ISSN: 1692-7257 - Volumen 2 – Número 20 - 2012

Revista Colombiana de Tecnologías de Avanzada

Recibido: 23 de mayo de 2012
Aceptado: 17 de junio de 2012

METHODOLOGY FOR FORENSIC ANALYSIS IN LINUX

METODOLOGÍA PARA EL ANÁLISIS FORENSE EN LINUX

MSc. Luz Marina Santos Jaimes, Ing. Anderson Smith Flórez Fuentes

Universidad de Pamplona
Grupo de Investigación Ciencias Computacionales
Ciudadela Universitaria. Pamplona, Norte de Santander, Colombia.
Tel.: 57-7-5685303, Fax: 57-7-58685303 Ext. 164.
E-mail: {lsantos, ansmith}@unipamplona.edu.co

Abstract: In this Project was conducted a study of forensic methodologies to structure a four-step general process applied to Linux systems. The forensic methodology comprises: a study of the affected area, data manipulation, analysis of evidence, and presentation of results. Three formats are presented for complementing the methodology in the documentation of cases and facilitating the work of forensic analyst for the handling and delivery of evidence.

Keywords: Analysis, computer forensic, evidence, methodology, Linux.

Resumen: En este trabajo se realizó un estudio de metodologías de análisis forense para estructurar un proceso general de cuatro pasos aplicado a sistemas Linux. La metodología de análisis forense comprende: estudio de la zona afectada, manipulación de los datos, análisis de la evidencia, y presentación de resultados. Se presentan tres formatos que complementan la metodología en la documentación de los casos y facilita el trabajo del analista forense para la manipulación y entrega de la evidencia.

Keywords: Análisis, informática forense, evidencia, metodología, Linux

1. INTRODUCCIÓN

El crecimiento constante de delitos informáticos como espionaje, robo de propiedad intelectual, fraude, entre otros, implica que las organizaciones tomen con mayor seriedad el proceso de computación forense que consiste en la aplicación de métodos científicos en investigaciones criminales y búsqueda de evidencias donde se involucran componentes digitales.

El analista forense para realizar su trabajo debe aplicar una metodología aprobada y certificada para que la evidencia presentada en un caso sea reconocida.

En el caso de computación forense (Interpol Colombia, 2008) se supone que se aplicó la metodología tomada del FBI por ser de competencia gubernamental; muchas empresas de la industria de seguridad aplican sus metodologías particulares que son desconocidas al público. Otras metodologías han sido divulgadas como resultado de trabajos científico-académicos, las cuales en su mayoría no reportan documentación.

El grupo de investigación Ciencias Computacionales creó y probó la metodología de análisis forense informático aplicado a sistemas Linux (Flórez, 2006), posteriormente fue verificada en un proyecto de pregrado del programa ingeniería de sistemas (Vargas, 2010), lo que demuestra que pese a los grandes cambios de la

tecnología esta metodología sigue vigente. Cabe resaltar que este trabajo ha sido revisado y mejorado por el grupo de investigación CICOM con aportes de trabajos existentes en el tema.

2. COMPUTACIÓN FORENSE

2.1 Conceptos de computación forense

Con el rápido avance en la tecnología de computadores y redes, la evidencia digital empieza a jugar un rol importante en las cortes en la última década. La computación forense, es una disciplina creciente basada en ciencia forense y tecnología de seguridad informática, se enfoca en adquirir evidencia electrónica de los sistemas de cómputo para procesar crímenes de computador (Wang, 2005).

El concepto general de análisis forense es la aplicación de métodos científicos en investigaciones criminales, no obstante el análisis forense donde la evidencia es de naturaleza digital recibe varias definiciones. Las siguientes definiciones de computación forense son una representación del amplio rango existente:

- El proceso de identificar, preservar, analizar y presentar la evidencia digital de forma que sea legalmente aceptada (McKemmish, 1999).
- Obtención y análisis de datos de una forma libre de distorsión para reconstruir datos o conocer lo que ha ocurrido en el pasado sobre un sistema (Farmer and Venema, 1999).
- El uso de métodos derivados y probados científicamente para la preservación, colección, validación, identificación, análisis, interpretación, documentación y preservación de evidencia digital entregados desde fuentes digitales con el propósito de facilitar o promocionar la reconstrucción de eventos criminales, o ayudar a anticipar acciones no autorizadas (Palmer, 2001).

El trabajo de (Broucek and Turner, 2006) muestra las implicaciones metodológicas por la falta de coherencia, revisa los modelos y trabajos existentes como una forma de explorar sus diferencias, y examina la ambigüedad de definiciones de la computación forense. El trabajo de la computación forense debe ser el resultado de la cooperación y colaboración entre las disciplinas que muestra la figura 1.

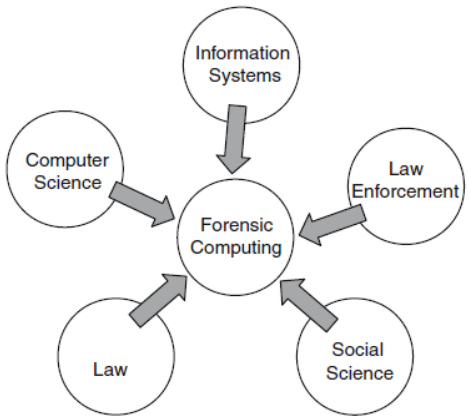

Fig. 1. Dominio de Computación Forense (Broucek and Turner, 2006)

2.2 Legislación sobre ataques informáticos en Colombia

Colombia ha sido objeto de ataques, un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "*hacktivista*" autodenominado *Anonymous* atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas.

Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet" (Conpes, 2011).

En la Policía Nacional de Colombia, la informática forense surgió como ciencia que apoya las investigaciones judiciales a partir del año 2004, con la creación del Gabinete de Informática Forense en la Dirección Central de Policía Judicial, hoy Dirección de Investigación Criminal.

El análisis forense en el campo de la informática fue conocido ampliamente en el país en el año 2008, por el mencionado caso de la incautación por parte de la Policía Nacional de ocho dispositivos pertenecientes a un insurgente, se realizó un análisis inicial por *The International Criminal Police Organization* – INTERPOL, el informe disponible al público concluyó que la toda la información contenida en estos dispositivos no había sido alterada por la policía colombiana (Interpol Colombia, 2008).

El Congreso de la República ha dado un paso importante con la ley 1273 de 2009 en la cual declara, preserva y protege los derechos que tienen las personas de acceder a un sistema informático seguro e impone sanciones y multas significativas (Congreso de Colombia, 2009).

La Ley adiciona al Código Penal colombiano el Título denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

3. METODOLOGÍA PARA ANÁLISIS FORENSE EN LINUX

En (Pollitt, 2007) revisa una colección de quince trabajos publicados acerca de modelos forenses digitales, lo que constituyó un punto de partida para la construcción de la metodología. En (ACPO 2007) se presenta información y sugerencias para asegurar la escena del crimen y preservar la evidencia digital. El trabajo de (Dittrich, 2002) constituyó un referente importante para el presente trabajo.

La metodología propuesta en cuatro etapas (ver figura 2) es un enfoque general de los trabajos estudiados de análisis forense que se presentan en la Tabla1. Las etapas que tienen cada una de las metodologías se han reflejado en este proyecto.

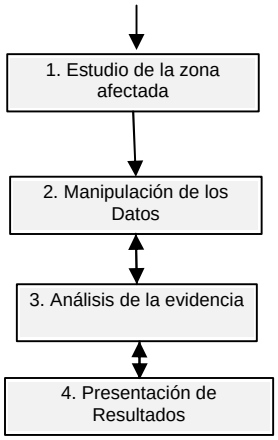

Fig. 2. Metodología forense CICOM

Tabla 1: Metodologías estudiadas

Metodología	Pasos
Modelo de tres fases	-Recopilación de los datos -Examinar los datos -Evaluación de los datos
Metodología de InetSecur (InetSecur S.L., 2004)	-Estudio preliminar -Adquisición de datos -Análisis -Presentación
Metodología de Carrier y Spafford (Carrier and Spafford, 2003)	-Examinar la evidencia -Clasificación de la evidencia -Construcción y prueba del acontecimiento -Acontecimiento ordenando -Prueba de la hipótesis.
Metodología de DragonJar (DragonJar, 2009)	-Acceso -Adquisición -Análisis -Reporte

A continuación se describe las etapas de la metodología propuesta.

3.1 Estudio de la zona afectada

Se identifica y recolecta una serie de información del equipo que ha sido afectado:

- Revisar el sistema, mirar que sistema operativo posee.
- Revisar el antivirus, si tiene, cual fue la última actualización instalada.
- Revisar el firewall, si está instalado y su versión.
- Revisar sistema de detección de intrusos, si está instalado, versión.

El analista debe poseer conocimiento del sistema afectado para revisar los *logs* de ingresos que le permita determinar si se realizaron cambios, hay herramientas que facilitan la búsqueda de esta información.

Después de llegar a la zona afectada, para facilitar el trabajo y no dejar pasar ningún detalle u olvidar alguna característica del equipo afectado se referencia el **formato 1** (Ver Anexo). Este formato contempla todos los detalles a la hora de congelar la escena: características físicas del equipo, características de la red y software instalado.

Congelar la escena: Este es uno de los puntos más críticos en el análisis forense, porque aquí es donde se captura la información sin que esta sea contaminada. Para realizar este levantamiento como se denominaría en un caso forense es

necesario contar con las herramientas adecuadas o poseer conocimiento de código de bajo nivel para poder realizar esta captura. La mejor forma de controlar estos casos es con la documentación utilizando el **formato 2** (Ver Anexo), el cual permite registrar la información necesaria y apropiada.

Para congelar la escena es recomendable detener el servidor afectado, y continuar trabajando con un servidor redundante para no afectar la actividad de los usuarios, en caso de no tener equipo redundante, se hace una copia lo más rápido posible cuidando de no desconectar el servidor, cuando el análisis puede demorar la mejor solución es desconectar el servidor por el tiempo que demore el copiado de las imágenes.

Además, se debe tener en cuenta que cada usuario que ingrese de manera legal o ilegal a un sistema modifica con o sin intención algunos archivos del sistema. Por ese motivo es importante asegurarse que al momento de haberse realizado la intrusión dejar inhabilitado el sistema para evitar estos imprevistos. Para ello se puede desconectar el servidor de la red o en caso más extremo apagar el equipo de golpe (desconectar la electricidad) lo cual puede afectar parte de la evidencia como lo es la memoria RAM.

Recolección de evidencia: Antes de apagar el sistema, será útil recoger algunos archivos con información que pudo ser cambiada por los intrusos, para eliminar cualquier rastro de su ingreso ilegal a un sistema, como la organización de sistema de ficheros de */etc/fstab*, el nombre del host, la dirección IP del fichero */etc/hosts* e información de algunos dispositivos desde los ficheros */var/log/dmesg* o ficheros de *log* del sistema */var/log/messages*. Esa información comprimida se puede guardar en almacenamiento secundario.

3.2 Manipulación de los datos

Es importante mantener los datos de modo estéril, es decir preparar el disco duro de tal forma que no se altere o contamine los datos, para que su análisis se realice de la mejor forma posible, para ello es bueno ayudarse del **formato 3** (ver Anexo) el cual hace responsable al analista de cualquier modificación realizada en la evidencia.

Para preservar la evidencia de modo original se debe recoger las evidencias lo más rápido posible y sin modificar los archivos del sistema instalando u apagando el mismo, para eso se puede utilizar hardware especializado para realizar estas tareas, o si el sistema fue apagado se puede utilizar herramientas tipo *live* (en algunos sistemas operativos estas herramientas trabajan en equipos con el sistema operativo funcionando, ejemplo: HELIX en el sistema Windows).

Cuando se manejan las evidencias hay que tener en cuenta que muchas de ellas pueden ser virus, o el daño pudo haber sido causado por una falla del hardware o software o una falla eléctrica, además se tiene que tener en cuenta que el intruso pudo haber dejado trampas para eliminar o modificar información al momento de hacer el análisis o utilizar herramientas anti-forense para evitar ser encontrado o rastreado.

Para evitar estos percances se recomienda hacer varias copias del sistema comprometido, para poder trabajar con las copias y realizar varios análisis para minimizar el error a la hora de realizar las pruebas.

La parte más importante de cualquier análisis forense es manipular y analizar la información. Si esa información no está disponible o es insuficiente será necesario realizar un análisis forense exhaustivo del sistema.

Clasificar la evidencia: La evidencia digital es volátil y susceptible al ser forzada. Para analizar la evidencia digital se debe utilizar una copia de la fuente original. En investigaciones criminales la evidencia digital se debe analizar en un laboratorio especializado por personal altamente calificado. Las investigaciones que manipulan la evidencia digital no deben cambiar la evidencia digital original de ninguna forma. Todas las actividades referentes como el asimiento, el acceso, el almacenaje o la transferencia de la evidencia digital deben ser documentadas completamente.

3.3. Análisis de la evidencia

El primer paso de cualquier análisis forense consiste en capturar la evidencia. Por evidencia se entiende todo aquella información que pueda ser procesada en un análisis detallado. El fin de este análisis es la interpretación lo más exacta posible del suceso ocurrido. El objetivo fundamental es que en el proceso de la captura no se altere la escena a analizar.

Lugar del análisis: Proceso en un laboratorio o en el sitio seguro**.** Los investigadores pueden quitar

algunos tipos de evidencia física (las muestras de pelo o de la fibra, por ejemplo) de escenas de crimen para analizar en laboratorios; otros tipos (tales como huellas digitales en una pared o marcas de carro en el pavimento) se deben examinar en el sitio y preservar fotográficamente o por otros medios. Al recoger datos digitales, los investigadores pueden hacer copias exactas usando las herramientas que copian exactamente los discos. Esto puede ser muy útil, por ejemplo, una investigación a una empresa con un solo servidor el cual no posee servidor redundante, esto puede influir en pérdidas de usuario o en el peor de los casos pérdida de dinero por cada minuto que se tenga desconectado el servidor, el copiado de los datos permitiría que la investigación procediera.

Documentación de la evidencia extraída: Cada paso que se da en el análisis forense debe ser documentado, por eso es imprescindible para la investigación y para el caso que el analista documente cualquier cambio, apertura de archivo, o modificación que realice al archivo a tratar o la imagen obtenida del copiado. Se recomienda que la información sea manipulada en ambientes controlados con dispositivos de grabación de audio y video.

3.4. Presentación de resultados

Cuando se habla de presentar resultados obtenidos es describir el momento, el cómo, desde donde vino la intrusión. Esto es lo fundamental y lo único que se puede presentar ante un juzgado si es el caso. Para que este documento redactado sea válido el analista debió haber documentado paso a paso lo que hizo desde que llego a la escena, que metodología utilizó, cuales herramientas incluyendo la hora y lugar en el que realizó el análisis, que otros investigadores o que personal estuvo en contacto con la escena o el laboratorio mientras se realizaba el análisis.

Procesar la información: En esta disciplina todos los procesos son igualmente importantes y cada uno se debe hacer con el mayor cuidado posible. El no vigilar la herramienta a lo largo del análisis puede dar resultados tanto negativos como positivos. Cuando el resultado de la evidencia es negativo es porque se omitieron pasos por creerse obvios o porque el atacante es muy bueno y utilizó herramientas anti forenses. Si el análisis es hecho por el analista forense solamente, el analista gana experiencia al resolver el caso, debe proporcionar algunas ideas en cuanto a qué palabras claves o frases específicas puede utilizar para iniciar la búsqueda. Por ejemplo, Si el caso es sobre pornografía de niños, entonces hojear todas las imágenes o videos en el sistema puede ser el primer paso. Si el caso es sobre una ofensa a través de Internet, entonces revisar los archivos de historial de Internet puede ser el primer paso.

4. CONCLUSIONES

Por medio del análisis forense se puede reconstruir una escena de un ataque informático, el personal que realiza el análisis debe ser altamente entrenado en seguridad, tener amplio conocimiento de las herramientas y el sistema operativo, además el analista debe poseer altas cualidades éticas con el fin de no manipular la información para el beneficio propio o de terceros.

Es importante que las empresas desarrollen buenas prácticas en seguridad que incluyan planes de respuesta a incidentes, que definan políticas y procedimientos que deben ser usados en caso de ocurrir un incidente para preservar la evidencia, que sirva de soporte en un proceso judicial.

Las personas que quieran incursionar en el mundo de la computación forense deben estudiar las diferentes metodologías existentes, mirar en cuántos casos han sido utilizadas y en cuantos se ha obtenido una solución positiva, para así definir si son viables o si se recomienda realizar modificaciones, teniendo en cuenta que los crímenes digitales cambian o evolucionan exponencialmente al igual que la tecnología. La presente metodología respondió favorablemente a la luz de los nuevos cambios tecnológicos, cuenta con documentación y se recomienda su aplicación en otros casos.

Las metodologías deben estar acompañadas por buenas herramientas forenses o *toolkits*, las cuales no se mencionan en este artículo ya que cada metodología puede variar de acuerdo al caso que se tenga por resolver.

Las empresas que cuentan con sistemas de información de acceso público deben contar con sistemas de detección de intrusos en lo posible inteligentes para alertar sobre posibles instrucciones a los sistemas.

REFERENCIAS

Interpol Colombia (2008). Informe forense de INTERPOL sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia.

Flórez F., Smith (2006). *Metodología para el análisis forense.* Proyecto de Grado Ingeniería de Sistemas, Universidad de Pamplona.

Vargas D., José (2010). *Proceso de análisis informático forense sobre plataforma linux*. Proyecto de Grado Ingeniería de Sistemas, Universidad de Pamplona.

Yun Wang, et al. (2005) *Foundations of computer forensics: A technology for the fight against computer crime.* Elseiver. Computer Forensics. doi:10.1016/j.clsr.2005.02.007

McKemmish, Rodney. (1999). *What is forensic computing*. Trends and issues in crime and criminal justice.

Farmer, D., and Venema, W. (1999). *Murder on the Internet Express*

Palmer, G. (2001). *A Road Map for Digital Forensic Research*. Report from the First Digital Forensic Research Workshop (DFRWS), Utica, New York

Broucek, Vlasti and Turner, Paul. (2006). *Winning the battles, losing the war? Rethinking methodology for forensic computing research*. Springer-Verlag France. J Comput Virol 2:3–12

Conpes. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación.

Congreso de Colombia. (2009). *Ley 1273 "de la protección de la información y de los datos"*

Pollitt, Mark M. (2007). *An Ad Hoc Review of Digital Forensic Models.* Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07).

ACPO (2007). *Good Practice Guide for Computer-Based Electronic Evidence.* Association of chief police officers.

Carrier, Brian and Spafford, Eugene. (2003) *"Getting phisycal with the digital investigationprocess*". International Journal of Digital Evidence. Economic Crime Institute (ECI),Utica College. Volume 2, issue 2

SITIOS WEB

Dittrich, David (2002). Análisis forense de sistemas GNU/Linux. http://es.tldp.org/Presentaciones/200211hispalinux/odisho/analisisforense.html. (Consultado: 10 de noviembre 2011)

DragonJAR. (2009). Metodología Básica de Análisis Forense.
http://www.dragonjar.org/curso-gratuito-de-anlisis-forense-basico.xhtml. (Consultado: 10 de noviembre 2011)

InetSecur S.L. (2004). *Análisis Forense* http://lgomez.es/wp-content/uploads/2011/05/2004-ncn-forensics-gomezmiralles.pdf. (Consultado: 10 de noviembre 2011)

ANEXOS

Formato 1: Estudio de la Zona Afectada
Número de caso: _____ Fecha y hora: __/__/__ __:__ __
A. Características del equipo:
Marca del Equipo: _____ Serial: _____
Procesador: _____
Memoria:_____
Disco Duro: _____ Tamaño: _____
Unidades:
CD: ð Floppy: ð USB: ð #___ Teclado: ð Mouse: ð
Dispositivos Adicionales:
Tarjeta de Video: ð Aceleradora: ð
Otros: _____

B. Característica de la red:
Dirección IP: _____Mascara de Subred: _____
Gateway: _____Dirección Física: _____
Servidor DNS: _____ DNS Alternativo: _____

C. Programas instalados:
El sistema actualmente es un servidor: ð
Posee servidor de respaldo: ð
Sistema Operativo: _____Versión: _____
Antivirus: ð, Cual: _____Versión: _____
Firewall: ð Cual: _____ Versión: _____
Sistema de Detección de Intrusos: ð
Cual: _____ Versión: _____
Manejo de Bases de datos para Usuarios externos e internos: ð
Clasificación por usuarios: ð
Aplicaciones Instaladas: Versión:
1. _____ _____
2. _____ _____
3. _____ _____
4. _____ _____
Cuentas Administradores:
1. _____
2. _____
3. _____

Formato 2: Congelar la Escena y Recoger los datos.
Numero de caso:_____ Fecha y hora inicio: __/__/__ __:__ __
Fecha y hora terminación: __/__/__ __:__ __
Testigos: _____ Documento: _____
Notario: _____ Documento: _____
Si el sistema está trabajando como servidor y no existe servidor de *Back up* la mejor opción es dejar fuera de servicio por unos momentos mientras se realiza el copiado de Copiado del Disco Duro (DD o HD):
Unidad a Realizar el análisis:
DD ð HD ð RAM ð
Nombre de la Unidad:
hdb ð hdb1 ð hdb2 ð hdb3 ð hdb4 ð dsa ð dsa1 ð loop0 ð
Sectores: ____ _____ Marca: _____
Opción solo para hdb:
Bus IDE: Primario ð Segundario ð : Slave ð Master ð
Herramientas o comando Utilizado para realizar el copiado del disco:_____
MD5:: _____ ó
SHA1::_____ ó
SHA256:_____

Copiado de la Memoria **RAM**:
Herramientas o comando Utilizado para realizar el copiado del disco:
_____
MD5:_____ ó
SHA1:_____ ó
SHA256:_____

Tamaño de la imagen resultante: _____
Nombre de los archivos generados:_____

En caso de que el análisis se realice en un laboratorio o en un lugar diferente al sitio donde ocurrió el ataque.
Cambio de Custodio: (Algunas herramientas Poseen esta plantilla**)**
Número del caso: _____
Nombre del Custodio: _____
Número de Custodio: _____
Serial del DD: _____Modelo del DD: _____

Detalles de la imagen:
Fecha y hora de la creación: __/__/__; __:__ __
Tipo de copiado: _____ Tipo de Hash: _____
Numero de archivos: ____ Nombre de la imagen: _____
Nombre del analista que realizo la imagen: _____

Formato 3: Manipulación de los datos Obtenidos.
Numero de caso: _____ Fecha y hora: __/__/__ __:__ __

A. Características del equipo:
Marca del Equipo: _____ Serial: _____
Procesador: _____ Memoria: _____
Disco Duro: _____ Tamaño: _____
Unidades:
CD: ð Floppy: ð USB: ð #___
Tarjeta de Video: ð Aceleradora: ð
Otros: _____
Nombre del archivo: _____
Nombre del Analista Responsable: _____

B. Tipo de manipulación
Manipulación: Interna __ Externa: __
Nombre de la cuenta por la que ingresaron: _____
Permisos de la cuenta: _____
Personas que manejan la cuenta: _____