

Laboratorio “Caso de Estudio Forense”.

Formar dos grupos de trabajo y desarrollar y documentar en el repositorio del curso el siguiente caso práctico haciendo uso de autopsy.
Para ello apoyarse y complementar la siguiente guía.

Nota: El repositorio <https://github.com/SVelizDonoso/forense-autopsy?tab=readme-ov-file> desarrolla el caso en cuestión, en virtud de lo cual puede ser empleado como complemento y guía de diseño del repositorio.

OBJETIVOS

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** <https://github.com/SVelizDonoso/forense-autopsy/blob/master/image.zip>

Hash MD5 del Archivo: **b676147f63923e1f428131d59b1d6a72**

Preguntas:

¿Quién es el proveedor de marihuana de Joe Jacobs y cuál 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 frecuentan?

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?

Primeros pasos para utilizar la herramienta Autopsy vía Web

1. Descargar imagen.zip
2. Verifica el hash con md5sum image.zip
3. Descomprime el achivo unzip image.zip
4. El archivo resultante es image

```
root@ubuntu:/home/usuario/Escritorio# md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
root@ubuntu:/home/usuario/Escritorio# unzip image.zip
Archive: image.zip
  inflating: image
```

Instala apt-get install sleuthkit autopsy

Para acceder: autopsy

```
root@ubuntu:/home/usuario/Escritorio# autopsy

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

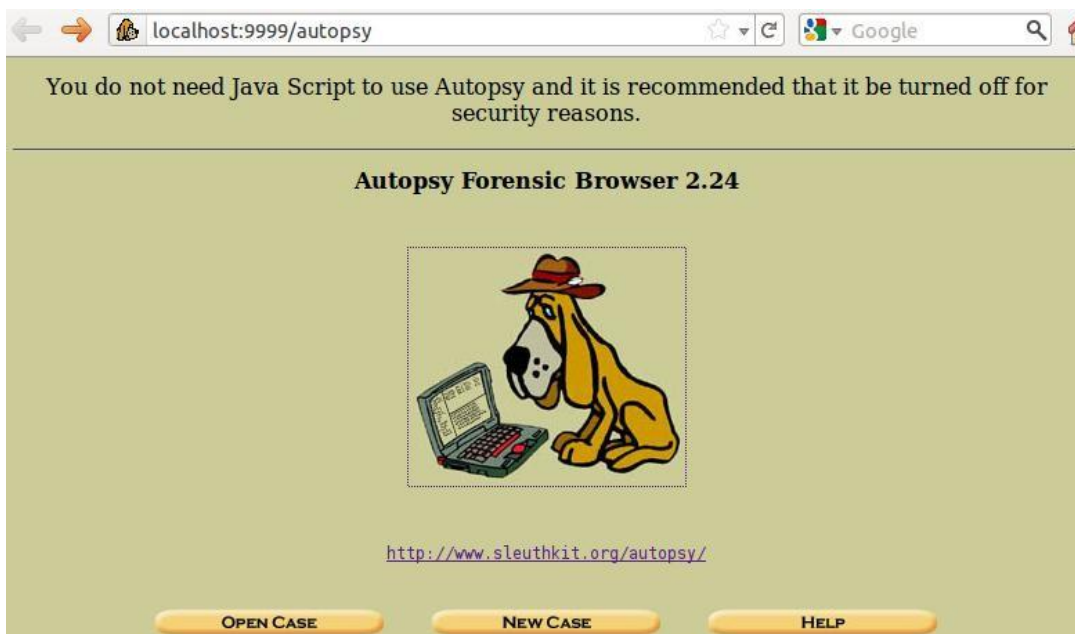
Evidence Locker: /var/lib/autopsy
Start Time: Thu Oct 27 13:51:40 2011
Remote Host: localhost
Local Port: 9999

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
```

Haz clic en el http para iniciar autopsy.



Crear Caso

Crearemos el caso marcando 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.

b.

c.

d.

e.

f.

g.

h.

i.

j.

NEW CASE

CANCEL

HELP

Haremos clic en New Case para ver el resultado.

Creating Case: Drogas

Case directory (/var/lib/autopsy/Drogas/) created

Configuration file (/var/lib/autopsy/Drogas/case.aut) created

We must now create a host for this case.

ADD HOST

Crear host

Creamos el nuevo hosts.

Case: Drogas

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **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.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the

3. **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.

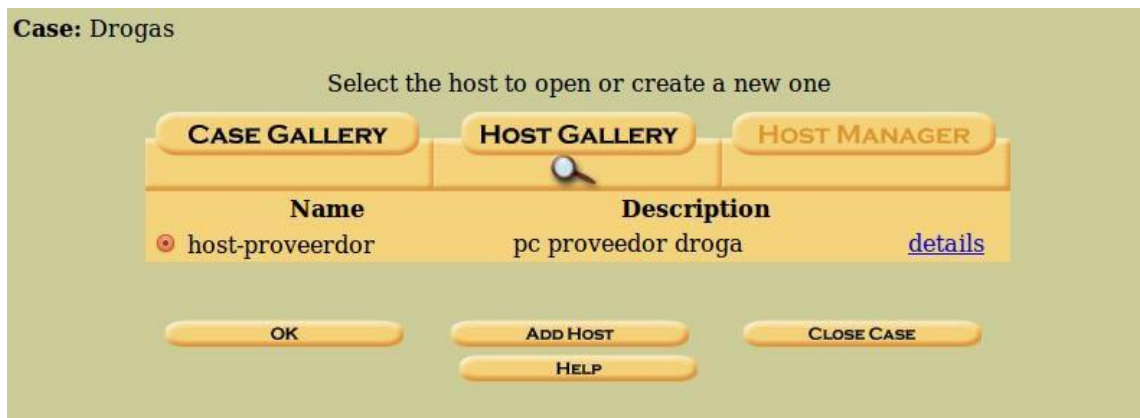
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

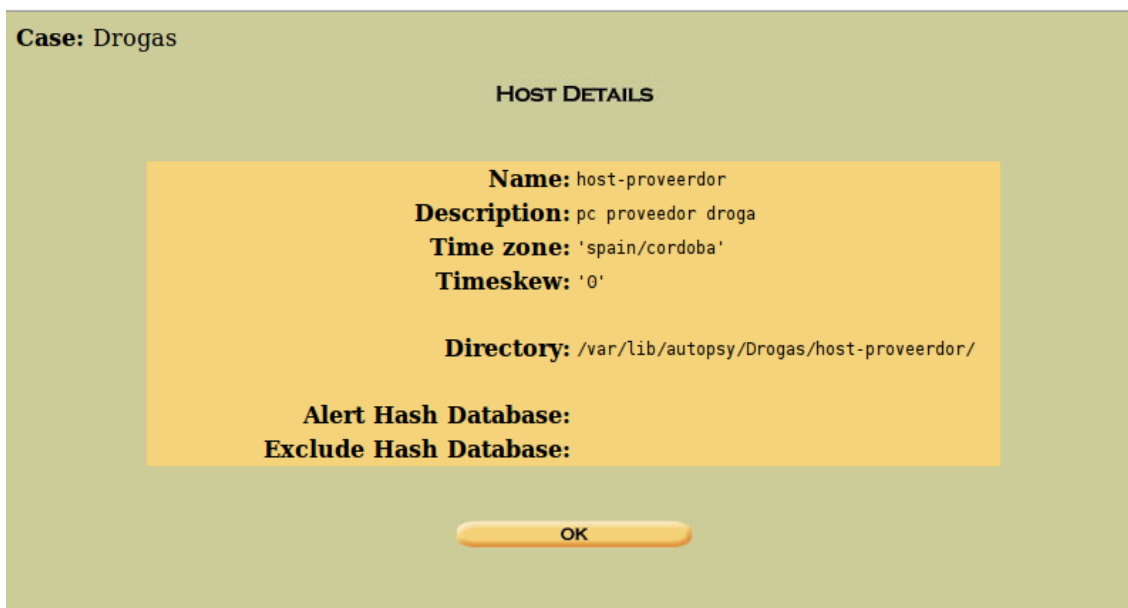
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

La zona daba error y la cambié. Marcamos Add host.

El caso se ha creado correctamente. Marcamos Ok para añadir la imagen.

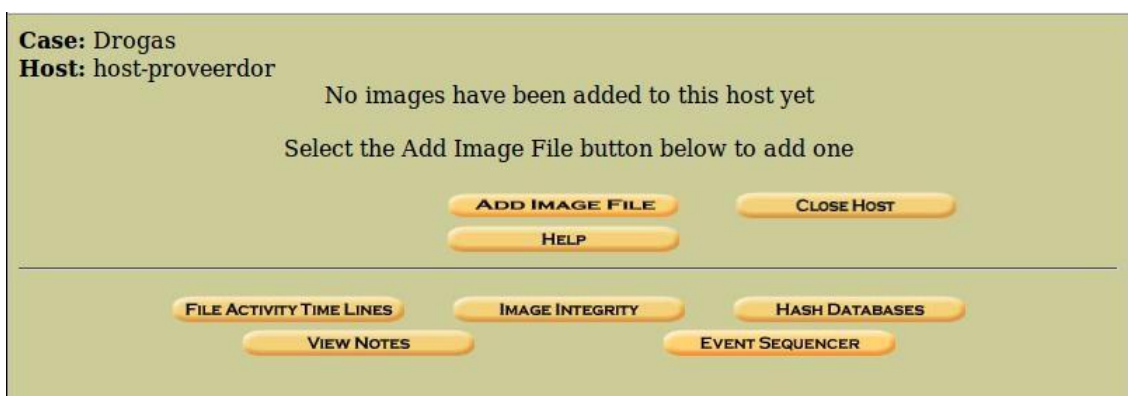


(Detalles)



Añadir imagen

Add image file



Añadimos la ruta donde se encuentra la imagen descargada y marcamos Next.

Case: Drogas
Host: host-proveedoror

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,

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**

Elegir tal cual viene.

Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table).
Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image ☐ Volume Image ☒

Volume System Type (disk image only):

OK

Detalles del archivo de imagen. ADD.

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:

☒ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat12)

Mount Point: File System Type:

OK.

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 - C:) added with ID vol1

Ahora es el momento de iniciar el análisis. Details.

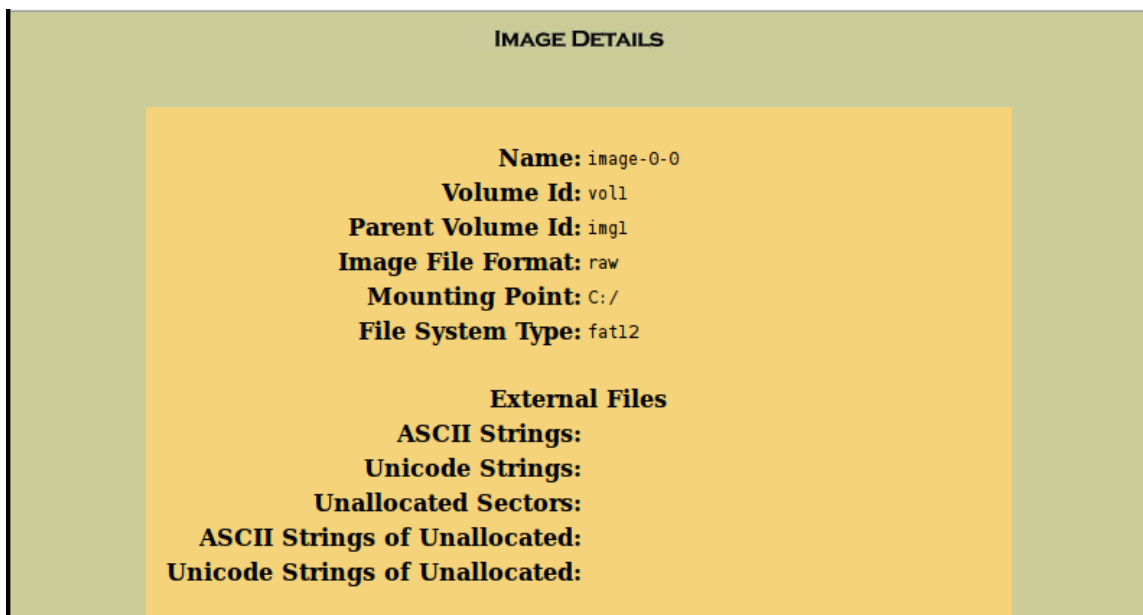
Case: Drogas
Host: host-proveedoror

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

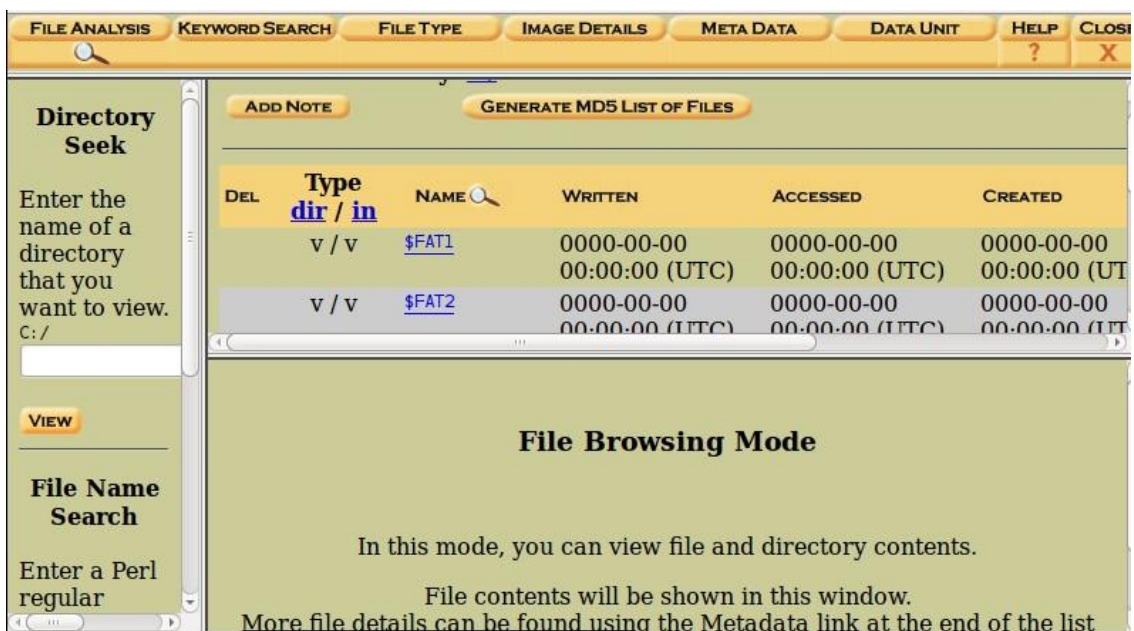
mount	name	fs type	
<input checked="" type="radio"/> C:/	image-0-0	fat12	details

Extraer archivos para analizar

Antes del proceso.



Extrae los dos hasta que queden los campos vacíos completamente rellenos. Luego File System.



Empezamos analizar los archivos uno por uno

Archivo cover page.jpgc.

The screenshot shows the File Analysis software interface. The 'Directory Seek' tab is active, displaying a table of files. The file 'cover page.jpgc' is selected. Below the table, the 'Hex Contents Of File: C:/cover page.jpgc' are shown, displaying a series of F6F6 hex values.

File Name	File Type	File Size	File Date	File Time	File Comment
v / v	\$FAT2	0000-00-00	00:00:00 (UTC)	00:00:00 (UTC)	00:00:00 (UTC)
v / v	\$MBR	0000-00-00	00:00:00 (UTC)	00:00:00 (UTC)	00:00:00 (UTC)
d / d	\$OrphanFiles/	0000-00-00	00:00:00 (UTC)	00:00:00 (UTC)	00:00:00 (UTC)
r / r	cover page.jpgc	2002-09-11	08:30:52 (spain)	00:00:00 (spain)	08:50:27 (spa

Hex Contents Of File: C:/cover page.jpgc

```
00000000: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....  
00000010: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....  
00000020: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....  
00000030: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....  
00000040: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....  
00000050: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
```

Visualizar los metadatos, en el directorio de entrada meter 8. Comprobamos la incoherencia en cuanto a tamaños comparando 15585 a un sector (512) 451.

The screenshot shows the File Analysis software interface with the 'Meta Data' tab active. The file 'COVERP~1.JPG' is selected. The 'Dir Entry Number' is 8. The 'SHA-1 of content' is displayed. The 'Details' section shows the directory entry, allocation, file attributes, size, and name. The 'Directory Entry Times' section shows the written, accessed, and created times. The 'Sectors' section shows the sector number 451.

Dir Entry Number: 8

SHA-1 of content: dcc13088a8389d974bc544ac32d6fccb4c904fba -

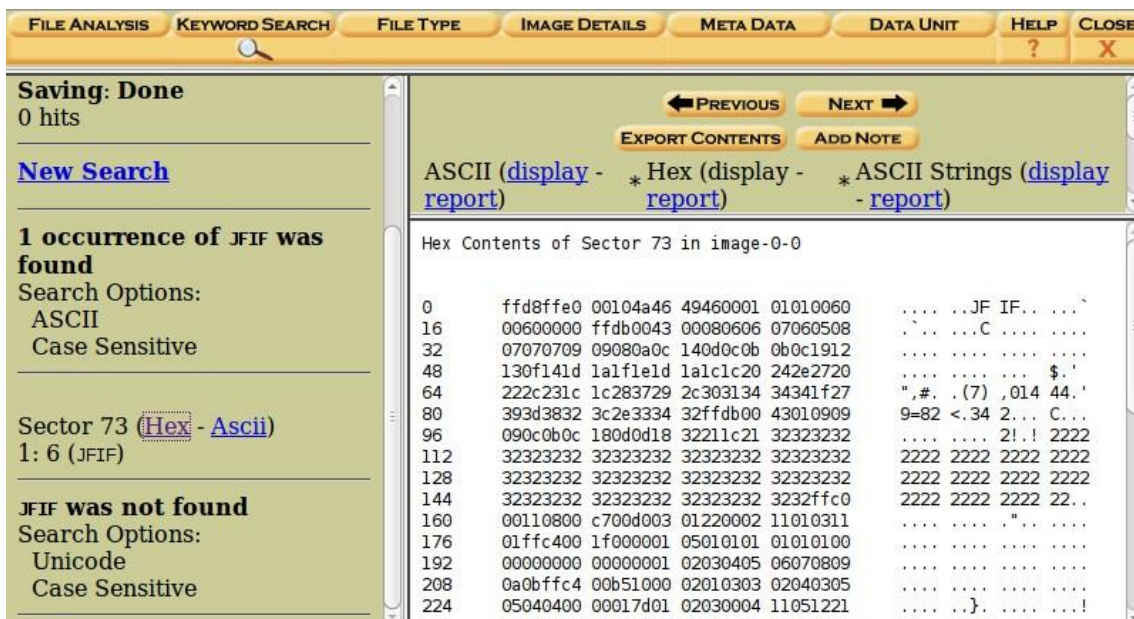
Details:

Directory Entry: 8
Allocated
File Attributes: File, Archive
Size: 15585
Name: COVERP~1.JPG

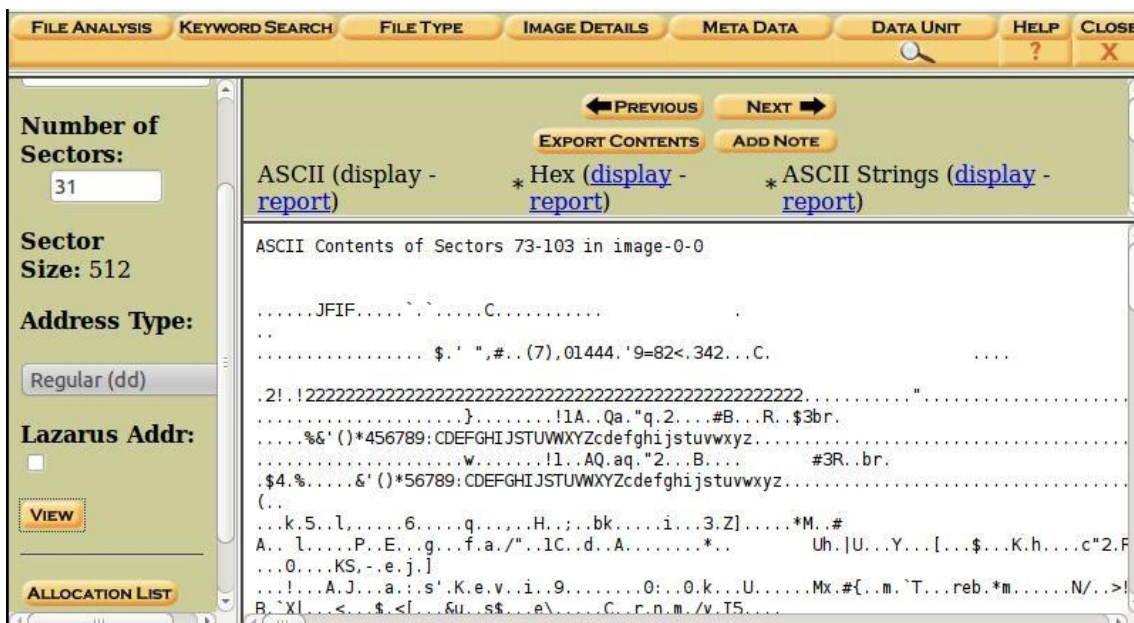
Directory Entry Times:
Written: Wed Sep 11 08:30:52 2002
Accessed: Wed Sep 11 00:00:00 2002
Created: Wed Sep 11 08:50:27 2002

Sectors: 451

Se procede a realizar la búsqueda de la firma jpeg (jif), se encuentra coincidencia en el sector 73.

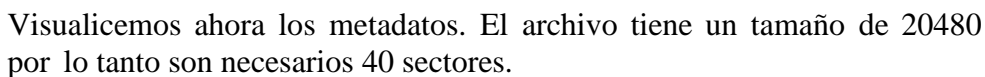


Se necesitan 31 sectores para almacenar 15585 bytes. Pero están asignados (36 sectores) del 73 hasta el 108. Pero solo 31 están asociados con el archivo; como se verifica más adelante; dado que la 104 y 105 están asignados a otro archivo.



Exportamos el contenido con la opción Export Contens. Y abrimos la imagen.

```
root@ubuntu:/home/usuario/Escritorio# dd skip=73 bs=512 count=31 if=/home/usuario/Escritorio/image of=/home/usuario/Escritorio/coverpage.jpg
31+0 registros de entrada
31+0 registros de salida
15872 bytes (16 kB) copiados, 0,000263441 s, 60,2 MB/s
root@ubuntu:/home/usuario/Escritorio#
```



Extraemos el archivo. Export contents.

The screenshot shows a web-based file analysis tool with a yellow header bar containing tabs: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, and DATA UNIT. On the left, a sidebar contains input fields for Sector Number (33), Number of Sectors (40), Sector Size (512), Address Type (Regular (dd)), and Lazarus Addr. The main area displays navigation buttons (PREVIOUS, NEXT), action buttons (EXPORT CONTENTS, ADD NOTE), and three report links: ASCII (display - report), Hex (display - report), and ASCII Strings (report). Below these, the ASCII content of sectors 33-72 is shown, including a header line 'ASCII Contents of Sectors 33-72 in image-0-0' and several lines of text: a header line with symbols, a line with 'R' and 'N', a line with 'R', a line with 'F' and '2', a line with '2', '8', 'N', 'v', 'T', 'D', and a backslash, and a line with '626 Jungle Ave Apt 2' and 'Jungle, NY 11111'. Below this, a message from 'Jimmy' is displayed: 'Dude, your pot must be the best . it made the cover of High Times Maga' and 'These kids, they tell me marijuana isn.t addictive, but they don.t sto'.

Visualizado del archivo.

Jimmy Jungle
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 soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

[illegible]

FILE ANALYSIS	KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA
				
Dir Entry Number: <input type="text" value="11"/> VIEW	<p>082a5cc64deea22a3a580ffbb5a6fa66 -</p> <p>SHA-1 of content: c8e7f25380d63c9034d9f27faab29de1f09240b5 -</p> <p>Details:</p> <p>Directory Entry: 11 Allocated File Attributes: File, Archive Size: 1000 Name: SCHEDU~1.EXE</p> <p>Directory Entry Times: Written: Fri May 24 08:20:32 2002 Accessed: Wed Sep 11 00:00:00 2002 Created: Wed Sep 11 08:50:38 2002</p> <p>Sectors: 104 105</p>			

13

JPG desde el sector 73 hasta el 108 se encuentra en el último sector el texto “Scheduled Visits.xls”.

```
root@ubuntu:/home/usuario# dd skip=104 bs=512 count=5 if=/home/usuario/Escritorio/image of=/home/usuario/Escritorio/scheduledvisits.exe
5+0 registros de entrada
5+0 registros de salida
2560 bytes (2,6 kB) copiados, 0,000152056 s, 16,8 MB/s
root@ubuntu:/home/usuario#
```

Password: goodtimes (gracias la primer archivo).

```
root@ubuntu:/home/usuario/Escritorio# ls
image      scheduledvisits.exe  voll-Sector105.raw  voll-Sector73.raw
image.zip  voll-Sector104.raw  voll-Sector33.raw
root@ubuntu:/home/usuario/Escritorio# unzip scheduledvisits.exe
Archive:  scheduledvisits.exe
[scheduledvisits.exe] Scheduled Visits.xls password:
password incorrect--reenter:
inflating: Scheduled Visits.xls
```

Abrimos el archivo con la aplicación pertinente.

B50	$f(x)$	Σ	=	Monday (1)
	A	B	C	
1	<u>Month</u>	<u>DAY</u>	<u>HIGH SCHOOLS</u>	
2	2002			
3	<u>April</u>	<u>Monday (1)</u>	<u>Smith Hill High School (A)</u>	
4		<u>Tuesday (2)</u>	<u>Key High School (B)</u>	
5		<u>Wednesday (3)</u>	<u>Leetch High School (C)</u>	
6		<u>Thursday (4)</u>	<u>Birard High School (D)</u>	
7		<u>Friday (5)</u>	<u>Richter High School (E)</u>	
8		<u>Monday (1)</u>	<u>Hull High School (F)</u>	
9		<u>Tuesday (2)</u>	<u>Smith Hill High School (A)</u>	
10		<u>Wednesday (3)</u>	<u>Key High School (B)</u>	
11		<u>Thursday (4)</u>	<u>Leetch High School (C)</u>	
12		<u>Friday (5)</u>	<u>Birard High School (D)</u>	
13		<u>Monday (1)</u>	<u>Richter High School (E)</u>	
14		<u>Tuesday (2)</u>	<u>Hull High School (F)</u>	
15		<u>Wednesday (3)</u>	<u>Smith Hill High School (A)</u>	
16		<u>Thursday (4)</u>	<u>Key High School (B)</u>	
17		<u>Friday (5)</u>	<u>Leetch High School (C)</u>	
18		<u>Monday (1)</u>	<u>Birard High School (D)</u>	
19		<u>Tuesday (2)</u>	<u>Richter High School (E)</u>	

RESPUESTAS DESPUÉS DEL ANÁLISIS

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

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