

# Análisis Forense con The Sleuth Kit & Autopsy

**Alonso Eduardo Caballero Quezada**

Consultor de NPROS Perú SAC

Consultor de iDev Consultores en TI SAC

GIAC – SSP CNSA

Brainbench Computer Forensics (U.S.)

Página web: <http://www.ReYDeS.com>

Correo electrónico: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Trujillo, Perú - 24 de Abril del 2010

---

## Temario

- \* ¿Computer Forensics?
- \* Elementos de un buen proceso Forense
- \* Proceso Forense
- \* Todo es 0 y 1
- \* Un Disco Flexible
- \* ¿Qué es The Sleuth Kit?
- \* ¿Qué es Autopsy?
- \* Demostración
- \* ¿Preguntas, comentarios, sugerencias?



## ¿Computer Forensics?

Es una rama de la ciencia forense pertinente a la evidencia legal encontrada en computadoras y medios de almacenamiento digitales. El cómputo Forense también se conoce como Forense Digital.

El objetivo del Cómputo Forense es explicar el estado actual de un artefacto digital. El término artefacto digital puede incluir un sistema de cómputo, un medio de almacenamiento (como un disco duro o DVD), un documento electrónico (un mensaje de correo electrónico o imagen JPEG) o una secuencia de paquetes en movimiento en una red de computadoras.

La explicación puede ser tan simple como

**¿Qué información hay aquí?** y que se explica como

**¿Cual es la secuencia de eventos responsables de la situación actual?**

Fuente: Wikipedia.



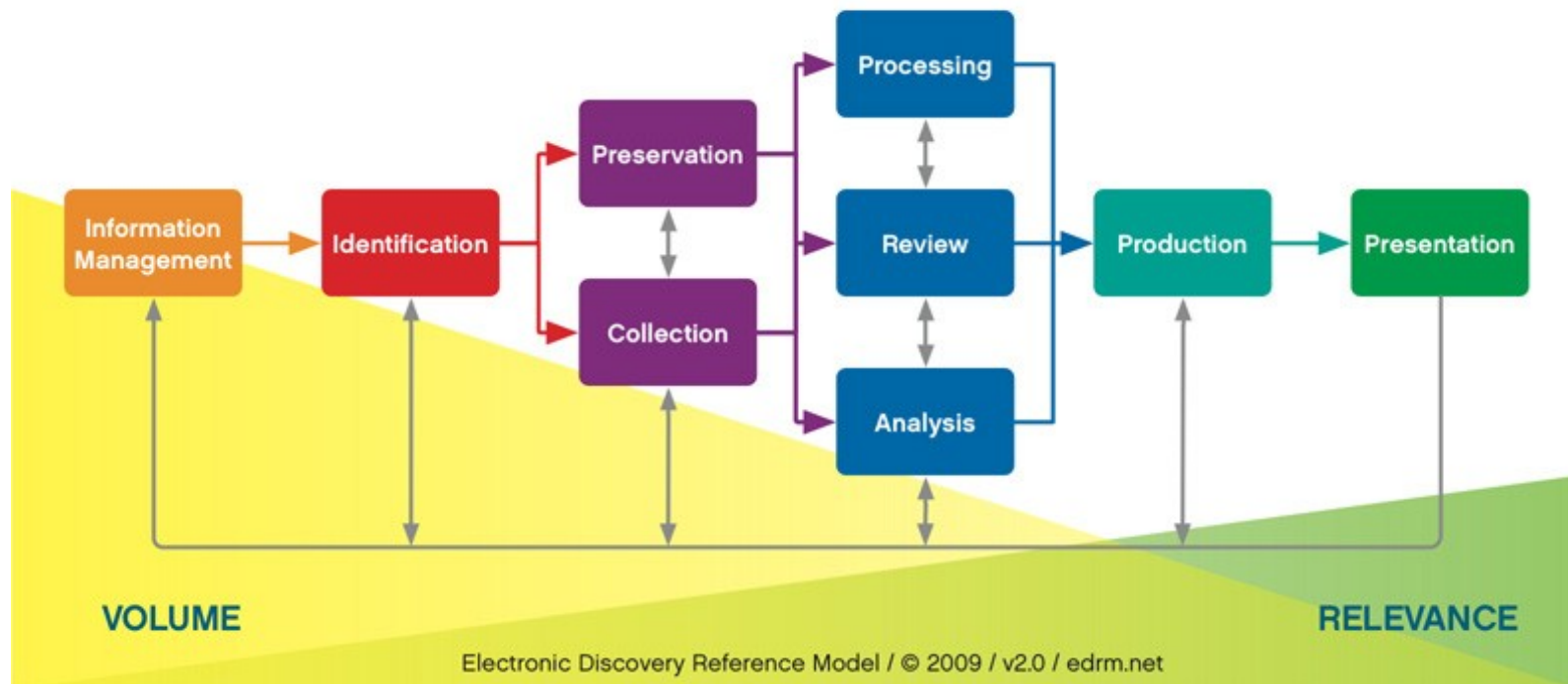
## Elementos de un buen proceso Forense

- \* Validación cruzada de los hallazgos
- \* Manejo adecuado de la evidencia
- \* Completar la investigación
- \* Administración de archivos (Backups, Originales)
- \* Competencia técnica
- \* Justificación y definición explícita del proceso
- \* Cumplimiento legal
- \* Flexibilidad

## Proceso Forense

Basado en Electronic Discovery Reference Model (EDRM) – Modelo de Referencia de Descubrimiento Electrónico.

### Electronic Discovery Reference Model



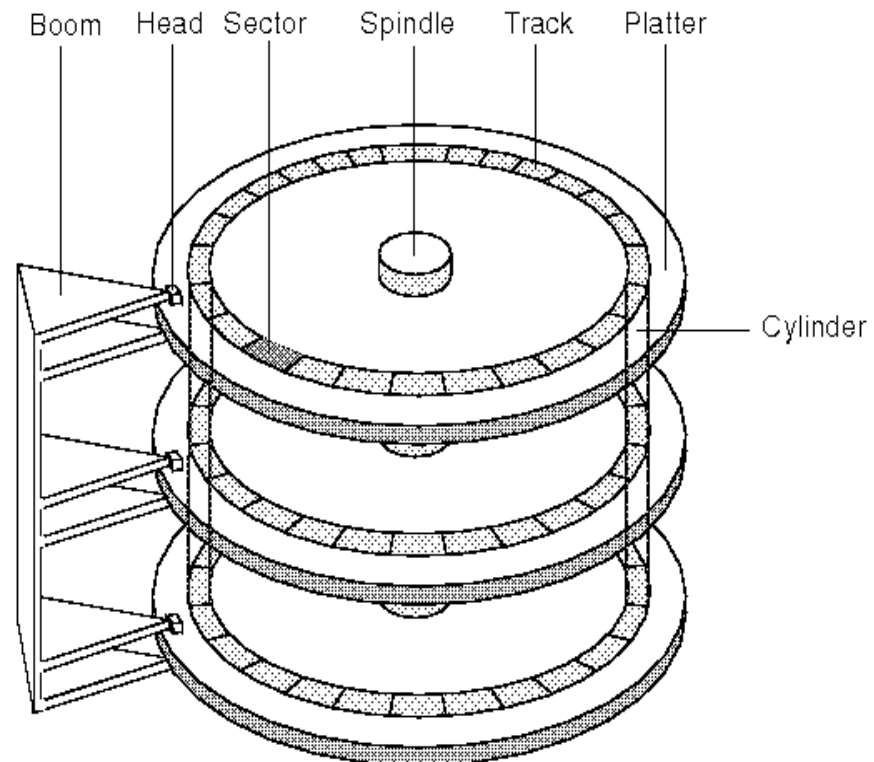
## Todo es 0 y 1

Las capas de una computadora

- **Aplicación** - **Sistema Operativo** - **BIOS (Basic Input Output System)** - **Hardware**

## Tipos de Medios

- Disco Duro (Hard Disk)
- Disco Flexible (Floppy Disk)
- CDROM
- DVD
- Unidades Flash USB



## Un disco Flexible (Floppy Disk)

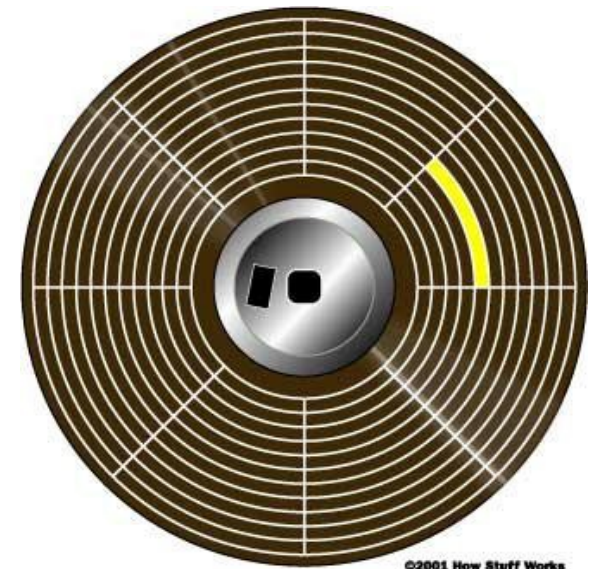
- Una pieza de plástico cubierta de ferro magnetita, o Metal flexible que rota bajo una cabeza o cabezal de Lectura / Escritura (Electro magneto)

- En la “lectura” el material ferro magnético magnetizado pasa por el aro de alambre que induce corriente en el alambre tal como se producen cambios en la densidad del flujo.

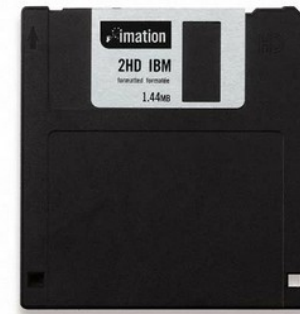
- 3,5 " de Diámetro

- 1440 K = 2880 Bloques

- 1 Bloque = 512 Bytes



©2001 How Stuff Works



## Un disco Flexible (Floppy Disk) [Continuación]

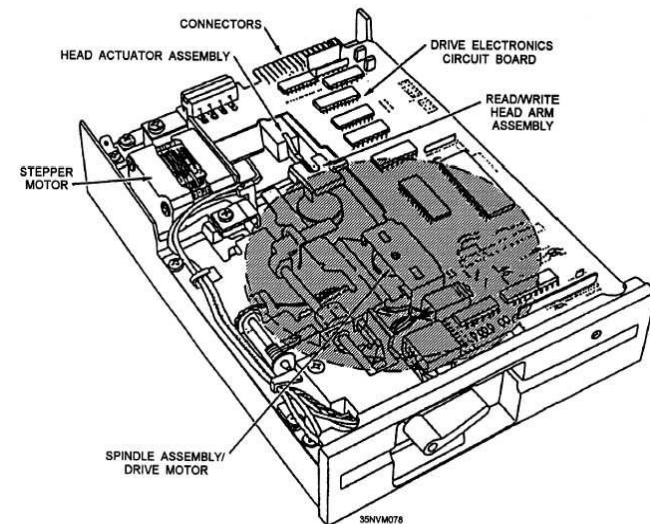
Una tarea típica y básica es utilizar “dd” para realizar la copia bit a bit de un disco flexible. La geometría común de un disco flexible de 3.5” es de:

- 18 Sectores por pista
- 2 cabezas
- 80 cilindros

Copiando un disco flexible de 3.5”

```
# dd bs=2x80x18b if=/dev/fd0 of=/caso07/discoflexible.dd
```

Los 18b especifican 18 sectores de 512 bytes, 2x multiplica el tamaño del sector por el número de cabezas, y el 80x es para los cilindros. Un total de 1474560 bytes. Lo anterior es una simple petición de lectura de 1474560 bytes a /dev/fd0 y una simple petición de lectura de 1474560 bytes a /caso0/discoflexible.dd



## ¿Qué es The Sleuth Kit?

The Sleuth Kit es una colección de herramientas en línea de comandos para análisis forense de archivos y volúmenes de sistema. Las herramientas del sistema de archivos permiten examinar el Sistema de Archivos de una computadora sospechosa sin comprometerla. Debido a que las herramientas no confían en el sistema operativo para procesar el Sistema de Archivos, se muestra contenido borrado u oculto.

Las herramientas de volumen del sistema permiten que se examine la disposición de los discos u otros medios. The Sleuth Kit soporta particiones DOS, BSD, Mac, Sun, etc. Con estas herramientas, se puede identificar donde están ubicadas las particiones para extraerlas, así pueden ser analizadas con las herramientas de análisis del Sistema de Archivos.

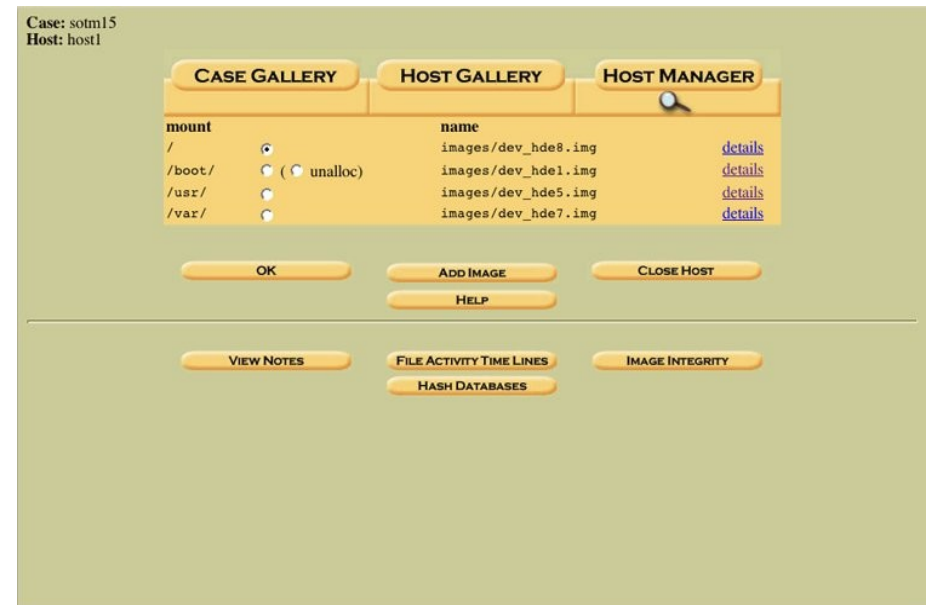
Cuando se realiza un análisis completo de un sistema, conocer todas estas herramientas en línea de comando puede resultar tedioso. Y aquí aparece Autopsy en escena.



## ¿Qué es Autopsy Forensics Browser?

Autopsy Forensics Browser es una interfaz gráfica de las herramientas de análisis en línea de comando para realizar investigación digital incluidas en The Sleuth Kit. Juntas pueden analizar discos y sistemas de archivos (NTFS, FAT, Ext2/Ext3, etc.)

The Sleuth Kit y Autopsy son Open Source y se ejecutan en plataformas Unix (Se puede utilizar también Cygwin para ejecutar ambos en entornos Windows). Como Autopsy está basada en HTML, se puede conectar al servidor Autopsy desde cualquier plataforma utilizando un navegador web. Autopsy proporciona un “Manejador de Archivos” como interfaz y muestra detalles sobre datos eliminados y estructuras del sistema de archivos.



## **Demostración: Scan 24 / <http://old.honeynet.org/scans/scan24/>**

Su misión es analizar un disco flexible recuperado y responder las preguntas formuladas. Se necesita leer el reporte antes de continuar el reto. Como una investigación del mundo real se necesita tener alguna información adicional y alguna evidencia, pero es la persona y sus conocimientos los que responderán las preguntas.

Nombre del Archivo: **image.zip**

Hash MD5 del Archivo: **b676147f63923e1f428131d59b1d6a72**

Preguntas:

¿Quién es el proveedor de marihuana de Joe Jacobs y cual es la dirección listada del proveedor?

¿Qué dato crucial está disponible dentro de coverpage.jpg y porque el dato es crucial?

¿Qué (si hay) otras escuelas vecinas a Snith Hill Joe Jacobs frecuenta?

Para cada archivo, que procesos hizo el sospechoso para enmascarar de otros.

¿Qué procesos (usted como analista) realizó para examinar el contenido completo de cada archivo?

## Demostración

- Descarga del archivo image.zip
- Verificación de su hash MD5.

```
root@reydes:/media/hda3# wget http://old.honeynet.org/scans/scan24/image.zip
--2010-04-15 15:42:13-- http://old.honeynet.org/scans/scan24/image.zip
Resolviendo old.honeynet.org... 64.236.114.1
Conectando a old.honeynet.org[64.236.114.1]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 18146 (18K) [application/zip]
Guardando: «image.zip»

100%[=====] 18.146      42,4K/s   en 0,4s

2010-04-15 15:42:13 (42,4 KB/s) - `image.zip' guardado [18146/18146]

root@reydes:/media/hda3# md5sum image.zip
b676147f63923elf428131d59b1d6a72 image.zip
root@reydes:/media/hda3# cat image.md5
b676147f63923elf428131d59b1d6a72 image.zip
root@reydes:/media/hda3#
```

- Descomprimir el archivo con: # unzip image.zip
- El archivo resultante es: image

## Demostración

La versión más reciente de The Sleuth Kit es la 3.1.1  
Y la versión más reciente de Autopsy es la 2.24

```
root@reydes:/media/hda3# cd tools/forensics/autopsy-2.24
root@reydes:/media/hda3/tools/forensics/autopsy-2.24# ./autopsy

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

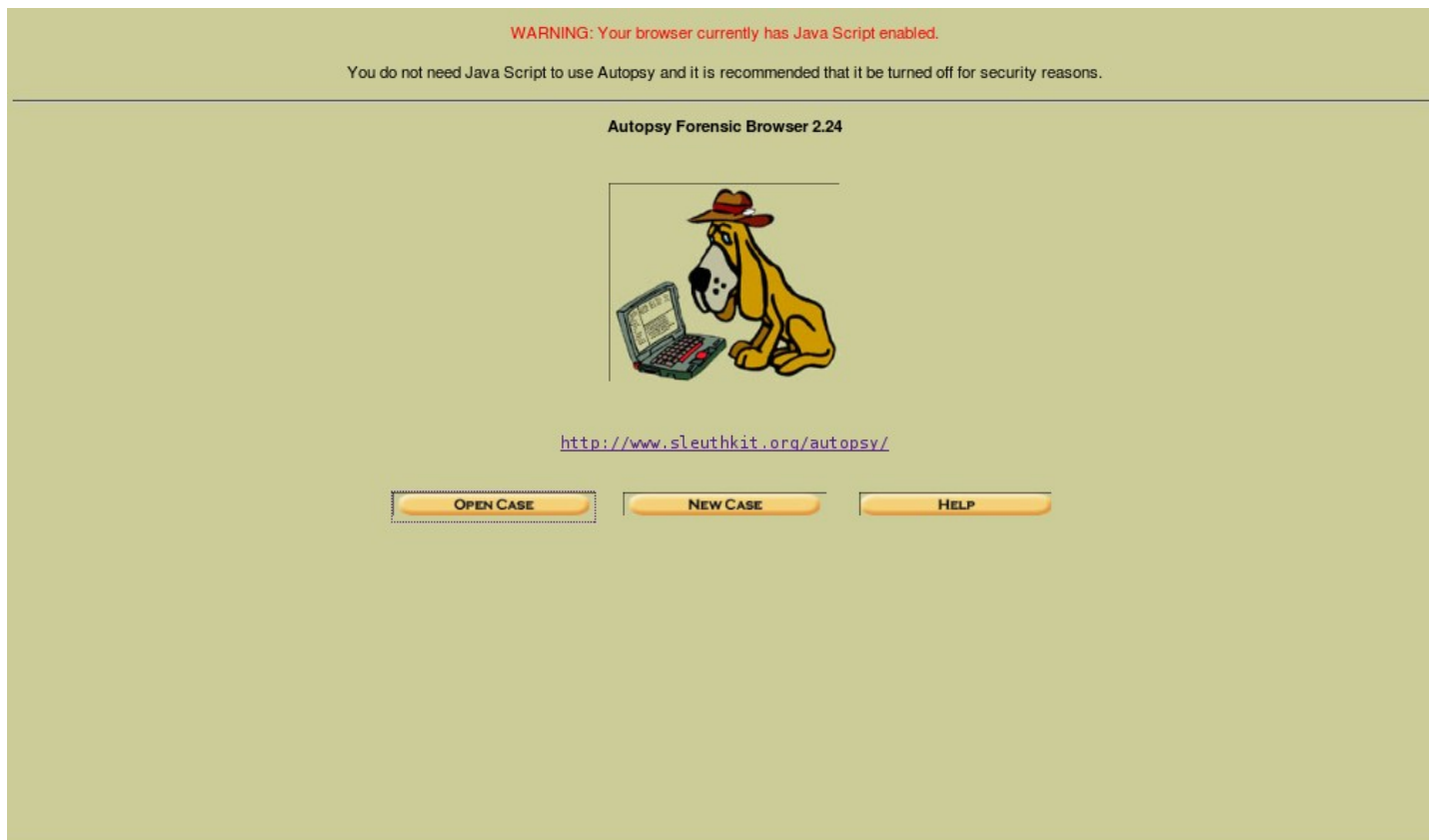
Evidence Locker: /media/hda3/EvidenciaCasos
Start Time: Thu Apr 15 16:03:06 2010
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

## Iniciando Autopsy



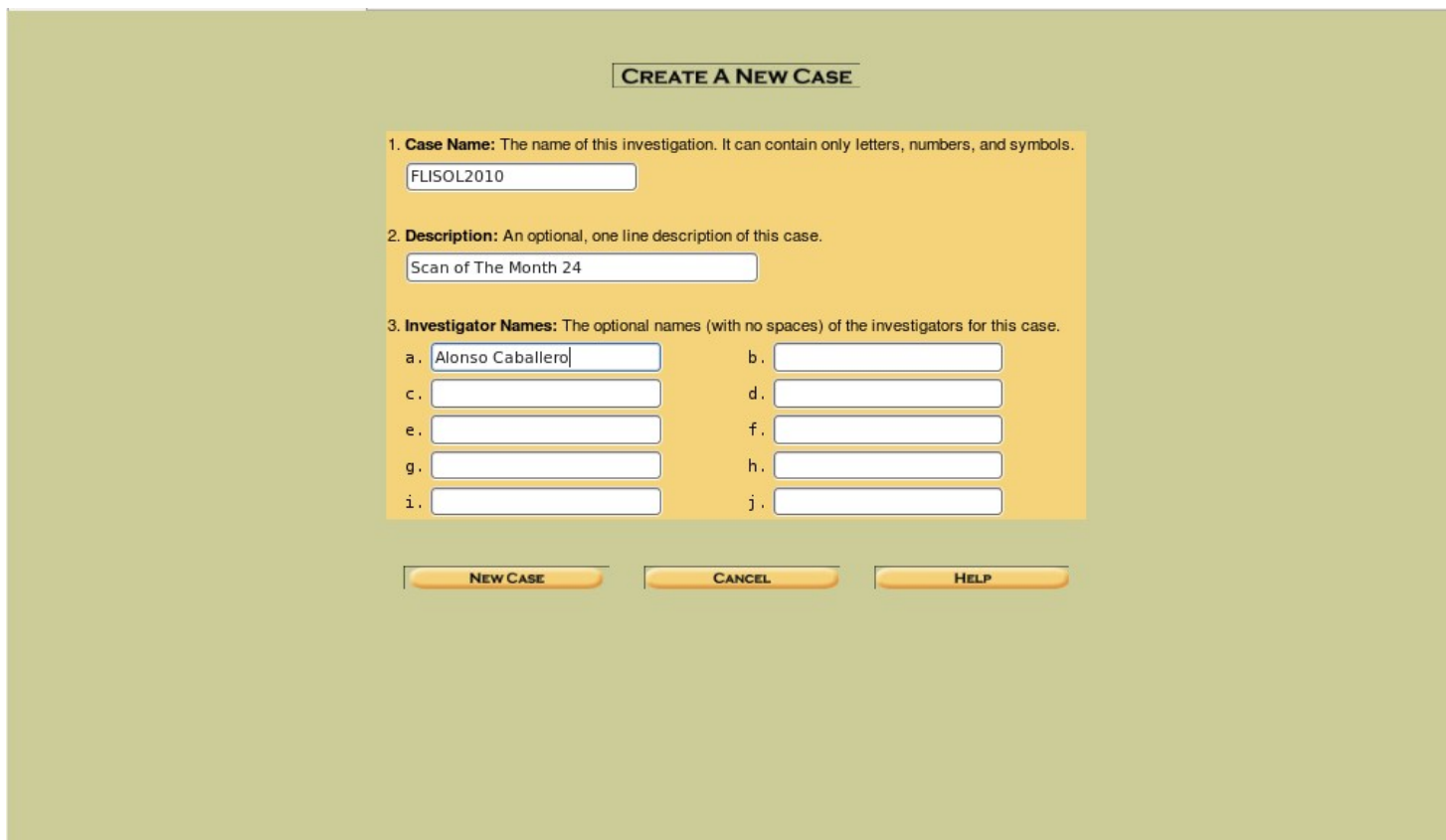
## Creación del caso

Creating Case: FLISOL2010

Case directory (/media/hda3/EvidenciaCasos/FLISOL2010/) created

Configuration file (/media/hda3/EvidenciaCasos/FLISOL2010/case.aut) created

We must now create a host for this case.



**CREATE A NEW CASE**

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	<input type="text" value="Alonso Caballero"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

## Creación del Host

Adding host: DiscoFlexible to case FLISOL2010

Host Directory (/media/hda3/EvidenciaCasos/FLISOL2010/DiscoFlexible/) created  
Configuration file (/media/hda3/EvidenciaCasos/FLISOL2010/DiscoFlexible/host.aut)  
created. We must now import an image file for this host

Case: FLISOL2010

**ADD A NEW HOST**

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
- Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
- Path of Alert Hash Database:** An optional hash database of known bad files.
- Path of Ignore Hash Database:** An optional hash database of known good files.

## Añadiendo una imagen (I)

Se indica donde está ubicado el archivo “image” a analizar

Case: FLISOL2010  
Host: DiscoFlexible

**ADD A NEW IMAGE**

**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.

**2. Type**  
Please select if this image file is for a disk or a single partition.

Disk  Partition

**3. Import Method**  
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink  Copy  Move

**NEXT**

**CANCEL** **HELP**

## Añadiendo una imagen (II)

Los discos flexibles de manera típica son volúmenes simples, sin embargo el investigador puede seleccionar manualmente “Volume Image” con un “Volume System Type” de DOS.



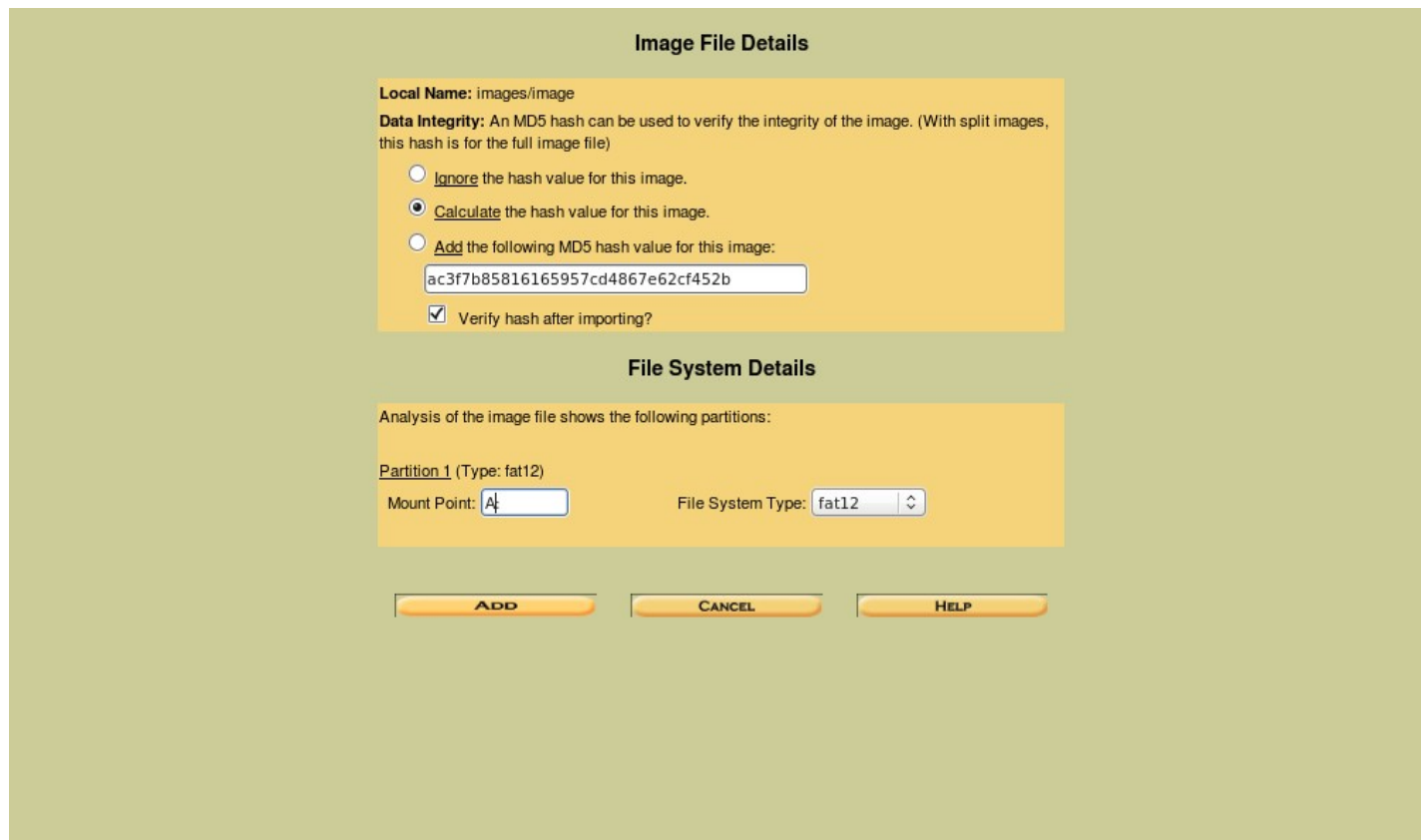
## Detalles del Archivo de imagen

Calculating MD5 (this could take a while)

Current MD5: AC3F7B85816165957CD4867E62CF452B

Testing partitions | Linking image(s) into evidence locker | Image file added with ID img1

Volume image (0 to 0 - fat12 - A:) added with ID vol1



**Image File Details**

Local Name: images/image

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.

Calculate the hash value for this image.

Add the following MD5 hash value for this image:

ac3f7b85816165957cd4867e62cf452b

Verify hash after importing?

**File System Details**

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat12)

Mount Point: A:

File System Type: fat12

ADD CANCEL HELP

## Inicio del análisis

Es momento de iniciar el análisis

Case: FLISOL2010  
Host: DiscoFlexible

Select a volume to analyze or add a new image file.

**CASE GALLERY**   **HOST GALLERY**   **HOST MANAGER**

mount	name	fs type	
<input checked="" type="radio"/> A: /	image-0-0	fat12	<a href="#">details</a>

**ANALYZE**   **ADD IMAGE FILE**   **CLOSE HOST**  
**HELP**

---

**FILE ACTIVITY TIME LINES**   **IMAGE INTEGRITY**   **HASH DATABASES**  
**VIEW NOTES**   **EVENT SEQUENCER**

## Creación de los índices de búsqueda

Antes del proceso

**IMAGE DETAILS**

**Name:** image-0-0  
**Volume Id:** vol1  
**Parent Volume Id:** img1  
**Image File Format:** raw  
**Mounting Point:** A: /  
**File System Type:** fat12

**External Files**

**ASCII Strings:**  
**Unicode Strings:**  
**Unallocated Sectors:**  
**ASCII Strings of Unallocated:**  
**Unicode Strings of Unallocated:**

**Extract Strings of Entire Volume**

Extracting the ASCII and Unicode strings from a file system will make keyword searching faster.

Generate MD5?

ASCII:  Unicode:

**EXTRACT STRINGS**

**Extract Unallocated Sectors**

Extracting the unallocated data in a file system allows more focused keyword searches and data recovery.

(Note: This Does Not Include Slack Space)

Generate MD5?

**EXTRACT UNALLOCATED**

## Creación de los índices de búsqueda (II)

Después del proceso



# Análisis de Archivos

Es necesario examinar cada uno de los archivos.

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP ? CLOSE X

**Directory Seek**

Enter the name of a directory that you want to view.  
A: /

**VIEW**

**File Name Search**

Enter a Perl regular expression for the file names you want to find.

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

Current Directory: [A: /](#)

**ADD NOTE** **GENERATE MDS LIST OF FILES**

DEL	Type <a href="#">dir / in</a>	NAME <input type="text"/>	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	<a href="#">\$FAT1</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<a href="#">45780</a>
	v / v	<a href="#">\$FAT2</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<a href="#">45781</a>
	v / v	<a href="#">\$MBR</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	<a href="#">45779</a>
	d / d	<a href="#">\$OrphanFiles/</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">45782</a>
	r / r	<a href="#">cover_page.jpvc</a>	2002-09-11 08:30:52 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:50:27 (PET)	15585	0	0	<a href="#">8</a>
<input checked="" type="checkbox"/>	r / r	<a href="#">Jimmy Jungle.doc</a>	2002-04-15 14:42:30 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:49:49 (PET)	20480	0	0	<a href="#">5</a>
	r / r	<a href="#">Scheduled Visits.exe</a>	2002-05-24 08:20:32 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:50:38 (PET)	1000	0	0	<a href="#">11</a>

**File Browsing Mode**

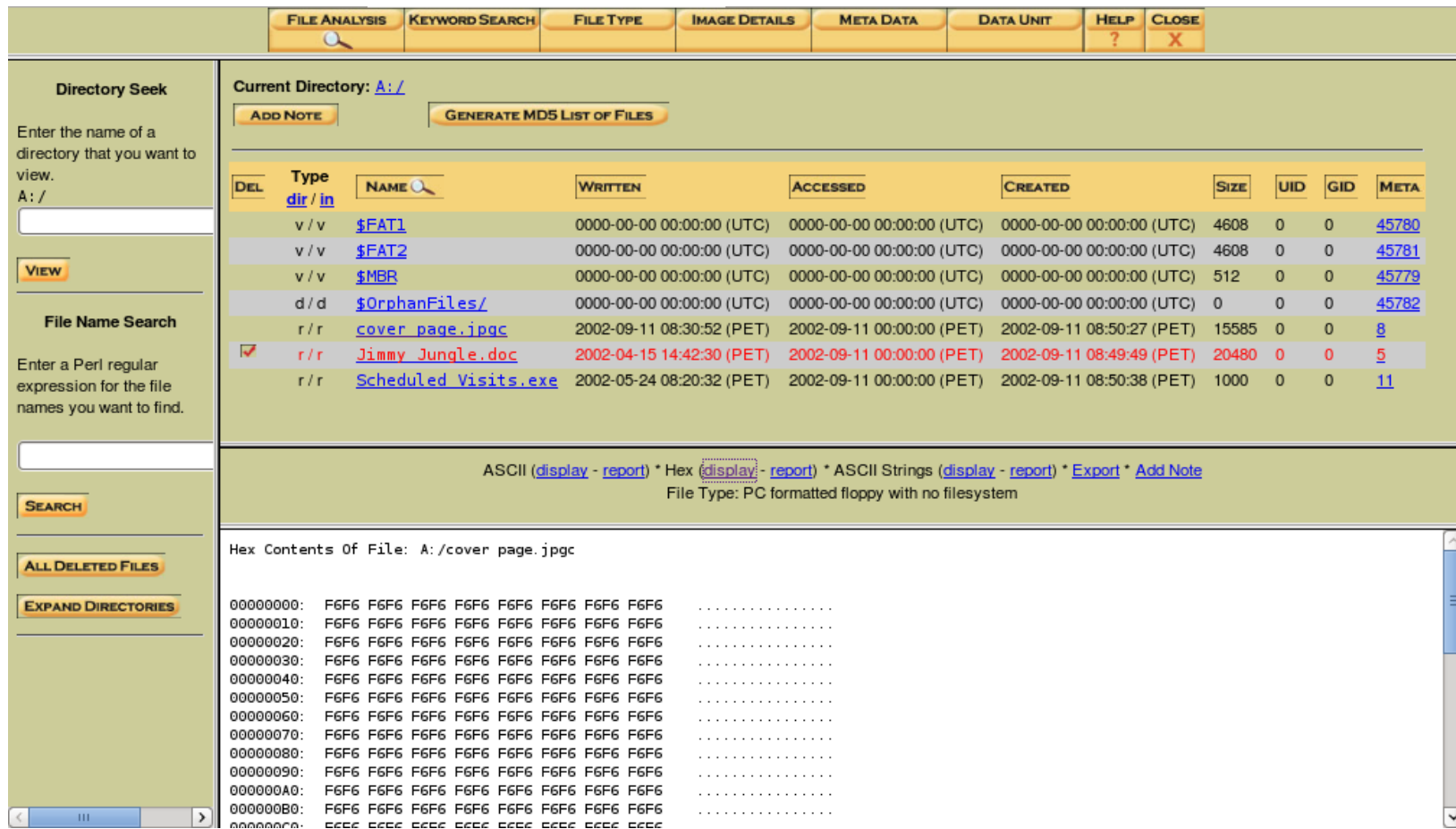
In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).  
You can also sort the files using the column headers

# Archivo cover page.jpgc (I)

Autopsy no ha reconocido este archivo como JPEG. (FF D8)



The screenshot shows the Autopsy interface with the following components:

- Navigation Bar:** FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE.
- Directory Seek:** Current Directory: A:/. Includes buttons for ADD NOTE and GENERATE MD5 LIST OF FILES.
- File List Table:**

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v/v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<a href="#">45780</a>
	v/v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<a href="#">45781</a>
	v/v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	<a href="#">45779</a>
	d/d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">45782</a>
	r/r	<a href="#">cover page.jpgc</a>	2002-09-11 08:30:52 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:50:27 (PET)	15585	0	0	<a href="#">8</a>
<input checked="" type="checkbox"/>	r/r	<a href="#">Jimmy Jungle.doc</a>	2002-04-15 14:42:30 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:49:49 (PET)	20480	0	0	<a href="#">5</a>
	r/r	<a href="#">Scheduled Visits.exe</a>	2002-05-24 08:20:32 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:50:38 (PET)	1000	0	0	<a href="#">11</a>
- File Type:** PC formatted floppy with no filesystem.
- Hex Contents:** Hex Contents Of File: A:/cover page.jpgc. The hex dump shows a repeating pattern of F6F6 hex values.

## Archivo cover page.jpgc (II)

Visualizando MetaDatos

Se reporta un tamaño del archivo de 15585 bytes, pero solo se asigna un sector (451) de 512 bytes. Lo cual no es “consistente”.

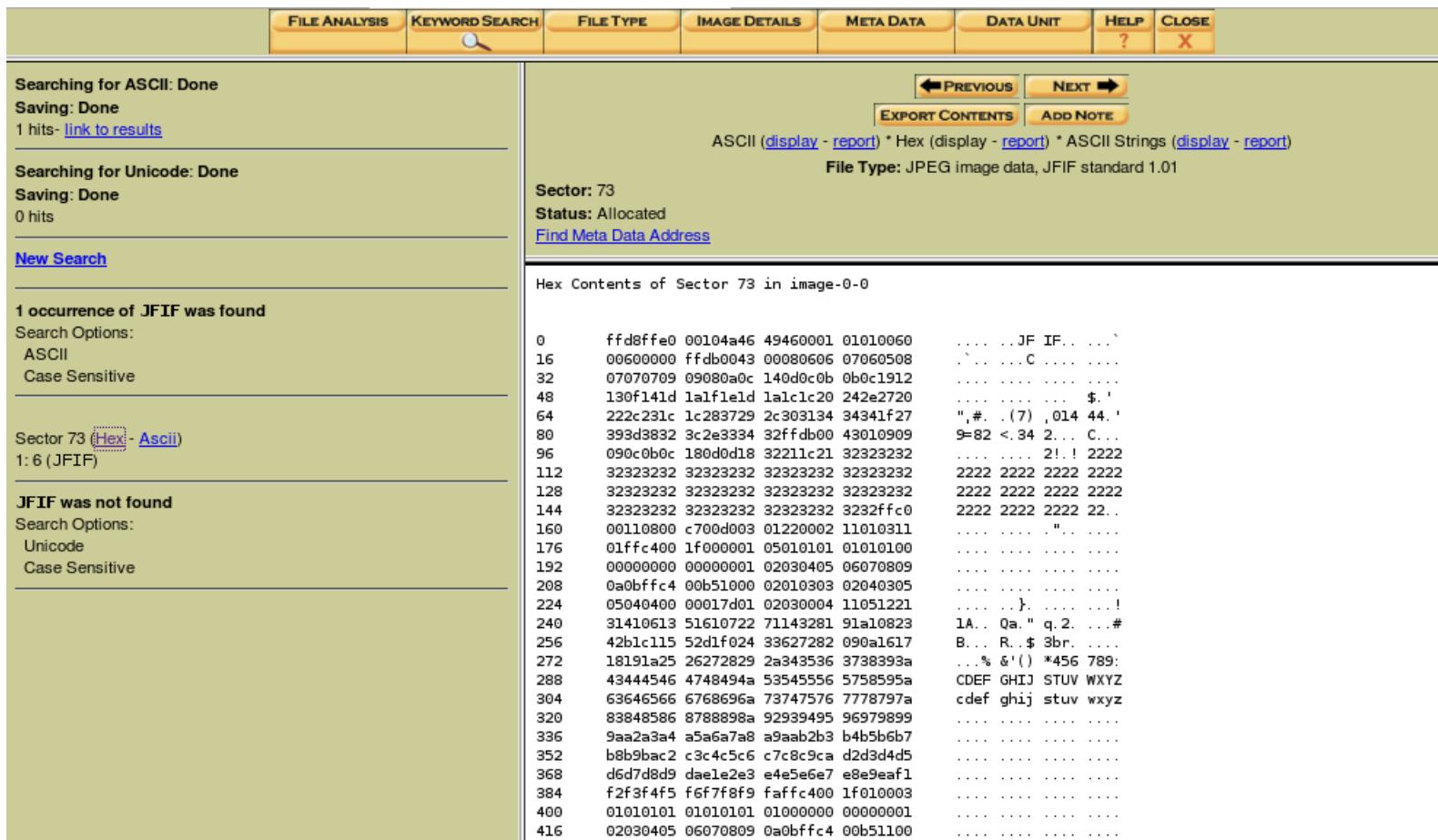


The screenshot shows the Autopsy interface with the following details:

- Navigation:** FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA (selected), DATA UNIT, HELP, CLOSE.
- Dir Entry Number:** 8
- Buttons:** VIEW, ALLOCATION LIST, PREVIOUS, NEXT, REPORT, VIEW CONTENTS, EXPORT CONTENTS, ADD NOTE.
- File Type:** PC formatted floppy with no filesystem
- MD5 of content:** f49ed788acc2753e5a1736808dccc138 -
- SHA-1 of content:** dcc13088a8389d974bc544ac32d6fccb4c904fba -
- Details:**
  - Directory Entry: 8
  - Allocated
  - File Attributes: File, Archive
  - Size: 15585
  - Name: COVERP~1.JPG
- Directory Entry Times:**
  - Written: Wed Sep 11 08:30:52 2002
  - Accessed: Wed Sep 11 00:00:00 2002
  - Created: Wed Sep 11 08:50:27 2002
- Sectors:** [451](#)

## Archivo cover page.jpgc (III)

Se procede a realizar una búsqueda de la firma JPEG (JFIF). Se encuentra una coincidencia en el sector 73.

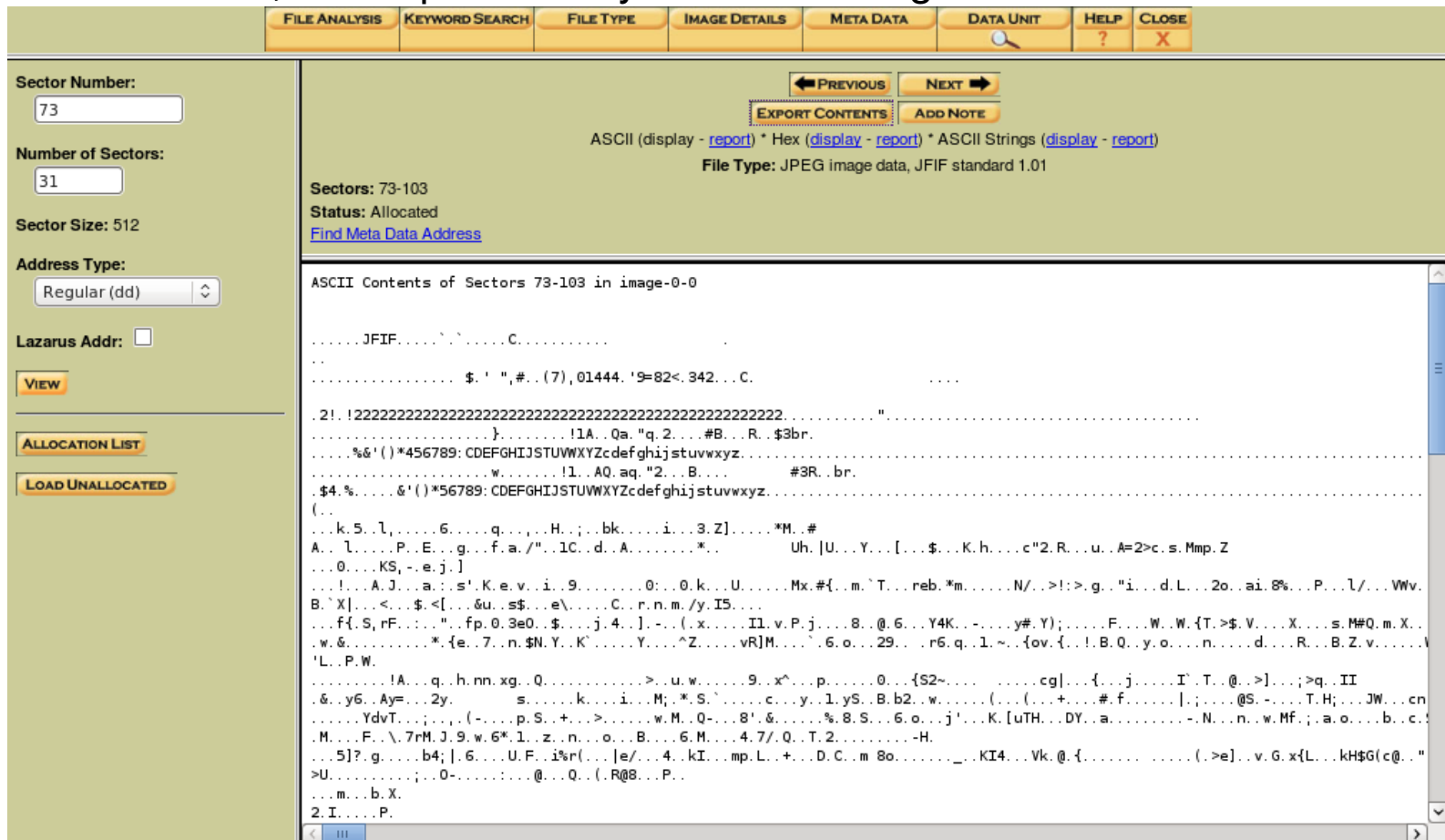


The screenshot shows the Autopsy interface with the 'KEYWORD SEARCH' tab selected. The search results on the left indicate that 1 occurrence of JFIF was found in Sector 73. The main pane displays the hex contents of Sector 73, with the JFIF signature 'ffd8ffe0 00104a46 49460001 01010060' visible at offset 0.

Offset	Hex	ASCII
0	ffd8ffe0 00104a46 49460001 01010060	... JF IF ...
16	00600000 ffdb0043 00080606 07060508	... C ...
32	07070709 09080a0c 140d0c0b 0b0c1912	... ..
48	130f141d 1a1f1e1d 1a1c1c20 242e2720	... \$..
64	222c231c 1c283729 2c303134 34341f27	.., #. (7) , 014 44. '
80	393d3832 3c2e3334 32ffdb00 43010909	9=82 <. 34 2... C...
96	090c0b0c 180d0d18 32211c21 32323232	... .. 2!.. 2222
112	32323232 32323232 32323232 32323232	2222 2222 2222 2222
128	32323232 32323232 32323232 32323232	2222 2222 2222 2222
144	32323232 32323232 32323232 3232ffc0	2222 2222 2222 22..
160	00110800 c700d003 01220002 11010311	... .. ". ..
176	01ffc400 1f000001 05010101 01010100	... ..
192	00000000 00000001 02030405 06070809	... ..
208	0a0bffc4 00b51000 02010303 02040305	... ..
224	05040400 00017d01 02030004 11051221	... .. }.. ..!
240	31410613 51610722 71143281 91a10823	1A.. 0a." q. 2. ...#
256	42b1c115 52d1f024 33627282 090a1617	B... R.. \$ 3br. ....
272	18191a25 26272829 2a343536 3738393a	...% &'()* *456 789:
288	43444546 4748494a 53545556 5758595a	CDEF GHIJ STUV WXYZ
304	63646566 6768696a 73747576 7778797a	cdef ghij stuv wxyz
320	83848586 8788898a 92939495 96979899	... ..
336	9aa2a3a4 a5a6a7a8 a9aab2b3 b4b5b6b7	... ..
352	b8b9bac2 c3c4c5c6 c7c8c9ca d2d3d4d5	... ..
368	d6d7d8d9 dae1e2e3 e4e5e6e7 e8e9eaf1	... ..
384	f2f3f4f5 f6f7f8f9 faffc400 1f010003	... ..
400	01010101 01010101 01000000 00000001	... ..
416	02030405 06070809 0a0bffc4 00b51100	... ..

## Archivo cover page.jpgc (IV)

Se necesitan 31 sectores para almacenar 15585 bytes. Pero están asignados (36 sectores) del 73 hasta el 108 . Pero solo 31 están asociados con el archivo; como se verifica más adelante; dado que la 104 y 105 están asignados a otro archivo.



The screenshot shows the 'FILE ANALYSIS' tab in The Sleuth Kit. The interface includes a sidebar on the left with input fields for 'Sector Number' (73), 'Number of Sectors' (31), 'Sector Size' (512), and 'Address Type' (Regular (dd)). The main area displays file details: 'File Type: JPEG image data, JFIF standard 1.01' and 'Status: Allocated'. Below this, the 'ASCII Contents of Sectors 73-103 in image-0-0' are shown as a hex dump. The hex dump contains JFIF header information and a large block of binary data represented by a long string of '2!' characters. Navigation buttons like 'PREVIOUS', 'NEXT', 'EXPORT CONTENTS', and 'ADD NOTE' are visible at the top of the main area.

## Archivo cover page.jpgc (V)

Exportamos el contenido con la opción “Export Contents” (vol1-Sector73.jpeg) Y obtenemos la siguiente imagen:



Rango de sectores	Estado de asignación
0-32	Asignado
33-72	Sin Asignar
73-108	Asignado
109-	Sin Asignar

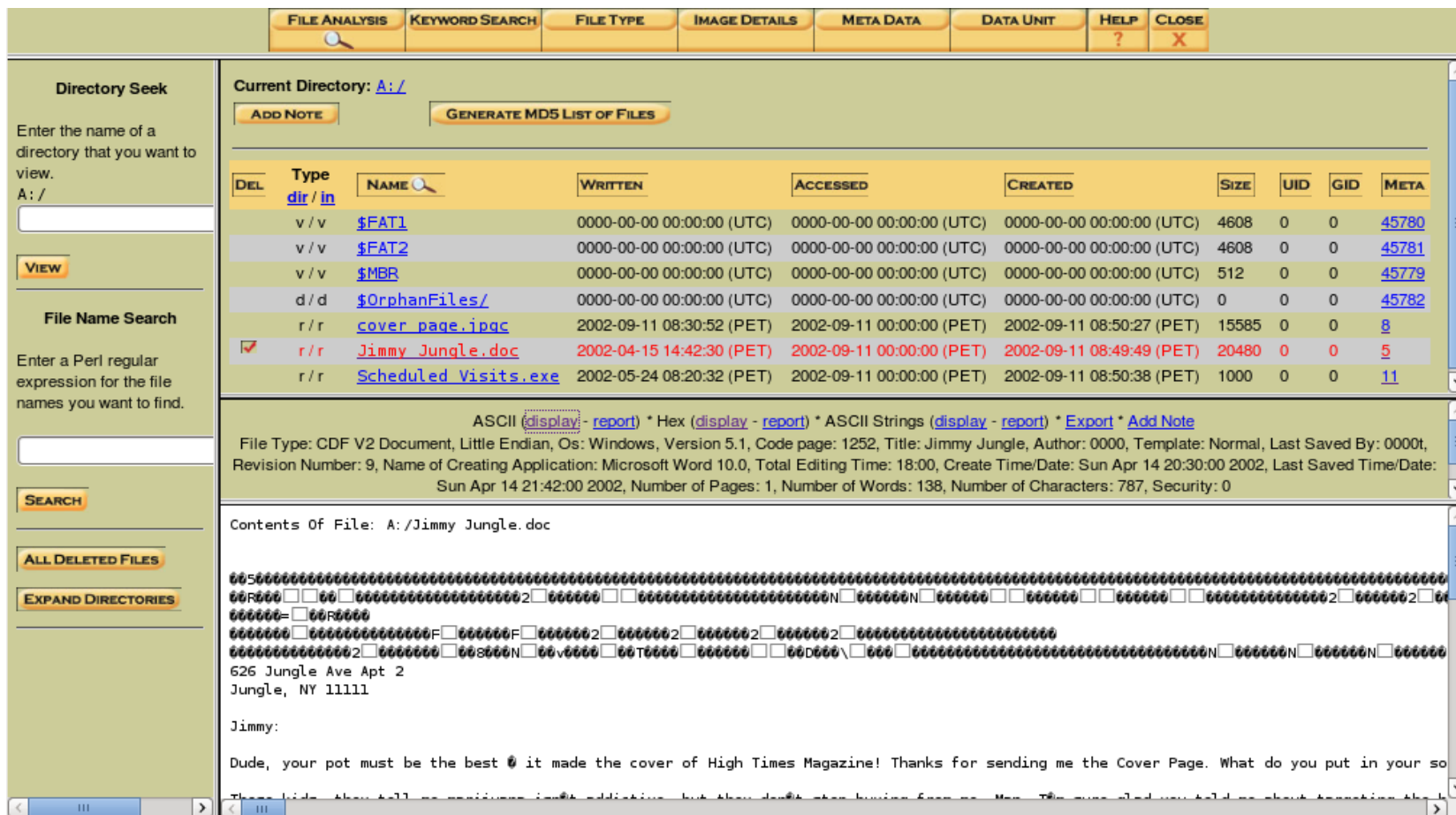
También es factible extraer la información con el siguiente comando:

```
# dd skip=73 bs=512 count=31 if=/media/hda3/image.dd of=/media/hda3/coverpage.jpg
```

Es muy importante tener en consideración que cuando se extraen los 36 sectores y se visualiza lo extraído con un editor hexadecimal se puede ver el texto ‘pw=goodtimes’ en el desplazamiento 0x3d20. Esta contraseña se utilizará más adelante para abrir otro archivo. Y el último sector la cadena de texto 'Scheduled Visits.xls'.

# Archivo Jimmy Jungle.doc (I)

Autopsy lo reconoce como un archivo Doc, M\$.



The screenshot shows the Autopsy interface with the following components:

- Navigation Bar:** FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE.
- Directory Seek:** Current Directory: A:/. Includes buttons for ADD NOTE and GENERATE MD5 LIST OF FILES.
- File List Table:**

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v/v	<a href="#">\$FAT1</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<a href="#">45780</a>
	v/v	<a href="#">\$FAT2</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<a href="#">45781</a>
	v/v	<a href="#">\$MBR</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	<a href="#">45779</a>
	d/d	<a href="#">\$OrphanFiles/</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">45782</a>
	r/r	<a href="#">cover_page.ipgc</a>	2002-09-11 08:30:52 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:50:27 (PET)	15585	0	0	<a href="#">8</a>
<input checked="" type="checkbox"/>	r/r	<a href="#">Jimmy Jungle.doc</a>	2002-04-15 14:42:30 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:49:49 (PET)	20480	0	0	<a href="#">5</a>
	r/r	<a href="#">Scheduled Visits.exe</a>	2002-05-24 08:20:32 (PET)	2002-09-11 00:00:00 (PET)	2002-09-11 08:50:38 (PET)	1000	0	0	<a href="#">11</a>
- File Metadata:** File Type: CDF V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Jimmy Jungle, Author: 0000, Template: Normal, Last Saved By: 0000t, Revision Number: 9, Name of Creating Application: Microsoft Word 10.0, Total Editing Time: 18:00, Create Time/Date: Sun Apr 14 20:30:00 2002, Last Saved Time/Date: Sun Apr 14 21:42:00 2002, Number of Pages: 1, Number of Words: 138, Number of Characters: 787, Security: 0.
- Contents of File:** A:/Jimmy Jungle.doc
 

```

626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

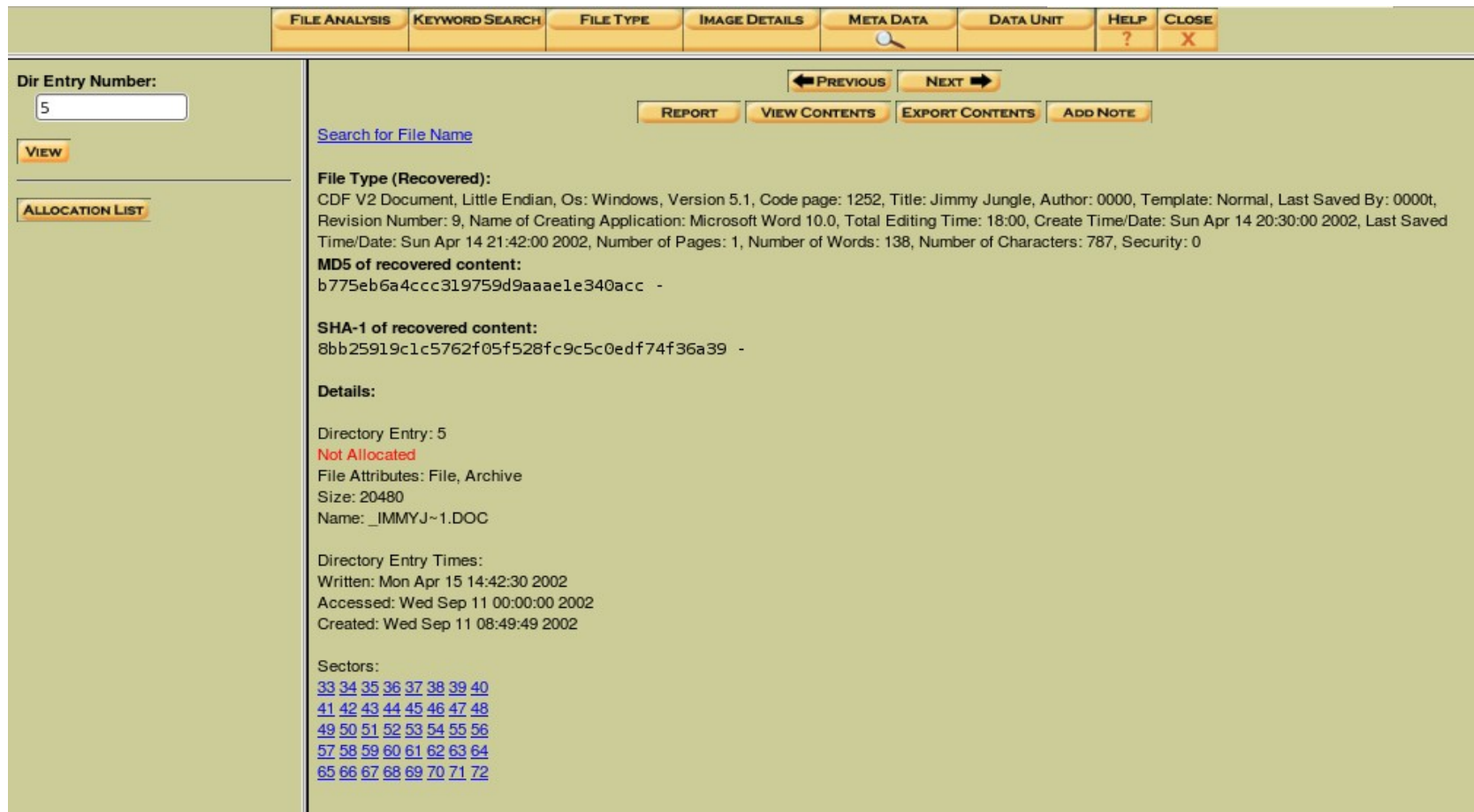
Dude, your pot must be the best @ it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your so

```

## Archivo Jimmy Jungle.doc (II)

Se procede a visualizar los metadatos.

El archivo tiene un tamaño de 20480 por lo tanto son necesarios 40 sectores.

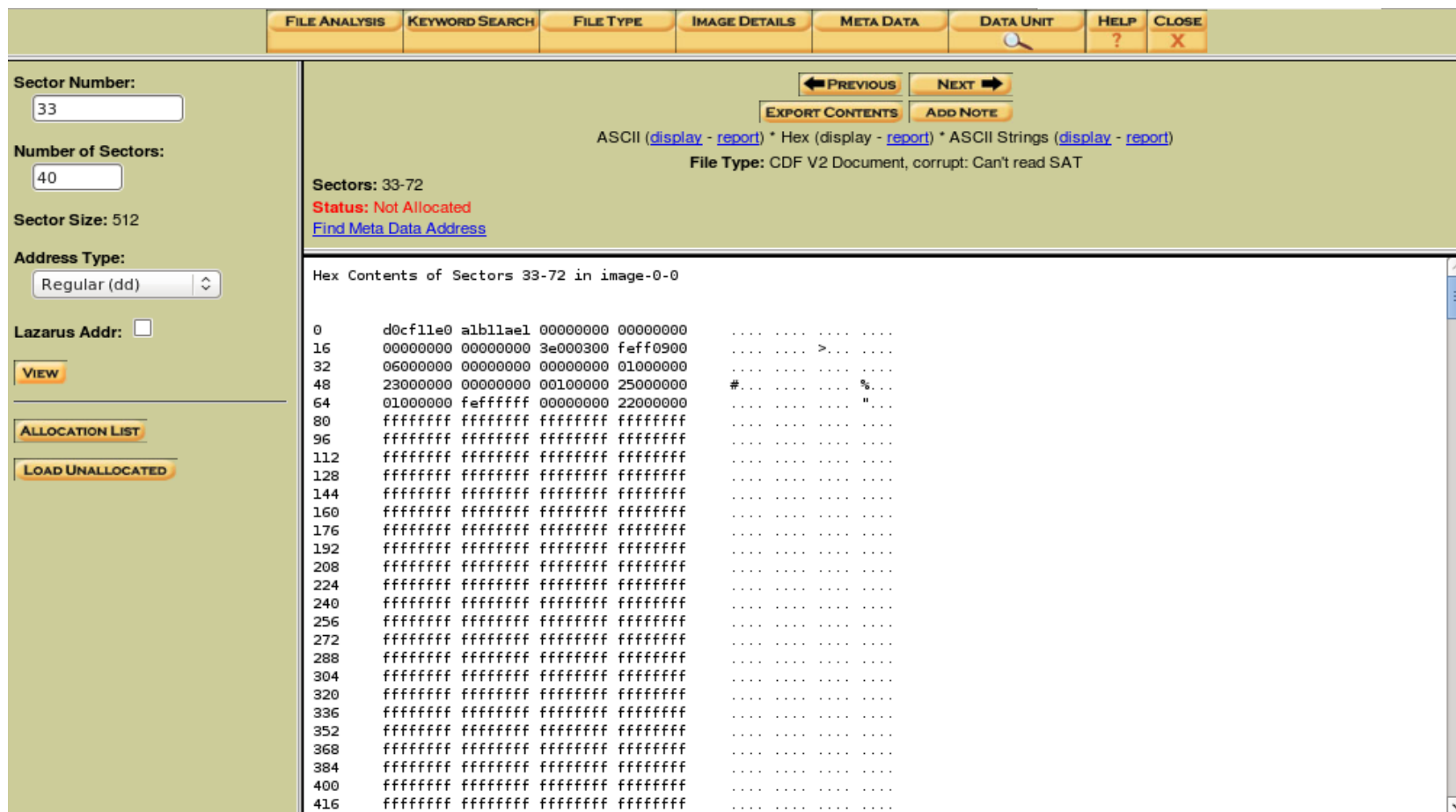


The screenshot displays the Autopsy forensic tool interface. At the top, there is a navigation bar with tabs for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. Below this, the main window is divided into two panes. The left pane shows the 'Dir Entry Number' set to 5, with a 'VIEW' button and an 'ALLOCATION LIST' button. The right pane displays the file's metadata, including the file type (Recovered), file type details (CDF V2 Document), MD5 and SHA-1 hashes of the recovered content, and directory entry details (Directory Entry: 5, Not Allocated, File Attributes: File, Archive, Size: 20480, Name: \_IMMYJ~1.DOC). At the bottom, it lists the directory entry times (Written, Accessed, Created) and a list of sectors (33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72).

## Archivo Jimmy Jungle.doc (III)

Extraemos el archivo también con:

```
# dd skip=33 bs=512 count=40 if=/media/hda3/image of=/media/hda3/jimmyjungle.doc
```



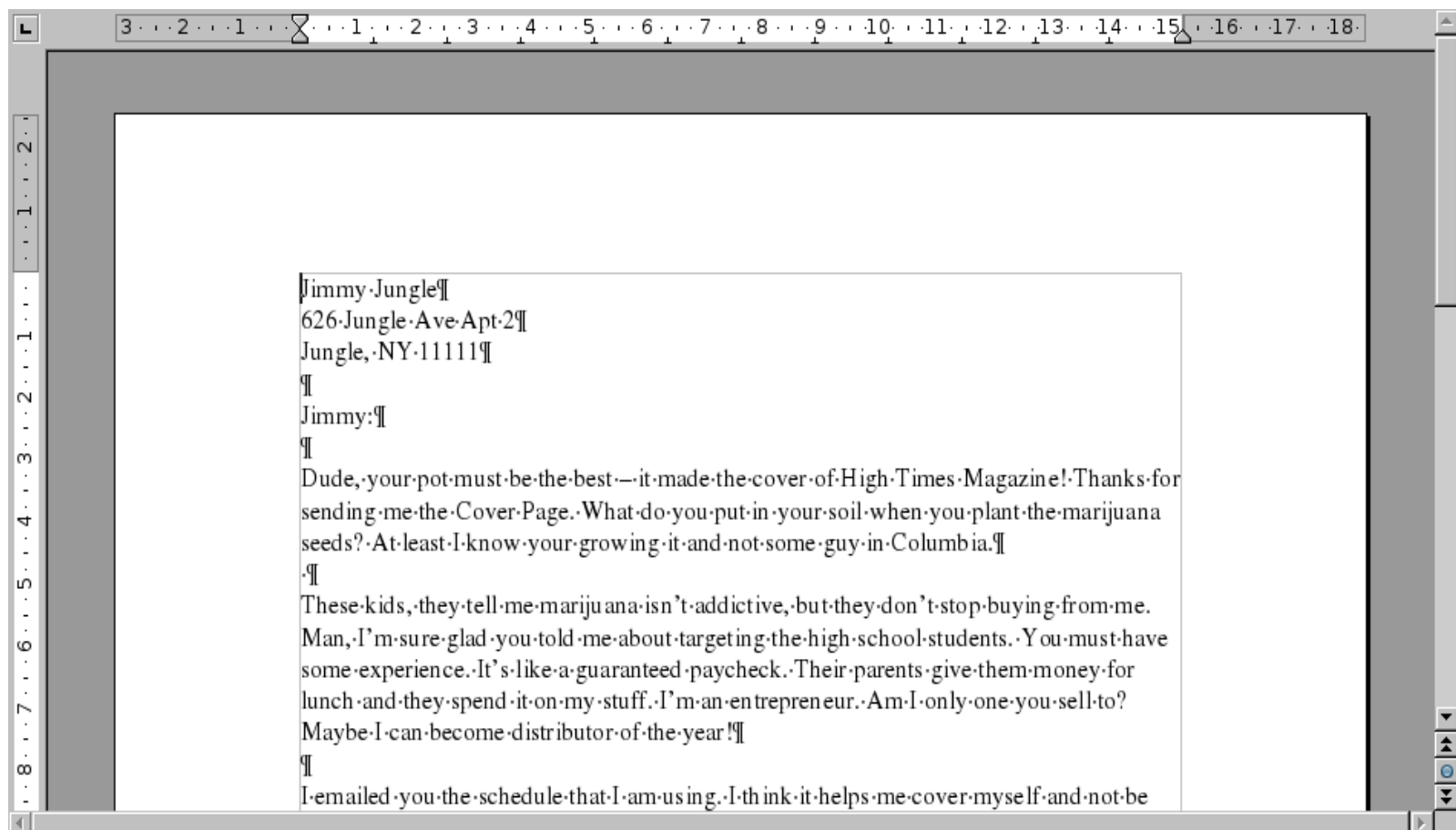
The screenshot shows the Autopsy interface with the following details:

- Navigation:** FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE.
- Navigation Buttons:** PREVIOUS, NEXT, EXPORT CONTENTS, ADD NOTE.
- File Information:** ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report). File Type: CDF V2 Document, corrupt: Can't read SAT.
- Analysis Parameters:** Sector Number: 33, Number of Sectors: 40, Sector Size: 512, Address Type: Regular (dd).
- Analysis Results:** Sectors: 33-72, Status: Not Allocated, Find Meta Data Address.
- Hex Contents:** Hex Contents of Sectors 33-72 in image-0-0. The hex dump shows a sequence of sectors, with most containing 'f' characters, indicating unallocated space.

Offset	Hex	ASCII
0	d0cf11e0 a1b11ae1 00000000 00000000	.....
16	00000000 00000000 3e000300 feff0900	..... >.....
32	06000000 00000000 00000000 01000000	.....
48	23000000 00000000 00100000 25000000	#..... %...
64	01000000 feffffff 00000000 22000000	..... "
80	ffffffff ffffffff ffffffff ffffffff	.....
96	ffffffff ffffffff ffffffff ffffffff	.....
112	ffffffff ffffffff ffffffff ffffffff	.....
128	ffffffff ffffffff ffffffff ffffffff	.....
144	ffffffff ffffffff ffffffff ffffffff	.....
160	ffffffff ffffffff ffffffff ffffffff	.....
176	ffffffff ffffffff ffffffff ffffffff	.....
192	ffffffff ffffffff ffffffff ffffffff	.....
208	ffffffff ffffffff ffffffff ffffffff	.....
224	ffffffff ffffffff ffffffff ffffffff	.....
240	ffffffff ffffffff ffffffff ffffffff	.....
256	ffffffff ffffffff ffffffff ffffffff	.....
272	ffffffff ffffffff ffffffff ffffffff	.....
288	ffffffff ffffffff ffffffff ffffffff	.....
304	ffffffff ffffffff ffffffff ffffffff	.....
320	ffffffff ffffffff ffffffff ffffffff	.....
336	ffffffff ffffffff ffffffff ffffffff	.....
352	ffffffff ffffffff ffffffff ffffffff	.....
368	ffffffff ffffffff ffffffff ffffffff	.....
384	ffffffff ffffffff ffffffff ffffffff	.....
400	ffffffff ffffffff ffffffff ffffffff	.....
416	ffffffff ffffffff ffffffff ffffffff	.....

## Archivo Jimmy Jungle.doc (IV)

Visualizando el archivo. El archivo aparentemente fue creado el 16/04/2002 a las 08:30:00, modificado el 16/04/2002 a las 09:42:00. Obtenido de los metadatos del formato de archivo DOC.





## Archivo Scheduled Visits.exe (II)

Visualizando los metadatos del archivo. El tamaño del archivo es de 1000 y requiere por lo tanto dos sectores asignados, el 104 y 105.



The screenshot displays the Autopsy file analysis interface. At the top, there is a navigation bar with tabs for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. Below this, a sidebar on the left contains a 'Dir Entry Number' field with the value '11', a 'VIEW' button, and an 'ALLOCATION LIST' button. The main pane shows file details for 'Scheduled Visits.exe' (entry 11). The 'File Type' is 'empty (Zip archive data, at least v2.0 to extract)'. The 'MD5 of content' is '082a5cc64deea22a3a580fbb5a6fa66 -'. The 'SHA-1 of content' is 'c8e7f25380d63c9034d9f27faab29de1f09240b5 -'. The 'Details' section lists: Directory Entry: 11, Allocated, File Attributes: File, Archive, Size: 1000, Name: SCHEDU~1.EXE. The 'Directory Entry Times' section lists: Written: Fri May 24 08:20:32 2002, Accessed: Wed Sep 11 00:00:00 2002, Created: Wed Sep 11 08:50:38 2002. The 'Sectors' section lists: 104 105. Navigation buttons include PREVIOUS, NEXT, REPORT, VIEW CONTENTS, EXPORT CONTENTS, and ADD NOTE.

## Archivo Scheduled Visits.exe (III)

Al extraer el archivo por el procedimiento ya descrito se muestra un mensaje de error de que indica que el archivo no está completo.

Se debe recordar que están asignado los sectores desde el 73 hasta el 108. También se descubrió que cuando inicialmente se extraen los datos de la imagen JPG desde el sector 73 hasta el 108 se encuentra en el último sector el texto “Scheduled Visits.xls”.

```

00004620 d7 79 ea e8 b5 9b 50 60 22 ff bb 32 fc aa f1 6e |.y....P`"...2...n|
00004630 63 15 b2 1e 98 92 96 e5 26 8a 7b 5f d5 cf 38 46 |c.....&{_.8F|
00004640 e7 90 cb 5d f7 5d 5b e2 c5 17 d2 c7 a7 50 fa 30 |...]}[.....P.0|
00004650 96 df 42 78 a9 a1 8e 97 db db e7 d2 87 f0 b7 10 |..Bx.....|
00004660 ff cd eb 18 42 75 ab 99 30 3f 95 ae c9 95 0b c4 |...Bu..0?.....|
00004670 ef f5 23 db fc d9 29 48 9b ae 85 5c 96 c4 e0 d8 |..#...)H...\...|
00004680 9e 89 e9 29 d7 19 7c bf 17 ad fd ea 71 0b fd 71 |...)|....q..q|
00004690 5b 04 c4 57 ab b3 6f 62 39 e1 a4 aa 79 05 9c 67 |[..W..ob9...y..g|
000046a0 23 36 55 96 c4 70 e6 27 f7 3d 2d 73 f7 d3 28 6a |#6U..p.'.-s..(j|
000046b0 75 df 87 1a 49 b3 07 42 f8 c3 3f ad 78 26 6e ff |u...I..B..?.x&n.|
000046c0 7f 0e 83 64 04 a0 c4 b6 7e 9e 1e 08 88 26 d7 8f |...d....~....&..|
000046d0 99 86 48 40 40 09 2b 55 1d df b2 94 9b 8c ff 0a |..H@+.U.....|
000046e0 3c 14 7e 45 fb fe 0f 55 49 f0 a4 d0 40 9e b0 ce |<..~E...UI...@...|
000046f0 69 3b 28 dd cc 14 47 35 00 ae cf 62 fc 09 83 da |i;(...G5...b....|
00004700 c6 c5 95 4e 28 c9 7d e7 48 d3 2d 1e b3 0f d7 dc |...N(.).H.-....|
00004710 9c 23 e6 76 51 aa ec 21 dd 21 06 71 50 4b 01 02 |.#.vQ...!.!.qPK..|
00004720 14 00 14 00 01 00 08 00 98 5a b7 2c c7 55 60 8d |.....Z...U`..|
00004730 ea 08 00 00 00 42 00 00 14 00 00 00 00 00 00 |.....B.....|
00004740 00 00 20 00 b6 81 00 00 00 00 53 63 68 65 64 75 |... ..Schedu|
00004750 6c 65 64 20 56 69 73 69 74 73 2e 78 6c 73 50 4b |led Visits.xlsPK|
00004760 05 06 00 00 00 00 01 00 01 00 42 00 00 00 1c 09 |.....B.....|
00004770 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00004800

```

## Archivo Scheduled Visits.exe (IV)

Con esta evidencia entonces resultaría útil extraer los datos desde el sector 104 al 108 y ejecutar la herramienta unzip.

```
# dd skip=104 bs=512 count=5 if=/media/hda3/image of=/media/hda3/scheduledvisits.exe
```

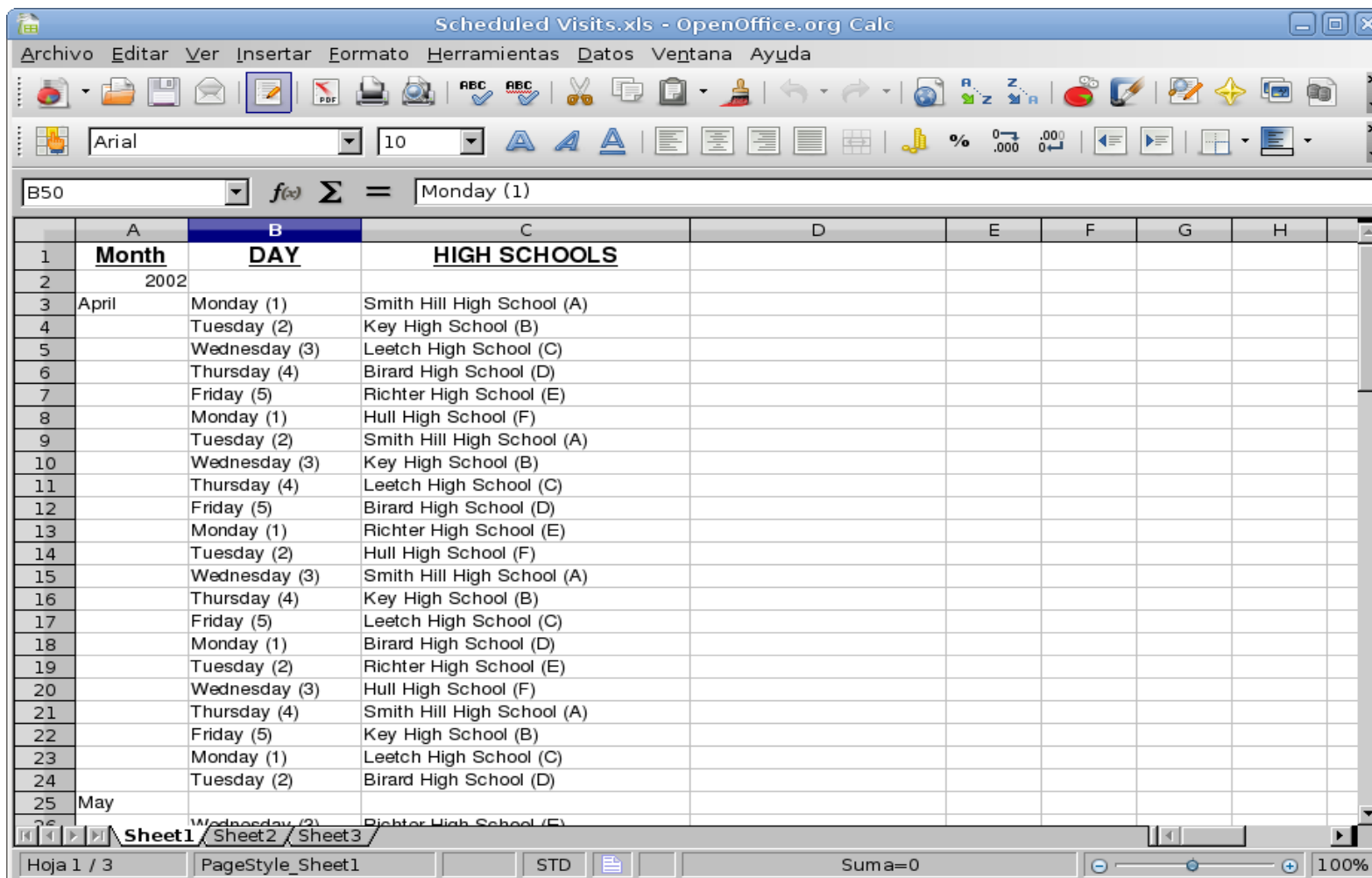
Al intentar extraer el archivo se pregunta por la contraseña. Se utiliza entonces la contraseña obtenida de el espacio de holgura del archivo JPG 'pw=goodtimes'.

```
000027d0 1c 2b c3 1d cc f7 49 2b 5e 4c c7 32 17 38 10 64 |+. . . . I+^L.2.8.d|
000027e0 46 84 79 84 6e c9 c8 07 80 5b 2b d0 c4 64 30 a1 |F.y.n. . . . [+..d0.|
000027f0 99 15 25 2a 37 aa 36 e5 07 b8 04 81 91 ef 81 f4 |. . %*7.6. . . . .|
00002800 ad 20 db dd 1c 38 88 53 83 4a 9c ae bf 5f eb e6 |. . . . 8.S.J. . . .|
00002810 b6 63 e8 a2 8a b3 9c 28 a2 8a 00 28 a2 8a 00 28 |.c. . . . (. . . (. . .|
00002820 a2 8a 00 28 a2 8a 00 28 a2 8a 00 28 a2 8a 00 28 |. . . (. . . (. . . (. . .|
*
00003cd0 a2 8a 00 28 a2 8a 00 28 a2 8a 00 28 a2 8a 00 ff |. . . (. . . (. . . (. . .|
00003ce0 d9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. . . . . . . . . . . .|
00003cf0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. . . . . . . . . . . .|
*
00003d20 70 77 3d 67 6f 6f 64 74 69 6d 65 73 00 00 00 00 |pw=goodtimes. . . .|
00003d30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. . . . . . . . . . . .|
*
00003e00 50 4b 03 04 14 00 01 00 08 00 98 5a b7 2c c7 55 |PK. . . . . . . . Z. . . U|
00003e10 60 8d ea 08 00 00 00 42 00 00 14 00 00 00 53 63 |^ . . . . . . B. . . . . Sc|
00003e20 68 65 64 75 6c 65 64 20 56 69 73 69 74 73 2e 78 |heduled Visits.x|
00003e30 6c 73 94 c8 31 2a e3 49 0b db a8 10 c2 70 9d fc |ls. . 1*.I. . . . p. .|
00003e40 10 03 31 a2 8e 48 e8 3c 4b 81 75 c9 8b 86 51 af |.l. . H.<K.u. . . . Q.|
00003e50 df 2a 36 c3 24 db 1a 7e 75 46 98 ee 4e 56 4f 05 |. *6.$ . . ~uF. . NVO. |
00003e60 ba 8d c4 60 36 54 0e 11 ab 2e 23 a5 e8 16 02 52 |. . . `6T. . . . #. . . . R|
00003e70 e2 1f ef 90 a3 f5 23 2d 34 10 02 48 54 c1 62 cb |. . . . . # -4. . HT.b. |
00003e80 5e f1 3f 91 52 72 e3 dc 66 0a 4a 20 d3 e2 02 cf |^ . ? . Rr. . . f. J . . .|
00003e90 78 9a 35 6b 55 4d b7 98 fb 88 61 5f 83 99 05 53 |x.5kUM. . . . a . . . S|
```

```
root@reydes:/tmp# unzip voll-Sector104.exe
Archive: voll-Sector104.exe
[voll-Sector104.exe] Scheduled Visits.xls password:
password incorrect--reenter:
  inflating: Scheduled Visits.xls
root@reydes:/tmp#
```

## Archivo Scheduled Visits.exe (V)

El archivo contiene una lista de fechas y nombres de colegios.



	A	B	C	D	E	F	G	H
1	<b>Month</b>	<b>DAY</b>	<b>HIGH SCHOOLS</b>					
2		2002						
3	April	Monday (1)	Smith Hill High School (A)					
4		Tuesday (2)	Key High School (B)					
5		Wednesday (3)	Leetch High School (C)					
6		Thursday (4)	Birard High School (D)					
7		Friday (5)	Richter High School (E)					
8		Monday (1)	Hull High School (F)					
9		Tuesday (2)	Smith Hill High School (A)					
10		Wednesday (3)	Key High School (B)					
11		Thursday (4)	Leetch High School (C)					
12		Friday (5)	Birard High School (D)					
13		Monday (1)	Richter High School (E)					
14		Tuesday (2)	Hull High School (F)					
15		Wednesday (3)	Smith Hill High School (A)					
16		Thursday (4)	Key High School (B)					
17		Friday (5)	Leetch High School (C)					
18		Monday (1)	Birard High School (D)					
19		Tuesday (2)	Richter High School (E)					
20		Wednesday (3)	Hull High School (F)					
21		Thursday (4)	Smith Hill High School (A)					
22		Friday (5)	Key High School (B)					
23		Monday (1)	Leetch High School (C)					
24		Tuesday (2)	Birard High School (D)					
25	May							
26		Wednesday (3)	Richter High School (E)					

## Respuestas:

Respuesta a un par de preguntas:

**¿Quién es el proveedor de marihuana de Joe Jacobs y cual es la dirección listada del proveedor?**

Como lo indica el documento 'Jimmy Jungle.doc' recuperado el proveedor de Joe Jacob es:

Jimmy Jungle

626 Jungle Ave, Apt 2, Jungle, NY 11111

**¿Qué dato crucial está disponible dentro de coverpage.jpg y porque el dato es crucial?**

La cadena 'pw=gootimes' que se encontró en el espacio de holgura al final de la unidades de asignación del archivo. Este dato es crucial porque es la contraseña del archivo protegido "Scheduled Visits.exe".

## ¿Preguntas, comentarios, sugerencias?

Los invito cordialmente a dos cursos a dictarse en la ciudad de Trujillo:

### **Cómputo Forense**

Sábado 29 & Domingo 30  
de **MAYO** del 2010

### **Hacking Ético (2do Grupo)**

Sábado 7 & Domingo 8  
de **AGOSTO** del 2010

Más información:

<http://www.npros.com.pe>



# ¡Muchas Gracias!

**Alonso Eduardo Caballero Quezada**  
Consultor de NPROS Perú SAC  
Consultor de iDev Consultores en TI SAC  
GIAC – SSP CNSA  
Brainbench Computer Forensics (U.S.)

Página web: <http://www.ReYDeS.com>  
Correo electrónico: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)  
Trujillo, Perú - 24 de Abril del 2010

---