ANÁLISIS DE HERRAMIENTAS PARA LA ADQUISICIÓN, PRESERVACIÓN Y ANÁLISIS DE RECUPERACIÓN DE DATOS

José Eduardo Isidor Galeana
Cd. Universitaria, Gro. Chilpancingo de los Bravos, Guerrero, México. C.P.39070
lalo_maniaco@hotmail.com

MC. León Julio Cortez Organista
Cd. Universitaria, Gro. Chilpancingo de los Bravos, Guerrero, México C.P.39070
jcortez@uagro.mx

Dr. Valentín Álvarez Hilario
Cd. Universitaria, Gro. Chilpancingo de los Bravos, Guerrero, México. C.P.39070
valentin_ah@yahoo.mx

MC. Eric Rodríguez Peralta
Cd. Universitaria, Gro. Chilpancingo de los Bravos, Guerrero, México. C.P.39070
erodriguez@uagro.mx

RESUMEN

Ante los desafíos que presenta la evidencia digital, atendiendo requerimientos identificados, se hizo una investigación sobre las herramientas de análisis forenses existentes que sirven de apoyo para la adquisición y gestión de evidencias digitales. Gracias a estas herramientas se hacen más accesibles para los usuarios y profesionales dedicados al análisis forense se localiza la evidencia requerida. El presente artículo describe las diferentes herramientas y la importancia de su elección al momento de aplicar un análisis forense.

INTRODUCCIÓN

Se define la **informática forense** como la ciencia de adquirir, preservar, obtener y presentar datos que hayan sido procesados electrónicamente y almacenados en soportes informáticos. [1]
La informática forense en la actualidad está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada, y al extenso uso de computadoras por parte de las compañías de negocios tradicionales. Es por esto que cuando se realiza una acción indebida, muchas veces la información queda almacenada en forma digital. [2]
La infraestructura informática que puede ser analizada puede ser toda aquella que tenga una Memoria (informática), por lo que se pueden analizar los siguientes dispositivos:

- Disco duro de una Computadora o Servidor
- Documentación referida del caso.
- Logs de seguridad.
- Credenciales de autentificación
- Trazo de paquetes de red
- Teléfono Móvil o Celular, parte de la telefonía celular
- Memoria USB

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo. Adicionalmente, un analista forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo. [3]

Este artículo evalúa y compara diferentes herramientas disponibles con el fin de mostrar la eficiencia, la facilidad de uso y la relación costo-efectividad en la conducción de un buen análisis forense.

CAPÍTULO I. HERRAMIENTAS PARA ANÁLISIS DIGITAL.

En este capítulo se dará una descripción general de lo que son las herramientas para el análisis forense, su clasificación y la manera en que estas ayudan a poder realizar un trabajo eficaz en las investigaciones correspondientes.
En la actualidad existen cientos de herramientas para un análisis forense el uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en una computadora.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de encriptación, o de contraseñas. [4]

A la hora de llevar a cabo el análisis forense, teniendo en cuenta principalmente las fases de adquisición y análisis de las evidencias, es necesario conocer un amplio abanico de métodos, técnicas y herramientas.
Existen 3 métodos distintos de extracción de evidencias: adquisición física, adquisición del sistema de archivos y adquisición lógica.

Adquisición física:

Es el método más utilizado habitualmente. Consiste en realizar una réplica idéntica del original por lo que se preservan la totalidad de las evidencias potenciales. Este procedimiento presenta la ventaja de que es posible buscar elementos eliminados. Su desventaja principal es su complejidad respecto a los otros métodos y el tiempo que lleva su realización.

Adquisición lógica:

Consiste en realizar una copia de los objetos almacenados en el dispositivo. Para ello, se utilizan los mecanismos implementados de manera nativa por el fabricante, es decir, aquellos que son utilizados de manera habitual para sincronizar el terminal con una computadora. De modo que se solicita la información deseada al sistema operativo del dispositivo. La ventaja que es un proceso mucho más sencillo que el anterior, si bien no permite acceder a multitud de información.

Adquisición del sistema de archivos:

Permite obtener todos los archivos visibles mediante el sistema de archivos, lo que no incluye archivos eliminados o particiones ocultas. Dependiendo del tipo de investigación puede resultar suficiente utilizar este método lo que supone una complejidad menor que la adquisición física.
Para llevarlo a cabo se aprovecha de los mecanismos integrados en el sistema operativo para realizar el copiado de los archivos, Android Device Bridge (ADB) en el caso de Android. Mediante este método es posible recuperar cierta información eliminada ya que algunos sistemas operativos como es el caso de Android e iOS se valen de una estructura que utiliza bases de datos SQLite para almacenar gran parte de la información. [5].

2.1. Clasificación de las herramientas forenses.

Es muy importante usar las herramientas adecuadas para cada tarea. En ese aspecto cada herramienta se crea y diseña para una o varias funciones determinadas, y por lo tanto podemos hablar de diversos tipos de herramientas informáticas.
Se definen las herramientas informáticas como programas, aplicaciones o instrucciones que se realizan para resolver una tarea específica en una computadora, celular, tablets. Etc.
Es por ello que existe una serie de herramientas de uso común para todo tipo de categoría.

2.2. Herramientas de disco

Recuperación de datos perdidos, borrados, búsqueda de patrones y archivos con contenido determinado como por ejemplo imágenes, vídeos. Recuperación de particiones y tratamiento de estructuras de discos. [6]

2.3. PhotoRec

Es un software para PC con Windows diseñado para recuperar archivos perdidos, incluidos videos, documentos y archivos de discos duros, CD-ROM, tarjeta SD o usb. La aplicación ignora el sistema de archivos y busca los datos subyacentes, por lo que seguirá funcionando incluso si el sistema de archivos de sus medios ha sido gravemente dañado o reformateado.
Funcionamiento del PhotoRec
Cuando se elimina un archivo, se pierde la metainformación sobre este archivo (nombre del archivo, fecha / hora, tamaño, ubicación del primer bloque / clúster de datos, etc.
Esto significa que los datos todavía están presentes en el sistema de archivos, pero solo hasta que algunos o todos sean sobrescritos por nuevos datos de archivos.
Para recuperar estos archivos perdidos, PhotoRec primero intenta
encontrar el tamaño del bloque de datos (o clúster). Si el sistema de archivos no está dañado, este valor puede leerse desde el superbloque (ext2 / ext3 / ext4) o el registro de inicio de volumen (FAT, NTFS). De lo contrario, PhotoRec lee los medios, sector por sector, buscando los primeros diez archivos, a partir de los cuales calcula el tamaño del bloque / clúster desde sus ubicaciones. [7]

2.3.1. NTFS Recovery

Es una utilidad completamente automática que recupera datos de discos dañados o formateados. Está **diseñado pensando en un usuario doméstico.** No necesita tener ningún conocimiento especial de recuperación de disco.
El usuario puede escanear no solo discos duros y SSD, sino también cualquier medio de almacenamiento extraíble con el sistema de archivos NTFS.
NTFS Recovery es compatible con los sistemas de archivos - NTFS, NTFS4, NTFS5. [8]

2.3.1.2 Recuva

Es un programa gratuito que permite recuperar archivos perdidos, borrados accidentalmente. El programa también puede ser usado para restaurar archivos borrados de memorias Flash/USB, tarjetas de memoria o reproductores MP3
Puede recuperar imágenes, música, documentos, videos, correos electrónicos o cualquier otro tipo de archivo que haya perdido. A diferencia de la mayoría de las herramientas de recuperación de archivos, Recuva puede recuperar archivos de unidades dañadas o recién formateadas. Mayor flexibilidad significa mayores posibilidades de recuperación. [9]

2.3.1.3 CNWrecovery

El software de recuperación de datos forenses CnW es de primera clase en la recuperación de archivos, pero también contiene registros extensos.

Los dos elementos clave de CnW es el sistema de registro que tiene detalles de todos los archivos, errores y medios.
El hash de los archivos recuperados asegura que cualquier cambio posterior, accidental o deliberado pueda ser rastreado. [10]

2.3.1.4 DMDE

Es un potente software para la búsqueda, edición y recuperación de datos en discos. Puede recuperar la estructura de directorios y archivos en algunos casos complicados mediante el uso de algoritmos especiales cuando otro software no puede ayudar.
DMDE tiene una serie de funciones gratuitas como editor de disco, administrador de particiones simple (permite la eliminación de particiones), una herramienta para crear imágenes de disco y clones, constructor RAID, recuperación de archivos desde el panel actual. Se ejecuta en Windows, Linux, macOS, DOS. [11]

2.3.1.5 Magnet ief.

Es un software utilizado por miles de profesionales dedicados al análisis forense en todo el mundo para encontrar, analizar e informar sobre las evidencias digitales de computadoras, teléfonos móviles y tablets. Magnet IEF realiza una búsqueda exhaustiva a bajo nivel analizando cientos de archivos en el espacio asignado de la memoria como en el espacio sin asignar para su análisis forense.

Características
- Admite los sistemas operativos Windows, Linux y Mac OSX
- Para usar en un entorno de laboratorio forense
- Soporte para imágenes E01, EX01, LX01, dd y dmg
- Busca información en vivo y eliminada en discos duros y en RAM

IEF proporciona información sobre datos de la comunicación de redes sociales, mensajería instantánea, aplicaciones basadas en la nube, aplicaciones P2P, archivos de respaldo, correo web, historial del navegador web, fotos, videos y más. El software también puede reproducir datos eliminados del espacio no asignado y la RAM gracias a las nuevas técnicas de tallado. Además, se puede utilizar para buscar volúmenes de unidades lógicas o físicas y archivos y directorios individuales. IEF busca a través de múltiples archivos o soportes de medios. [12]

2.4 Recuperación de contraseñas

Las herramientas de recuperación de la contraseña de Windows se utilizan para recuperar o restablecer las contraseñas perdidas del usuario y administrador que se utilizan para iniciar sesión en los **sistemas operativos** Windows.
Las herramientas que se utilizan para la recuperación de la contraseña a menudo se denominan herramientas «cracker de contraseñas» porque a veces los hackers las utilizan para descifrar las contraseñas. [13]

2.4.1Ntpwedit

Es un editor de contraseña para los sistemas basados en Windows NT, se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory.
Cambia las contraseñas modificando directamente el archivo **C: \ WINDOWS \ SYSTEM32 \ CONFIG \ SAM.** Cuando se ejecuta, el sistema operativo bloquea cualquier acceso a este archivo, por lo que el editor de contraseñas debe ejecutarse en otra copia de Windows. [14]

2.4.2 Ntpassword

El descifrador de contraseñas Offline NT Password & Registry Editor es una de las herramientas gratuitas de recuperación de contraseñas de Windows más rápidas que se utilizan. Incluso es mucho mejor que algunas herramientas sobre cualquier programa Premium de recuperación de contraseña que hayamos probado.

Ventajas y desventajas
Ventajas
- Herramienta muy rápida para descifrar contraseñas
- No se necesita acceso a Windows o conocimiento de contraseñas antiguas
- Funciona con Windows 10 y Windows 8 (solo contraseñas locales), así como con Windows 7, Windows Vista y Windows XP
- La imagen ISO del programa es mucho más pequeña que la de otras herramientas de recuperación de contraseña.

Desventajas
- La herramienta de contraseña NT sin conexión está completamente basada en texto, lo cual es un poco inconveniente
- La imagen ISO debe grabarse en un CD o unidad flash antes de que se puedan restablecer las contraseñas

Características
- Offline NT Password & Registry Editor puede eliminar cualquier contraseña de casi cualquier instalación de Windows casi al instante.
- No se requiere instalación en Windows, por lo que este programa es una alternativa fácil a muchas otras herramientas de recuperación de contraseña.
- Offline NT Password & Registry Editor simplemente elimina las contraseñas en lugar de mostrarlas, lo que lo hace rápido y fácil de usar.
- Offline NT Password & Registry Editor es completamente gratuito
- Restablece las contraseñas de Windows 10 y Windows 8 (solo cuentas locales, no cuentas de Microsoft). [15]

2.4.3 pwdump7

Es un volcador de contraseñas para Windows llamado PWDUMP7. La principal diferencia entre pwdump7 y otras herramientas de pwdump es que esta herramienta se ejecuta extrayendo el archivo binario SAM y SYSTEM del sistema de archivos y luego se extraen los hashes.
Para esa tarea se utilizan los controladores del sistema de archivos Rkdetector NTFS y FAT32. Pwdump7 también puede extraer contraseñas sin conexión seleccionando los archivos de destino.
Una de las potentes características de pwdump7 es que también se puede usar para volcar archivos protegidos. Siempre puede copiar un archivo usado simplemente ejecutando: pwdump7.exe -dc: \ lockedfile.dat backup-lockedfile.dat.
Se debe tener en cuenta que esta herramienta solo se puede utilizar con archivos SAM y SYSTEM. [16]

2.4.4 L0phtcrack

Es una aplicación de auditoría y recuperación de contraseñas producida originalmente por Mudge de L0pht Heavy Industries. Se utiliza para probar la seguridad de la contraseña y, a veces, para recuperar contraseñas perdidas de Microsoft Windows, utilizando el diccionario, la fuerza bruta, los ataques híbridos y las tablas de arco iris.
Era una de las herramientas preferidas de los crackers, aunque la mayoría usa versiones antiguas debido a su bajo precio y alta disponibilidad. L0phtCrack identifica y evalúa la vulnerabilidad de la contraseña en máquinas y redes locales en una aplicación optimizada, con informes integrados y herramientas de corrección. [17]

2.5 Herramientas para Dispositivos móviles

Estas herramientas disponen de utilidades para la recuperación de datos y análisis forense de dispositivos móviles.
En la siguiente figura se muestra una pirámide la cual pretende servir de guía para clasificar las herramientas de análisis forense de acuerdo a diferentes criterios como: complejidad, tiempo de análisis requerido, riesgo de pérdida o destrucción de evidencias, nivel invasivo y lo que se conoce como "forensically sound" que viene a significar algo similar al nivel de fiabilidad, si bien se trata únicamente de una percepción ya que todas las herramientas y técnicas utilizadas deben tener una fiabilidad contrastada.
La manera de interpretar el esquema es desde abajo de la pirámide hacia arriba, de modo que las capas superiores poseen una complejidad técnica mayor, un mayor tiempo requerido y más "forensically sound".

Figura **4**. Guía para las herramientas de análisis forense [5]

2.5.1 Dispositivos iOS

El análisis forense de dispositivos iOS inicia como cualquier otro análisis forense, solo debemos tener en cuenta que algunos de estos dispositivos con iOS son teléfonos móviles, por tanto, debemos tener las precauciones necesarias para estos dispositivos en especial. [18]
La protección de la información enfocada a este tipo de dispositivos abre un campo de investigación que tiene incidencia a nivel mundial, es por ello que se genera la necesidad de analizar y determinar cuáles son los puntos más vulnerables y posiblemente aquellos por medio de los cuales será posible acceder y violentar la privacidad del propietario, con el fin de realizar un análisis de vulnerabilidades que permite encontrar las mejores prácticas para la protección de la información de dichos dispositivos. [19]
Lo que se debe realizar en esta fase es la evaluación de los recursos a los que tenemos acceso y cuáles son los objetivos para realizar la investigaron interna, pasando por cada una de las siguientes etapas:

- Notificar y obtener la autorización
- Realizar una evaluación
- Prepararse para la adquisición de pruebas [18]

Para continuar se describirá una descripción de algunas herramientas forenses para dispositivo móviles iOS

2.5.1.2 iPhoneBrowser

Accede al sistema de archivos del iphone desde entorno gráfico.
Es un pequeño programa para el sistema operativo Windows que se encarga de administrar los archivos de tu iPhone.
Con este software se puede subir o bajar archivos, realizar copias de seguridad, restaurar datos, copiar imágenes, textos, iconos, renombrar archivos, cambiar nombres de carpetas, en definitiva, todo lo que se dispongas en el iPhone. Todo lo que no te permite hacer Mac debido a la limitación de uso con iTunes, se puede hacer con este sencillo programa. [20]

2.5.1.3 iPhone Analyzer

Es una aplicación ligera de Windows cuyo propósito es ayudarlo a explorar la estructura interna de archivos del iphone utilizando archivos de respaldo.
Explora la estructura interna de archivos de un iPhone (o de un teléfono incautado en el caso de equipos forenses) utilizando los archivos de respaldo propios del iPhone o ssh.

Características

- Navegación de respaldo de iPhone
- Búsqueda incluyendo expresiones regulares
- Acceso ssh para teléfonos con jailbreak (beta)
- Informes
- Restaurar archivos
- Recuperar copias de seguridad
- Ver todas las fotos de iPhone
- examinar la libreta de direcciones, sms y muchos otros
- encontrar y recuperar contraseñas
- Exportar archivos al sistema de archivos local
- Mapeo en línea y fuera de línea
- Geo track donde ha estado un dispositivo
- IOS5 y versiones anteriores compatibles. [21]

2.5.1.4 iPhoneBackupExtractor

El iPhone backup extractor es una solución de software ideal para tratar una serie de cuestiones tales como fallo de hardware, software de accidentes etc.
Recupera fotos, mensajes, videos, historial de llamadas, notas, contactos, contraseñas de Screen Time, mensajes de whatsapp, y otros datos de aplicaciones de iTunes y de iCloud Backups.

Transfiere fotos, mensajes y más

- Copia e imprime textos y WhatsApps
- Transfiere fotos desde iPhone a PC
- Transferir contactos de iPhone a iPhone

Descargar fotos y datos de iCloud

- Descarga tus fotos de iCloud
- Descargar iCloud Photo Library
- Explore los contactos de iCloud y la transmisión de fotos
- Recupera iMessages de iCloud

Recuperar datos perdidos, eliminados o corruptos

- iPhone recuperación de datos y forense
- Recuperar mensajes de texto eliminados
- Recupere la contraseña olvidada de Screen Time
- Te ayuda a reparar "Copia de seguridad de iPhone corrupta" [22]

2.5.1.5 sPyphone

Es un programa que instala directamente en el celular que deseamos controlar. Una vez instalado y configurado el mismo trabajará en forma invisible para el usuario, recolectará las actividades a un papel web privado donde usted podrá revisar todas las grabaciones de voz, texto, videos e imágenes que se hicieron.
Los datos almacenados en los servidores de sPyphone se eliminan automáticamente y permanentemente después de 90 días. [23]

2.6 Dispositivos Android

La investigación forense de dispositivos móviles Android es un campo de reciente desarrollo en el que la disponibilidad de conocimientos técnicos, están en proporción inversa al interés generado hacia los mismos. [24]

2.6.1 Androguard

Es una biblioteca de herramientas y python para interactuar con archivos de android. Por lo general, vienen en forma de paquetes de android (APK) o archivos ejecutables de Dalvik (DEX). Androguard tiene herramientas para leer el formato binario de Android para archivos XML (AXML) y también es adecuado con un descompilador para DEX.
Androguard no solo se puede usar como una herramienta para aplicaciones únicas de ingeniería inversa, sino que también ofrece muchas funciones para el análisis automatizado. [25]

2.6.2 LIME- Linux Memory Extractor

Es un software permite la adquisición de memoria volátil de Linux y dispositivos basados en Linux, como Android. Esto hace que LiME sea único, ya que es la primera herramienta que permite capturas de memoria completa en dispositivos Android.

También minimiza su interacción entre el usuario y los procesos del espacio del kernel durante la adquisición, lo que le permite producir capturas de memoria que son más sólidas de forma forense que las de otras herramientas diseñadas para la adquisición de memoria de Linux.

Características

- Adquisición de memoria completa de Android
- Adquisición a través de la interfaz de red
- Proceso mínimo de huella
- Hash de memoria descargada [26]

2.6.3 Mobiledit forensic express

Es un software el cual permite la extracción del celular y cloud analizador de datos y generador de reportes en una solución. Es

la aplicación potente de 64-bit, usando el método de adquisición de datos físicos y lógicos, MOBIledit es excelente por su avanzado analizador de aplicaciones, recuperación de los datos eliminados, live updates, la variedad amplia de los celulares compatibles incluso los modelos nuevos, procesamiento de los celulares competidores y uso fácil de interfaz de usuario. Con la contraseña y PIN rompedor puede obtener acceso a cerrados ADB o iTunes reserva con GPU aceleración y "multi-threaded" operaciones para maximizar la rapidez. [27]

CAPÍTULO II. ANÁLISIS FORENSE APLICANDO HERRAMIENTAS DE RECUPERACIÓN DE DATOS.

Disponer de un conjunto de herramientas específicas para el análisis de evidencias que nos ayudaran a completar de forma más eficiente una investigación.

Dejando aparte el software comercial, en el que podrá encontrar herramientas específicas como EnCase de la empresa Guidance Software, considerado un estándar en el análisis forense de sistemas, nos centraremos en herramientas de código abierto (Open Source) que podrá descargar libremente desde la página sus correspondientes autores o miembros del proyecto.

Software de Libre Distribución y Open Source

Se comenzará con una recopilación de herramientas que necesitan ser ejecutadas bajo un sistema operativo anfitrión, bien sea MS Windows o UNIX/Linux.

3.1 The Forensic ToolKit

Se trata de una colección de herramientas forenses para plataformas Windows, creadas por el equipo de Foundstone. Donde además encontrará gran cantidad de herramientas de seguridad.
Este ToolKit le permitirá recopilar información sobre el ataque, y se compone de una serie de aplicaciones en línea de comandos ver tabla 1 que permiten generar diversos informes y estadísticas del sistema de archivos a estudiar. Para poder utilizarlos deberá disponer de un intérprete de comandos como cmd.exe.

Tabla 1. Comandos para generar informes y estadísticas.

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.

3.2 The Sleuth Kit Y Autopsy

Este conjunto de herramientas puede analizar archivos de datos de evidencias generadas con utilidades de disco como por ejemplo dd. Incluye funciones como registro de casos separados e investigaciones múltiples, acceso a estructuras de archivos y directorios de bajo nivel y eliminados, genera la línea temporal de actividad de los archivos (timestamp), permite buscar datos dentro de las imágenes por palabras clave, permite crear notas del investigador e incluso genera informes y mucho más.

Para analizar sus datos debido a la gran cantidad de opciones se necesitaría un documento solamente dedicado a esta herramienta, así que, a modo de resumen, algunas de las funciones básicas con las que podrá contar son las siguientes opciones de análisis que se encuentran en la tabla 2.

Tabla 2. Funciones básicas del the Sleuth

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.
Matadatos	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 ASCII o en hexadecimal.

Las herramientas expuestas anteriormente necesitan de la ejecución sobre un sistema operativo ya instalado. En ocasiones le será de gran utilidad disponer de un entorno tipo Live, que le permita realizar un examen forense de imágenes sin tener que dedicar un equipo específico para ello y sin necesidad cargar otro sistema operativo. Estas soluciones suelen encontrarse en CDs o DVDs preparados para tal fin.

3.3 HELIX CD

Se trata de un Live CD de respuesta ante incidentes, basado en una distribución Linux denominada Knoppix (que a su vez está basada en Debian). Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes de discos.
Este CD ofrece dos modos de funcionamiento, tras ejecutarlo nos permitirá elegir entre arrancar un entorno MS Windows o uno tipo Linux.
Nos permite principalmente interactuar con sistemas "vivos", pudiendo recuperar la información volátil del sistema.
En el arranque Linux, disponemos de un Sistema Operativo completo, con un núcleo modificado para conseguir una excelente detección de hardware, no realiza el montaje de particiones swap, ni ninguna otra operación sobre el disco duro del equipo sobre el que se arranque.

Es ideal para el análisis de equipos “muertos”, sin que se modifiquen las evidencias pues montará los discos que encuentre en el sistema en modo sólo lectura. Además de los comandos de análisis propios de los entornos UNIX/Linux, se han incorporado una lista realmente interesante de herramientas de ToolKits algunos de ellos comentados anteriormente como el Sleuth Kit y Autopsy.

3.4 F.I.R.E. Linux

Se trata de otro CD de arranque que ofrece un entorno para respuestas a incidentes y análisis forense, compuesto por una distribución Linux a la que se le han añadido una serie de utilidades de seguridad, junto con un interfaz gráfico que hace realmente fácil su uso.

Al igual que el kit anterior, por su forma de montar los discos no realiza ninguna modificación sobre los equipos en los que se ejecute, por lo que puede ser utilizado con seguridad. [28]

3.5 Dispositivo Modo Encendido

En esta situación se aplicará el siguiente axioma “Si esta encendido no apagarlo y si está apagado no encenderlo”. Una vez clarificada esta acción, se procederá a tomar las siguientes evidencias (a grandes rasgos y no importa el orden)

• Volcado de la memoria RAM
• Obtención del archivo pagefile.sys
• Obtención del NTUSER.DAT
• Prefetch
• Procesos, sesiones, conexiones, tareas, políticas, configuración de red, protocolos...
• Archivos del registro (SAM, SECURITY, SOFTWARE.)
• Archivos de logs de windows, etc.

3.6 Equipo Modo Apagado

Esto se entiende como equipo muerto o modo “sleep”. Extraer el disco duro y clonarlo resulta el modo más recomendado. Aunque de esta forma se pierde todo lo que contenía la memoria RAM, en el archivo de paginación. Sin embargo, se puede lograr el acceso a todo lo que estaba en el disco.

3.7 Virtualización

Es el modo más recomendable. Actualmente muchas empresas tienen todo virtualizado vía web porque les resulta más cómodo, por lo tanto, se puede clonar la máquina y la memoria RAM. De esta forma se admiten los modos encendido y apagado.

En los siguientes puntos se describen cual es el propósito, los métodos, el procedimiento para realización un análisis, la cual permite realizar de manera adecuada el proceso forense.

4. Propósito

Comparar las diferentes herramientas forenses informáticas utilizadas para la copia de medios digitales.

4.1 Métodos

Tipos de investigación

Investigación documental:

Consultas en diversas fuentes de investigación como son: bases de datos digitales, libros, revistas, manuales, internet, entre otros.

Científico:

Es un estudio sistemático, lógico y organizado de la proposición hipotética planteada para adquirir conocimientos y brindar una solución.

Descriptivo:

Se realizó un estudio descriptivo que consiste en llevar a conocer situaciones relevantes a través de la descripción de las variables de investigación para exponer de manera cuidadosa los resultados a fin de extraer generalizaciones significativas.

Instrumentos y materiales
1. Microsoft Office
2. Sistema Operativo (Windows)
3. Herramientas Forense Informático
4. Computadora
5. Norma ISO 9126:1998

4.2 Procedimiento

El primer paso fue la selección de las herramientas de software a ser estudiadas. Para la realización de la selección de herramientas, se estudió el libro Herramientas para copias de datos bit a bit [29], en el cual se indica que el copiado bit a bit consiste en realizar una copia íntegra de un medio o dispositivo completamente para trabajar sobre una copia que posee las mismas características que la original.

Posteriormente, para estas cuatro herramientas se realizó la selección final para tener como objetivo identificar las que serían estudiadas en la presente investigación. Para la realización de la selección se tomaron en cuenta los siguientes criterios presentados en la Tabla 3:

Tabla 3. Criterios de selección de herramientas para informática forense.

No.	NOMBRE	DESCRIPCIÓN
1	Utilidad	Fin con el que se utiliza la herramienta en la Informática Forense.
2	Adaptabilidad	No necesita complementos para instalarse o utilizarse en los equipos.
3	Mantenimiento	Se estudiarán herramientas que cuenten con actualizaciones permanentes, ya que la evolución de la informática es constante.
4	Portabilidad	No es necesaria su instalación sobre el sistema operativo o puede ejecutarse en diferentes plataformas de hardware.
5	Accesibilidad	Que esté disponible su obtención para el respectivo estudio.
6	Documentación	Se estudiarán herramientas de las que exista documentación suficiente para obtener la información necesaria.
7	Estabilidad	Robustez de la aplicación en cuanto a operatividad en la plataforma que vaya a ser utilizada.

En base a la matriz de los criterios procedemos a la siguiente selección de herramientas forenses informáticas a seleccionar:
Las herramientas para copias de datos bit a bit seleccionadas son:

- HD Clone
- EnCase
- Norton Ghost
- XWay Forensics

5. Resultados

La propuesta de herramientas forenses informáticas se basará en la jerarquización de las herramientas estudiadas y analizadas de la siguiente manera:
1. Definir con qué criterios se medirán las herramientas que necesitamos comparar.
2. Para todas las herramientas forenses informáticas seleccionadas, medir el nivel de desempeño de cada criterio.
3. Realizar la comparación de cada herramienta forense para determinar cuáles son las que obtienen mejores puntuaciones en los criterios definidos anteriormente, para lo cual se utilizará la tabla de criterios ver tabla anterior, Tabla 3. Las puntuaciones se obtendrán de acuerdo al criterio seleccionado.
4. Establecer la jerarquía de propuestas ordenadas descendentemente.

5.1. Los criterios a tomar en cuenta para la comparación de las herramientas

1. Portabilidad

Capacidad de la herramienta para ser utilizada tanto en un entorno de hardware y software determinado como en otro, conservando la funcionalidad de esta.
Se refiere al nivel en que la misma herramienta puede ser utilizada en los diferentes entornos (combinaciones de hardware y software) donde se pueda encontrar la evidencia. Este criterio también incluye la facilidad de instalación con que las herramientas puedan instalarse en los entornos en los que puede funcionar.

2. Confiabilidad de los resultados

Para que una herramienta sea confiable en los resultados que proporciona, es necesario comparar el resultado de ésta con el de las otras herramientas del mismo tipo y, si son similares, se podrá tomar como confiable, pero si no, se considerará no confiable.
Por ejemplo, con las herramientas Hash, el resultado de cálculo del mismo tipo de hash al mismo archivo debe dar igual para todas las herramientas.

3. Mayor capacidad operativa

Este criterio se refiere a que, si dos herramientas realizan la misma función, se debe seleccionar la herramienta que tenga mayor capacidad para realizar dicha función.

4. Soporte para la herramienta:

Es necesario que las herramientas seleccionadas tengan soporte para solventar problemas que puedan surgir con esta y las actualizaciones que los fabricantes ponen a disposición para asegurar el correcto funcionamiento de la herramienta.
Las características a evaluar en el método utilizado para ponderar las herramientas forenses informáticas están basadas en el método de criterios ponderados.

El peso del factor depende de la importancia del mismo. Los criterios y subcriterios tomados en cuenta y su respectiva ponderación son:

1. Adaptabilidad al entorno:

- No requiere de sistema operativo
- Requiere de sistema operativo, pero funciona sobre más de uno
- Soporta más de una arquitectura de computadora. El primero y el segundo criterio son excluyentes, si una herramienta cumple con el primero, no puede cumplir con el segundo y viceversa.

2. Confiabilidad de resultados:

- Los resultados son iguales a los anteriores.

3. Coso de adquisición de la herramienta:

- No existe costo para la herramienta.

4. Facilidad de uso y aplicación.

- Tiene interfaz gráfica amigable.
- Presenta ayuda en pantalla.

5. Capacidad operativa.

- Soporta lo más común del hardware en el mercado.
- Tiene soporte para elementos de hardware especiales o puede operar sobre ellos.

6. Soporte para la herramienta.

- Tiene desarrollo y actualizaciones constantes de las herramientas.

Los criterios de comparación fueron elegidos en base a la Norma ISO 9126:1998, la cual define los criterios y subcriterios que debe tener un software para ser considerado de calidad.

La norma está orientada al desarrollo de software, para lo cual se considerará en la jerarquización de las herramientas de informática forense analizadas, ver la Tabla 4.

Tabla 4. Comparación de herramientas para copia de medios.

HERRAMIENTAS PARA COPIA DE MEDIOS											
HERRAMIENTAS	CRITERIO 1			CRITERIO 2	CRITERIO 3	CRITERIO 4		CRITERIO 5		CRITERIO 6
	A	B	C	A	A	A	B	A	B	A
HD Clone	Si	No	No	Si	Si	Si	Si	Si	Si	Si
EnCase	No	No	No	Si	Si	Si	Si	Si	No	Si
Norton Ghost	No	No	No	Si	Si	Si	Si	Si	Si	Si
XWay Forensics	Si	No	No	Si	No	Si	No	Si	Si	Si

Las ponderaciones dadas a cada uno de los criterios y subcriterios fueron definidas por el grupo de investigación, basados en las investigaciones realizadas por profesionales que utilizan las herramientas forenses informáticas. El máximo puntaje que una herramienta puede alcanzar será de 65, que es la sumatoria total, como se muestra en la Tabla 5.

Tabla 5**.** Puntuaciones de herramientas para copia de medios.

HERRAMIENTAS PARA COPIA DE MEDIOS (PUNTAJES)								
HERRAMIENTA	CRITERIOS						TOTAL	
	1	2	3	4	5	6	Cant. / 65	%
HD Clone	10	15	0	10	15	5	55	84,62
EnCase	0	15	0	10	8	5	38	58,46
Norton Ghost	0	15	0	10	15	5	45	69,23
XWay Forensics	10	15	5	5	15	5	55	84,62

Las puntuaciones de herramientas según ponderaciones de criterios presentan los puntajes obtenidos para cada herramienta, recordando que el criterio de puntuación está basado en el método de los factores ponderados ver Figura 1.

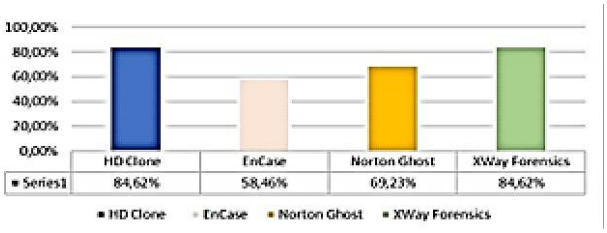

Figura 1. Gráfica de herramientas para copia de medios digitales [30].

CAPITULO III. CASO DE USO

Para este capítulo se realizó la práctica con el programa photorec para la recuperación de datos eliminados en una computadora con las siguientes características:

- Marca de la computadora: Toshiba
- S.O: Windows 8.1 de 64 bits
- Memoria RAM: 4 GB
- Procesador: Intel celeron de 2.16GHz

Al momento de hacer la ejecución del programa se abre esta interfaz, el programa se ejecuta a través de línea de comando. En esta ventana el programa muestra el modelo del disco, la capacidad que tiene.
Se usan las teclas Arriba/Abajo Para seleccionar el disco que se va a analizar, y ya habiendo seleccionado el disco se presiona la tecla ENTER.

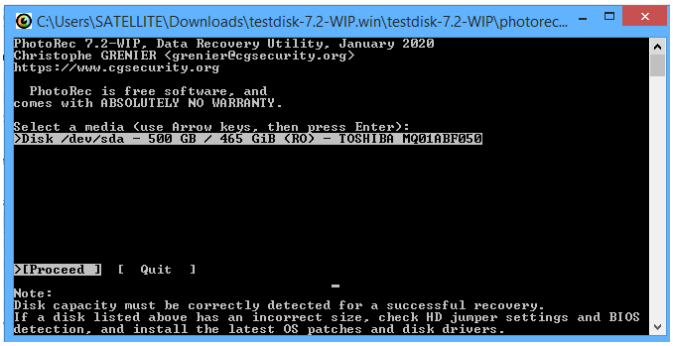

Figura 2. Recuperación de datos del programa photorec.

En la siguiente imagen se muestra los sistemas de archivos que tiene el disco en el cual se va a realizar el análisis.

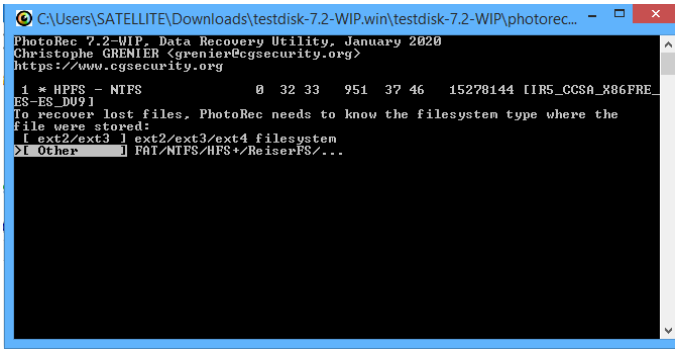

Figura 3. Sistema de archivo del disco a analizar.

Habiendo seleccionado el sistema de archivos correcto, el programa comienza a realizar la búsqueda de los archivos que se van a recuperar.

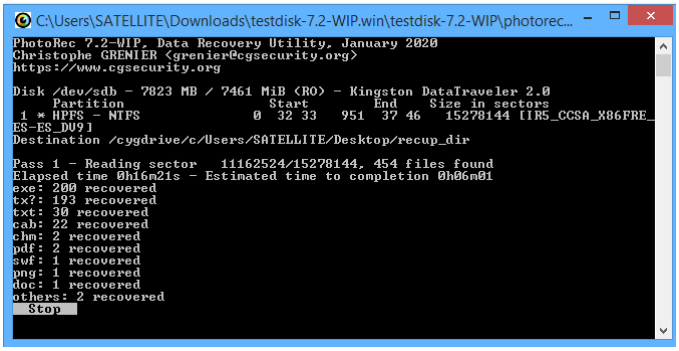

Figura 4. Proceso de recuperación.

Al momento de finalizar el escaneo y recuperar los datos eliminados, el programa crea una carpeta con el nombre de "recup_dir2" y es en la cual se encuentran los archivos que se recuperaron.

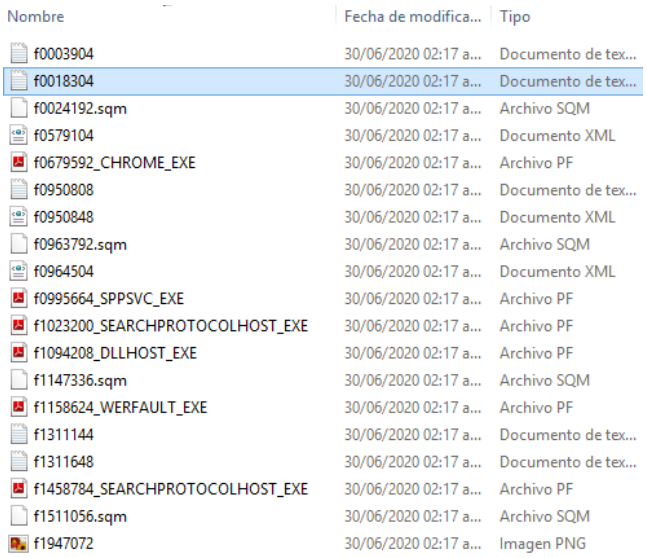

Figura 5. Archivos que se recuperaron.

CONCLUSIONES

Al finalizar este trabajo se concluyó que para poder elegir una herramienta de análisis forense es necesario tener bien definidas las necesidades para las que se va a utilizar y los criterios que se busca evaluar.

La ventaja del uso de estas herramientas es evidente ya que nos garantizan mayor rapidez en el análisis y también una gran facilidad al momento de utilizarlas.

Así también existen herramientas de alto nivel que permiten extraer metadatos de las evidencias eliminadas.

REFERENCIAS

[1] isecauditors. (2020). *Informática Forense y Peritajes*. Obtenido de isecauditors: https://www.isecauditors.com/informatica-forense-peritajes

[2] Zuccardi, G. G., & Gutiérrez, J. D. (Noviembre de 2006). *Informática Forense.* Obtenido de Nanopdf.com: https://nanopdf.com/download/informatica-forense-4_pdf

[3] Dragonjar. (s.f.). *Laboratorios: Informática Forense, Introducción y Contenido*. Obtenido de Dragonjar: https://www.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido.xhtml

[4] Manuel. (06 de Junio de 2014). *Seguridad Informatica Forense*. Obtenido de ¿Porque utilizar software de Analisis forense?: https://avancesdeseguridadinformatica-forense.blogspot.com/2014/06/software-de-analisis-forense.html

[5] Martinez, A. (23 de Febrero de 2016). *incibe-cert_*. Obtenido de Herramientas para realizar análisis forenses a dispositivos móviles: https://www.incibe-cert.es/blog/herramientas-forense-moviles

[6] Sánchez Cordero, P. (13 de Septiembre de 2013). *Conexion inversa*. Obtenido de forensics powertools (listado de herramientas forenses): http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html

[7] Photorec. (23 de Julio de 2019). Obtenido de https://www.cgsecurity.org/wiki/PhotoRec

[8] Diskinternals. (s.f.). *Software de recuperación de datos NTFS*. Obtenido de Diskinternals: https://www.diskinternals.com/ntfs-recovery/

[9] ccleaner. (s.f.). *Recuva ®*. Obtenido de ccleaner: https://www.ccleaner.com/recuva

[10] Forensic Data Recovery. (s.f.). *Recuperación de datos forenses vs recuperación de datos*. Obtenido de Forensic Data Recovery: https://www.cnwrecovery.com/html/forensic_dr.html

[11] dmde. (s.f.). *DMDE Nueva versión*. Obtenido de dmde: https://dmde.com/

[12] Iman IEF. (s.f.). *Imán IEF*. Obtenido de DataExpert: https://www.dataexpert.nl/en/products/digital-forensics-magnet-forensics/ief/

[13] Rivas, M. (27 de Mayo de 2019). *7 Herramientas gratuitas para recuperar la contraseña de Windows*. Obtenido de Neoguias: https://www.neoguias.com/recuperar-contrasena-windows/

[14] Druzhin, V. (26 de Noviembre de 2014). *NTPWEdit*. Obtenido de cdslow: http://cdslow.webhost.ru/en/ntpwedit/

[15] Fisher, T. (05 de Febrero de 2020). *Contraseña de NT sin conexión y editor de registro*. Obtenido de Lifewire: https://www.lifewire.com/offline-nt-password-and-registry-editor-review-2626147

[16] Tarasco Acuña, A. (s.f.). *Pwdump v7.1 - extractor de contraseña sin procesar*. Obtenido de Tarasco: https://www.tarasco.org/security/pwdump_7/

[17] hackingtools. (s.f.). *L0phtCrack*. Obtenido de hackingtools: https://www.hackingtools.in/free-download-l0phtcrack/

[18] Dragonjar. (s.f.). *Análisis Forense de Dispositivos iOS – Fase de Evaluación*. Obtenido de Dragonjar: https://www.dragonjar.org/analisis-forense-de-dispositivos-ios-fase-de-evaluacion.xhtml

[19] Guzman, J. A., & Forero, L. A. (02 de Octubre de 2013). *Analisis de Vulnerabilidades y seguridad de dispositivos moviles con sistemas operativos ios 6.1.4.*

[20] iPhoneBrowser. (30 de Abril de 2012). *iPhoneBrowser*. Obtenido de waxoo: https://iphonebrowser.waxoo.com/

[21] sourceforge. (02 de Enero de 2010). *Analizador de iPhone*. Obtenido de sourceforge: https://sourceforge.net/projects/iphoneanalyzer/

[22] iphonebackupextractor. (s.f.). *iphonebackupextractor*. Obtenido de iphonebackupextractor: https://www.iphonebackupextractor.com/

[23] Spyphone. (s.f.). *¿Ques es Spyphone o Celular espia?* Obtenido de Spyphone: https://www.spyphone.com.ar/comofunciona.html

[24] Dominguez, L. F. (21 de Noviembre de 2014). *Investigación forense de dispositivos móviles Android.* Obtenido de Grupo editorial ra-ma: https://www.ra-ma.es/libro/investigacion-forense-de-dispositivos-moviles-android_47960/

[25] Androguard. (18 de Febrero de 2019). *Descripcion del proyecto*. Obtenido de Androguard: https://pypi.org/project/androguard/

[26] Avila, F. (25 de julio de 2019). *LiME ~ Linux Memory Extractor*. Obtenido de Disoftin: http://www.disoftin.com/2019/07/lime-linux-memory-extractor.html

[27] compelson MOBIledit Forensic Express. (s.f.). *digitoforense*. Obtenido de compelson MOBIledit Forensic Express: https://www.digitoforense.cl/productos/compelson-mobiledit-forensic-express/

[28] Miguel Lopez Delgado, (Junio 2007). *Analisis Forense Digital.*

[29] Pato Rodriguez, A. (2006). *Metodología para realizar el manejo de incidentes de seguridad de TI mediante actividades de forensica digital.* Caracas.

[30] Hidalgo Cajo, I. M., Pucuna Yasaca, S., Hidalgo Cajo, B. G., Cevallos Paredes, K. A., Hidalgo Cajo, D. P., & Manuel, O. C. (Diciembre de 2018). *Análisis Comparativo De Herramientas Forenses Informáticas Para La Realización De Peritajes En.* http://eujournal.org/index.php/esj/article/viewFile/11578/11045