Análisis forense empresa "Draft Complete"

1 Ángel Jiménez, 2 Jonathan Zevallos
Licenciatura en Redes y Sistemas Operativos (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía perimetral
1 Cdla. La Fragata, Guayaquil-Ecuador, pappo08zaruma@hotmail.com
2 Estero Nato y Las Américas, Daule-Ecuador, jzevallo@espol.edu.ec

Directora de Tesis Ing. Karina Astudillo, mail
karina.astudillo@elixircorp.biz

Resumen

El presente informe se basó en realizar un plan para el análisis forense de un dispositivo de medio extraíble, el cual nos permitió realizar los pasos adecuados para la óptima examinación y recuperación de la información. Es muy necesario e importante determinar todos los hechos ocurridos de una forma eficaz y ordenada, facilitando una clara síntesis de todos los sucesos que se realizaron. Este análisis se efectuó exclusivamente en un ambiente de software libre, en el cual se utilizaron herramientas forenses de excelente calidad, con la finalidad de poder garantizar y preservar la integridad de los datos contenidos de nuestra evidencia original. Como resultado, esta solución nos permitirá profundizar el respectivo aprendizaje en el análisis de archivos borrados, los correctos procedimientos a seguir en la protección de nuestra información confidencial y los métodos apropiados en busca de nuevas medidas informáticas que nos prevengan del robo de información.

Palabras Claves: *Preservar, evidencia, eliminar, análisis, imagen forense.*

Abstract

This report was based on a plan to conduct forensic analysis of a removable media device, which allowed us to make the right steps for optimal testing and information retrieval. It is very necessary and important to identify all the events in an efficient and orderly manner, providing a clear overview of all the events that took place. This analysis was performed in an environment of free software, but forensic-quality tools were used in order to guarantee and preserve the integrity of the data contained in our original evidence. As a result of this solution this will enable us to deepen the learning relevant in the analysis of deleted files, the correct procedures to follow to protect our confidential information and the appropriate methods to use for taking new computer measures that prevent information theft.

Palabras Claves: *Preserve, evidence, remove, analysis, forensic image.*

1. Introducción

En esta nueva era de tecnología y alta competitividad comercial, muchas empresas buscan innovar cada vez más la seguridad informática en sus equipos de comunicaciones, como resultado de estas implementaciones notablemente se marca la diferencia entre sus competidores.

No obstante, la mayoría de las organizaciones realizan una gran inversión, en este tipo de tácticas, además de lidiar con los problemas de amenazas externas como hacking, robos, etc., uno de los mayores temas de seguridad en cuanto a la protección de información confidencial de la empresa tienen que ver con amenazas internas, lo cual estas amenazas podrían facilitar información de gran utilidad para la competencia o realizar algún tipo de ataque.

En muchos casos, las empresas no consideran las debidas seguridades informáticas en sus estrategias y es por esta razón que Draft Complete, una empresa especializada en el desarrollo artístico de alta joyería, fue posiblemente víctima de un ataque de robo de información confidencial,

por parte de un empleado llamado Bruce Armiter.

En el caso analizado se nos indicó que un guardia de seguridad se dio cuenta que el mencionado empleado escondía un dispositivo de almacenamiento en sus zapatos, por lo que el guardia tuvo la corazonada que Armiter pudo realizar contrabando de información como imágenes de nuevos productos y planos del edifico hacia otras empresas, con lo cual un ladrón tendría el tiempo suficiente para planificar mejor su ataque.

El trabajo del Investigador forense consiste en probar o refutar las pretensiones del guardia de seguridad.

2. Herramientas Utilizadas

2.1. Caine

Es una distribución de Linux diseñada para investigadores forenses, la cual proporciona métodos óptimos para el análisis forense.

Ventajas

- Es una distribución de código abierto.
- Diseñada para soportar nuevas arquitecturas.
- Contiene una fácil interoperabilidad en su entorno.
- No monta ningún dispositivo automáticamente.

2.2. Autopsy

Es una herramienta forense que nos proporciona Caine, contiene excelentes utilidades, ya que cuenta con diferentes opciones que nos facilitan el análisis optimo en la investigación forense.

Ventajas

- Permite recuperar información.
- Permite la validación de integridad.
- Contiene distintos modos de búsqueda en su configuración.

2.3. Stegsecret

Esta herramienta permite detectar diferentes técnicas estenográficas y permite realizar un estegoanálisis de la información, para poder determinar si la información esta alterada con alguna herramienta estenográfica.

Ventajas

- Diseñada en java en un entorno Linux, es decir que es una herramienta de software libre.
- Permite asegurar la integridad de la información que utiliza.

2.4. Air

Es una herramienta forense que nos permite generar copias de imágenes forenses.

Ventajas

- Posee toda la interpretación del comando dd.
- Posee un entorno grafico sencillo y fácil de usar.
- Es una herramienta gratuita.

3. Acciones Realizadas

3.1. Proceso de adquisición

El proceso de la adquisición de la imagen forense ya fue establecido por el profesor, dicha imagen forense fue entregada en un CD como evidencia para su posterior análisis.

Dentro del CD se encuentró la imagen forense que se extrajo del dispositivo de medio extraíble que se le incautó a Bruce Armiter.

3.2. Preservando Evidencia

Este es un punto muy importante al momento de realizar una auditoría forense, debido a que todos los análisis y experimentos realizados se trabajan sobre copias de evidencia original.

En dichas copias tomadas de la evidencia, nosotros como investigadores forenses podremos realizar sin problemas todas las tareas que creamos convenientes y así mantener íntegra nuestra cadena de custodia.

3.3 Montar Evidencia Original

Primeramente se procede a insertar el CD en donde se encuentra nuestra evidencia y como podemos observar en la imagen, el dispositivo del CDROM está asociado con el **/dev/sr0**. Ahora montaremos nuestro dispositivo en modo lectura para evitar la manipulación de los datos contenidos en la evidencia hacia un directorio llamado

media/cdrom, a través del comando: **mount –o ro /dev/sr0 /media/cdrom.**

El parámetro **–o** nos ayuda a desplegar las opciones en modo lectura **(ro)** y modo escritura **(rw).**

Con el comando **df –h** nos permitirá identificar todas las unidades montadas actualmente.

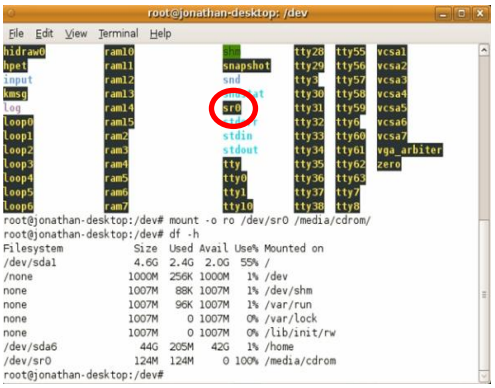

Figura 3.3-1 Montado Evidencia Original

3.4. Iniciando Air

Desde la línea de comandos digitamos **air&**, esto iniciará el proceso de arranque del programa, una vez ejecutado el programa en la parte del origen colocamos el directorio en donde se encuentra el CDROM, en este caso es el **/dev/sr0** y el destino es un directorio creado en **/home/caine/caso,** con el nombre de la copia de imagen forense llamada **Respaldo.img**.

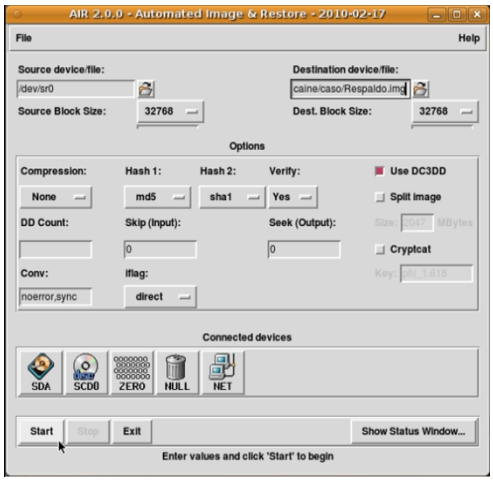

Figura 3.4-1 Ejecutando Air

3.5. Montar Copia de Evidencia Original

Una vez terminada la respectiva copia forense, procederemos a montarla en un directorio temporal en modo lectura asignado a un dispositivo **loop**, con la finalidad de no manipular los datos contenidos en nuestra copia forense, con la ayuda del comando:

- ✓ **mount –o ro,noexec,loop Respaldo.img /mnt.**

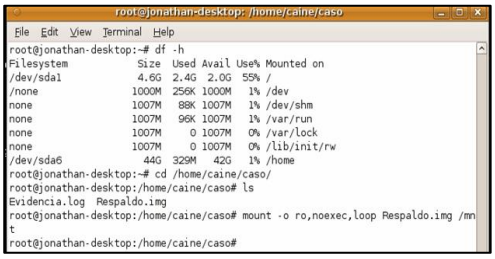

Figura 3.5-1 Montar Copia de Evidencia Original

Ahora lo que nos queda es cambiarnos a los respectivos directorios en donde se encuentra nuestra imagen forense llamada **cf.dd**, esta es la imagen forense que se obtuvo del dispositivo de medio extraíble de Bruce Armiter.

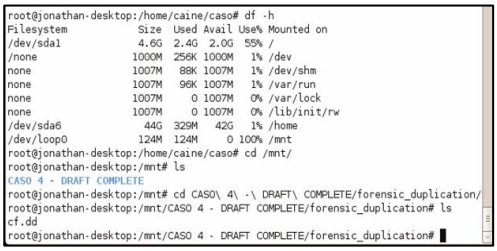

Figura 3.5-2 Imagen Forense cf.dd

3.6. Hashes y Duplicación de la Imagen Forense.

Mediante la utilización del comando md5sum nos permitirá extraer el hash en md5 de la imagen forense, es decir todo su contenido lo exportamos hacia un archivo llamado forense.log. El algoritmo matemático en md5 nos permitirá asegurar que no existan cambios en la imagen.

Luego de haber generado el hash realizamos la duplicación de la imagen forense, con el comando **dd_rescue,** en este caso digitaríamos **dd_rescue cf.dd /home/caine/caso/cfcopia.dd**, lo que significaría que **cfcopia** es nuestra copia duplicada.

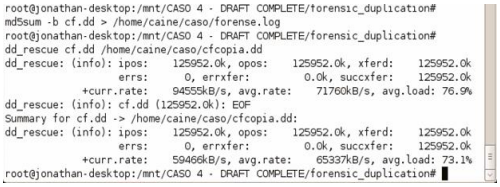

Figura 3.6-1 Duplicación de la imagen forense

Luego lo que nos quedaría es generar el hash de nuestra copia y realizar la respectiva comparación entre el original llamado forense.log y la copia forensecopia.log, ambos hashes como lo observamos en la imagen son idénticos.

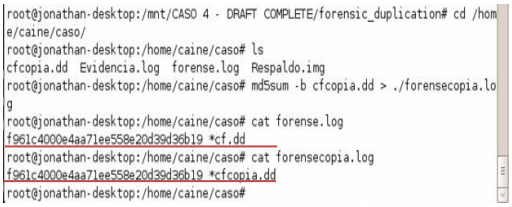

Figura 3.6-2 Comparación de hashes

3.7. Extracción de la información

Para llevar al cabo este punto vamos hacer uso de nuestra herramienta Autopsy, la cual procedemos a ejecutarla mediante la línea de comandos digitando **autopsy&**.

Llenaremos todos los datos necesarios de acuerdo a los parámetros y pasos que vemos en la tabla:

Tabla 1. Pasos para crear nuevo caso

#	Parámetros	Resultado
1	Nombre del Caso	DraftComplete
2	Descripción	Tesis
3	Nombre de los Investigadores	Ángel Jiménez, Jonathan Zevallos
4	Dar Clic en Nuevo Caso	
5	Dar Clic en Añadir Host	
6	Host	host1
7	Zona	/America/Guayaquil
8	Dar Clic en Añadir Host	
9	Dar clic en Añadir Imagen	

3.8. Insertar Imagen Forense en Autopsy.

En la siguiente ventana procedemos a insertar la ruta en donde se encuentra nuestra imagen forense, el resto de los parámetros se los deja por defecto y luego realizamos el cálculo de los hashes en md5 mediante autopsy.

Figura 3.8-1 Insertar Imagen Forense en Autopsy

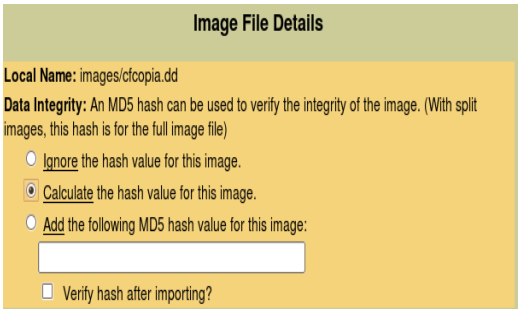

Figura 3.8-2 Opción para Calcular Hash

3.9. Comparación de Hashes en Autopsy

Mediante la comparación y el cálculo de los hashes de la imagen original y la copia podemos verificar que no se manipuló en ningún momento la evidencia.

Lo que significa que todos los datos que están contenidos dentro de la copia imagen forense están íntegros.

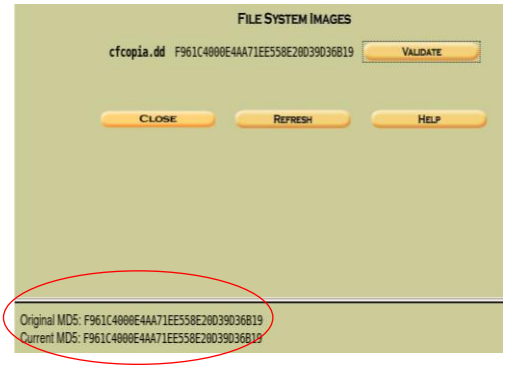

Figura 3.9-1 Validación de los Hashes en Autopsy

3.10. Recuperación de archivos borrados

Mediante la utilización de nuestra herramienta Autopsy, se procedió a realizar la respectiva recuperación de todos los archivos que habían sido eliminados.

Los archivos borrados se identifican mediante el color rojo, así como lo podemos observar en la imagen y aquellos que no están borrados se los identifica por el color azul.

Haciendo clic derecho sobre el archivo eliminado y mostrándolo en nueva ventana del explorador, se podrá visualizar con claridad los archivos que estaban borrados.

Además realizando una exportación de la información, se podrá recuperar con éxito estos archivos.

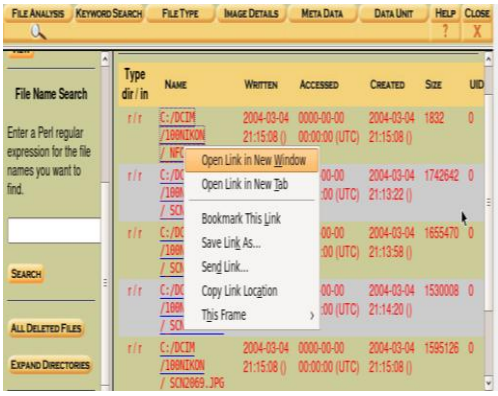

Figura 3.10-1 Recuperación de archivos borrados

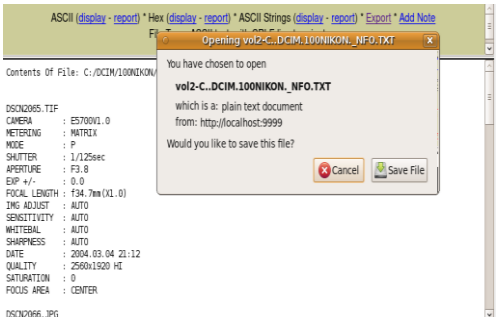

Figura 3.10-2 Almacenar Archivos Recuperados

3.11. Vista preliminar de archivos recuperados

Todos estos archivos se lograron recuperar con éxito, la mayoría de los archivos recuperados eran imágenes.

Cinco de estos archivos pertenecían a joyas, dos a los planos del edificio y un archivo de texto llamado NFO_.TXT.

Figura 3.11-1 Archivos Recuperados

3.12. Análisis mediante la Línea de Tiempo

Mediante un análisis más influyente, Autopsy nos provee esta opción, en la cual nos permite saber todos los sucesos ocurridos ordenadamente. Esta ventana nos proporciona un análisis óptimo sobre sobre la actividad que tuvieron cada uno de los archivos al momento de ser eliminados y explorados.

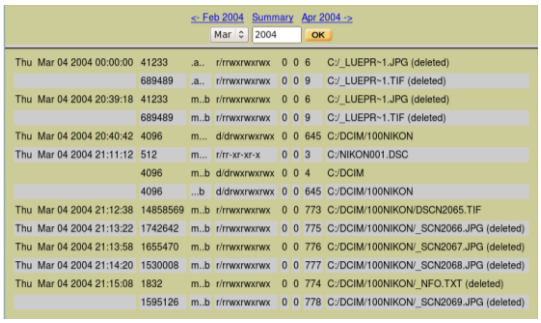

Figura 3.12-1 Actividad de los Archivos Eliminados

3.13. Análisis de Metadatos

Los metadatos son aquella información que se inserta en los archivos una vez que son creados. Esta información es de gran importancia, debido a que podemos demostrar en qué tipo de cámara fueron tomadas las fotos y aquella información contenida en cada uno de estos archivos.

Como podemos ver el archivo llamado **_LUEPR~1.JPG,** sí es una imagen JPG, pero de tipo JFIF. El estándar JPG tiene diferentes variaciones, en la cual los dos tipos más comunes son EXIF y JFIF, pero ambos archivos se clasifican como archivos JPG.

```
                    META DATA INFORMATION

Directory Entry: 6
Not Allocated
File Attributes: File, Archive
Size: 41233
Name: _LUEPR~1.JPG

Directory Entry Times:
Written:        Thu Mar  4 20:39:18 2004
Accessed:       Thu Mar  4 00:00:00 2004
Created:        Thu Mar  4 20:39:18 2004

Sectors:
42097 42098 42099 42100 42101 42102 42103 42104
42105 42106 42107 42108 42109 42110 42111 42112
42113 42114 42115 42116 42117 42118 42119 42120
42121 42122 42123 42124 42125 42126 42127 42128
42129 42130 42131 42132 42133 42134 42135 42136
42137 42138 42139 42140 42141 42142 42143 42144
42145 42146 42147 42148 42149 42150 42151 42152
42153 42154 42155 42156 42157 42158 42159 42160
42161 42162 42163 42164 42165 42166 42167 42168
42169 42170 42171 42172 42173 42174 42175 42176
42177 0 0 0 0 0 0 0

File Type: JPEG image data, JFIF standard 1.01, comment: "AppleMark"
```

Figura 3.13-1 Análisis de Metadato del Archivo _LUEPR~1.JPG

Nuestra segunda imagen llamada _LUEPR~1.TIF, estaba relacionada a un plano, pero a través de un análisis, se logró mostrar la informacion metadata del archivo, en la cual se puede observar con claridad que fue creado en un software llamado CoreGraphics que pertenece al sistema operativo MAC.

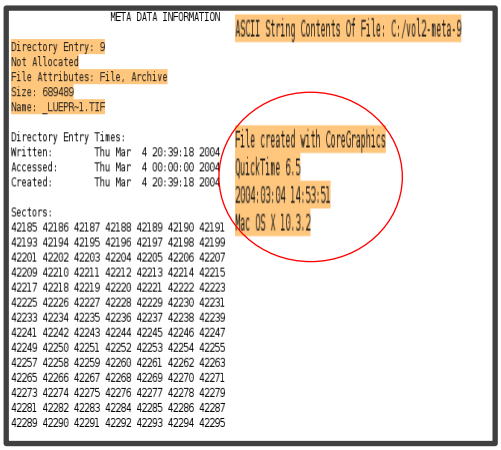

Figura 3.13-2 Análisis de Metadato del Archivo _LUEPR~1.TIF

El archivo _NFO.TXT, es aquel el que se encarga de almacenar toda la información de las todas fotos de la cámara, por esta razón Armiter tuvo que eliminar este archivo, además se realizó el análisis de metadata y se comprobó que se trataba de un archivo de texto.

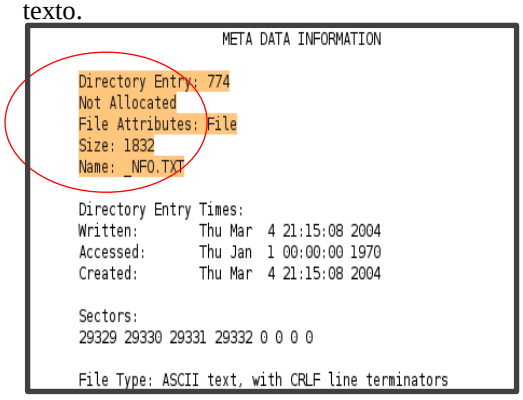

Figura 3.13-3 Análisis de Metadato del Archivo _NFO.TXT

4. Recuperación de Información Mediante Línea de Comandos

Primeramente nosotros deberíamos montar nuestra imagen forense llamada cfcopia.dd. Para poder realizar este proceso primeramente digitaremos el comando **fdisk –lu**, este comando se encarga de listar todas las particiones y además nos permite visualizar el tamaño de los sectores de nuestra imagen forense.

Como podemos observar nuestra imagen forense empieza desde los 32 bytes, cada sector está valorado en 512 bytes, es decir como vamos a tomar la única partición que contiene esta imagen forense el resultado sería 32*512=16384.

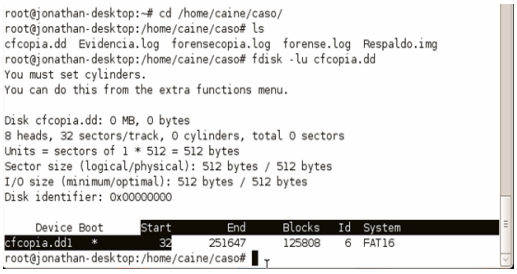

Figura 4-1 Utilizando Comando fdisk -lu

Ahora procedemos a añadir esta imagen forense en un dispositivo **loop**, lo cual nos ayudará a no manipular la información de nuestra imagen forense duplicada y luego realizamos el respectivo montado en modo lectura a un directorio temporal.

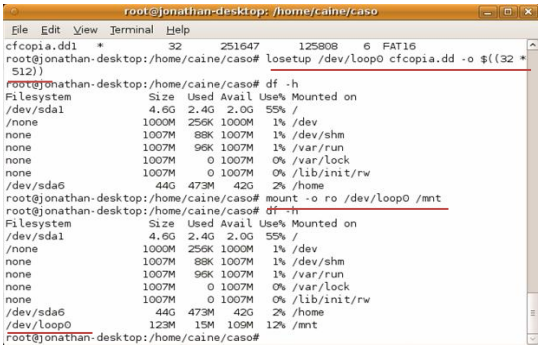

Figura 4-2 Montando Imagen Forense Duplicada.

4.1. Comando FLS

Este comando nos va a permitir listar todos los archivos y directorios borrados recientemente en dispositivo. Este comando dispone de varias opciones en la cual nosotros utilizaremos 4 de ellas que son:

Tabla 2. Parámetros del Comando FLS

Parámetro	Descripción
-r	Muestra todos los directorios de una forma recursiva

-l	Despliega todos los detalles en un formato largo
-p	Muestra la ruta completa por cada entrada
-f	Permite especificar el tipo de sistema de archivo.

Aquellos archivos que se muestren con el signo *, son los archivos que han sido eliminados.

Entonces nuestro comando quedaría de la siguiente manera:

- ✓ **fls –r –l –p –f fat /dev/loop**

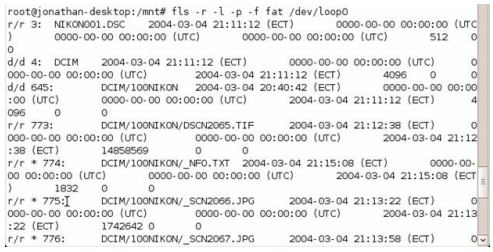

Figura 4.1-1 Comando FLS

4.2. Recuperación mediante Icat

El comando **icat** nos permite realizar la recuperación de archivos que han sido borrados en un dispositivo.

Los parámetros que utilizaremos es la opción **–f**, que significa que vamos a especificar nuestro sistema de archivo, luego el dispositivo en el que está montado, luego el inodo al cual están asociados los archivos, así como anteriormente los observamos listados con la ayuda del comando **fls** y por ultimo establecemos el nombre del archivo, pero de acuerdo al inodo al que está apuntando.

Figura 4.2-1 Recuperación de Archivos Mediante Icat

4.3. Recuperación mediante Fatback

Este comando es de gran utilidad al momento de realizar una recuperación de ficheros en sistemas de archivos FAT.

Para la utilización del comando simplemente digitaremos **fatback /dev/loop0**, este apunta al dispositivo loop en donde se encuentra nuestra imagen forense montada. Luego con el comando **ls** listaremos su contenido y como podemos observar existen archivos que contienen el signo **?**, este nos indica que son archivos que han sido eliminados y simplemente con el comando **cp** recuperamos rápidamente los archivos.

Figura 4.3-1 Recuperación de 2 Archivos Mediante Fatback

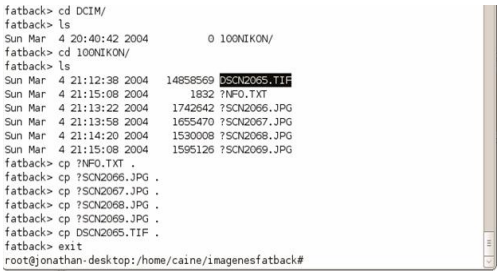

Figura 4.3-2 Recuperación de 6 Archivos Mediante Fatback

5. Verificación de Esteganografía

Mediante la utilización de la herramienta StegSecret, realizaremos un estegoanálisis de las imágenes JPG.

Dicha herramienta se ejecuta en Windows, en la cual trabaja exclusivamente con la plataforma de JAVA.

Como podemos ver en la imagen, esta herramienta realiza un análisis en busca de alguna manipulación por parte de otra herramienta y como podemos observar, no se detectó ningún acto estenográfico en las imágenes recuperadas.

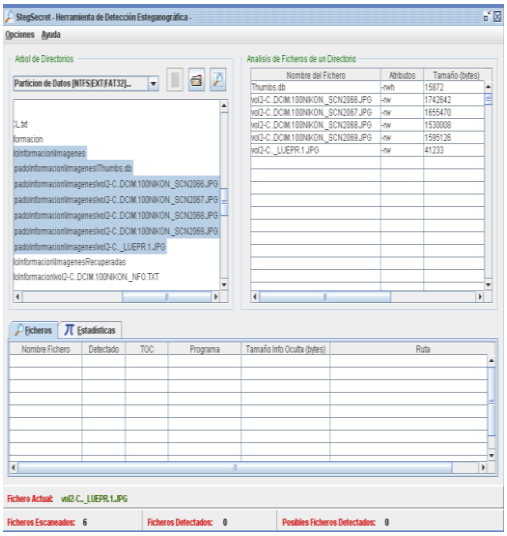

Figura 5-1 Verificando Esteganografía.

6. Conclusiones y Recomendaciones

- A través de nuestro análisis forense se determinó que existía información que había sido eliminada y toda esta información se logró recuperar con éxito.

- A través de la línea de tiempo se logró determinar cuál fue el orden en que se eliminó la información.

- Mediante un análisis de metadatos se logró comprobar la información contenida en cada uno de los archivos que fueron recuperados. Además en cada uno de estos archivos se comprobó que no existía ningún tipo de esteganografía.

- Con respecto a todas las evidencias encontradas se concluye que Bruce Armitter es culpable de la acusación del robo de información.

- Se recomienda elaborar una Política de Seguridad basada en el estándar ISO 27001 e implementar un Sistema de Gestión Informática que permita gestionar indicadores de cumplimiento de la política.

- Rediseñar la arquitectura de red para incluir controles de seguridad informática que garanticen la confidencialidad, disponibilidad e integridad de la información.

- Incluir dentro de la Política de Seguridad Informática procedimientos para el buen uso del internet y del correo electrónico, con el fin de prevenir que se filtre información confidencial o que se pierdan datos importantes para la organización.

7. Referencias

[1] Steve Gibson y Nanni Bassetti, AIR. Fecha de la última actualización Enero 2011. Disponible en: http://sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page.

[2] Alfonso Muñoz, StegSecret. Una simple herramienta estegoanálisis. Fecha de la última actualización Diciembre del 2007. Disponible en: http://stegsecret.sourceforge.net/indexS.html.

[3] Alejandro Sánchez, Ataques desde el interior de la red corporativa. Fecha de la actualización Marzo del 2002. Disponible en: http://www.robota.net/index.rsws?seccion=6&submenu=1&articulo=112.

[4] Developer.apple.com, Descripción de la tecnología MAC. Fecha de la última actualización Julio del 2012. Disponible en: http://developer.apple.com/library/mac/#documentation/MacOSX/Conceptual/OSX_Technology_Overview/MediaLayer/MediaLayer.html.