Análisis Forense desde una Perspectiva Práctica

Díaz, Danny
pankarn@outlook.com
Seminario de la Gestión de la Seguridad y el Riesgo
Universidad Piloto de Colombia

***Abstract*—Computer forensics is very important in the electronic information area, this due to its increased value and its use in storage devices. Several times, information is stored in a digital way, which can be retrieved applying strict and rigorous procedures; which could help to the collection, analysis and validation of all types of digital evidence. In this paper, I present a rigorous procedure about computer forensics accompanied by a practical test using the software tool called Backtrack, in order to recover files from electronic devices.**

***Keywords*—Backtrack, Computer forensics, Digital evidence, Electronic information.**

***Resumen*—La informática forense es muy importante en el ámbito de la información electrónica, debido al incremento del valor de ésta y el uso que se le da a la misma a través de dispositivos de almacenamiento. Muchas veces la información se almacena en formato digital, por lo que puede ser recuperada mediante la aplicación de procedimientos estrictos y rigurosos que ayudan a la recopilación, análisis y validación de todos los tipos de evidencia digital. En este trabajo se presenta un procedimiento riguroso sobre informática forense, acompañado de uncaso práctico usando la herramienta Backtrack, para recuperar archivos de dispositivos electrónicos.**

***Palabras Clave*–Backtrack, Evidencia digital, Informática forense, Información electrónica.**

I. INTRODUCCIÓN

En los últimos años el hombre ha creado y mejorado sistemas de comunicaciones, implementando cada vez más la seguridad en dichos sistemas. Lo anterior puesto que la vulnerabilidad en la seguridad afecta a usuarios y empresas a través de los delitos informáticos; los cuales hacen referencia a todo acto o conducta ilícita que es considerada criminal y con el objetivo de alterar, destruir o manipular cualquier sistema de información. Debido a esto, varias ciencias que protegen la información han surgido; una de estas es la denominada *Informática Forense*, la cual, en el mundo de hoy se ha convertido en un aspecto importante para cada país y una de las partes de interés es el análisis de dispositivos o información recuperada [1].

La informática forense se encarga de aplicar técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Lo anterior permite un buen manejo de la evidencia y los procedimientos judiciales correspondientes a cada país y cada caso a tratar [1].

Los investigadores de delitos informáticos deben seguir un conjunto de procedimientos estándar en los que se debe aislar físicamente la evidencia, con el fin de que no se contamine accidentalmente. Luego se debe realizar una copia digital de los medios de almacenamiento del dispositivo para guardar la evidencia y no modificarla, ya que la mayor parte de investigación se realiza sobre copias digitales. Para lo anterior existe una gran variedad de herramientas tanto software como hardware; de las cuales unas licenciadas y otras de uso libre [2-3].

Este artículo presenta un procedimiento de informática forense simplificado, acompañado de una evaluación práctica usando la herramienta Backtrack para la recuperación de archivos de un dispositivo electrónico. Para esto, este artículo se divide en las siguientes secciones: la Sección II presenta la base teórica de la informática forense; la Sección III describe un caso práctico de recuperación de información usando Backtrack y en la Sección IV se muestran las conclusiones y recomendaciones que deja el desarrollo del proyecto.

II. BASE TEÓRICA

Cabe aclarar que todo proceso que se realice en la informática forense debe quedar documentado junto

con los aspectos legales y normativos de las políticas de seguridad [3].

Básicamente la metodología para realizar un análisis forense digital consta de 3 pasos, los cuales son: extracción y preparación de los datos, identificación de los datos y análisis de los datos obtenidos junto con un reporte forense. La Figura 1 [4] muestra gráficamente dichos pasos.

Fig. 1. Metodología forense general. Por el autor.

Esta metodología permite reconstruir las pruebas que se obtienen de un delito informático, lo que conlleva a analizar los datos residuales y presentar las características importantes de los datos y bienes informáticos.

Para realizar el proceso forense adecuado descrito en la Figura 1, para la adquisición de evidencias se debe tener en cuenta lo descrito en la norma RFC 3227; la cual presenta una guía de buenas prácticas para la recolección y trato de información. Esto permitirá una mayor posibilidad de establecer el camino hacia el intruso y obtener más pruebas para judicializar a dicho intruso [5-6].

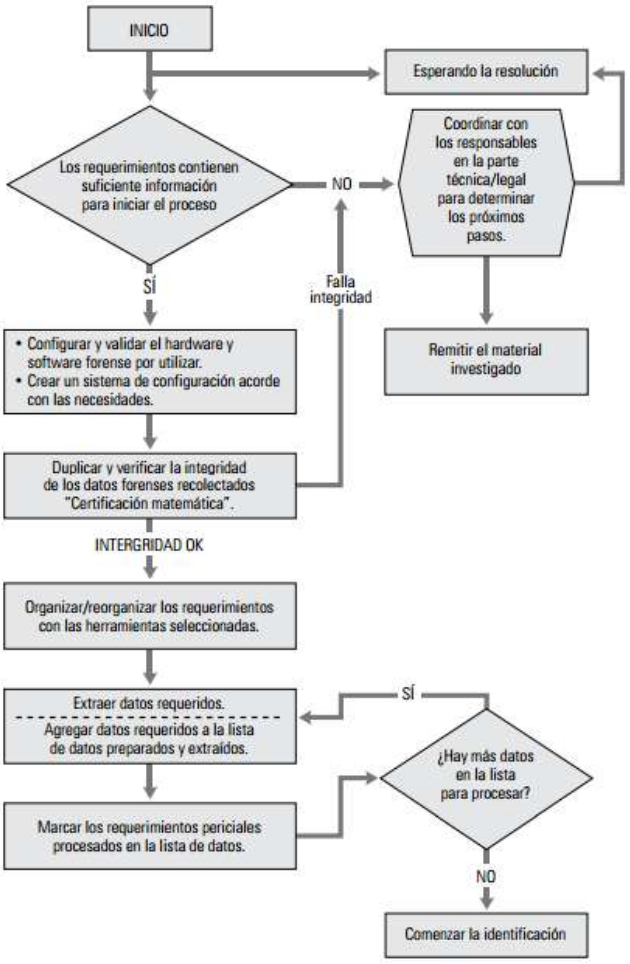
Algunas de las premisas de la norma RFC 3227 son:

- Establecer políticas de seguridad con el equipo de atención de incidentes y personas del campo jurídico.
- Recoger evidencias desde la más volátil hasta la menos volátil.
- Generar reportes sobre las pruebas encontradas, lo cual sirve como evidencia.
- No usar hardware o software que modifique la evidencia.

A. Preparación y Extracción de Datos

La Figura 2 indica el respectivo diagrama de flujo para la recolección de datos o pruebas. Para esto es necesario identificar las fuentes de información con el fin de extraer una imagen de los datos y no modificar o dañar la evidencia [7].

Fig. 2. Diagrama de flujo de preservación y extracción de datos [7].



La información es almacenada en computadores, CDs, DVDs, USBs (dispositivo con el cual se va a realizar la práctica), discos duros, celulares, entre otros. Según la Figura 2, los pasos para la extracción de datos informáticos son:

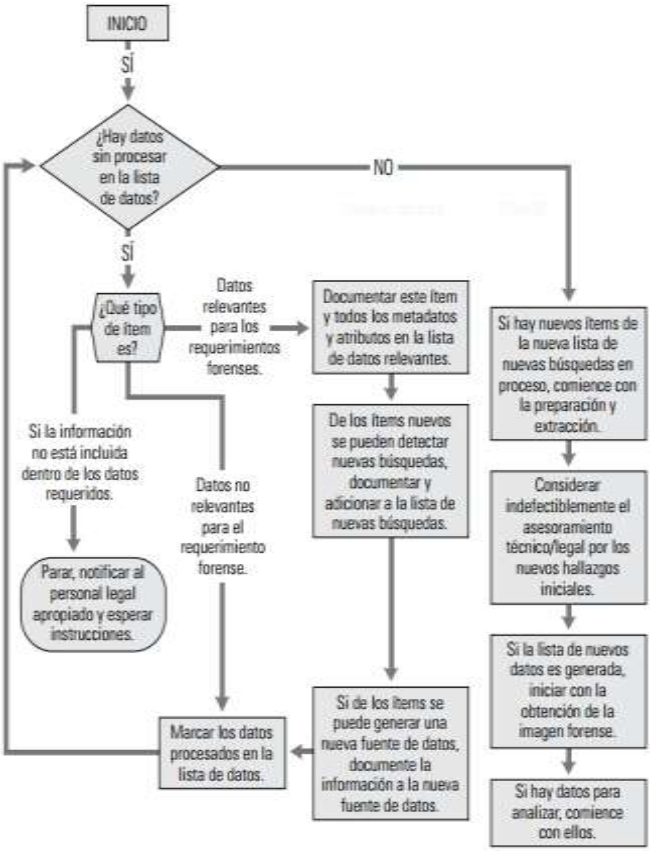
- Recolección de suficiente información para iniciar el proceso.
- Configuración y validación del software y hardware para el análisis de los datos.
- Extracción de una imagen (copia) de los datos por medio de una herramienta. Para este caso es una distribución de Linux denominada Backtrack. El tiempo en extraer toda la información del dispositivo depende de la capacidad del dispositivo y las características que tenga el computador.

El procedimiento para extraer una imagen o copia de un dispositivo USB se indicará en la Sección III.

B. Identificación de Datos

Una vez que se tienen los datos, se procede a realizar su respectiva identificación. El diagrama de flujo correspondiente a esta parte es el mostrado en la Figura 3, el cual indica cómo se puede extraer de forma general el tipo de información con el que se está tratando.

Fig. 3. Identificación de datos [7].



En algunos casos, los datos pueden ir ocultos en diferentes formatos de archivos. Debido a este problema hay que tener cuidado con el tipo de archivos que se suele abrir; puesto que los sistemas operativos como Windows® los aceptan como una extensión confiable cuando en realidad no lo son porque está camuflada. Para analizar este tipo de problemas, una de las herramientas que posee Backtrack consiste en hallar el número real y único que identifica a los archivos, este número es denominado **número mágico**.

Los números mágicos son constantes utilizadas para identificar el formato de los archivos y diferenciarlos de los demás. Éstos presentan una cabecera que los distingue y algunos tienen colas que también ayudan a distinguirlos mejor [8].

En la literatura existen muchos formatos de archivos, para dar una idea de estos, cuando se tiene un archivo con extensión "**.docx**", la cabecera del número mágico debe iniciar con "**50 4B 03 04 14 00 06 00**", el cual es un numero en hexadecimal. Así mismo para los miles de tipos de archivos que existen. En la sección III se realizará el análisis de una prueba con los números mágicos [8].

Para sacar provecho de los datos que se obtienen, es necesario utilizar los famosos *metadatos*; los cuales se definen *como datos sobre datos* y contienen gran cantidad de información que permite identificar, describir, gestionar y localizar recursos digitales. Una analogía de lo que son los metadatos con un elemento de la cultura cotidiana son las etiquetas que tienen los libros de una biblioteca. Los metadatos tienen tres elementos esenciales [9]:

- **Contenido**: asunto cobre lo que trata un documento.
- **Contexto**: características relacionadas con la creación de los objetos de información, como quién, cómo, por qué, dónde y cómo.
- **Estructura**: hace referencia al conjunto formal de relaciones con otros objetos de información.

Existen tres tipos de metadatos, los cuales se describen a continuación:

- **Metadatos descriptivos**: los cuales describen e identifican los recursos que permiten la búsqueda y recuperación de una determinada categoría de archivos.

- **Metadatos estructurales**: facilitan la navegación y presentación de los recursos electrónicos, lo que proporciona información de una estructura interna como una página, sección, tabla de contenido, etc. Además relaciona la información obtenida.

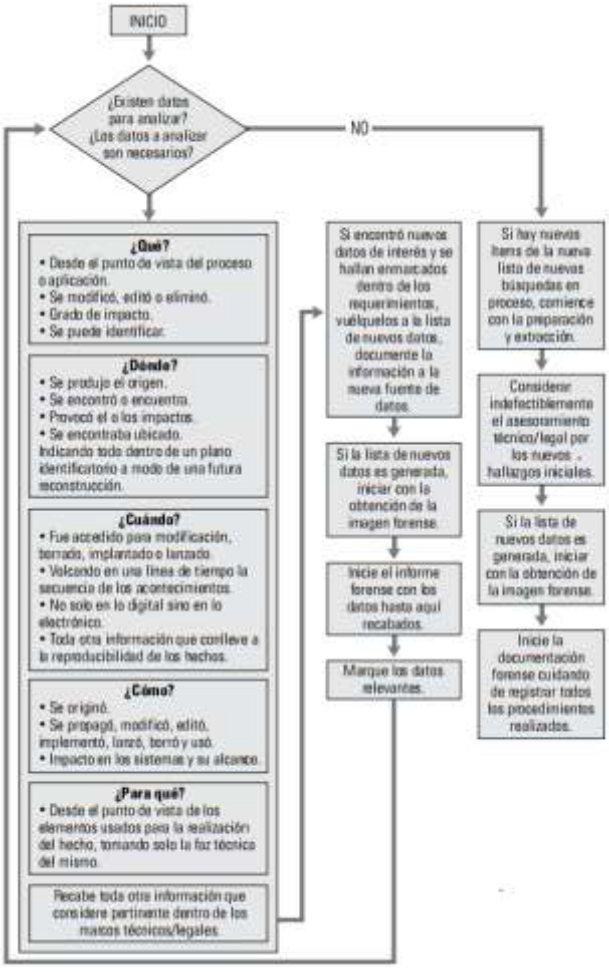
- **Metadatos administrativos**: organizan la información que se obtuvo con el fin de presentarla en un orden establecido según el criterio del forense.

Un caso práctico de estos se mostrará en la Sección III.

C. Análisis y Reporte Forense

Respecto al análisis de los datos, una vez que se extraen y se identifican se procede a obtener conclusiones propinadas de estos. Este análisis debe incluir la identificación de personas, lugares, objetos, eventos y la relación entre estos mismos. Estos subprocesos se muestran en la Figura 4.

Fig. 4. Análisis y reporte forense [7].



La Figura 4 indica si la información que se recolectó es necesaria para proseguir con el análisis o se requiere una consulta más profunda. Además permite identificar si el archivo ha sido creado, modificado o eliminado; y dónde se realizó, cuándo y en qué lugar. Luego marcar los datos más importantes.

Con lo anterior se da paso a documentar la información encontrada, desde lo más hasta lo menos importante. Una nota importante a tener en cuenta es que se debe proteger la intimidad y la confidencialidad de los datos encontrados.

Un aspecto relevante debe ser la elaboración de un informe, el cual debe informar acerca de la ley existente en Colombia relacionada con los delitos informáticos.

Existen básicamente tres tipos de informe, los cuales se describen a continuación:

- **Informe técnico**: en esta parte se documentan los resultados obtenidos en los subprocesos anteriores, con el fin de que el personal calificado presente un documento estructurado con las siguientes partes:

  - ✓ Antecedentes del delito informático.
  - ✓ Pruebas reunidas y examinadas minuciosamente.
  - ✓ Descripción de la metodología que se utilizó, herramientas HW y SW utilizadas, descripción de los hallazgos y orden en que sucedieron.
  - ✓ Conclusiones teniendo en cuenta las evidencias.
  - ✓ Anexos con información adicional.

- **Informe ejecutivo**: este tipo de informe está más orientado a un resumen del análisis efectuado, con el fin presentar una manera más fácil los resultados obtenidos. Éste debe ser preciso y debe contener los siguientes puntos:

  - ✓ Introducción a los objetivos del análisis.
  - ✓ Descripción sobre el entorno de trabajo, herramientas utilizadas y tiempo empleado.
  - ✓ Conclusiones a las que se llegó después del proceso, es decir descripción del

incidente, solución del incidente y recomendación final del hecho.

- **Prueba pericial**: en esta parte se indican los campos de interés de las pruebas reunidas. Para el caso de Colombia está vigente la ley 1273 de 2009, la cual protege la información y los datos de los atentados contra la confidencialidad, integridad y disponibilidad de los mismos y de los sistemas informáticos [10].

Esta ley incurre penas de prisión desde los 3 hasta los 10 años. Además multas desde 100 S.M.L.M.V (Salarios Mínimos Legales Mensuales Vigentes) hasta los 1500 S.M.L.V. en Colombia. Según la literatura, esta es una de las leyes que castiga en gran forma a los delitos informáticos a los cuales acude la informática forense.

Para dar una idea de lo que hace esta ley, en el Capítulo 1, Artículo 269A cita: "*Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes*" [10].

III. ANÁLISIS FORENSE PRÁCTICO

En esta parte se realizaron pruebas de un caso práctico usando la herramienta de simulación Backtrack, la cual es una distribución de Linux de uso libre. Con el fin de implementar un ambiente de virtualización, se utilizó un SW de máquina virtual, denominado *Virtual Box*, la cual permite instalar varios sistemas operativos en un solo computador.

Siguiendo la metodología descrita anteriormente, lo primero que se realizó fue instalar Virtual Box en un computador portátil con Windows® 7. Luego, en la máquina virtual se instaló Backtrack.

Es preciso insistir que, las Figuras 5 a la 19 muestran capturas de pantallas de los procedimientos realizados utilizando la herramienta Backtrack.

A) Recuperación de información

Para este procedimiento se utilizó una memoria USB con una capacidad de 256MB, esto con el fin de recuperar rápidamente la información. El procedimiento es el siguiente:

1- Conexión hardware

Lo primero que se debe realizar es conectar el dispositivo y que lo reconozca la máquina virtual.

2- Extracción de la imagen

Luego, para no alterar la evidencia, se obtiene una imagen (copia) de la memoria USB, de la que algunos de sus archivos han sido borrados. Se abre una ventana de terminal (CMD) y se escribe la siguiente línea de comando:

"#/dd if=/dev/sda1 of=/dev/im_fiet_usb.dd bs=512"

El comando "**dd**" (Dataset Definition), se utiliza para sacar una imagen (copia) lógica del dispositivo USB. El formato "**if=archivo_de_entrada**" asocia lo que se quiere copiar, "**of=archivo_de_salida**" asocia el destino del archivo o donde se van a copiar los datos. El comando "**bs**" especifica la velocidad con la que se está procesando la copia. Finalmente, la imagen queda guardada en el escritorio de Backtrack, con el nombre "**im_fiet_usb.dd**", como se especificó en la línea de comandos.

3- Montar la imagen

El paso a seguir es el montaje de la imagen. Para esto se debe descargar y descomprimir una herramienta disponible para Backtrack denominada **TestDisk,** la cual permite recuperar información de dispositivos de almacenamiento o partes lógicas como las imágenes. Esta herramienta se ubica en el escritorio y se procede como lo muestra la Figura 5:

Fig. 5. Comandos para montar la imagen. Por el autor.

En el primer recuadro amarillo de la Figura 5 se destaca la instrucción "**ls**", comando que muestra todo lo que hay en el *root*. De aquí se ve claramente la imagen lógica de la memoria USB. En el segundo recuadro se encuentran comando importantes para este proceso, estos son: "**mount**", que permite montar una imagen, "**-t**" es el tipo de unidad ya sea imagen o disco real, "**vfat**" es el formato de la memoria USB, "**-o loop.rw**" monta localmente la imagen con lectura y escritura, "**im_fiet_usb.dd**" es el nombre de la imagen y "**/mnt**" es la carpeta en donde se monta la imagen.

El tercer recuadro indica que la imagen quedo montada correctamente y se llama "**loop0**". Es preciso insistir que, hasta aquí, este procedimiento es el mismo cuando se conecta una memoria USB y es reconocida por el sistema.

En el cuarto recuadro se muestra el acceso al "**TestDisk**", al cual se le dan los permisos de lectura y escritura ("**chmod 777 photorec_static**") para que recupere la información que ha sido eliminada o formateada. Luego se ejecuta el comando "**./photorec_staticdev/loop0**".

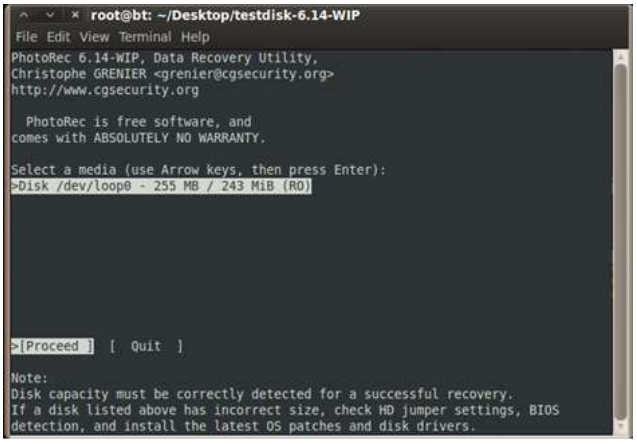
4- Procedimiento para la extracción de la información

Al finalizar los anteriores pasos, se obtiene una imagen similar a la mostrada en la Figura 6.

Fig. 6. Ejecución del *photorec*. Por el autor.

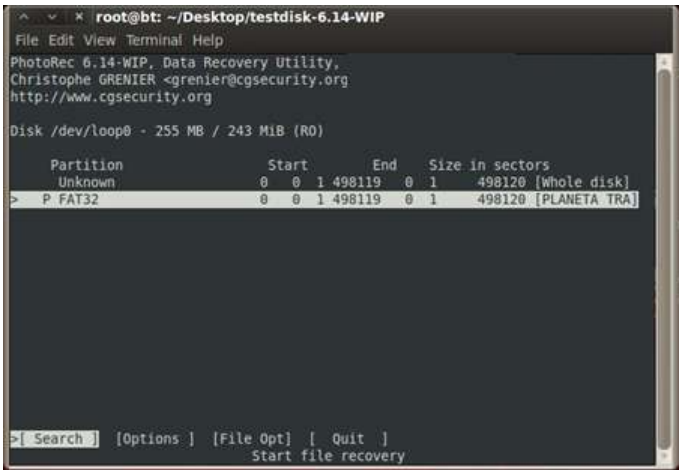
En esta parte de digita "**N**" para continuar con una nueva sesión. Esto genera otra ventana como la mostrada en la Figura 7, la cual indica claramente el tamaño de las unidades lógicas que están instaladas en la máquina virtual; en este caso tiene un tamaño de 255 MB. El comando "**dev**" significa la abreviación de dispositivo.

Fig. 7. Selección del dispositivo lógico montado. Por el autor.



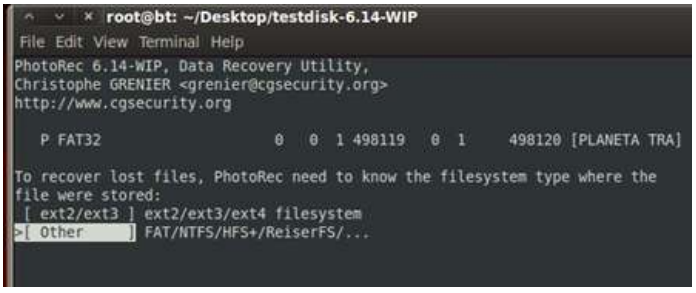
Acto seguido, se selecciona la imagen "**loop0**", puesto que es de la que se quiere recuperar información. Se confirma la selección con la tecla *enter* para proceder con la operación. Esto genera otra ventana como la de la Figura 8, la cual indica la partición que tiene la unidad lógica (**FAT32** en este caso).

Fig. 8. Tipo de partición lógica. Por el autor.



Confirmando de nuevo con un *enter*, se genera otra ventana como la de la Figura 9. Esta indica el tipo de archivo del sistema (por lo general es FAT/NTFS).

Fig. 9. Tipos de archivos. Por el autor.

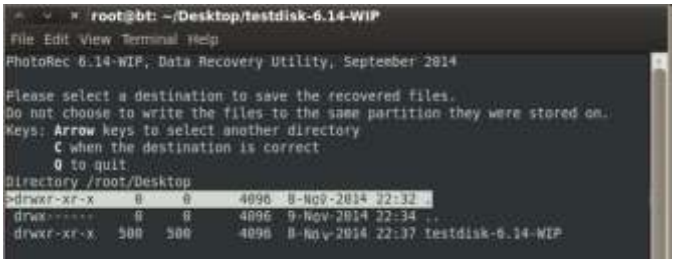


Se selecciona "**other**" y esto da paso a otra ventana como se muestra en la Figura 10. En donde se escanea el espacio libre.

Fig. 10. Escaneo del espacio libre. Por el autor.

Al seleccionar "**free**" aparece otra ventana. En ese instante, la dirección actual en donde se está trabajando es "**/root/Desktop/testdisk-6.14-wip**", luego se da un *enter* para devolverse a la dirección "**/root/Desktop**" como se muestra en la Figura 11, la cual indica el lugar donde se quiere guardar la información que se recupere.

Fig. 11. Lugar de recuperación de información. Por el autor.



Es preciso insistir que la información recuperada se debe guardar en un lugar deferente a la unidad lógica. Lo anterior para evitar posibles pérdidas. Por este motivo se guardó en el escritorio, como lo indica la Figura 11.

Seguidamente se presiona la tecla "**c**" e inmediatamente se inicia la recuperación, como se ve en la Figura 12.

Fig. 12. Información recuperada. Por el autor.

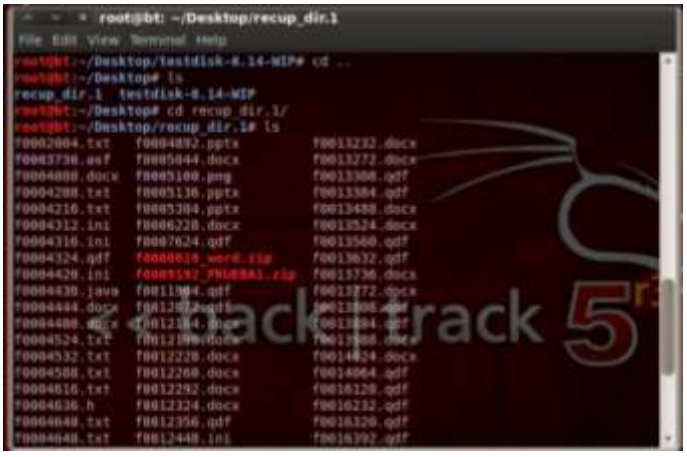
Para este caso, entre los archivos que se recuperaron están: 29 archivos en formato "txt", 29 comprimidos "zip", 27 "pdf", entre otros. Además se muestra el tiempo que se tardó (1 min 26 seg); tiempo que crecerá cuando el dispositivo o imagen es de mayor capacidad.

Ahora al seleccionar "**stop**", se muestra otra ventana como la de la Figura 13; acto seguido se presiona la tecla "**y**" para que se muestre el total de archivos recuperados y la carpeta creada en el escritorio para colocarlos. Cabe aclarar que, en diversas ocasiones se recupera una gran cantidad de archivos innecesarios, por lo que es conveniente analizar cada archivo recuperado.

Fig. 13. Creación de carpeta de recuperación. Por el autor.

Al terminar, se aborta la operación con la opción "**Quit**" y se llega al directorio "**TestDisk**". Para salir e ir al escritorio se coloca el comando "**cd..**", luego se accede con el comando "**cd recup_dir.l/**" a la carpeta de recuperación en el escritorio, como lo muestra la Figura 14.

Fig. 14. Carpeta de recuperación. Por el autor.



La Figura 14 muestra los datos recuperados, a los cuales les es posible realizar otro análisis para verificar si son datos con el formato o extensión adecuada. Esto para una correcta verificación de dichos formatos o extensiones.

B) Identificación del Formato de Archivos

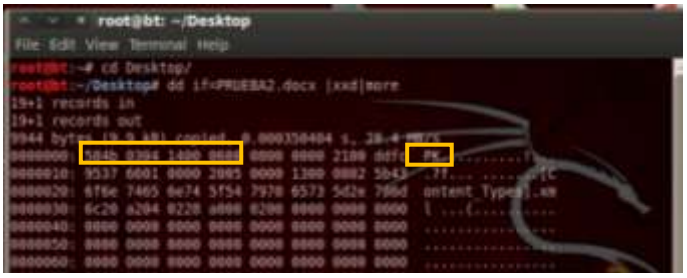
Una prueba adicional del análisis forense consiste en utilizar los números mágicos como se mostrará en el siguiente caso práctico. Para este caso se colocaron una serie de archivos en el escritorio de la máquina virtual, a los cuales se realizó un análisis mediante los números mágicos con el fin de observar si en verdad son los archivos con el formato original.

Estando en el escritorio y abriendo un terminal, se ingresa con el comando "**cd Desktop**", seguidamente se digita la línea de comando "**dd if=nombre_del_archivo.XXX |xxd|more**". Esto permite que los resultados se muestren en páginas.

Los formatos DOCX, PPTX y XLSX son versiones de documentos de Microsoft Office® 2007 y posteriores. Dichos formatos presentan igual cabecera: **50 4B 03 04 14 00 06 00**, y al final (cola) presentan la secuencia **50 4B 05 06**. Adicionalmente, el número mágico de estos archivos inicia con la secuencia "**pk**".

Las Figuras 15 y 16 muestran tanto el inicio como la cola de la cabecera del documento **prueba2.docx**.

Fig. 15. Cabecera del archivo PRUEBA2.docx.Por el autor.

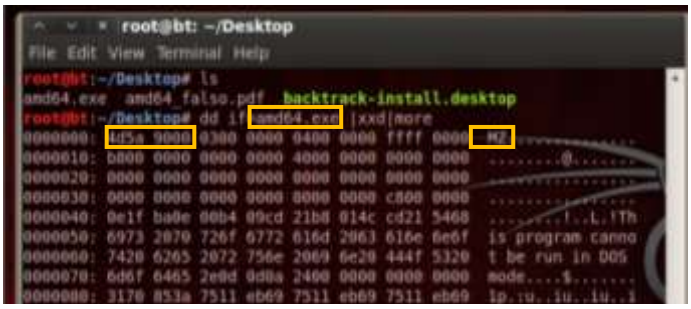


Para llegar al final de las páginas se presiona la tecla espacio.

Fig. 16. Terminación cola. Por el autor.

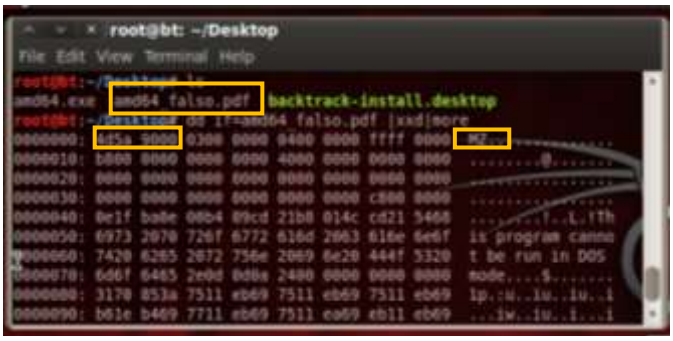
De lo anterior se concluye que, a este documento no se le ha cambiado la extensión. Potencialmente se pueden realizar más casos prácticos con archivos XLSX y PPTX**.** Otro caso práctico se presenta con los formatos COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS; los cuales presentan igual cabecera: **4D 5A**. Esto indica que son archivos ejecutables. Además, estos formatos se caracterizan con las letras "**MZ**", como se observa en la Figura 17 y este tipo de formato no presenta una terminación de cola conocida.

Fig. 17. Cabecera del archivo amd64.exe. Por el autor.



Un caso en particular se presenta cuando se modifica el formato del archivo. Para ilustrar esto se modificó la extensión del archivo "**amd64.exe**" a "**amd64_falso.pdf**". Para los archivos tipo pdf, se tiene que su cabecera debe iniciar con **25 50 44 46** y, en algunos casos, en la parte superior derecha aparece la versión del pdf. También se puede rectificar el tipo de archivo según cómo termine su cola. La terminación debe ser **0D 0A 25 25 45 4F 46 0D 0A.** Este caso se muestra en la Figura 18.

Fig. 18. Cabecera archivo amd64_falso.pdf. Por el autor.



En la Figura 18 se observa que, así la extensión de los archivos sea cambiada, no se puede pasar por alto el número mágico que lo identifica. En este caso, realmente corresponde a un archivo ejecutable.

C) Caso Metadatos

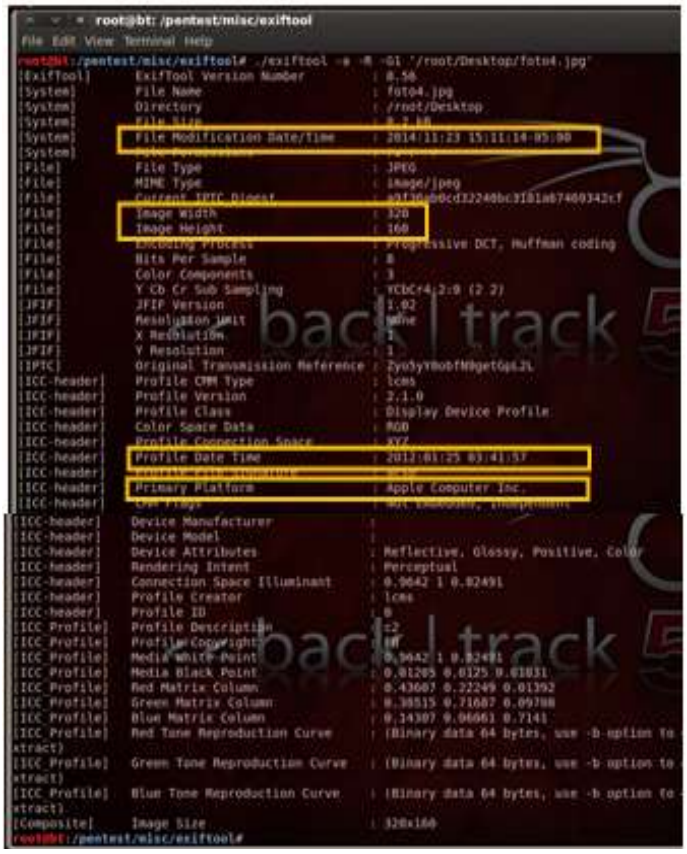
Una última herramienta que es de gran ayuda para el análisis forense son los metadatos. Para trabajar con ellos se colocó una foto en el escritorio de Backtrack, se abrió un terminal y se accedió a la dirección del escritorio. Acto seguido se compiló la siguiente línea de código:

/pentest/misc/exiftool# ./exiftool –a –R –G1 '/root/Desktop/foto4.jpg'

De aquí se tiene que "**Exiftool**" lee múltiples archivos para ordenarlos y además permite ver con que han sido relacionados. "-a", "-R" y "-G1" permiten visualizar de una mejor forma la información que se extrae del archivo, es decir los metadatos.

En la Figura 19 se observa la fecha de modificación, dimensiones, la fecha exacta cuando se creó y en qué computador se colocó inicialmente. Esto es útil cuando se recupera evidencia y se saca una imagen para ser procesada.

Fig.19. Caso práctico metadatos. Por el autor.



IV. CONCLUSIONES

La conclusión que deja este artículo de investigación es que el mundo de la tecnología es bastante amplio, y con ello los delitos informáticos; para los cuales la rama de la informática forense, llevando una metodología de investigación y leyes de cada país, permiten una buena gestión de todas las pruebas que se consiguen cuando sucede atentado contra la información. Este artículo aunque está orientado a herramientas software como

Backtrack, permite visualizar qué tan vulnerable es la información y cómo se le puede hacer seguimiento mediante un análisis forense. Las copias de las evidencias digitales, el análisis de los datos y los metadatos permiten abstraer suficiente información para aplicar las leyes judiciales correspondientes a cada país.

REFERENCIAS

[1] S. Donado, "INFORMATICA FORENSE," Octubre 2014, Universidad del Cauca, departamento de sistemas, Popayán, Cauca, Colombia.

[2] D. Brezinski y T. Killalea, "RFC 3227: Guía Para Recolectar y Archivar Evidencia," Febrero 2012. [Online], disponible en: https://prezi.com/qj7v6amnusy5/rfc-3227-guia-para-recolectar-y-archivar-evidencia/

[3] G. Zuccardi y J. Gutiérrez, "Informática Forense," Noviembre 2006. [Online], disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

[4] O. Carrol, et al., "Computer Forensci: Digital Forensic Analysis Methodology,"Enero 2008. [Online], disponible en: http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf

[5] D. Smith y S. Petreski, "A new Approach to Digital Forensic Methodology," November 2014. [Online], disponible en: https://www.defcon.org/images/defcon-18/dc-18-presentations/DSmith/DEFCON-18-Smith-SPM-Digital-Forensic-Methodlogy.pdf

[6] J. Cano, "Conceptos y Retos en la Atención de Incidentes de Seguridad y la Evidencia Digital," Noviembre 2014. [Online], disponible en: https://revistaing.uniandes.edu.co/pdf/rev15art9.pdf

[7] L. Ángel, "La informática forense, una herramienta para combatir la ciberdelincuencia," Noviembre 2014. [Online], disponible en: www.minseg.gob.ar/download/file/fid/893

[8] Garykessler, "File SignaturesTables," Septiembre 2012. [Online], disponible en:http://www.garykessler.net/library/file_sigs.html

[9] Classora, "Metadatos: definición aplicaciones y estándares," Febrero 2013. [Online], disponible en: http://blog.classora.com/2013/02/28/metadatos-definicion-aplicaciones-y-estandares/

[10] Alcaldía Mayor de Bogotá, "Ley 1273 de 2009," Enero 2009. [Online], disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492