# 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 empleado mencionado 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.

Source device/file:			Destination	device/file:
/dev/sr0		-	caine/caso/H	tespaldo.img
Source Block Size:	32768 -	-	Dest. Block	Size: 32768 -
		Optic	ins	
Compression:	Hash 1:	Hash 2:	Verify:	Use DC3DD
None	md5	sha1 -	- Yes -	_ Split image
DD Count:	Skip (Input):		Seek (Output):	Size: 2047 MByte
	0	1	0	_ Cryptcat
Conv:	iflag:			Key: phi_1.618
noerror,sync	direct	1		
		Connected	devices	
SDA SCDO	ZERO NULL	NET		

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.

9	loor@jona	innam-	aesktu	ibe. Jui	ome/came/caso
<u>File Edit ⊻iew</u>	<u>Terminal</u> <u>H</u> e	р			
root@jonathan-	desktop:~# df	-h			
Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	4.6G	2.4G	2.0G	55%	1
/none	1000M	256K	1000M	1%	/dev
none	1007M	88K	1007M	1%	/dev/shm
none	1007M	96K	1007M	1%	/var/run
none	1007M	0	1007M	0%	/var/lock
none	1007M	0	1007M	0%	/lib/init/rw
/dev/sda6	44G	329M	42G	1%	/home
root@jonathan-	desktop:~# cd	/home	e/caine	e/cas	0/
root@jonathan-	desktop:/home	/caine	e/caso	# ls	
Evidencia.log	Respaldo.img				
root@jonathan-	desktop:/home	/caine	e/caso	# mou	nt -o ro,noexec,loop Respaldo.img /m
t					
root@ionathan-	desktop:/home	/caine	caso	¥	

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.

root@jonathan-d	esktop:/home	/cain	e/caso#	# df	-h
Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sdal	4.6G	2.4G	2.0G	55%	1
/none	1000M	256K	1000M	1%	/dev
none	1007M	88K	1007M	1%	/dev/shm
none	1007M	96K	1007M	1%	/var/run
none	1007M	0	1007M	0%	/var/lock
none	1007M	0	1007M	0%	/lib/init/rw
/dev/sda6	44G	329M	42G	1%	/home
/dev/loop0	124M	124M	0	100%	/mnt
root@jonathan-d	esktop:/home	/cain	e/caso#	t cd ,	/mnt/
root@jonathan-d	esktop:/mnt#	ls			
CASO 4 - DRAFT	COMPLETE				
root@jonathan-d	esktop:/mnt#	cd C	450\ 4	1 -11	DRAFT\ COMPLETE/forensic_duplication/
root@jonathan-d cf.dd	esktop:/mnt/	CASO ·	4 - DR/	AFT C	OMPLETE/forensic_duplication# ls
root@jonathan-d	esktop:/mnt/	CASO 4	4 - DR/	AFT C	DMPLETE/forensic_duplication#

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.

root@jonathan-desktop:/mnt	/CASO 4 - DRAFT COMP	LETE/torensic duplica	tion#
md5sum -b cf.dd > /home/ca	ine/caso/forense.log		
root@ionathan-desktop:/mnt	/CASO 4 - DRAFT COMP	LETE/forensic duplica	tion#
dd rescue cf.dd /home/cain	e/caso/cfcopia.dd		
dd rescue: (info): ipos:	125952.0k. opos:	125952.0k. xferd:	125952.0k
errs:	0. errxfer:	0.0k, succxfer:	125952.0k
+curr.rate:	94555kB/s, avg.rat	e: 71760kB/s. avg.	load: 76.9%
dd rescue: (info): cf.dd (	125952.0k): EOF		
Summary for cf.dd -> /home	/caine/caso/cfcopia.	dd:	
dd rescue: (info): ipos:	125952.0k, opos:	125952.0k, xferd:	125952.0k
errs:	0, errxfer:	0.0k, succxfer:	125952.0k
+curr.rate:	59466kB/s, avg.rat	e: 65337kB/s, avg.	load: 73.1%
root@jonathan-desktop:/mnt	/CASO 4 - DRAFT COMP	LETE/forensic duplica	tion#

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:

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

 Tabla 1. Pasos para crear nuevo caso

# **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.

1. Location Enter the full path (starting with /) to the image file. If the image is split (either raw or EnCase), then enter ''' for the extension. /home/caine/Tesis/ImagenForense/cfcopia.dd

Figura 3.8-1 Insertar Imagen Forense en Autopsy

	Image File Details
ocal N	lame: images/cfcopia.dd
l <b>ata Int</b> nages,	tegrity: An MD5 hash can be used to verify the integrity of the image. (With split this hash is for the full image file)
0	gnore the hash value for this image.
0	Calculate the hash value for this image.
0 <u>4</u>	Add the following MD5 hash value for this image:
	Verify hash after importing?

#### 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.

		<u>&lt;- Fe</u>	b 2004 Summ Mar ≎ 2004	har	x	Apr 2 OK	<u>1004 -&gt;</u> ⊑
Thu Mar 04 2004 00:00:00	41233	.a	r/mwxrwxrwx	0	0	6	C:/_LUEPR~1.JPG (deleted)
	689489	.a	r/rrwxrwxrwx	0	0	9	C:/_LUEPR~1.TIF (deleted)
Thu Mar 04 2004 20:39:18	41233	mb	r/rrwxrwxrwx	0	0	6	C:/_LUEPR~1.JPG (deleted)
	689489	mb	r/rrwxrwxrwx	0	0	9	C:/_LUEPR~1.TIF (deleted)
Thu Mar 04 2004 20:40:42	4096	m	d/drwxrwxrwx	0	0	645	C:/DCIM/100NIKON
Thu Mar 04 2004 21:11:12	512	m	r/rr-xr-xr-x	0	0	3	C:/NIKON001.DSC
	4096	mb	d/drwxrwxrwx	0	0	4	C:/DCIM
	4096	b	d/drwxrwxrwx	0	0	645	C:/DCIM/100NIKON
Thu Mar 04 2004 21:12:38	14858569	mb	r/rrwxrwxrwx	0	0	773	C:/DCIM/100NIKON/DSCN2065.TIF
Thu Mar 04 2004 21:13:22	1742642	mb	r/rrwxrwxrwx	0	0	775	C:/DCIM/100NIKON/_SCN2066.JPG (deleted)
Thu Mar 04 2004 21:13:58	1655470	mb	r/rrwxrwxrwx	0	0	776	C:/DCIM/100NIKON/_SCN2067.JPG (deleted)
Thu Mar 04 2004 21:14:20	1530008	mb	r/mwxrwxrwx	0	0	777	C:/DCIM/100NIKON/_SCN2068.JPG (deleted)
Thu Mar 04 2004 21:15:08	1832	mb	r/mwxrwxrwx	0	0	774	C:/DCIM/100NIKON/_NFO.TXT (deleted)
	1595126	mb	r/mwxrwxrwx	0	0	778	C:/DCIM/100NIKON/_SCN2069.JPG (deleted)

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 I	(NFORM)	TION		
Direct	tory Er	ntry: 0	5					
Not Al	llocate	ed						
File /	Attribu	ites: F	≕ile, /	Archive	е			
Size:	41233							
Name:	LUEPF	R~1.JP0	3					
Direct	tory Er	ntry Ti	imes:					
Writte	en:	Th	nu Mar	4 20	39:18	2004		
Access	sed:	Th	nu Mar	4 00	00:00	2004		
Create	ed :	Tł	nu Mar	4 20	39:18	2004		
Sector	rs:							
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	000	000	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.

META DATA INFORMATION ASCII String Contents Of File: C:/vol2-meta-9
Directory Entry: 9
Not Allocated
File Attributes: File, Archive
Size: 689489
Name: LUEPR~1 TTE
Directory Entry Times: File created with CoreGraphics
Written: Thu Mar 4 20:39:18 2004
Accessed: Thu Mar 4 00:00:00 2004
Created: Thu Mar 4 20:39:18 2004
2004:03:04 14:53:51
Sectors:
42185 42186 42187 42188 42189 42190 42191 VGC US X 10.3.2
42193 42194 42195 42196 42197 42198 42199
42201 42202 42203 42204 42205 42206 42207
42209 42210 42211 42212 42213 42214 42215
42217 42218 42219 42220 42221 42222 42223
42225 42226 42227 42228 42229 42230 42231
42233 42234 42235 42236 42237 42238 42239
42241 42242 42243 42244 42245 42246 42247
42249 42250 42251 42252 42253 42254 42255
42257 42258 42259 42260 42261 42262 42263
42265 42266 42267 42268 42269 42270 42271
42273 42274 42275 42276 42277 42278 42279
42281 42282 42283 42284 42285 42286 42287
42289 42290 42291 42292 42293 42294 42295

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.

META DATA INFORMATION
Directory Entry: 774 Not Allocated File Attributes: File Size: 1832 Name: _NFD.TXT
Directory Entry Times: Written: Thu Mar 4 21:15:08 2004 Accessed: Thu Jan 1 00:00:00 1970 Created: Thu Mar 4 21:15:08 2004
Sectors: 29329 29330 29331 29332 0 0 0 0
File Type: ASCII text, with CRLF line terminators

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.

root@jonathan-desktop:-# cd /home/caine/caso/ root@jonathan-desktop:/home/caine/caso# ls cfcopia.dd Evidencia.log forensecopia.log forense.log Respaldo.img root@jonathan-desktop:/home/caine/caso# fdisk -lu cfcopia.dd		
You must set cylinders.		L
You can do this from the extra functions menu.		L
		L
Disk cfcopia.dd: 0 MB. 0 bytes		L
8 heads, 32 sectors/track, 0 cylinders, total 0 sectors		L
Units = sectors of 1 * 512 = 512 bytes		L
Sector size (logical/physical): 512 bytes / 512 bytes		Ł
I/O size (minimum/optimal): 512 bytes / 512 bytes		L
Disk identifier: 0x00000000		L
		L
Device Root Start Fod Blocks Id System		L
cfcopia dd] * 32 251647 125808 6 EAT16	-	
rest dispethen desisters (here (sine (see t		
rootgjonathan desktop:/none/carne/caso# Y		11

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.

0		root@	Jonathar	rdeskto	ap: /h	ome/came/caso	
<u>File Edit</u>	⊻iew	Terminal	Help				
cfcopia.d root@jona	d1 * than-c	⊧ desktop:/h	32 nome/cai	25164 ne/caso	7 # los	125808 6 FAT16 etup /dev/loop0 cfcopia.do	d -o \$((32 *
rootaiona	than-c	lesktop:/h	nome/cai	ne/caso	# df	- h	
Filesyste	m	Si	ze Use	d Avail	Use%	Mounted on	
/dev/sdal		4.	6G 2.4	G 2.0G	55%	/	
/none		100	DOM 256	K 1000M	1%	/dev	
none		100	07M 88	K 1007M	1%	/dev/shm	
none		100	07M 96	K 1007M	1%	/var/run	
none		100	07M	0 1007M	0%	/var/lock	
none		100	07M (	0 1007M	0%	/lib/init/rw	
/dev/sda6		4	4G 473	M 42G	2%	/home	
root@jona	than-c	lesktop:/h	nome/cai	ne/caso	# mour	nt -o ro /dev/loop0 /mnt	
root@jona	than-c	lesktop:/h	nome/cai	ne/caso	# df	-h	
Filesyste	m	Si	ze Use	d Avail	Use%	Mounted on	
/dev/sdal		4.	6G 2.4	G 2.0G	55%	1	
/none		100	DOM 256	K 1000M	1%	/dev	
none		100	07M 88	K 1007M	1%	/dev/shm	
none		100	07M 96	K 1007M	1%	/var/run	
none		100	07M (	0 1007M	0%	/var/lock	
none		100	07M (	0 1007M	O%	/lib/init/rw	
/dev/sda6		4	14G 473	M 42G	2%	/home	
/dev/loop	0	12	23M 15	4 109M	12%	/mnt	
root@jona	than-c	lesktop:/h	nome/cai	ne/caso	#		

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	Des	cripción	
-r	Muestra directorios recursiva	todos de una	los forma

-1	Despliega todos los detalles en un formato largo
-р	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

root@jonathan-d	esktop:/mnt# fls -r -l -p -f fat /dev/loop0
r/r 3: NIKONOO	1.DSC 2004-03-04 21:11:12 (ECT) 0000-00-00 00:00:00 (UTC
) 0000-00	-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 512 0
0	
d/d 4: DCIM	2004-03-04 21:11:12 (ECT) 0000-00-00 00:00:00 (UTC) 0
000-00-00 00:00	:00 (UTC) 2004-03-04 21:11:12 (ECT) 4096 0 0
d/d 645:	DCIM/100NIKON 2004-03-04 20:40:42 (ECT) 0000-00-00 00:00
:00 (UTC)	0000-00-00 00:00:00 (UTC) 2004-03-04 21:11:12 (ECT) 4
096 0	0
r/r 773:	DCIM/100NIKON/DSCN2065.TIF 2004-03-04 21:12:38 (ECT) 0
000-00-00 00:00	:00 (UTC) 0000-00-00 00:00:00 (UTC) 2004-03-04 21:12
:38 (ECT)	14858569 0 0
r/r * 774:	DCIM/100NIKON/_NF0.TXT 2004-03-04 21:15:08 (ECT) 0000-00-
00 00:00:00 (UT	C) 0000-00-00 00:00:00 (UTC) 2004-03-04 21:15:08 (ECT)
) 1832	0 0
r/r * 775:]	DCIM/100NIKON/_SCN2066.JPG 2004-03-04 21:13:22 (ECT) 0
000-00-00 00:00	:00 (UTC) 0000-00-00 00:00:00 (UTC) 2004-03-04 21:13
:22 (ECT)	1742642 0 0
r/r * 776:	DCIM/100NIKON/_SCN2067.JPG 2004-03-04 21:13:58 (ECT) 0

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  $-\mathbf{f}$ , 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.

root@jonathan-desktop:/mnt# cd /home/caine/imagenesicat/ root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 774 > _N= 0.TXT	
<pre>root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 755 &gt; _SC N2066.JPG</pre>	
Invalid metadata address (fatfs inode lookup: 755 is not an inode)	
root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 775 > _SC	
<pre>N2067.JPG N2067.JPG</pre>	
<pre>N2068.10FG root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 777 &gt; _SC N2068.10FG</pre>	
<pre>root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 778 &gt; _SC N2069.JPG</pre>	
<pre>root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 6 &gt; _LUEP R~1.JPG</pre>	
<pre>root@jonathan-desktop:/home/caine/imagenesicat# icat -f fat /dev/loop0 9 &gt; _LUEP R~1.TIF</pre>	=
root@jonathan-desktop:/home/caine/imagenesicat#	

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.

root@jonathan-desktop:/home,	/caine/in	magenesfatback	# fatback /dev/loop0
No audit log specified, usir	ng "./fa	tback.log"	
Parsing file system.			
\ (Done)			
fatback> ls			
Sun Mar 4 21:11:12 2004	512	NIKON001.DSC	
Sun Mar 4 21:11:12 2004	0	DCIM/	
Sun Mar 4 20:39:18 2004	41233	?LUEPR~1.JPG	blueprint.jpg
Sun Mar 4 20:39:18 2004	689489	?LUEPR~1.TIF	blueprint.tiff
fatback> cp blueprint.jpg .			
fatback> cp blueprint.tiff .			
fatback>			

Figura 4.3-1 Recuperación de 2 Archivos Mediante Fatback

fatback>	cd DCIM/			
fatback>	ls			
Sun Mar	4 20:40:42 2004	0	100NIKON/	
fatback>	cd 100NIKON/			
fatback>	ls			
Sun Mar	4 21:12:38 2004	14858569	DSCN2065.TIF	
Sun Mar	4 21:15:08 2004	1832	?NF0.TXT	
Sun Mar	4 21:13:22 2004	1742642	?SCN2066.JPG	
Sun Mar	4 21:13:58 2004	1655470	?SCN2067.JPG	
Sun Mar	4 21:14:20 2004	1530008	?SCN2068.JPG	
Sun Mar	4 21:15:08 2004	1595126	?SCN2069.JPG	
fatback>	cp ?NFO.TXT .			
fatback>	cp ?SCN2066.JPG			
fatback>	cp ?SCN2067.JPG			
fatback>	cp ?SCN2068.JPG			
fatback>	cp ?SCN2069.JPG			
fatback>	cp DSCN2065.TIF			
fatback>	exit			-
root@ion	athan-desktop://h	ome/caine/in	magenesfatback#	2

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.

ciones Ayuda							
Arbal de Directorios				Analisis de Ficheros de un Direc	toria		
		[		Nombre del Fichero		Atributos	Tamaño (bytes)
Particion de Datos (NTFS)EX	T FAT32]	• •	= ڬ 🔼	Thumbs.db		-rwh	15872
				vol2-C.DCIM.100NIKON_SCN	2068.JPG	-11/	1742642
			÷.	VOI2-C. DCIM.100NIKON_SCN	2067.JPG	-04	1655470
LM				vol2-C.DCIM.100NIKON_SCN	2068.JPG	-1W	1530008
ormacion				vol2-C.DCIM.100NIKON_SCN	2069.JPG	-06	1595126
oInformacion/Imagenes				vol2-CLUEPR.1.JPG		-14	41233
padoinformacioniimagenesii	humbs.dd	1					
padolnformacionlimagenesiv	el2-C.DC	M 100NKON	SCN2066JPG				
nadolnformacionlimananach	el2.0 DO	M 100NKON	SCN2067. IPG				
padolinformación integrito de		88.4000-81-0014	00000000000			-	
paduniumaciunimagenesi	02-0.00	III. TUUNIKUN.	_SUN2008.JPG				
padoinformacioniimagenesii	el2-C.DC	M.100NKON,	_SCN2069.JPG				
padoinformacionilmagenesi	cl2-CLL	JEPR.1.JPG				-	
padolnformacionilmagenesk cinformacionilmagenesReci	ol2-CLL peradas	JEPR.1.JPG					
padoinformacioniimagenes) cinformacioniimagenesReci cinformacionivol2-C.DCIM.1	ol2-CLL peradas DONIKON,	JEPR: 1 JPG					
padoinformacionilmagenes) oinformacionilmagenesReci oinformacionivol2-CDCIM.1	ol2-CLL peradas JONIKON	IEPR.1.JPG	-				
padolinformacionilmagenesk olnformacionilmagenesReci olnformacionivol2-C. DCIM 1 4 (	dl2+CLL peradas DONIKON_	IEPR.1.JPG NFO.TXT	¥	( T			)
padoinformacionilmagenesk cinformacionilmagenesRecu cinformacionivol2-C. DCIM.1	dl2-CLU peradas DONIKON_	IEPR.1.JPG	Þ	(			•
padoinformacionilmagenesk cinformacionilmagenesRec cinformacionilvot2-C. DCIM1 	ticas	IEPR.1.JPG NFO.TXT	v F	(			
padoinformacionilmagenesk oinformacionilmagenesk oinformacionilvo12-C. DCIM 1 ( <b>PEcheros TEstadis</b> Nombre Fichero Def	dl2-CLL peradas DONIKON_ ticas ectado	NFO.TXT	Programa	Tamaño Info Ocuita (bytes)		R	) <b>)</b>
padoinformacionilmagenesis oinformacionilmagenesis oinformacionivo12-C. DCIM 1 Piccheros         T Estadis           Nombre Fichero         Def	dl2-CLL peradas DONIKON_ ticas	NFO.TXT	Programa	Tamaño Info Oculta (bytes)		R	luta
padoinformacioniimagenesis loinformacioniimagenesReci loinformacionivo12-C. DCIM 1 ∢ P Bcheros T Estadis Nombre Fichero Def	dl2-CLU peradas JONIKON_ ticas ectado	NF0.TXT	Programa	Tamaño Into Ocuita (bytes)		R	luta
padoinformacionilmagenesis loinformacionilmagenesis loinformacionivo12-C. D.CIM 1 4 P Bicheros T Estadis Nombre Fichero Def	dl2-CLU peradas DONIKON_ ticas	NFO.TXT	Programa	Tamafo Info Couta (bytes)		R	iuta
padoinformacioniimagenesis oinformacioni/imagenesiRecc oinformacioni/ot2-C.DCIM1 ∢[ ♪ Bicheros	dl2-CUU peradas DONIKON_ dicas ectado	IEPR 1 JPG	Programa	Tamafo into Ocuta (bytes)		R	iuta
padoinformacionilimagenesik oinformacionilimagenesiRec oinformacionikot2-C. DCIM 1	el2+CUL peradas DONIKON ticas ectado	IEPR 1.JPG	Programa	Tamafa Into Coutta (bytes)		R	►
pablinformationflimagenesi linformationflimagenesiRec linformationfol2⊂. DCIM 1 < ✓ Picheros (	el2+CU peradas DONIKON ticas ectado	IEPR 1.JPG	Programa	Tamafa into Ocula (bytes)		R	) Iuta
padoinformacionilmagenesis oinformacionilvot2-C. DOIM 1	el2+CUL peradas DONIKON ticas ectado	NF0.TXT	Programa	Tamafo teb Ocuta (bytes)		R	►
padothomacionimagenesi dintomacionimagenesi energia dintomacionivol2-0. DOIN 1 Pipcheros T Estadisi Nombre Fichero   Del	el2+CLL peradas DONIKON_ ticas ectado	IEPR 1 JPG	Ptograma	Tamafa Into Coulta (bera)		R	) Iuta
padoinformacionilmagenesis oinformacionilvei2-0.00 M 1	el2-CLU peradas DONIKON_ ticas	NFO.DIT	Programa	Tamafa teb Ocuta (bytes)		R	luta
padothomacionimagenesis dontomacionimagenesis dontomacionikol2-C. DCIM 1 P (pcheros) T (Estade Del Nombre Fichero)   Del	el2-CLU peradas DONIKON_	INFOLTUT	Programa	Tamalo teo (culo (otro)		R	luta

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: <u>http://sourceforge.net/apps/mediawiki/air-</u> <u>imager/index.php?title=Main\_Page</u>.

[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: <u>http://www.robota.net/index.rsws?seccion=6</u> <u>&submenu=1&articulo=112</u>.

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