CAPÍTULO III

"La duda es la madre del descubrimiento."
Ambrose Bierce

HERRAMIENTAS DE INVESTIGACIÓN FORENSE

3.1. Herramientas de informática forense.

3.2. Herramientas para la recolección de evidencia digital.

3.3. Herramientas para el monitoreo y/o control de computadores.

3.4. Herramientas de marcado de documentos.

3.5. Herramientas de Hardware.

3.1. HERRAMIENTAS DE INFORMÁTICA FORENSE

En los últimos años se ha disparado el número de herramientas para computación forense, es posible encontrar desde las más sencillas y económicas, como programas de prestaciones muy limitadas y con costos de menos de US$300, hasta herramientas muy sofisticadas que incluyen tanto software como dispositivos de hardware. Con esa amplia cantidad de alternativas, es necesario tener claro el objetivo que se persigue, ya que existen varios tipos básicos de herramientas, no todos los productos sirven para todo, algunos están diseñados para tareas muy específicas y más aún, diseñados para trabajar sobre ambientes muy específicos, como determinado sistema operativo.

Siendo la recolección de evidencia una de las tareas más críticas, y donde asegurar la integridad de esta es fundamental, el objetivo es entonces establecer el nivel de integridad, ya que algunas herramientas no permiten asegurar que la evidencia recogida corresponda exactamente a la original. Igual de importante es que durante la recolección de la evidencia se mantenga inalterada la escena del crimen.

Todas estas consideraciones son las que se deben tener en cuenta a la hora de seleccionar una herramienta para este tipo de actividad, claro sin dejar de lado los detalles normales en cualquier caso de adquisición de tecnología, como presupuesto, soporte, capacitación, idoneidad del proveedor, etc.

Una de las alternativas que siempre se deberá evaluar es si incurrir en una inversión de este tipo, a la que muy seguramente se tendrá que adicionarle el valor de la capacitación que en algunos casos puede superar el costo mismo del producto, o, contratar una firma especializada para esta tarea, que generalmente cuenta no solo con una herramienta, sino con varias herramientas.

A continuación se presenta una clasificación que agrupa en cuatro, los tipos de herramientas de computación forense, se hace mención de algunos productos sin pretender en ningún momento dar una calificación, de igual forma la omisión de alguno no significa la desaprobación del mismo.

3.2. HERRAMIENTAS PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL

Las herramientas para la recolección de evidencia representan el tipo de herramienta más importante en la informática forense, porque su centro de acción se enfoca en el que para muchos es el punto central. Su uso es necesario por varias razones:

- Gran volumen de datos que almacenan los computadores actuales.
- Variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- Necesidad de recopilar la información de una manera exacta, que permita verificar que la copia es idéntica al original y además mantener inalterada la escena del delito.
- Limitaciones de tiempo para analizar toda la información.
- Volatilidad de la información almacenada en los computadores, alta vulnerabilidad al borrado, con una sola instrucción se pueden eliminar hasta varios gigabytes.
- Empleo de mecanismos de encriptación, o de contraseñas.
- Diferentes medios de almacenamiento, discos duros, CDs y cintas.

Según las características que se acaba de mencionar, las herramientas de recolección de evidencia deben reunir características que permitan manejar estos aspectos, pero además incluir facilidades para el análisis. A continuación se presentan las principales facilidades de recolección y análisis que se esperaría de una buena herramienta, para lo cual se

siguió como guía las que ofrecen Encase de Guidance Software y la familia de productos Image Master de Law Enforcement & Comp. Forensic:

- Dispositivos que permitan copiara gran velocidad, de diferentes medios, y de diferentes tipos de dispositivos, como cables paralelos, seriales, USB, etc.
- Asegurar un copiado sin pérdida de datos y que corresponde a una copia idéntica del dispositivo afectado.
- Copia comprimida de discos origen para facilitar el manejo y conservación de grandes volúmenes de información. Además muy práctico cuando se deben manejar investigaciones de varias computadoras o varios casos a la vez.
- Búsqueda y análisis de múltiples partes de archivos adquiridos. Debe permitir la búsqueda y análisis de múltiples partes de la evidencia en forma paralela en diferentes medios como discos duros, discos extraíbles, CDs y otros.
- Capacidad de almacenamiento en varios medios: También es necesario poder almacenarla información recabada en diferentes medios, como discos duros IDE o SCSI, ZIP driver. Uno de los medios idóneos son los CD-ROM porque contribuyen a mantener intacta la integridad forense de los archivos.
- Variables de ordenamiento y búsqueda: debe permitir el ordenamiento y búsqueda de los archivos de la evidencia de acuerdo con diferentes campos, incluyendo campos como lastres marcas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos, extensiones y propiedades.
- Capacidad para visualización de archivos en diferentes formatos, además de galerías de archivos gráficos.
- Capacidad para representar en forma gráfica estructuras de datos, archivos, volúmenes, directorios, árboles, organización y en general tópicos de interés que faciliten el trabajo de análisis.

- Búsqueda automática y análisis de archivos de tipo Zip, Cab, Rar, Arj[1] y en general formatos comprimidos, así como archivos adjuntos de correos electrónicos.
- Identificación y análisis de firmas de archivos, es decir aquellos bytes que generalmente se encuentran al comienzo de un archivo y están directamente relacionadas con el tipo de archivo y por consiguiente con su extensión. Con la capacidad de análisis de firmas es posible detectar si un archivo fue renombrado, pues el solo cambio de su extensión para hacerlo aparecer de otro tipo, no genera cambios en su firma.
- Análisis electrónico del rastro de intervención. Facilidades para recuperar de manera eficiente y no invasiva información crítica como sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento.
- Soporte de múltiples sistemas de archivo. Una herramienta de recopilación de evidencia debe estar en capacidad de recuperar información de diversos sistemas de archivos; DOS, Windows (95/98/NT/2000/XP/2003 Server), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, OpenBSD), CD-ROM, y los sistemas de archivos DVDR. Esta es la limitación de algunas herramientas, porque están diseñadas para un número limitado de sistemas de archivos o es necesario adquirir módulos por separado, lo que incrementa su costo.
- Captura y manejo automático de cualquier sistema operativo: reconocimiento automático del sistema operativo origen, haciendo cero invasiva la extracción de la información y asegurando la más alta fidelidad.
- Vista de archivos y otros datos en el espacio unallocated[2]: Una buena herramienta deberá proveer facilidades para tener una vista del disco duro de origen, de los archivos borrados y todos los datos en el espacio unallocated, el espacio ocupado por el archivo dentro

[1]Algoritmos de compresión, que sirven para reducir el tamaño de los archivos y así ocupar menos espacio y tiempo de transferencia.
[2] Espacio sin asignar, sin un sistema de archivos.

del clúster, archivos Swap[3] y Print Spooler (Cola de impresión), todo esto de manera gráfica.

- Recuperación de passwords: en muchas ocasiones la información recuperada puede estar protegida con passwords por lo que será necesario descifrarlos. Generalmente esta facilidad no viene incluida en estas herramientas, se deben comprar por separado.
- Herramientas de gestión; una herramienta debería incluir facilidades de gestión para el manejo de los expedientes y reportes de las investigaciones.

A continuación se relacionan algunas herramientas de este tipo, aunque no necesariamente reúnen todas las características mencionadas:

3.2.1. EnCase

EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc. (http://www.guidancesoftware.com), permite asistir al investigador forense durante el análisis de un crimen digital.

Se escogió detallar sobre esta herramienta por tratarse del software líder en el mercado, el producto más ampliamente difundido y de mayor uso en el campo del análisis forense.

Algunas de las características más importantes de EnCase son:

- **Copiado Comprimido de Discos Fuente.** Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los originales. Esta característica ahorra cantidades importantes de espacio en el disco del computador del laboratorio forense, de esta

[3]Archivo que cumple las mismas funciones que una partición Swap, o sea proveer de memoria virtual.

forma permite trabajar en una gran diversidad de casos al mismo tiempo, examinándola evidencia y buscando en paralelo.

- **Búsqueda y Análisis de Múltiples partes de archivos adquiridos.** EnCase permite al investigador buscar y analizar múltiples partes de la evidencia. Muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos zip y otros tipos de dispositivos de almacenamiento de información. Con Encase, el investigador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista. En varios casos la evidencia puede ser ensamblada en un disco duro grande o un servidor de red y también buscada mediante Encase en un solo paso.
- **Diferente capacidad de Almacenamiento.** Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.
- **Varios Campos de Ordenamiento, Incluyendo marcas de tiempo.** Encase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres marcas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.
- **Análisis Compuesto del Documento.** EnCase permite la recuperación de archivos internos y meta-datos[4] con la opción de montar directorios como un sistema virtual para la visualización de

[4] Los metadatos son datos altamente estructurados que describen información, describen el contenido, la calidad, la condición y otras características de los datos.

la estructura de estos directorios y sus archivos, incluyendo el *slack*[5] interno y los datos del espacio *unallocated*.

- **Búsqueda Automática y Análisis de archivos de tipo Zip y adjuntos de E-Mail.** Al igual que un antivirus EnCase es capaz de leer este tipo de archivos, pero en este caso no en busca de virus, sino en busca de evidencia.
- **Firmas de archivos, Identificación y Análisis.** La mayoría de los gráficos y de los archivos de texto comunes contienen una pequeña cantidad de *bytes* en el comienzo del sector, los cuales constituyen una firma del archivo. EnCase verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que un sospechoso haya escondido un archivo o simplemente lo haya renombrado, EnCase detecta automáticamente la identidad del archivo, e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle.
- **Análisis Electrónico del Rastro de Intervención.** Sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación por computador. EnCase proporciona los únicos medios prácticos de recuperar y de documentar esta información de una manera no invasora y eficiente. Con la característica de ordenamiento, el análisis del contenido de archivos y la interfaz de EnCase, virtualmente toda la información necesitada para un análisis de rastros se puede proporcionar en segundos.
- **Soporte de Múltiples Sistemas de Archivo.** EnCase reconstruye los sistemas de archivos forenses de DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVDR.

[5] Espacio que queda libre en un clúster luego de almacenar un archivo.

Con EnCase un investigador es capaz de ver, buscar y ordenar archivos desde estos discos con otros formatos, en la misma investigación de una manera totalmente limpia y clara.

- **Vista de archivos y otros datos en el espacio Unallocated.** EnCase provee una interfaz tipo Explorador de Windows y una vista del Disco Duro de origen, también permite ver los archivos borrados y todos los datos en el espacio *Unallocated*.

  También muestra el *Slack File* con un color rojo después de terminar el espacio ocupado por el archivo dentro del *clúster*, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos *Swap* y *Print Spooler*son mostrados con sus marcas de datos para ordenar y revisar.
- **Integración de Reportes.** EnCase genera el reporte del proceso de la investigación forense como un estimado. En este documento realiza un análisis y una búsqueda de resultados, en donde se muestra el caso incluido, la evidencia relevante, los comentarios del investigador, favoritos, imágenes recuperadas, criterios de búsqueda y tiempo en el que se realizaron las búsquedas.
- **Visualizador Integrado de imágenes con Galería.** EnCase ofrece una vista completamente integrada que localiza automáticamente, extrae y despliega muchos archivos de imágenes como .gif y .jpg del disco. Seleccionando la Vista de Galería se despliega muchos formatos de imágenes conocidas, incluyendo imágenes eliminadas. El investigador puede después escoger las imágenes relevantes al caso e inmediatamente integrar todas las imágenes en el reporte de EnCase. No es necesario ver los archivos gráficos usando software de terceros, a menos que el formato de archivo no sea muy conocido y todavía no sea soportado por EnCase.

EnCase es un software costoso, y en Estados Unidos los costos se dividen así:

- Gobierno y Educación US$2,850
- Sector Privado US$3,600

Actualmente EnCase se encuentra en su versión 6.13+.

3.2.2. The Coroner's Toolkit

The Coroner's Toolkit (TCT) es un suite de aplicaciones escritas por Dan Farmer y Wietse Venema para un curso organizado por IBM sobre un estudio forense de equipos comprometidos, estas herramientas funcionan bajo sistemas UNIX, este kit de herramientas fue presentado por primera vez en agosto de 1999.

TCT requiere Perl 5.004 o superior, aunque Perl 5.000 es suficiente para usar el kit TCT y hacer el análisis, la última versión conocida de este kit es la 1.19. [25]

Las aplicaciones más importantes de la suite son:

- **grave-robber.-** Una utilidad para capturar información sobre inodes[6], y que luego pueda ser procesada por el programa mactime del mismo toolkit.
- **unrm y lazarus.-** Herramientas para la recuperación de archivos borrados (logs, RAM, swap, etc.). Estas aplicaciones identifican y recuperan la información oculta en los sectores del disco duro.
- **Mactime.-** El programa sirve para visualizar en los archivos y directorios su timestamp MAC (Modification, Access, y Change).

De estas herramientas, las más útiles e interesantes son grave-robber y mactime; unrm y lazarus son buenas si se tiene mucho tiempo y espacio

[6] Un inodo contiene las características (permisos, fechas, ubicación, pero NO el nombre) de un archivo regular, directorio, o cualquier otro objeto que pueda contener el sistema de archivos.

libre en el disco, ya que el programa necesita identificar información en los sectores del disco para recuperar los archivos (logs, fuentes, etc.) borrados por los intrusos.

La función más básica de grave-robber es de escanear algunas o todos los sistemas de archivos con función stat() para obtener información de los inodes. Grave-robber crea en la carpeta /data un directorio llamado como el nombre del host de la máquina y allí almacena los inodes, dentro del archivo body. El programa mactime luego ordena los resultados y los muestra según el tiempo, el tipo de archivo, tamaño y a quién pertenece junto con el path.

Desde el listado, se puede sacar algunas conclusiones sobre la actividad que ha ejercido el o los intrusos durante el tiempo que estuvieron dentro del sistema. Eso puede incluir instalación de caballos de Troya, backdoors (puerta trasera), sustitución de archivos legítimos del sistema operativo, descarga de herramientas, modificación de las librerías del sistema o instalación de rpm's/deb's/pkg's etc. También se puede ver desde aquí la creación de directorios ocultos, ejecución de los comandos de sistema operativo, compilación y ejecución de aplicaciones. Toda esa información que nunca se almacena de forma directa, puede ser extraída de la información que da mactime.

3.2.3. ByteBack - TechAssist, Inc

Software especializado en copia de discos duros de cualquier formato, transferencia a otros medios internos o externos, sistema de análisis binario para recuperación no destructiva de particiones y sectores de arranque tipo FAT y NTFS (NT), búsqueda binaria, md5 hash integrado, solución multi ambiente, acceso directo, diagnóstico de superficie, control de bajo nivel de hardware. Disponible la versión de prueba enwww.toolsthatwork.com/computer-forensic.htm.

3.2.4. The Access Data Forensic Toolkit (FTK)

Reconocimiento de 270 formatos, explorador gráfico, generación de logs y reportes de casos, recuperación de passwords, indexación por texto, búsqueda avanzada de imágenes JPEG y texto de internet, patrones binarios para búsqueda, recuperación automática de archivos y particiones borradas, creación personalizada de filtros de archivos, sistemas de archivo soportados NTFS, NTFS compressed, FAT 12/16/32, y Linux ext2 & ext3, análisis de archivos de correo electrónico y Zip, identificación de firmas de archivos de sistemas operativos estándar y programas de archivos.

Sus características más importantes son:

- Búsqueda en el índice de texto completo para resultados de búsqueda de texto instantánea.
- Creación de informes avanzados.
- Recupera automáticamente archivos y particiones eliminados.
- Extraer datos automáticamente desde archivos comprimidos PKZIP, WinZip, WinRAR, GZIP y TAR.
- Identifica el tipo de archivo por el contenido y no por la extensión.

Disponible en el enlace http://www.accessdata.com/downloads.html.

3.2.5. Data Recovery Kit - LCTechonogy

Suite compuesta por File recovery for windows, File recovery professional, y Photo recovery, todas estas utilidades brindan múltiples opciones de recuperación en computadoras IBM basadas en Intel, compatibles con sistemas operativos Windows.

FILERECOVERY[24] para Windows es una multiplataforma imborrable para Windows 95/98/Me/NT/2000/2008/XP/Vista/Windows 7, etc. Además de ser compatible con formatos FAT12, FAT16, FAT32 y NTFS. Las opciones de Búsqueda y Filtro hacen que la recuperación de archivos sea rápida y fácil preservando completamente la estructura del directorio.

FILERECOVERY Professional permite al usuario recuperar datos de discos dañados en varias partes. Puede escanear y encontrar particiones perdidas, sectores de inicialización y otros componentes del sistema de archivos. Puede detectar unidades de discos aun cuando no están visibles en el explorador. Aparece en la pantalla la estructura completa del directorio del disco incluso cuando se trata de un sistema de archivos NTFS.

Se puede descargar una versión de prueba desde http://www.lc-tech.com/software/fusdetail.html.

3.2.6. COFEE

COFEE (Computer Online Forensic Evidence Extractor) es un dispositivo USB que dispone de 150 comandos que facilitan la obtención de pruebas desde una máquina sospechosa de haber intervenido en un delito. Permite descifrar contraseñas, rastrear la actividad reciente en Internet y acceder a los datos almacenados en el computador, todo ello sin necesidad de hacer una incautación de la máquina, ya que el análisis puede realizarse in situ.

Este es un producto desarrollado por Microsoft y que es distribuido de forma gratuita a las entidades policiales desde Junio del año 2008.

3.2.7. Safe Back - New Technologies Inc

Permite hacer copias espejo de archivos de backups o de discos duros completos (completo o partición), para creación de evidencia en sistemas de computador basados en Intel, transferencia de información a otros medios y preservación de evidencia.

Algunas características que presenta:

- Basado en DOS ya que Windows puede alterar los datos.
- Indaga la existencia de archivos ocultos cuando los sectores no presentan semejanza con el enlace de disco duro.
- Copia al 100% todas las áreas del disco duro.

Más información en: http://www.forensics-intl.com/safeback.html

3.2.8. The Forensic Tool Kit[21]

Consiste en un conjunto de herramientas diseñadas para funcionar en sistemas operativos Windows. Se pude descargar desde www.foundstone.com, en donde además se puede encontrar una serie de herramientas de seguridad adicionales para realizar investigaciones. Esta herramienta utiliza el intérprete de comandos cmd.exe para ejecutar las diferentes funciones que posee. Entre Ella se encuentran:

Comando	Función
afind	Realiza búsqueda de archivos por su tiempo de acceso, sin modificar la información de acceso al mismo.
hfind	Busca archivos ocultos en el Sistema Operativo.

sfind	Busca flujos de datos ocultos en el disco duro, éstos son distintos de los archivos ocultos y no aparecerán con herramientas normales del sistema operativo. Su importancia radica en que pueden usarse para ocultar datos o software dañino.
filestat	Ofrece una lista completa de los atributos del archivo que se le pase como argumento (uno cada vez).
hunt	Permite obtener información sobre un sistema que utiliza las opciones de sesión NULL, tal como usuarios, recursos compartidos y servicios.

Tabla. 3.1. Funcionalidades de The Forensic Toolkit

3.2.9. The Sleuth Kit and Autopsy [22]

Consiste en un conjunto de herramientas desarrolladas por *Brian Carrier* para entornos UNIX/Linux. Puede analizar archivos de datos de evidencias generados en discos duros, la cual permite obtener una imagen, es decir, una copia exacta bit a bit del disco duro que se desea investigar. Se puede descargar directamente desde www.sleuthkit.org e incluye la posibilidad de realizar múltiples investigaciones y guardar los resultados de manera separada.

Por otro lado, permite el acceso a estructuras de archivos y directorios de bajo nivel lo cual conlleva a la recuperación de archivos borrados. Además de esto, permite generar una línea temporal de archivos (*timestamp*), buscar palabras clave dentro de archivos como imágenes, generar notas para el investigador y generar informes detallados de los hallazgos realizados entre otras opciones.

En resumen, las funciones básicas de la herramienta son las siguientes:

Opción	Descripción
Análisis de archivos	Muestra la imagen como archivos y directorios, permitiendo ver incluso aquellos que estarían ocultos por el sistema operativo.
Búsqueda por palabra clave	Permite buscar dentro de la imagen palabras clave, pueden ser archivos o cualquier otra referencia que se le pase como argumento.
Tipo de archivo	Permite tanto la búsqueda como la ordenación de archivos según su tipo.
Detalles de la imagen	Muestra en detalle la imagen a examinar, permitiendo saber dónde se encuentran físicamente los datos dentro de ella.
Metadatos	Permite ver elementos del sistema de archivos que no se muestran habitualmente, como las referencias a directorios o los archivos eliminados.
Unidad de datos	Ofrece la posibilidad de entrar en el máximo detalle de cualquier archivo, permitiendo examinar el contenido real del mismo, ya sea en ASCCI o en hexadecimal.

Tabla. 3.2. Funcionalidades de The Sleuthkit

Estas herramientas se pueden utilizar mediante un intérprete de comandos o mediante el *Autopsy Forensic Browser* el cual le proporciona a la herramienta una interfaz gráfica la cual facilitará notablemente la labor y, a su vez, podrá generar vistosas salidas gráficas de los informes generados para la investigación.

3.2.10. Helix CD

Esta herramienta pertenece a la categoría de *Live CD's*. Este tipo de herramientas tienen, entre otras ventajas propias de ellas, que no necesitan tiempo para ser instaladas ni tampoco es necesario cargar otro

sistema operativo; de ser necesario, simplemente se inicia la herramienta desde el CD y queda lista para utilizar.

Helix es un *Live CD* de respuesta ante incidentes, basado en una distribución de Linux llamada Knoppix[23]. Helix contiene una serie de herramientas que permiten realizar análisis forenses de forma efectiva y práctica tanto de equipos de cómputo como de imágenes de discos. La herramienta puede ser descargada directamente de http://www.e-fense.com/helix. Además ofrecedos modos de funcionamiento[20]:

1. **Entorno Windows**: Contiene un conjunto de herramientas que permiten recuperar la información volátil del sistema.
2. **Entorno Linux:** Contiene un sistema operativo completo modificado óptimamente para el reconocimiento de hardware. También está diseñado para no realizar ninguna operación en el disco duro del equipo donde se arranque ya que esto tendría como resultado la pérdida o alteración de la evidencia digital lo cual sería perjudicial y poco deseable para la investigación en curso.

Finalmente es importante resaltar que éste *Live CD* cuenta, además de los comandos de análisis propios de Linux, con una serie de herramientas forenses importantes como el anteriormente comentado *The Sleuth kit & Autopsy*[20].

3.2.11. F.I.R.E (Forensics and Incident Response Bootable CD)

Esta herramienta entra también en la categoría de *Live CD* o CD de arranque y basada en una distribución de Linux la cual contiene una serie de utilidades de seguridad además de una interfaz gráfica cómoda, sencilla y agradable la cual la hace de fácil uso[20]. La herramienta puede ser descargada de forma gratuita desde http://biatchux.dmzs.com.

Posee una serie de características que facilitan y optimizan los análisis forenses realizados a equipos de cómputo e imágenes de disco entre las cuales encontramos[20]:

- Recolección de datos de un sistema informático comprometido.
- Búsqueda de algún tipo de *malware* que se encuentre en el sistema comprometido, realizado desde un entorno fiable.
- Posibilidad de realización de pruebas de penetración y vulnerabilidad.
- Recuperación de datos de particiones dañadas.

Al igual que Helix, F.I.R.E cuenta con una serie de herramientas forenses y de seguridad informática muy útiles para la realización de análisis forenses, entre las cuales encontramos: Nessus, nmap, whisker, hping2, hunt, fragrouter, ethereal, snort, tcpdump, ettercap, dsniff, airsnort, chkrootkit, F-Prot,TCT, Autopsy, Testdisk, fdisk, gpart, ssh, vnc, mozilla, ircII, mc, Perl, biew, fennis y pgp.[20]

3.3. HERRAMIENTAS PARA EL MONITOREO Y/O CONTROL DE COMPUTADORES

Si lo que se requiere es conocer el uso de los computadores, es necesario contar con herramientas que los monitoreen para recolectar información. Existen herramientas que permiten recolectar desde las pulsaciones de teclado hasta imágenes de las pantallas que son visualizadas por los usuarios, y otras donde las máquinas son controladas remotamente.

En ocasiones lo que se necesitaría es información sobre el uso de los computadores, para esto también existen herramientas que monitorean el uso de los computadores para poder recolectar información.

3.3.1. Keylogger

Existen algunos programas simples como key loggers o recolectores de pulsaciones del teclado que guardan información sobre las teclas que son presionadas. Estas herramientas pueden ser útiles cuando se quiere detectar o comprobar actividades sospechosas, ya que guardan los eventos generados por el teclado, por ejemplo, cuando el usuario teclea ‘retroceder', esto es guardado en un archivo o enviado por e-mail. Los datos generados son complementados con información relacionada del programa que tiene el foco de atención, con datos sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen otras herramientas que guardan imágenes de la pantalla que ve el usuario del computador, o hasta software que permite controlar la máquina remotamente.

Es importante tener en cuenta que herramientas de este tipo han llegado a ser usadas con fines delictivos como por ejemplo la captura de claves de los clientes en cafés Internet u otros sitios públicos. Los atacantes prefieren hacer instalaciones remotas de programas sencillos que registran toda la actividad del usuario en el teclado, esta es almacenada en un archivo que es obtenido de forma remota. El uso de estas herramientas debe estar plenamente autorizada y un investigador no debería tomar el solo la decisión de su uso.

3.3.1.1 Revealer Keylooger

Revealer Keylooger es una utilidad que permite controlar y grabar todos los textos que se introducen en un computador. Textos como páginas web, conversaciones e incluso usuarios y contraseñas.

Concretamente, el programa se encarga de registrar cualquier texto seguido de la tecla Enter. Ya sea un texto introducido en el navegador, en un e-mail, en un documento o en un programa de mensajería. Revealer Keylogger lo guarda todo.

Cada uno de los registros está clasificado e identificado con su fecha de creación, el proceso o aplicación en la que se ha introducido el texto, un título descriptivo y el texto en sí.

Obviamente, el programa funciona de un modo invisible. Una vez instalado y ejecutado, no aparece como activo ni tan siquiera en el Administrador de tareas. Solo quién lo instale puede saber de su presencia.

¿Por qué utilizar Revealer Keylogger?

Por los administradores: Sobre una red, la amenaza más grande viene del interior. Se puede utilizar para asegurarse que no hay escape de información confidencial, o para detectar actividades ilegales sobre los computadores de la red.

Por los patronos: Se puede instalar el software en una computadora que esté utilizando una persona que esté en periodo de prueba, con el fin de determinar si pasa más tiempo en internet o en sus labores diarias.

Por los particulares: Se puede controlar a los hijos para saber qué es lo que están haciendo cuando no se los puede estar vigilado.

Todas las opciones anteriores parecen extremas pero con los niveles de delincuencia que se presentan actualmente, toman importancia.

3.4. HERRAMIENTAS DE MARCADO DE DOCUMENTOS

Básicamente el objetivo de este tipo de herramientas es el de insertar una marca a la información sensible para poder detectar el robo o tráfico con la misma, si bien no equivale al sistema LoJack de rastreo y localización de vehículos hurtados, si podría compararse con las marcas

que se hace a los vehículos. A través de estas herramientas es posible marcar no solo documentos, sino también software.

Existen en el mercado programas que permiten marcar el software para que, en caso de robo de información, sea posible detectarlo fácilmente. "Algunos sitios en Internet que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes"[11].

Cuando se dice "robo de información" no se refiere solamente al robo de software sino también al robo de imágenes, música, videos y documentos. Desde luego este robo es perpetuado en obras digitales y es por esto que existe este tipo de herramientas de marcado de documentos las cuales utilizan la tecnología llamada comúnmente "*Digital Watermarking*" o marcas de agua digitales.

Los orígenes de esta tecnología vienen de otra técnica anterior llamada esteganografía (en inglés *steganography*). "La esteganografía no nació con la intención de proteger el copyright[7], ni mucho menos. Su utilidad básica no es otra que la de proteger la información. Cuando se trata de proteger la información, esta se puede cifrar"[12]. Para ilustrar mejor el uso de esta técnica se expone el siguiente escenario: Se desea enviar información confidencial a un determinado país en donde los derechos humanos son casi inexistentes. La persona que recibe dicha información puede resultar en prisión por el solo hecho de venir cifrada, aunque en realidad ni se conozca el contenido. "Esa es la utilidad real de la esteganografía: Cifrar esta información y enviarla camuflada dentro de un archivo de otro tipo, como puede ser una imagen, un archivo de sonido o un texto" [12].

[7] Es el derecho que ejerce cada autor sobre su propia obra, sobre su distribución y su utilización.

Ahora que ya se entiende el concepto de esteganografía, se puede dar a conocer la tecnología de las marcas de agua digitales. Marcas perceptibles de propiedad o autenticidad han existido por siglos en forma de sellos, firmas o marcas de agua clásicas, “esa marca que se imprime por presión cuando se está fabricando el papel moneda”[12], sin embargo, dadas las actuales tecnologías de manipulación digital, marcas de agua digitales imperceptibles son obligatorias en la mayoría de las aplicaciones actuales[12]. Una marca de agua digital es una pieza de información especial que es adherida a los datos que se quieren proteger, esto significa que debe ser difícil de extraer o remover[12].

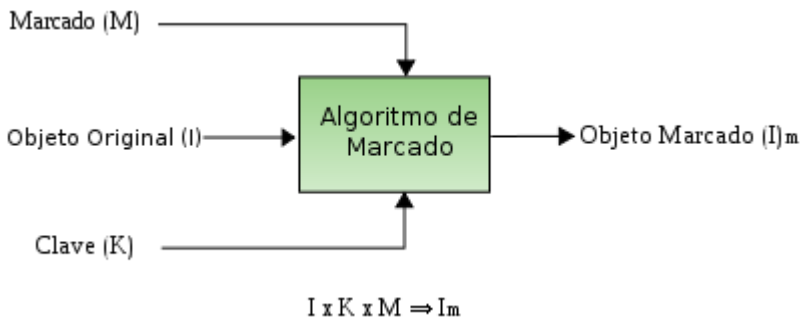

Figura 3.1. Diagrama de generación de un objeto marcado

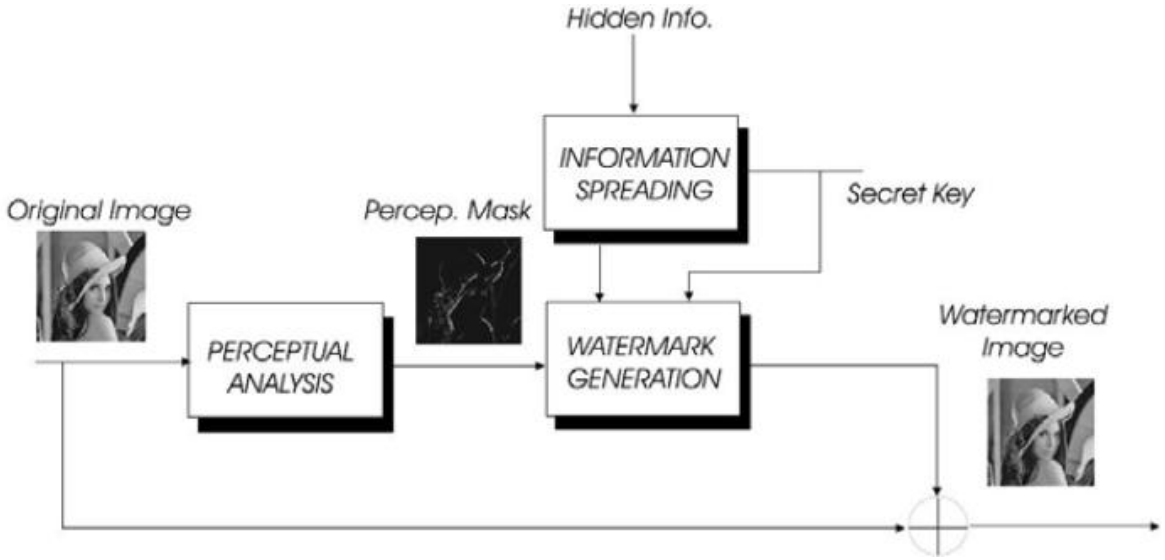

Figura 3.2. Proceso de inserción de una marca de agua digital.

En general se concluye que “La marca de agua digital admite la introducción de información referente al autor, fecha de creación, etc., permitiéndose de esta forma identificar y autenticar al verdadero autor. La marca de agua no impide la copia de un determinado archivo, pero si puede establecer, sin ninguna duda, quien es el autor”[12].

Existe una gran variedad de herramientas para realizar este proceso de inserción de marcas de agua digitales, entre ellas encontramos popular software de tratamiento de imágenes Adobe Photoshop[14] el cual utiliza la tecnología Digimarc[15] para la inserción de marcas de agua digitales. Además de esto, Digimarc también realiza el proceso en archivos de audio, video y en documentos digitales. Por otro lado, se encuentran herramientas especializadas en un solo tipo de archivo para realizar el proceso, es el caso de WatermarkIt[16] el cual solo permite las marcas de agua digitales en imágenes y fotos.

3.4.1. WatermarkIt[26]

Si se es un poco realista cuando alguien publica las fotos en Internet va a ser muy difícil que no se las copien, se las “roben” o se las cojan para ponerlas en otra web. Poco se puede hacer ante estos amigos de lo ajeno, pero al menos se les puede poner las cosas un poco más difíciles con WatermarkIt.

Esta herramienta inserta una marca de agua en las fotos, es decir, un texto que identifica la imagen en cuestión como propia, poniéndole un texto personal o un mensaje de copyright.

WatermarkIt cuenta con varias opciones a la hora de “marcar” las fotos: personalizar el texto, seleccionar tipo de letra y color, elegir su ubicación en la imagen, añadir efectos como sombra o transparencia, etc.

De esta forma se puede dejar tu sello personal en todas las fotos que se vaya a publicar en web y así, si las cogen, quedará bien claro quién es su auténtico dueño y su legítimo autor.

3.4.2. Sandmark

Finalmente están las herramientas para la protección del software, en esta categoría se encuentra Sandmark[17]. Esta herramienta protege al software de la piratería, la manipulación y la ingeniería inversa. La meta del software es la de desarrollar técnicas que le permitan a los usuarios determinar empíricamente cuales algoritmos para la inserción de marcas de agua digitales tienen el mejor rendimiento y la mayor resistencia a ataques[18].

Sandmark en realidad es un *framework* que está diseñado para la implementación y evaluación de técnicas como las marcas de agua digitales.

Las herramientas ya incluyen una serie de algoritmos base en *plug-ins* para ser aplicados y evaluados en cualquier aplicación que se realice en el lenguaje de programación Java. Actualmente se puede descargar la versión 3.4 desde http://cgi.cs.arizona.edu/~sandmark/download.html.

3.5. HERRAMIENTAS DE HARDWARE

El proceso de recolección de evidencia debe ser lo menos invasivo posible con el objeto de no modificar la información. Esto ha dado origen al desarrollo de herramientas que incluyen dispositivos como conectores, unidades de grabación, etc. Es el caso de herramientas como DIBS “Portable Evidence Recovery Unit” y una serie de herramientas de Intelligent Computer Solutions; Link MASSter Forensic Soft Case, Link MASSter Forensic Hard Case, Image MASSter Solo 2 Forensic Kit With Hard Case.

Figura. 3.3. Td1 - Duplicador Forense

3.5.1. Portable Evidence Recovery Unit (DIBS)

La empresa DIBS USA Inc. produce el más grande y más conocido rango de software y hardware forense en el mundo. El Equipo DBS está diseñado para copiar, analizar, y presentar datos digitales de una forma forense y ha sido utilizado por cerca de una década. Evidencia recolectada usando las herramientas DIBS ha sido presentada en múltiples juicios alrededor del mundo en miles de ocasiones. Los equipos DIBS están diseñados para ser de fácil uso aprovechando las condiciones estándares de operación.

La herramienta DIBS Mobile Forensic Workstation[19] es el equipamiento de cómputo forense más avanzado disponible en la actualidad y, aun así, continua con un fácil e intuitivo uso. La herramienta viene con un disco duro configurado y optimizado para el análisis forense, equipado con el último sistema operativo Windows.

Figura. 3.4. DIBS Mobile Forensic Workstation

El software para análisis forense viene completamente instalado y configurado, permitiendo el uso inmediato. Las operaciones de copiado y análisis están diseñadas para realizarse en unidades de almacenamiento externas conectadas a través de una interfaz USB 2, asegurando una alta velocidad de transferencia de los datos. Una de las interfaces externas viene con protección de escritura, con el fin de preservar la seguridad de los datos sospechosos.

El kit contiene: Un laptop de última generación con sistema operativo Windows XP, software forense previamente instalado, dos interfaces para unidades de almacenamiento externas, quemador de DVD, una cámara digital con memory stick, una impresora a color, dos maletines corrugados a prueba de agua , adaptadores cables y conectores. La disponibilidad es de 10 días luego de realizar la orden de compra.

3.5.2. MASSter Forensic Soft Case

El sistema LinkMASSter es un dispositivo de adquisición de software hecho para aprovechar los datos de los equipos que no se puede abrir en el campo. Se puede realizar la transferencia de datos entre unidades de disco duro a alta velocidad de transferencia a través del FireWire del computador o el puerto USB 1.1/2.0. Compatible con algoritmos MD5, SHA1 y CRC32 durante y después de la adquisición. Se suministra un CD

de arranque para arrancar el computador del sospechoso y ejecutar el programa de adquisición de LinkMASSter.

Este sistema es capaz de copiar la información de cualquier sistema operativo, sin importar el número de particiones, los creadores garantizan que se hará una copia exacta de la unidad del sospechoso, incluyendo los archivos eliminados, espacio libre y muerto de los archivos.

La tasa de transferencia o de copiado es de aproximadamente 1.5GB/min, claro siempre dependiendo de la interfaz que se utilice.

La desventaja que presenta esta unidad es que si el sistema del sospechoso presenta una contraseña en el BIOS no se podrán realizar las copias.

3.5.3. Conclusiones y características de Hardware forense

En conclusión, existen una gran variedad de herramientas forenses para asistir a los investigadores en el proceso de recolección y análisis de evidencia digital, cada una de ellas tiene sus ventajas y sus limitaciones y con cada una de ellas se pueden realizar diferentes procesos. Es por esto que es importante contar con una gran variedad de herramientas ya que agilizan el trabajo de búsqueda de información, importante para la investigación además que permite identificar datos que una herramienta en especial no pudo detectar y esto, finalmente, hace la investigación más confiable y formal frente a los entes judiciales y legales.

Solo para hacerse una idea a continuación se detalla las características de uno de los equipos que ofrece la empresa DIGITAL INTELLIGENCE, con su equipo FREDL (Forensic Recovery of Evidence Device– Laptop).

FREDL (Forensic Recovery of Evidence Device – Laptop)

Especificaciones:

- Intel Core i7-720QM (1.60GHz) Processor (Upgradeable)
- Intel PM55 Express Chipset
- 4GB DDR3-1333 Dual Channel SDRAM (Upgradeable)
- 15.6" Full HD (1920x1080) LED Backlit Display
- nVidia GeForce GTX 280M 1GB GDDR3 Graphics Processing Unit
- 320 GB, 2.5” 9.5mm, Internal SATA Hard Drive
- Internal 8x DVD±R/2.4x +DL Super Multi Combo Drive
- Integrated Components:
  - 10/100/1000 Mbps Ethernet LAN
  - 802.11A/B/G/N Wireless LAN (Intel PRO 5300AGN)
  - 56K MDC Modem
  - 7-in-1 Card Reader (MMC/RSMMC/MS/MS Pro/MS Duo/SD/Mini-SD)
  - Digital Video Camera (2.0MP)
  - Bluetooth EDR 2.1
  - Integrated Microphone
  - Integrated Speakers
  - Full-Sized Keyboard With MS-Windows Functions and Keypad
  - Touch Pad With Scrolling Function
  - Fingerprint Reader

- 1 DVI-I Port for External Display
- 1 HDMI Port
- 1 Headphone-out Jack (SPDIF)
- 1 Microphone-in Jack
- 1 RJ11 Modem Jack
- 1 RJ45 LAN Jack
- 4 USB 2.0 Ports
- 1 IEEE 1394a
- 1 E-SATA Port
- 1 Express Card Slot (34/54 mm)
- Li-Polymer 3800mAh 42.18Wh Battery Pack
- Universal AC Adapter (100~240V AC 50/60hz)
- Dimension: 14.75" (w) x 10" (d) x 1.65"~2" (h)
- Weight: 7.38 lbs (Complete System + Battery)
- 3-1/2" External USB Floppy Drive
- 2 Port ExpressCard FireWire 800 Adapter Card
- Digital Intelligence Integrated Forensic Media Card Reader - One Switchable Read-Only/Read-Write (MSC, MS Pro, SMC, CFC, MD, XD, SDC, and MMC Memory Card compatible)
- Hard-sided, Cushioned, Travel Attaché Case With Padded Laptop Insert

Precio estimado: US$ 4, 999

3.6. BIBLIOGRAFÍA

[1] Herramientas de informática forense. Tomado de: http://www.nist.gov/itl/

[2] Informática forense: generalidades, aspectos técnicos y Herramientas; Óscar López, Haver Amaya, Ricardo León; Beatriz Acosta; Universidad de Los Andes, Bogotá, Colombia.

[3] COFEE para todos. Microsoft invita. Tomado de: http://www.krip topolis.org /cofee-microsoft-invita

[4] FCA - Forensic Computer Advisor. Tomado de: http://www.nobosti. com/ spip.php?article598

[5] Sistemas de Detección de Intrusiones de Diego González Gómez. Tomado de: http://www. dgonzalez.n et/pub/ ids/html/

[6] F.I.R.E.: Destaca dentro de las distribuciones Linux específicas para informática forense. Tomado de: http://biatchux.dmzs.com

[7] WinHex: Editor Hexadecimal de Archivos, Discos y RAM. Tomado de: http://www.x-ways.net http://www.x-ways.net/

[8] Encase. Tomado de: http://www.guidancesoftware.com/

[9] Snort. Tomado de: http://www.snort.org

[10] The Autopsy; Browser para la informática forense. Tomado de: http://www.sleuthkit.org

[11] López, H Amaya, R León, B Acosta. “Informática forense: Generalidades, aspectos técnicos y herramientas”. Universidad de los Andes (2002). Bogotá, Colombia. Tomado de: http://www.criptored.upm.es/guiateoria/gt_m180b.htm

[12] J Labodía. “Marcas de agua digitales. A vueltas con la protección de nuestros derechos”. Protección Seguridad. Tomado de: http://www.acta.es/articulos_mf/17043.pdf

[13] Pérez-Gonzales, J Hernández. “A TUTORIAL ON DIGITAL WATERMARKING”. Departamento de Tecnologías de las Comunicaciones, Universidad de Vigo, España. Tomado de: http: //www.gts.tsc.uvigo.es/gpsc/publications/wmark/carnahan99.pdf

[14] Adobe. “Adobe Photoshop CS3. Tomado de: http://www. adobe.com/es/products/photoshop/photosho

[15] Digimarc Corporation. “Digital Watermarking”. Tomado de: http://www.digimarc.com/tech/

[16] Salo Storm Software. “WatermarkIt”. Tomado de: http://www. watermarksoft.com/index.htm

[17] C Collberg. “Sandmark”. Department of Computer Science, The University of Arizona. Tomado de: http://sandmark.cs.arizona.edu/ index.html

[18] C Collberg, G Myles y A Huntwork. “Sandmark - A tool for Software Protection Research”. University of Arizona, IEEE SECURITY & PRIVACY. Tomado de: http://ieeexplore.ieee.org/ Xplore/login.jsp?url=/iel5/8013/27399/01219058.pdf

[19] DIBS USA INC. “DIBS Mobile Forensic Workstation”. Tomado de: http://www.dibsusa.com/products/ mws.asp

[20] M López. “Análisis Forense Digital”. Universidad Nacional de Educación a Distancia. Junio de 2006. España. Tomado de: http://www.criptored.upm.es/guiateoria/gt_m 335a.htm

[21] The Forensic Toolkit. Foundstone Network Security (2007). Tomado de: http://www.foundstone.com/us/resources/proddesc/forensictoolkit.htm

[22] B Carrier, “The Sleuthkit& Autopsy”. Tomado de: http://www.sleuthkit.org/

[23] Knnopix en español. KNOPPIX (2008). Tomado de: http://www.knoppix-es.org/

[24] Filerecovery Software. Tomado de: http://www.filerecovery.in/

[25] The Coroner's Toolkit (TCT). Tomado de: http://www.porcupine.org/forensics/ tct.html

[26] Watermark, Herramienta de marcado de software. Tomado de: http://www.watermark-software.com/