SOFTWARE LIBRE PARA EL ANÁLISIS FORENSE DIGITAL UTILIZANDO CAINE

Santos Ireneo Juchasara Colque,M.Sc.
sijucol@hotmail.com, sijucol@gmail.com
Docente Ingeniería Informática
Universidad Nacional Siglo XX
Llallagua, Bolivia

Resumen – *La red hoy en día pese a que existen forma de asegurar, no está a salvo de los intrusos que día a día roban información de los ordenadores, lo llamaremos como intrusos, y que la perdida delos datos para una empresa implica quiebre y perdidas en cuanto a los ingresos que se generan.*

Es así que surgen o juegan un papel muy importante los peritos informáticos en investigar sobre los casos que se suscitaron, para lo se puede utilizar una de las herramientas libres como el caine Linux, ya que esta permite realizar una análisis forense apoyado en herramientas específicos para es te área, en este caso se utilizó autospy para analizar una imagen de disco.

Palabras Claves *– Análisis forense, caine, Linux, GNU/Linux, autospy, intruso.*

I. INTRODUCCIÓN

Los ordenadores almacenan gran cantidad de información cotidianamente de forma estructurada, ya sea en instituciones públicas y privadas. Sin embargo estas carecen de seguridad en cuanto a la seguridad de los datos ocasionando el extravió o perdida de información sin que se tenga importancia por nosotros. Vale decir que pareciera la perdida de información no afecta en cuanto a la funcionalidad, la toma de decisiones, la investigación, etc. Sin embargo lo descrito anteriormente esta puede ocasionar la quiebra de la empresa precisamente por estas situaciones.

Los peritos en informática forense precisamente se encargan de descubrir y reunir evidencias esto con el fin de poder encontrar a los infractores o causantes de la perdida de información, para este proceso es necesario la aplicación de metodologías, técnicas y herramientas ya sean de software libre y/o propietarias. Puesto que con el avance del internet hay personas más llamados como intrusos, que se dedican a interceptar datos en la autopista de la información, y que estas personas utilizan técnicas y procedimientos para no dejar rastros en cuanto a acceso a nuestra información de esta manera se hace más difícil seguir las investigaciones, precisamente por el hecho de eliminar todas las huellas o rastros con la cual accedió a los datos.

Es así que surge a raíz de lo descrito en el anterior punto el análisis forense en la cual se encarga sobre la extracción, identificación, conservación, documentación, interpretación y la respectiva presentación de las evidencias digitales encontradas en el peritaje realizado, de esta manera sea útil para afrontar proceso jurídico legal ante las diferentes instancias competentes.

Para tal efecto en esta oportunidad se presenta un estudio sobre una de las herramientas libres para encarar el análisis forense a un ordenador, para ello vamos a utilizar CAINE Linux, una de las distribuciones en la cual cuenta con una serie de utilidades y herramientas especializadas en dar soporte a cada una de las cuatro fases de la Informática Forense: Estudio preliminar, recolección de la evidencia, análisis de la evidencia y la elaboración del informe final.

II. DESARROLLO

1. Análisis Forense

El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad. (Rifà Pous, y otros, 2009)

Un incidente de seguridad es cualquier acción fuera de la ley o no autorizada: ataques de denegación de servicio, extorsión, posesión de pornografía infantil, envío de correos electrónicos ofensivos, fuga de información confidencial dentro de la organización, en el cual está involucrado algún sistema telemático de nuestra organización.

Las fuentes de información que se utilizan para realizar un análisis forense son:

- Correos electrónicos.
- IDS / IPS.
- Archivo de logs de los cortafuegos.
- Archivo de logs de los sistemas.
- Entrevistas con los responsables de seguridad y de los sistemas.

2. Software libre para la informática forense

Software libre es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el software libre es una cuestión de libertad, no de precio. (Arteaga Mejía, 2001)

El Software libre es muy aceptado en las ciencias forenses para las tareas de análisis, ya que al ser libre se puede acceder al código fuente del mismo para luego estudiar y modificar según necesidades especificas y distribuir con la filosofía de GNU/Linux.

En este sentido existen diferentes herramientas y distribuciones GNU/Linux algunos instalables directamente en el disco duro local del ordenador, mientras que otros pueden ejecutarse desde un Live CD, mencionar que las mismas distros incorporar muchas de las herramientas para el análisis forense, a continuación se mencionan algunas de las distribuciones más conocidas y más utilizadas en este ámbito de las ciencias forenses:

a) **ForLEx**. Esta distribución está basada en Debían y se caracteriza por ser liviana, flexible y orientada a aplicaciones de Informática Forense. Además, incluye la herramienta FTK Imager, la cual es muy útil para adquisiciones forenses y no está presente en versiones Live de otras distribuciones.
b) **DEFT Linux**. La distribución de Linux para análisis forense informático basada en Ubuntu que incluye herramientas para el análisis forense de móviles y/o dispositivos con iOS o Android.
c) **CAINE**. Es una distribución Live DVD y versión para pendrive, basada en Ubuntu de origen italiano, enfocada a realizar análisis forenses informáticos. Incluye numerosas herramientas y scripts para facilitar el trabajo.
d) **SIFT (SANS Investigate Forensic Toolkit, SIFT)**. Constituye otra distro basada en Ubuntu y que también incluye herramientas como SleuthKit/Autopsy, Wireshark, Pasco, entre otras herramientas.
e) **KALI Linux.** Es una distribución basada en Debian/Linux, diseñada para la auditoria y seguridad informática en general. Se desarrolló a partir de la reescritura de backtrack, por Offenseive Security Ltd.
f) **Autopsy**. Es una de las herramientas forense es una interfaz gráfica para la línea de comandos y herramientas de análisis de investigación digital en el Sleuth Kit. Juntos, pueden analizar los discos de Windows y UNIX y sistemas de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3).

Son algunas de las herramientas y distribuciones Linux que se utilizan para las ciencias forenses, cada con las diferentes ventajas así como desventajas, en este artículo vamos a hacer énfasis en la distribución libre CAINE Linux.

Podemos mencionar que la mayoría de los sistemas desarrollados para el análisis forense responden a distintos estándares o metodologías. Por eso, generarán resultados que podrán ser presentados como evidencia digital en una corte.

3. Análisis forense asistido por CAINE Linux.

CAINE (Computer Aided INvestigative Environment o Entorno de Investigación Asistido Por Computadora) es una de las distribuciones GNU/Linux más completas para realizar análisis forense informático. Esta distribución funciona como Live DVD y no toca absolutamente ningún dato del disco duro donde lo arranquemos, ya que para realizar un análisis forense es fundamental no alterar las pruebas, en este caso los datos del almacenamiento interno. (Wikipedia, 2015)

CAINE es completamente software libre y de esta manera se basa plenamente en el espíritu de la filosofía Open Source, ya que se tiene acceso al código fuente y que todos están en el derecho de modificar, estudiar, distribuir y usar de manera libre.

3.1. Herramientas

CAINE viene incorporado con varias de las herramientas para facilitar el análisis forense, utilidades y recursos, que lo convierte en una de las distribuciones más populares a nivel de la informática forense. A continuación se describe algunas de las utilidades más populares:

Mount Manager: Esta herramienta permite detectar, montar, desmontar, examinar y administrar las unidades de almacenamientos, conectadas a disco duro, tanto las unidades internas como las externas.

Guymager: Es una herramienta forense, con la capacidad de crear copias bit a bit o réplicas de imagen de disco, es bastante ágil en su funcionamiento y crea replicas en formatos dd, EWF, AFF.

Air(Imagen y Restauración Automática): Air Es una aplicación en modo grafico para el uso del comando dd/dclfdd (Datataset Definition (dd)). Fue diseñado como una mejora en modo gráfico de todas las variantes de dd, su fácil uso permite crear imágenes forenses de discos y de particiones completas del mismo. Soporta MD5/SHAx hashes, cintas SCSI, proyección de

imágenes sobre una red TCP/IP, imágenes partidas, y registración detallada de la sesión.

Autopsy: Tal vez la mejor herramienta libre que existe para el análisis de evidencia digital. Su interfaz gráfica es un browser que basado en las herramientas en línea de comandos del Sleuth Kit, permite un análisis de diversos tipos de evidencia mediante una la captura de de una imagen de disco.

Hexeditor: Permite cargar los datos de cualquier archivo, ver y editar en formato hexadecimal o ASCII. Por medio del editor hexadecimal, el usuario puede ver, redactar, reparar o modificar el contenido intacto y exacto de un archivo binario.

PhotoRec: Recupera datos y archivos perdidos incluyendo vídeo, documentos y archivos de discos duros y CD/DVD. Incluyendo la búsqueda en el espacio no asignado en disco, examinando cabecera tipo de archivo específico y los valores de pie de página.

Gtkhash: Una magnifica herramienta para el cálculo de diferentes funciones hash de un archivo y sumas de comprobación de mensajes. Actualmente los tipos soportados incluyen funciones de hash MD5, SHA1, SHA256, SHA512, RIPEMD, HAVAL, TIGER y WHIRLPOOL. Esta herramienta es bastante útil, para comprobar el correcto estado de un archivo, o la comparación entre dos(2) archivos iguales, para comprobar su integridad.

Hfsutils: HFS es una herramienta para leer y escribir volúmenes de Macintosh, de su "sistema de ficheros jerárquico", el formato de volumen nativos utilizados en los modernos ordenadores Macintosh. hfsutils es el nombre de un completo paquete de software están desarrollando para permitir la manipulación de los volúmenes HFS de UNIX y otros sistemas.

Dvdisaster: Dvdisaster es una fabulosa herramienta que examina CD / DVD / BD, con el fin de recuperar archivos, incluso después de algunos errores de lectura. Esto permite rescatar información dañada o de difícil lectura a un nuevo medio de almacenamiento tras su recuperación.

Ophcrack: Utilidad para romper u obtener contraseñas de usuario en el sistema operativo Windows. Su funcionamiento se basa en el análisis de las tablas rainbow para el acceso a las claves de la SAM (Security Accounts Manager).
SAM es el gestor de seguridad para cuentas de usuario, de los actuales sistemas operativos Microsoft Windows. Este servicio se emplea durante los procesos de acceso al sistema, y retiene información del usuario que se ha logeado ante el sistema.

Tesdisk: TestDisk es una buena herramienta diseñada para recuperar particiones perdidas de almacenamiento de datos, o recuperar la capacidad del disco para hacerlo booteable. Estas funciones son exitosas cuando los problemas son causados por software con fallas, ciertos tipos de virus o en caso de borrar accidentalmente una tabla de particiones. Su función no aplica para discos duros con daños físicos, sin embargo puede intentar el acceso a las particiones dañadas u ocultas.

III. RESULTADOS

En este apartado todo lo mencionado en el anterior punto vamos a concretar la teoría a la práctica con la distribución descrita CAINE Linux y poder aplicar una de las muchas herramientas con la cual cuenta dicha distro desde un modo Live DVD.
Lo primero necesitamos descargar la distribución desde la siguiente pagina oficial de la distro Linux: http://www.caine-live.net/.

CAINE no requiere instalación, ya que se trata de un Live DVD, es así que se puede trabajar desde una maquina virtual, pero si embargo tiene ciertas dificultades al emplear una maquina virtual ya que en el próximo reinicio toda la información realizada con CAINE se perderá, salvo unas copias de seguridad.

Tras la ejecución de caine Linux vamos utilizar una de las herramientas sin duda es la mejor y muy utilizada el Autopsy

El programa autopsy corre en diversos sistemas operativos como Linux, Unix y hasta en el sistema operativo Microsoft.

Al ejecutar autopsy, inmediatamente se abre el navegador, que debe estar configurado para navegar en line, es decir debemos deshabilitar la opción work offline, desde la barra de menú, opción archivo (ver figura 1) y de esta manera accedemos a la primera presentación de en case.


Figura 1: Inicio Autospy.

Para iniciar por primera vez una recolección y análisis de evidencia digital, es importante previamente haber obtenido la réplica o imagen del disco donde reside la evidencia. Una vez iniciada la interfaz gráfica de autopsy, se procede a la creación de un nuevo caso.

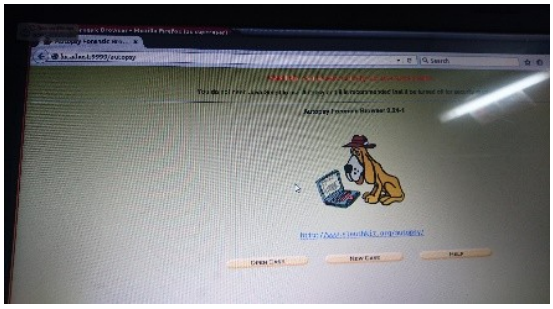

Figura 2: Iniciando el caso.

Al dar click a newcase, se despliega un formulario para diligenciar los datos básicos del nuevo caso (Nombre del caso, descripción, investigador), como se observa en la siguiente figura.

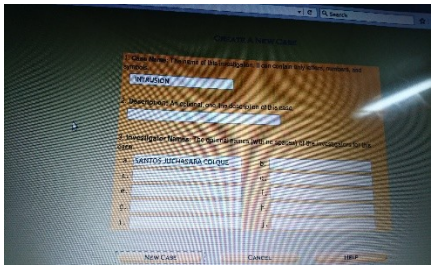

Figura 3: Formulario de datos.

Previamente se debe contar con una réplica o imagen bit a bit del disco donde reside la evidencia. Previamente hemos creado un archivo de imagen llamado imagen.dd. Se introduce la ruta de ubicación y nombre del archivo, las demás opciones permanecen por defecto.

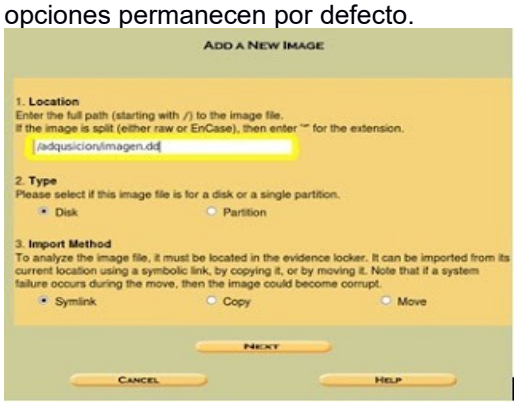

Figura 4 Obteniendo Imagen.

Una vez efectuado paso a paso los procesos anteriormente descritos, se obtienen los volúmenes que fueron encontrados en la imagen, para su respectiva exploración.

Figura 5: Volúmenes encontrados

Al ingresar a la opción de análisis, podemos evidencia cada uno de los archivos tanto temporales, permanentes, eliminados o averiados, que residen en la imagen o replica extraída del medio de almacenamiento original.

Figura 6: Evidencias Obtenidas

Como se observa en la figura anterior, los archivos que no son permanentes o que han sido borrados, se encuentra en color rojo, los demás archivo de color azul son permanentes. Teniendo en cuenta que la cantidad de archivos encontrados en la imagen puede ser demasiadamente extensa, autopsy cuenta con una barra de menús, que tienen la opción de buscar archivos o evidencias, por palabras claves, iniciales, tipo de archivos, matadatos, sectores específicos del disco y otras series de opciones, que permiten optimizar al máximo la búsqueda de evidencia.

Por cada evidencia encontrada Autopsy genera un completo reporte sobre el estado, atributos, características y contenido de dicha evidencia. Estos reportes son de gran ayuda en el momento del análisis de la evidencia y como elemento probatorio, en caso de que exista un proceso legal llevado a juicio.

Es una herramienta muy imprescindible que un perito informático forense debe aplicar para analizar la imagen de disco más aun cuando los procesos son jurídicas ante una instancia competente.

IV. CONCLUSIÓN

Las computadoras cotidianamente están sujetos ser atacados por intrusos en la cual acceden

mediante la red para apoderarse de los datos que existen en los ordenadores de una empresa y debido a esto la empresa entraría en quiebra total debido a que los datos en el recurso mas valioso con la cual cuenta para la toma de decisiones.

Sin embargo tanto es el avance de la ciencia y la tecnología lo cual nos provee de ciertas herramientas para poder realizar un peritaje al sistema informático en su conjunto, este peritaje deberá ser realizado por un profesional entendido en ciencias forenses, para poder descubrir, documentar, evidenciar, analizar, ante un crimen informático cometido en una organización.

Para lo cual este perito forense realizaría un análisis siguiendo una metodología asistido por un software específico, en este caso existen multitud de software libres y comerciales, pero sin embargo en esta oportunidad se ha utilizado software libre, específicamente CAINE Linux la cual es una distribución Live DVD asado en debían Ubuntu.

Esta distribución os ofrece una variedad de herramientas y utilidades para el área de la ciencia forense digitales. No se necesita instalarse como e la prueba se demostró, con solo ejecutar del DVD se puede aplicar el análisis forense.

Autospy es una de las mejores herramientas para el análisis forense y que trata de descubrir información borrada de un disco duro a través de una imagen de disco. La herramienta es de fácil manejo basado en web, por su puesto existen muchas herramientas en la cual uno pude aplicar según necesidades como para: redes, disco duro, archivos, etc.

V. BIBLIOGRAFIA

Arquillo Cruz, José . 2007. HERRAMIENTA DE APOYO PARA EL ANÁLISIS FORENSE DE COMPUTADORAS. jaen : s.n., 2007.

Arteaga Mejía, Luis Miguel . 2001. El sistema operativo GNU. [En línea] 2001. [Citado el: 1 de Julio de 2016.] https://www.gnu.org/philosophy/free-sw.es.html.

Martínez Retenaga, Asier . 2014. Guia de toma de evidencias en windows. 2014.

Rifà Pous, Helena , Serra Ruiz, Jordi y Rivas López, José Luis . 2009. Análisis forense de sistemas informáticos. Catalunya : Eureca Media, SL, 2009.

Wikipedia. 2015. CAINE Linux. [En línea] 18 de Mayo de 2015. [Citado el: 1 de Julio de 2016.] https://es.wikipedia.org/wiki/CAINE_Linux.