Modelo para el Análisis Forense de una Plataforma Windows

González Rodríguez, John Ricardo
johntato26@hotmail.com
Universidad Piloto de Colombia

Resumen—En el proceso de una investigación forense es primordial seguir los procedimientos adecuados sobre la identificación, obtención, análisis y presentación de una evidencia digital. Asegurado lo anterior se garantiza que estas muestras sean admitidas y que no serán material de controversia por la contraparte en un juicio. Actualmente hay diversidad de plataformas de usuario o sistemas operativos que requieren de un tratamiento particular al momento de recolectar evidencias digitales. Se destacan una serie de elementos claves que se deben considerar sobre los medios contendores de la información, ya que esto nos permite tener mayor claridad sobre los datos que se quieren conseguir y la ubicación precisa en donde pueden ser consultados para su posterior análisis.

Índice de Términos—Evidencia, partición, clúster, MBR, VBR, volátil, hashes, file slack, drive slack.

I. INTRODUCCIÓN

El siguiente Documento de estudio plantea procedimientos estándar para la recolección de datos en una plataforma Windows, igualmente describe los aspectos técnicos que todo investigador debe involucrar en la fase de recolección de evidencias digitales para que estás conserven las propiedades originales tomadas del equipo que es sujeto de la investigación.

Los procesos que se desarrollan en torno a una investigación forense deben desarrollarse por parte de un grupo especializado en la respuesta a incidentes o investigación forense, el cual se encarga de documentar de manera detallada teniendo siempre en cuenta la importancia de la trazabilidad sobre los elementos que puedan considerarse como evidencias dentro de un proceso judicial. [4] En un proceso de análisis forense digital (AFD) se pueden destacar 5 fases que son:

1. Identificación de la escena u incidente
2. Recopilación de evidencias
3. Preservación de la evidencia
4. Análisis de la evidencia
5. Documentación y presentación de la evidencia.

En el siguiente documento se hará una descripción especifica de cómo se pueden obtener evidencias digitales de un equipo que tiene instalada una distribución Windows.

II. CONCEPTOS PRELIMINARES

A. *Sistemas de Archivos*

Un sistema de archivos es la estructura subyacente que un equipo usa para organizar los datos de un disco duro. Si está instalando un disco duro nuevo, tiene que realizar las particiones y formatearlo empleando un sistema de archivos para poder comenzar a almacenar datos o programas. En Windows, las tres opciones del sistema de archivos que tiene para elegir son NTFS, FAT32 y la anterior y poco usada FAT (también conocida como FAT16).

B. *NTFS*

Es el sistema de archivos preferido para esta versión de Windows. Tiene muchos beneficios respecto al sistema de archivos FAT32, entre los que se incluye:

- La capacidad de recuperarse a partir de algunos errores relacionados con el disco automáticamente, lo que FAT32 no puede hacer.

- Compatibilidad mejorada para discos duros más grandes.
- Mejor seguridad porque puede utilizar permisos y cifrado para restringir el acceso a archivos específicos para usuarios aprobados.

C. FAT

Es el sistema menos usado, FAT se usa en versiones anteriores de sistemas operativos de Windows, incluyendo Windows 95, Windows 98 y Windows Millennium Edition.[4]

D. FAT32

Este sistema de archivos FAT32 no tiene la seguridad que NTFS proporciona, por lo que si tiene una partición FAT32 o volumen en el equipo, cualquier usuario que tenga acceso al equipo puede leer el archivo incluido. FAT32 también tiene limitaciones de tamaño. No puede crear una partición FAT32 mayor que 32GB en esta versión de Windows y no puede almacenan un archivo mayor que 4GB en una partición FAT32.

III. Estructura Física del Disco Duro

Los discos duros que comúnmente utilizamos IDE, SATA, SCSI está compuesto por las siguientes estructuras:

A. Platos:

También llamados discos. Estos discos están elaborados de aluminio o vidrio recubiertos en su superficie por un material ferromagnético apilados alrededor de un eje que gira gracias a un motor, a una velocidad muy rápida. El diámetro de los platos oscila entre los 5cm y 13 cm.

B. Cabezal de lectura/escritura:

Es la parte del disco duro que lee y escribe los datos del disco.

C. Impulsor de Cabezal:

Es un motor que mueve los cabezales sobre el disco hasta llegar a la pista adecuada, donde esperan que los sectores correspondientes giren bajo ellos para ejecutar de manera efectiva la lectura/escritura.

D. Pistas:

La superficie de un disco está dividida en unos elementos llamadas pistas concéntricas, donde se almacena la información. Las pistas están numeradas desde la parte exterior comenzando por el 0. Las cabezas se mueven entre la pista 0 a la pista más interna.

E. Cilindro:

Es el conjunto de pistas concéntricas de cada cara de cada plato, los cuales están situadas unas encima de las otras. Lo que se logra con esto es que la cabeza no tiene que moverse para poder acceder a las diferentes pistas de un mismo cilindro. Dado que las cabezas de lectura/escritura están alineadas unas con otras, la controladora de disco duro puede escribir en todas las pistas del cilindro sin mover el rotor. Cada pista está formada por uno o más cluster.

F. Sector:

Las pistas están divididas en sectores, el número de sectores es variable. Un sector es la unidad básica de almacenamiento de datos sobre los discos duros. Los discos duros almacenan los datos en pedazos gruesos llamados sectores, la mayoría de los discos duros usan sectores de 512 bytes cada uno. Comúnmente es la controladora del disco duro quien determina el tamaño de un sector en el momento en que el disco es formateado, en cambio en algunos modelos de disco duro se permite especificar el tamaño de un sector.(Ver imagen 1).

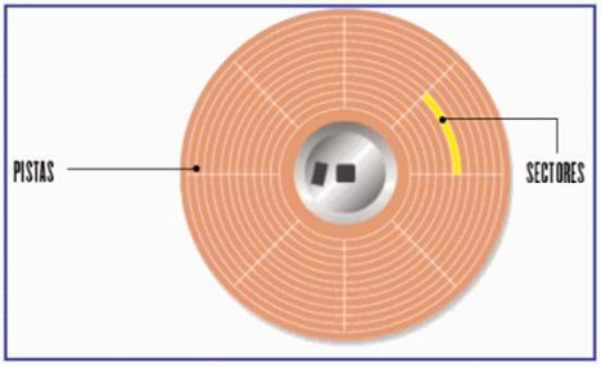

Imagen No.1

G. Cluster:

Es un grupo de sectores, cuyo tamaño depende de la capacidad del disco.

IV. GEOMETRÍA DEL DISCO DURO

La geometría del disco se refiere al análisis intrínseco que verifica las propiedades del medio de almacenamiento material de estudio, tales como tamaño, sistema de archivos y espacio sin particionar.

Todo disco tiene geometría la cual se puede visualizar en la configuración del BIOS, en la tarjeta madre del computador se puede ver esto representado como Cilindros, Cabezas y Sectores.

Lo que se busca a través de este análisis es establecer patrones y características propias del material probatorio que conduzcan al investigador a la ubicación de pruebas sustanciales.

A. File Slack

Un FILE SLACK es la información que no pertenece a un archivo pero que forma parte de los sectores del clúster que no utiliza.

B. Drive Slack

Un DRIVE SLACK es el espacio sin particionar del disco duro o medio de almacenamiento.

V. PLATAFORMAS

En un análisis forense con frecuencia se debe analizar información relacionada con el sistema, lo cual implica conocer cómo llegar los archivos que de acuerdo a la plataforma pueden estar situados en diferentes ubicaciones.

A. Microsoft Windows

En este sistema los archivos de registro podrán encontrarse en la aplicación del sistema *regedit.exe* o con un medio aislado del disco duro como pendrive, usb o cdrom empleando sus propias herramientas como *OSForensics*, podrá exportar el registro en formato plano sin modificarlo para realizar posteriormente las consultas que requiera dentro de la investigación mediante la opción *Registry viewer. (Ver figura 2).*

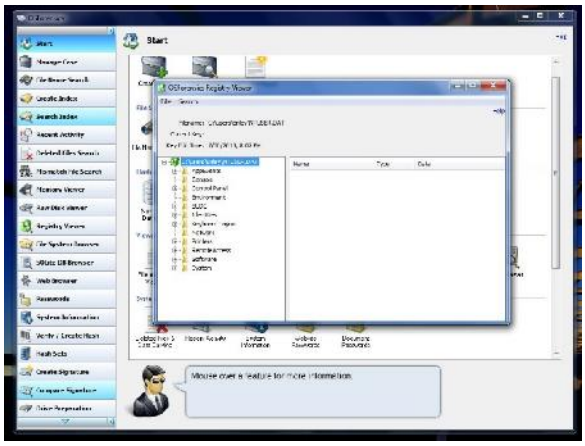

Figura No. 2

Las claves principales que conforman la estructura del registro de Windows HKLM son:

- HARDWARE
- SAM
- SECURITY
- SOFTWARE
- SYSTEM

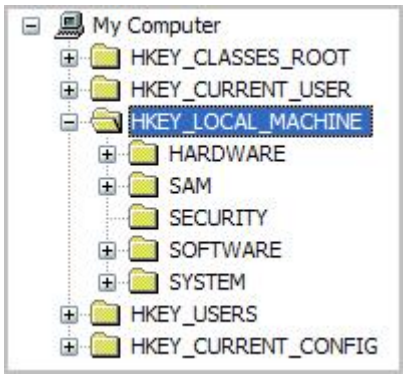

Figura No. 3

En estos archivos se puede ubicar una cantidad importante de información que nos permitirá identificar datos propios de la sesión de usuario (SAM), configuración de Windows (SYSTEM), programas (SOFTWARE), detalles de la configuración (DEFAULT) y configuración de software de usuario (NT USER.DAT) entre otros. *(Ver figura 3).*

VI. PARTICION DE DISCO

Una partición es una división lógica de un medio o unidad de almacenamiento de datos que actúan como si fuese dispositivos independientes en un sistema operativo. En las versiones más

recientes de Windows el sistema de archivos comúnmente empleado es NTFS sobre la cual se crea una partición reservada para el sistema la cual no es visible para el sistema operativo.

El registro MBR es el sector 0 de un dispositivo de almacenamiento de datos, es empleado para el arranque de un sistema operativo o para almacenar la tabla de particiones. El sector 0 está compuesto de 512 bytes, de los cuales los primeros 446 bytes son para el gestor de arranque, los 64 bytes siguientes para la tabla de particiones que pude alojar máximo 4 particiones primarias divididas en registros de 16 bytes o tres particiones primarias y 1 extendida que a su vez puede contener varias particiones lógicas hasta un máximo de 23, los 2 últimos bytes son para la firma de la unidad booteable.

La VBR es el sector de inicio de una partición, toda partición debe iniciar con una VBR.
Las particiones pueden ser de tres tipos:

A. Partición primaria

Son las divisiones primarias del disco, solo puede haber 4 de éstas o 3 primarias y una extendida. Depende de una tabla de particiones. Un disco físico completamente formateado consiste, en realidad, de una partición primaria que ocupa todo el espacio del disco y posee un sistema de archivos.[3] A este tipo de particiones, prácticamente cualquier sistema operativo puede detectarlas y asignarles una unidad, siempre y cuando el sistema operativo reconozca su formato (sistema de archivos).

B. Partición extendida:

También conocida como partición secundaria es otro tipo de partición que actúa como una partición primaria; sirve para contener múltiples unidades lógicas en su interior. Fue ideada para romper la limitación de 4 particiones primarias en un solo disco físico. Solo puede existir una partición de este tipo por disco, y solo sirve para contener particiones lógicas. Por lo tanto, es el único tipo de partición que no soporta un sistema de archivos directamente. [3]

C. Partición lógica

Ocupa una porción de la partición extendida o la totalidad de la misma, la cual se ha formateado con un tipo específico de sistema de archivos (FAT32, NTFS, ext2, etc.) y se le ha asignado una unidad, así el sistema operativo reconoce las particiones lógicas o su sistema de archivos. Puede haber un máximo de 23 particiones lógicas en una partición extendida. [3]

VII. FASES DE LA INVESTIGACION FORENSE

Realizar una investigación forense digital implica tomar una serie de precauciones y seguir procedimientos que permitan presentar de manera adecuada y legal una evidencia digital antes un juez, a continuación se listan 5 fases primordiales que debe seguir el investigador. [1]

A. Identificación del incidente o escena

Asegure el lugar que hace parte del entorno donde se presume que se ha cometido la conducta delictiva, debe identificar los elementos tecnológicos que puedan constituir una evidencia digital como medios de almacenamiento, pc's, servidores, laptops, etc. Utilice los medios de fijación necesarios como fotografía, video, planimetría y descriptivos.

B. Recopilación de evidencias

Asegúrese de tener listas sus herramientas en un medio de almacenamiento booteable como cd-rom, pendrives, usb que le permitan mantener inmodificables las evidencias. Tome nota de cada tarea realizada y sea lo más descriptivo en el proceso de recolección de evidencias.

Entre los aspectos a considerar en la extracción de datos volátiles de un pc que se encuentre encendido tenemos:

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros

- Contenido de otros dispositivos de almacenamiento.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real [4]:

- Fecha y hora.
- Procesos activos.
- Conexiones de red.
- Puertos TCP/UDP abiertos y aplicaciones asociadas "a la escucha".
- Usuarios conectados remota y localmente.

Tenga en cuenta que los datos extraídos deben almacenarse en un medio esterilizado que no esté comprometido y que cuenta con el suficiente espacio para contener los datos.

Como norma general es recomendable que se realicen siempre imágenes forenses de los discos duros para su posterior análisis previniendo trabajar directamente sobre el medio físico original, las imágenes puede hacerse con herramientas como FTK Imager, OS Forensics, previniendo la escritura sobre el medio físico empleando bloqueadores en las conexión al PC del investigador.

C. Preservación de la evidencia

Aunque el primer motivo que le habrá llevado a la recopilación de evidencias sobre el incidente sea la resolución del mismo, puede que las necesite posteriormente para iniciar un proceso judicial y en tal caso deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación utilizando métodos adecuados para el almacenamiento y etiquetado de las evidencias.

Como primer paso deberá realizar dos copias de las evidencias obtenidas, genere una suma de comprobación de la integridad de cada copia mediante funciones de hash tales como MD5 o SHA1. Incluya estas firmas en la etiqueta de cada copia de la evidencia sobre el propio CD o DVD, incluya también en el etiquetado la fecha y hora de creación de la copia, nombre cada copia.

Realice cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia.

D. Análisis de la evidencia

Una vez que se tienen las evidencias digitales recopiladas y almacenadas de forma adecuada, se procede con el Análisis Forense, cuyo objetivo es reconstruir con todos los datos disponibles la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior a la conducta delictiva, hasta el momento de su descubrimiento.

Antes de comenzar el análisis de las evidencias deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar. Lo más recomendable es no manipular los discos duros o medios de almacenamiento originales para lo cual deberá trabajar con las imágenes que recopiló como evidencias, o mejor aún con una copia de éstas, tenga en cuenta que necesitará montar esas imágenes tal cual estaban en el sistema comprometido haciendo uso de su pool de herramientas.

El objetivo es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes.

Para recuperar archivos eliminados puede emplear herramientas tales como Recuva, File Recovery o Diskdigger que cuentan con versiones de uso libre y que permiten buenos resultados.

Piense que está buscando "una aguja en un pajar", por lo que deberá ser metódico, vaya de lo general a lo particular, por ejemplo parta de los archivos borrados, intente recuperar su contenido, anote su fecha de borrado y compárela con la actividad del resto de los archivos, tenga presente que debe pensar similar al presunto para determinar los sucesos que se desarrollaron frente a la conducta.

E. Documentación de la evidencia

Entre de los documentos que debería preparar tenemos:

- Documento de cadena de custodia de la evidencia.
- Rótulos para cada una de las evidencias
- Acta de la diligencia
- Informe Técnico
- Informe Ejecutivo

El informe técnico consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. [1] Entre los puntos que deberá contener dicho informe se tienen los siguientes:

- Introducción
- Descripción y evidencia del hash
- Geometría del disco
- Recuperación de información eliminada
- Reparación de archivos dañados
- Análisis del sistema operativo
- Definición de Heurística
- Contextualización de la conducta identificada
- Capturas de las evidencias recopiladas

El Informe Ejecutivo consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Debe constar de unas pocas páginas para exponer lo sucedido a personal no especializado en sistemas informáticos, como por ejemplo el departamento de Recursos Humanos, Administración o Directivos. [1]

VIII. CONCLUSIONES

El éxito de una investigación depende de que se sigan procedimientos adecuados y dentro de un marco legal en la recopilación de evidencias de tipo digital, solo así podrá presentarse con toda seguridad ante un juez de un tribunal.

El investigador forense debe tener en cuenta el tipo de licenciamiento de las herramientas que utilice para la investigación ya que omitir estos detalles puede abrir la posibilidad a que las evidencias halladas sean controvertidas por la contraparte.

REFERENCIAS

[1] M. L. Delgado, “Analisis Forense Digital,” 2nd ed, jun 2007.
[2] J. Ashcroft, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement". U.S. Dep. of Justice, Apr. 2004
[3] D. Ditrich y E. Sarkisov, “Análisis Forense Digital GNU/Linux”. 2002
[4] I. V. Espejo, “Anáisis Forense de un Sistema Windows,” *ISOFT PLS*, 3ra Jornada Tecnológica Informando. 2008

URL’s

http://www.elhacker.net/InfoForenseWindows.html
http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
http://blog.ismaelvalenzuela.com/wp-content/uploads/2008/04/forense_windows-ismael_valenzuela.pdf
http://www.monografias.com/trabajos37/discos-duros/discos-duros2.shtml
http://www.hostingyvirtualizacion.com/conceptos-logicos-de-un-disco-duro/
http://registryonwindows.com/es/registry-structure.php
http://www.xatakawindows.com/bienvenidoawindows8/que-son-las-particiones-de-disco-y-como-puedo-crearlas-en-windows-8
http://www.wadalbertia.org/foro/viewtopic.php?t=4630

Autor
John Ricardo González R.
Especialista en Seguridad Informática
Universidad Piloto de Colombia
2013