el crimen.

La metodología básica del Análisis Forense de Sistemas Computacionales consiste en:

1.- Adquirir las evidencias sin alterar ni dañar el original. La forma ideal de examinar un sistema consiste en detenerlo y examinar una copia de los datos originales, es importante tener en cuenta que no se puede examinar un sistema presuntamente comprometido utilizando las mismas herramientas del sistema.

2.- Comprobar que las evidencias recogidas y que van a ser la base de la investigación sonidénticas a las abandonadas por el delincuente en la escena del crimen.

3.- Analizar los datos sin modificarlos. En este punto es crucial proteger las evidencias físicas originales trabajando con copias idénticas, de modo que en caso de ocurrir algún error se pueda recuperar la imagen original y continuar con el análisis de forma correcta. Es básico realizar siempre un control de integridad de la copia antes de comenzar algún análisis.

De los puntos anteriores se puede deducir un conjunto de ventajas que presentan las evidencias digitales respecto de las evidencias físicas, estas ventajas son:

1.- Pueden ser duplicadas de forma exacta., pudiendo examinarse una copia como si fuese el original. Si se intenta destruir la evidencia, se puede contar con múltiples copias de esta lejos del alcance del delincuente.

2.- Con la utilización de herramientas adecuadas es fácil determianr si la evidencia ha sido modificada o falsificada, comparándola con la original.

3.- Es relativamente difícil detruir una evidencia digital, incluso borrándola puede se recuperada del disco.

Vantajas de Linux como Herramienta Forense.

El sistema operativo Linux presenta algunas características que lo dotan de grandes ventajas a la hora de ser utilizado como herramienta de análisis forense, estas características son:

1.- Todo, incluido el HW, se trara y representa como un archivo.
2.- Soporta una gran cantidad de sistemas de archivos, muchos no reconocidos por Windows.
3.- Permite montar los sistemas de archivos.
4.- Permite revisar un sistema en funcionamiento de forma sencilla y poco invasiva.
5.- Permite redirigir la salida de un comando a la entrada de otro (múltiples comandos en una sola línea)
6.- Permite revisar el código fuente de la mayoría de sus utilidades.
7.- Permite generar dispositivos de arranque.
8.- Es gratuito, así como la mayoría de las herramientas utilizadas en el análisis forense.

Respecto del análisis forense en sistemas linux, este sistema operativo presenta un conjunto de herramientas y comandos que pueden ser utilizados para cumplir con los procedimientos indicados en los diferentes modelos de computación forense, permitiendo a los investigadores poder desarrollar una investigación acuciosa y dirigida, utilizando herramientas potentes y bastante conocidas, con lo que la credibilidad de los resultados es poco cuestionable.

The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors

Autor: Jesse D. Kornblum (Information Technology Specialist for the Computer Crime and Intellectual Property Section of the United States Department of Justice)

Versiones oficiales del kernel de linux, hasta la versión 2.4 (incluída) no permiten a procesos de usuarios acceder al último sector de un disco con un número de sectores impar. A pesar de este problema, la normal operación dentro del sistema no se veía afectada, pero impedía poder generar imágenes completas de un disco de estas características. El problema fue tratado en la versión del kernel 2.5, la que luego incluyó los cambios en la versión 2.6. los sitemas que utilizan la versión 2.6 del kernel pueden acceder al último sector sin problemas, pudiendo así adquirir imágenes del disco sin problemas.

La adquisición de datos forence corresponde al proceso de generar una copia bit a bit (o imagen) de un medio digital. Estas imágenes son usadas a menudo en procesos legales, o procedimientos civiles, por lo tanto se requiere de una gran exactitud de los datos copiados.
Para el desarrollo de este tipo de procedimientos, la aplicación normalmente utilizada es el comando "dd", que genera copias bit a bit, junto con el comando "md5sum", que corre el algoritmo de MD5, generando una salida de 128 bits para los datos procesados.

Al utilizar este programa para adquirir datos, se observó que en discos con una cantidad de sectores impar, la cantidad de sectores porcesados era "n-1", donde n es un un número impar, por lo tanto se perdía el último sector. Esto sucedía en sistemas Linux que corrian bajo la versión de kernel 2.4. En sistemas operativos como FreeBSD 4.4, la cantidad de sectores era n.
Se pensó en un principio que el problema estaba en el comando, pero el Dr. James Lyle del NIST identificó la discrepancia como una función en el kernel de Linux, el escribió que el problema no estaba en el comando dd, sino que en el kernel de Linux.

Los discos normalmente almacenan información en sectores de 512 bytes. Hasta la versión de kernel 2.4, el kernel de linux accedia a bloques de 1024 bytes, o también dicho, dos bloques de 512 byts por vez. En general la diferencia entre bloques y sectores no es problema, esto hasta que se desea acceder al último sector del disco en el caso de que el número de sectores sea impar, en donde no hay forma de que un proceso usuario pueda acceder a este punto del dicso.

A pesar de la imposibilidad de acceder al último sector de un disco no fue problema para los usuarios normales, esto si representa un problema para los examinadores forenses. El problema de no poder acceder al último sector no representaba una mayor complicación entre los usuarios, esto debido a los grandes tamaños de discos existentes, sólo los usuarios que necesitaban o deseaban acceder a este sector, en discos formateados bajo otros sistemas operativos notaban el problema. Esta falla fue un caso notorio para investigadores forense que utilizaban sistemas linux para adquirir datos desde discos formateados bajo otros sistemas operativos, en donde no podían acceder a este sector. Sistemas operativos como Windows pueden utilizar el último sector durante la operación normal del sistema, por ello, para obtener una imagen completa de este disco, se requiere de poder leer todos los sectores del disco, incluídos los últimos 512 bytes.

La metodología del experimento para comprobar que el problema correspondía al kernel 2.4 consistió en utilizar el comando dd y el comando md5sum, utilizando las versiones del kernel 2.4 y 2.6.
se utilizó dos discos duros, uno ATA, en el cual se creó una partición DOS con un número impar de sectores. La partición fue creada mediante el comanfo “fdisk”. El segundo disco, un disco SCSI con un número impar se sectores.

Se utilizó cuatro entornos de sistemas operativos, dos de ellos fueron RedHat 7.1 y FreeBSD 4.4, los que se instalaron en los discos duros. Los otros dos sistemas operativos fueron Knoppix 3.4-2004-05-10-EN, el que permite al usuario escoger entre el kernel 2.4 y 2.6.

para cada sistema operativo se corrió el comando dd de forma tal de enviar los datos del disco duro completo a la partición “/dev/null”. En ambos casos el programa al termianr desplegó por la pantalla el número de sectores procesados.

Como resultado, el número de sectores porcesado por cada sistema operativo, en ambos discos es el siguiente:

Sistema Operativo	**Versión del Kernel**	**Versión de dd**	**Sectores procesados**
RedHat 7.1	2.4.2-2	4.0.36	60416
FreeBSD 4.4	------	------	60417
Knoppix 3.4	2.4.26	5.0.91	60416
Knoppix 3.4	2.6.5	5.0.91	60417

Basado en los resultados se puede observar que el kernel 2.6 de Linux corrige el error de acceso al último sector presentado en las versiones anteriores. Ahora con esto ya resuelto se puede realizar imágenes de discos formateados bajo otros sistemas operativos son plena confianza en que la images será realmente representativa.