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

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

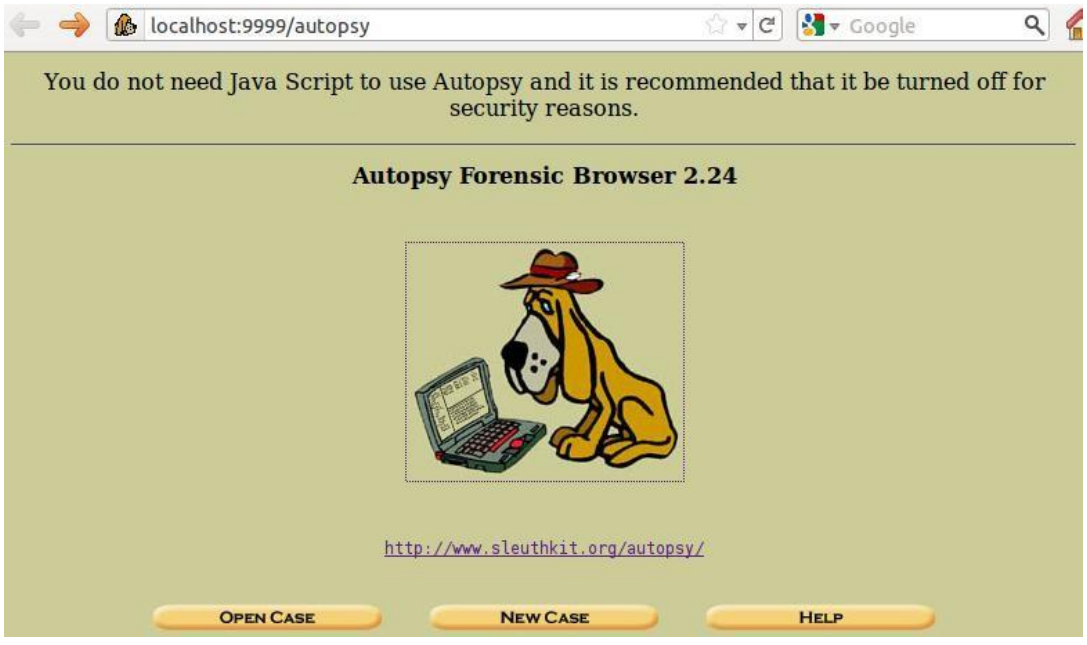
```
root@ubuntu:/home/usuario/Escritorio# md5sum image.zip
b676147f63923e1f428131d59b1d6a72  image.zip
root@ubuntu:/home/usuario/Escritorio# unzip image.zip
Archive:  image.zip
  inflating: image
```

Instala apt-get install sleuthkit autopsy

Para acceder: autopsy

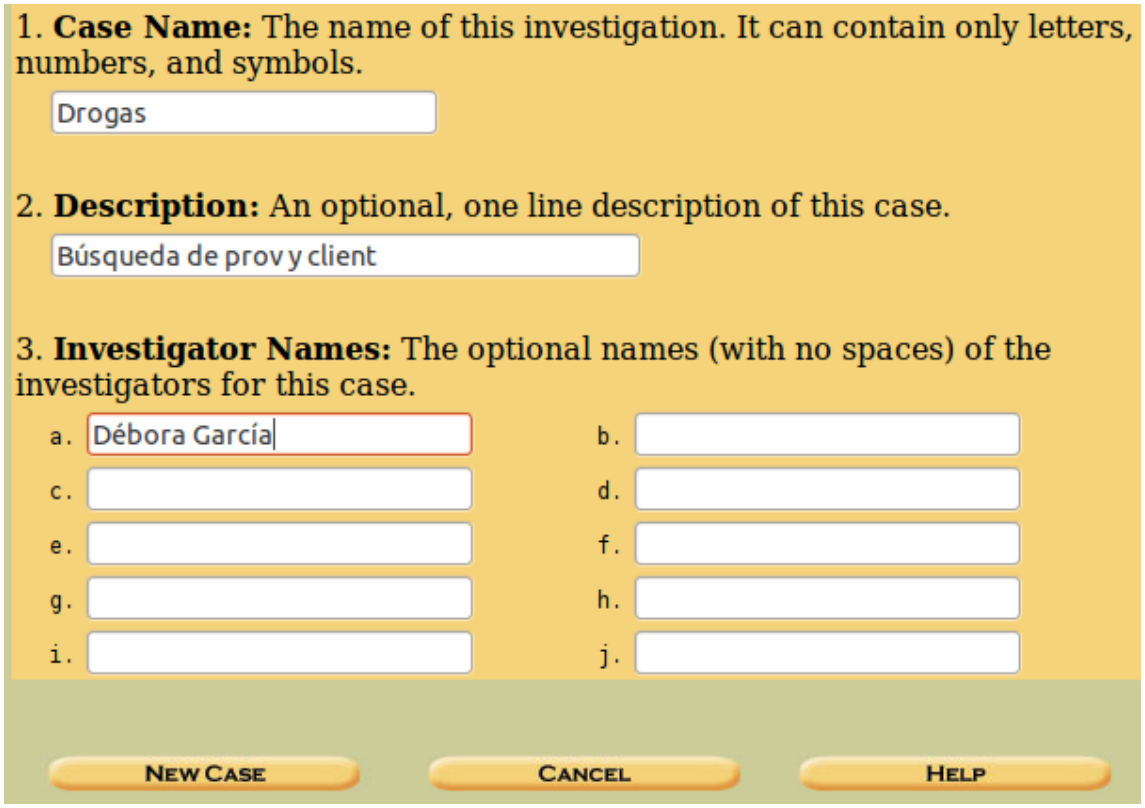
```
root@ubuntu:/home/usuario/Escritorio# autopsy

================================================================

                    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.

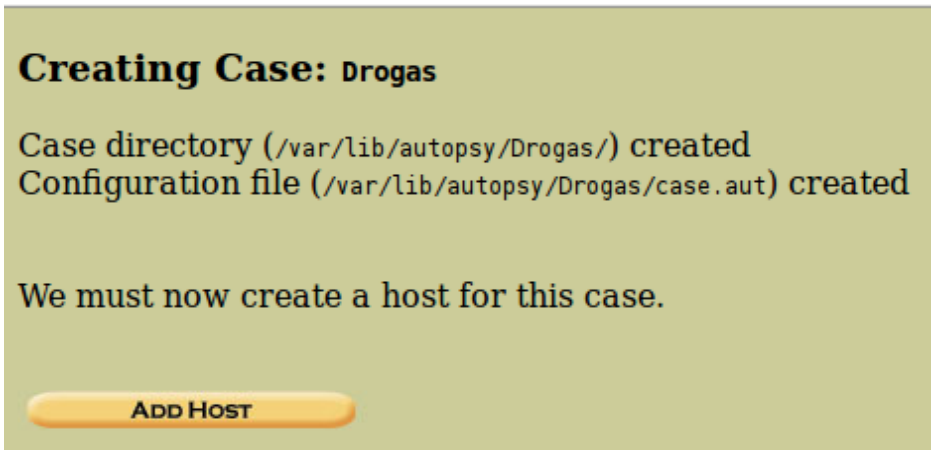


Crear Caso

Crearemos el caso marcando New Case

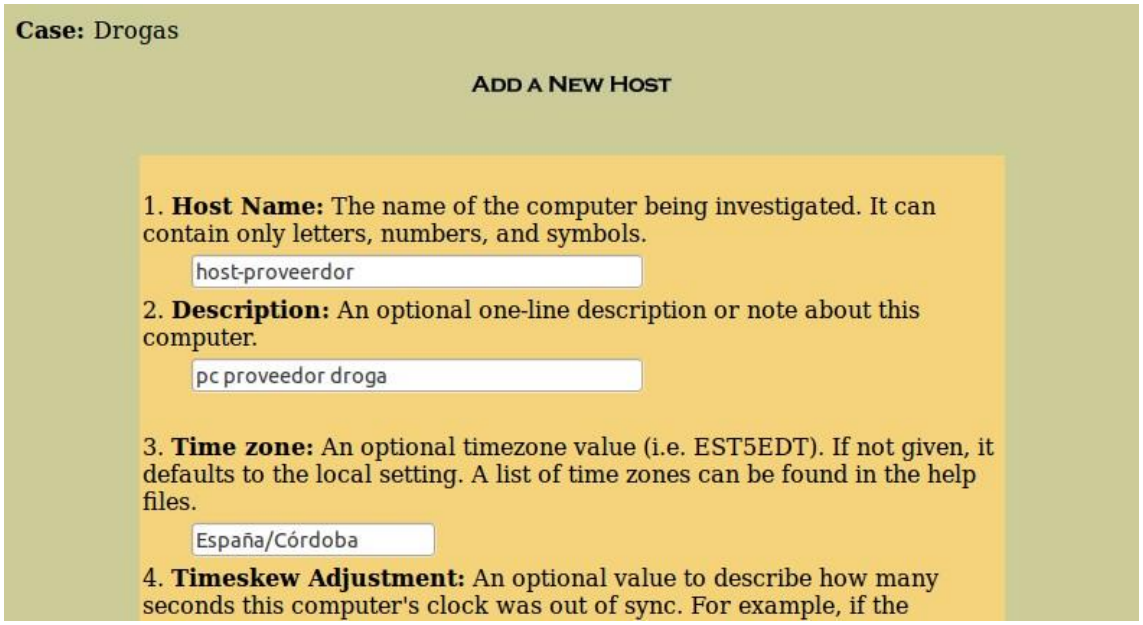


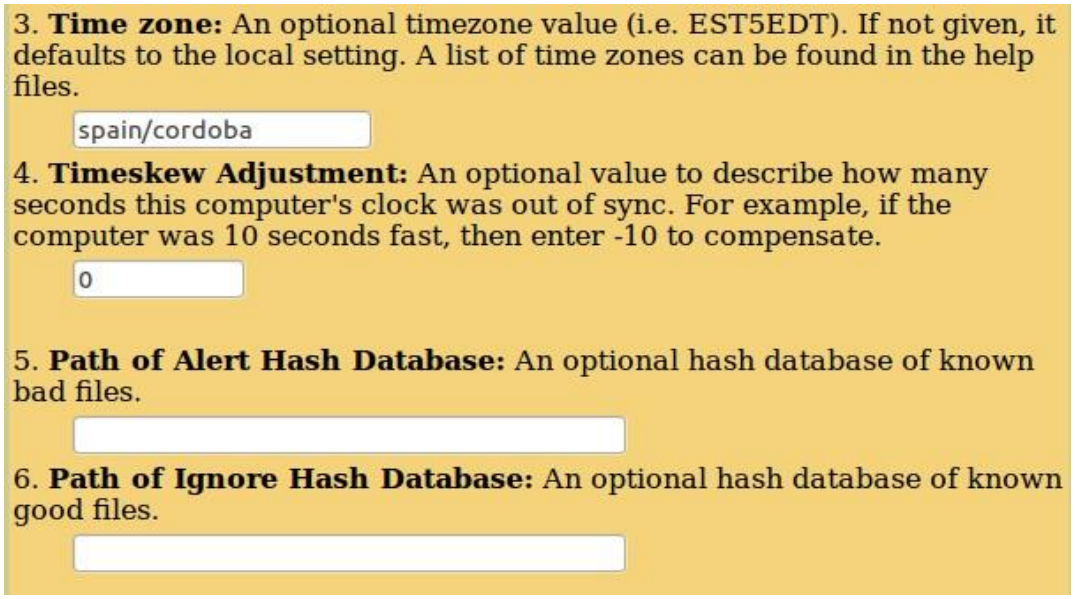
Haremos clic en New Case para ver el resultado.



Crear host

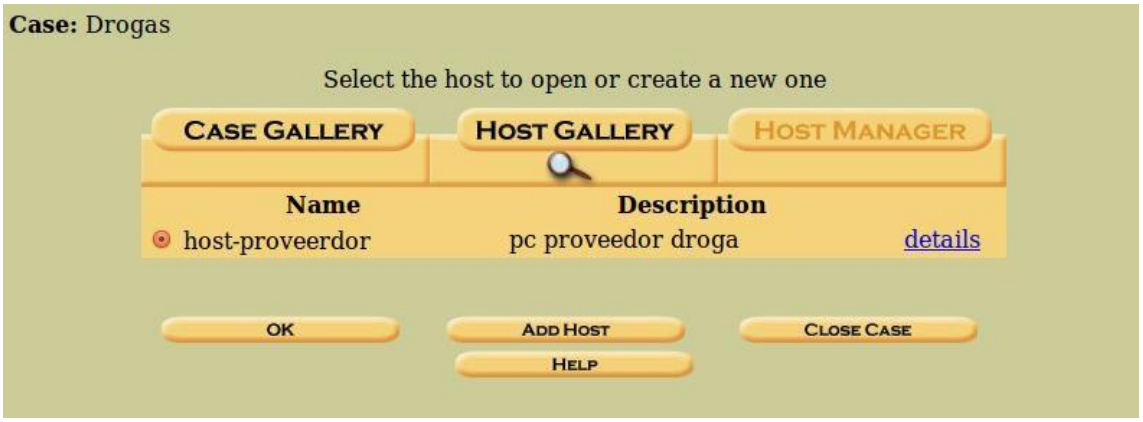
Creamos el nuevo hosts.



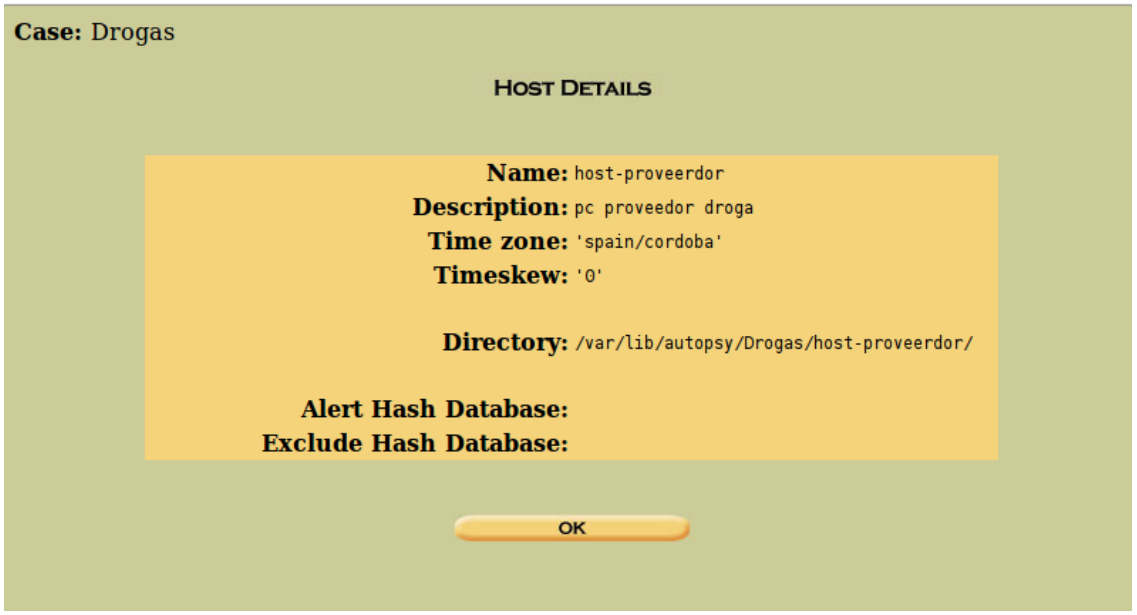


La zona daba error y la cambié. Marcamos Add host.

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

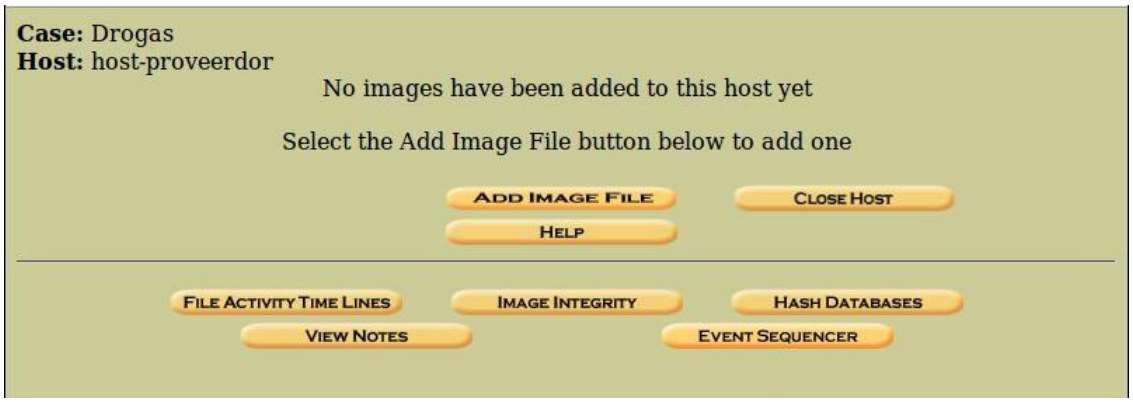


(Detalles)

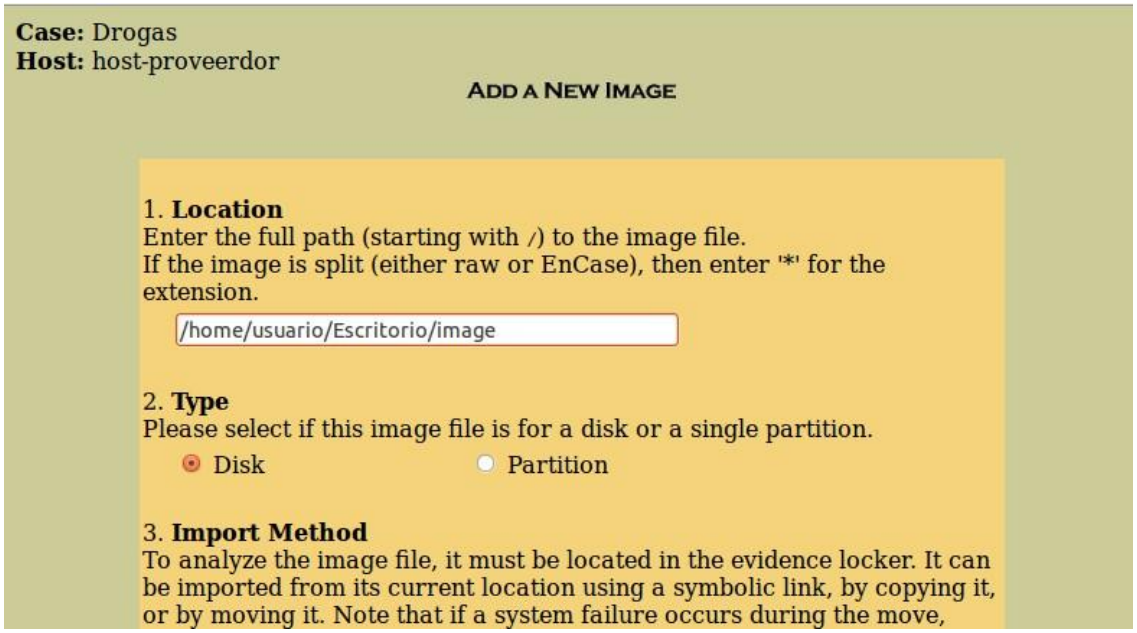


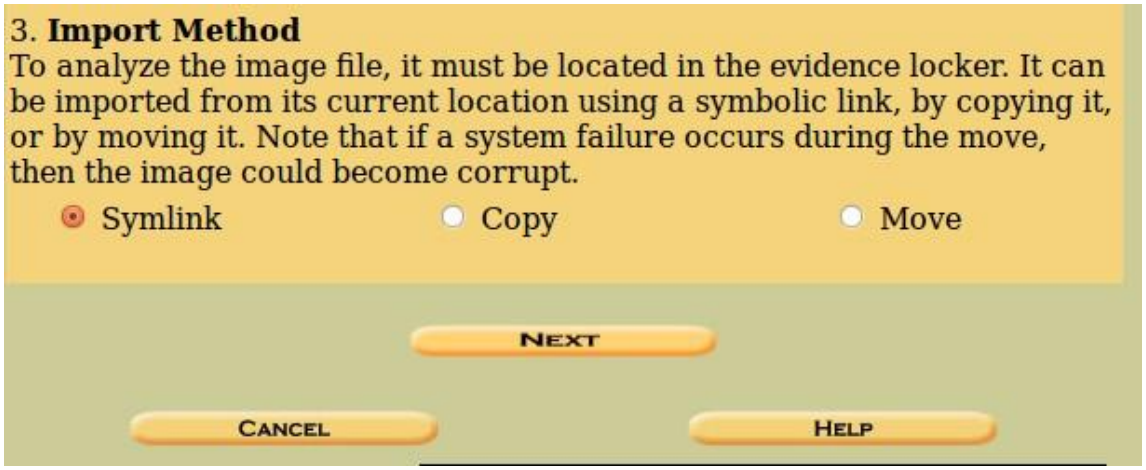
Añadir imagen

Add image file

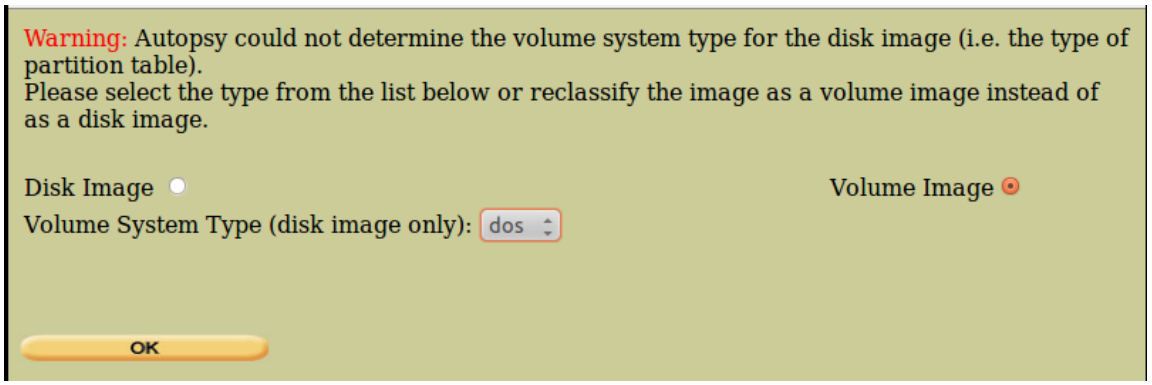


Añadimos la ruta donde se encuentra la imagen descargada y marcamos Next.

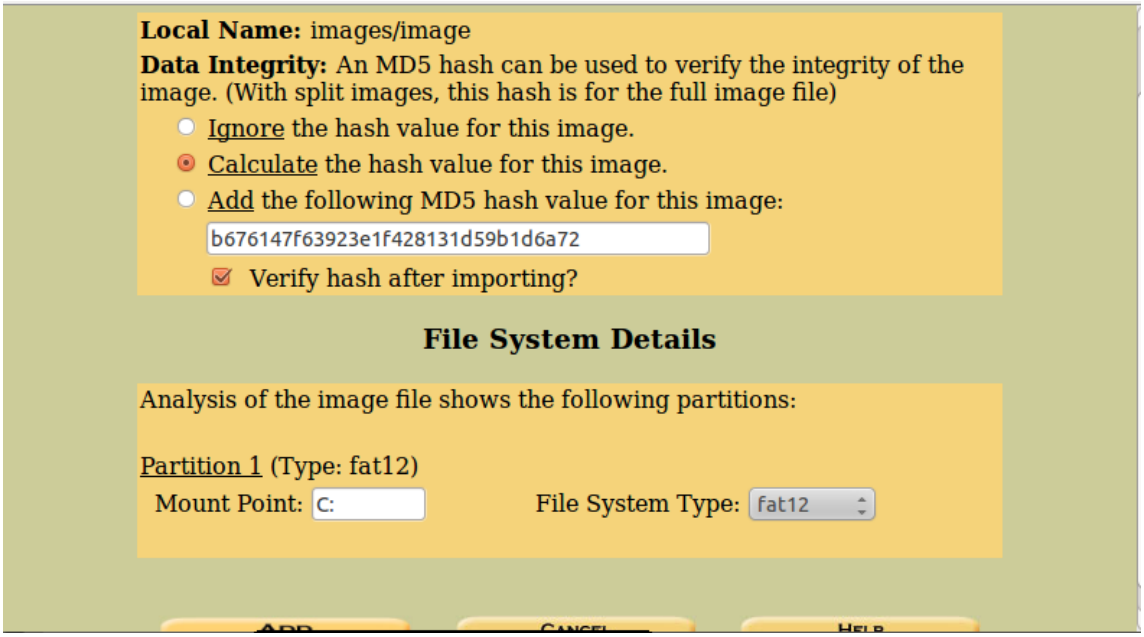




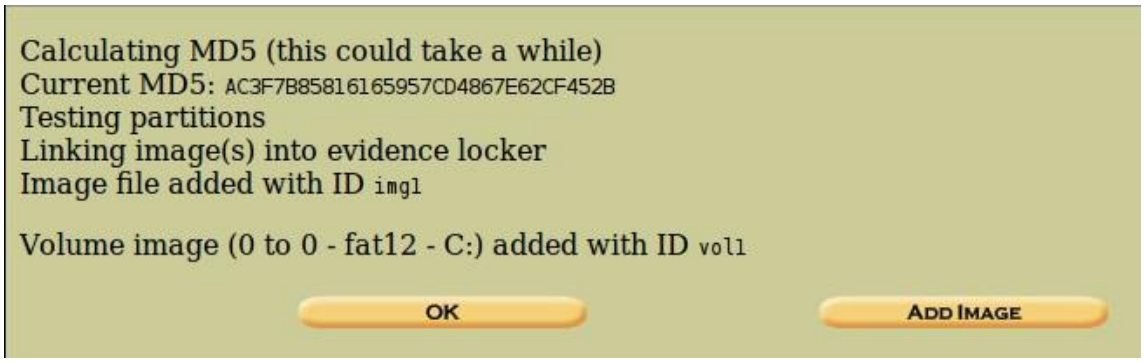
Elegir tal cual viene.



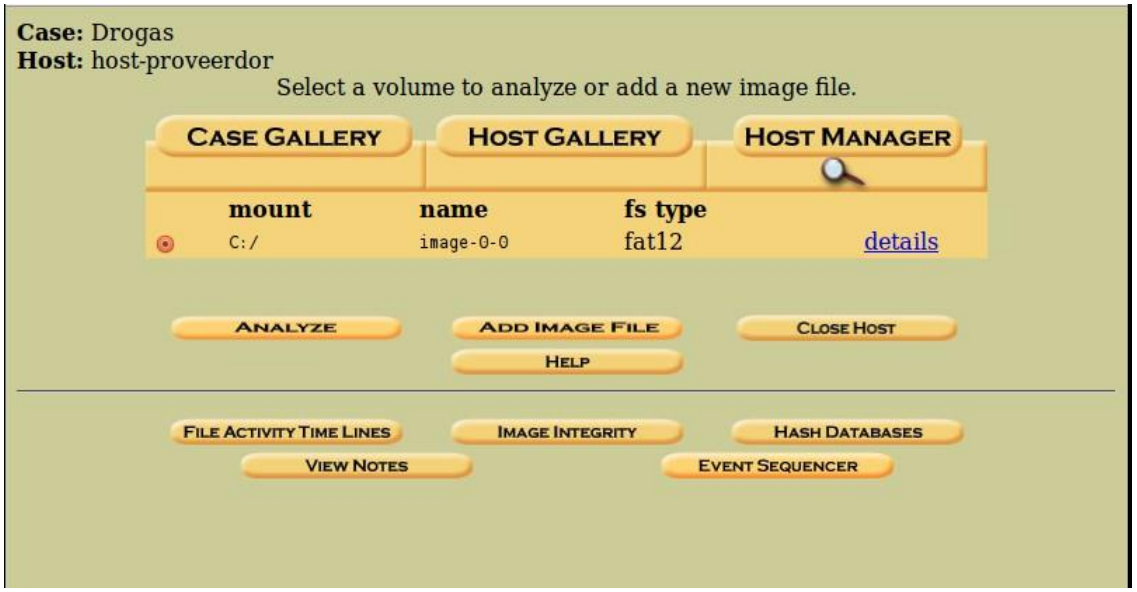
Detalles del archivo de imagen. ADD.



OK.

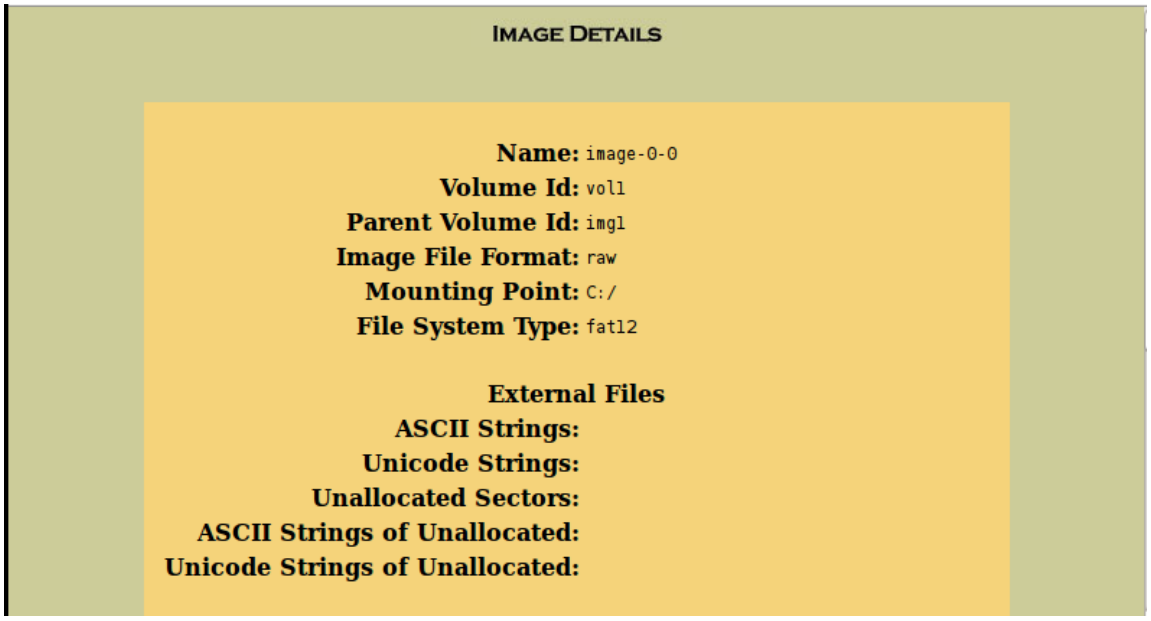


Ahora es el momento de iniciar el análisis. Details.

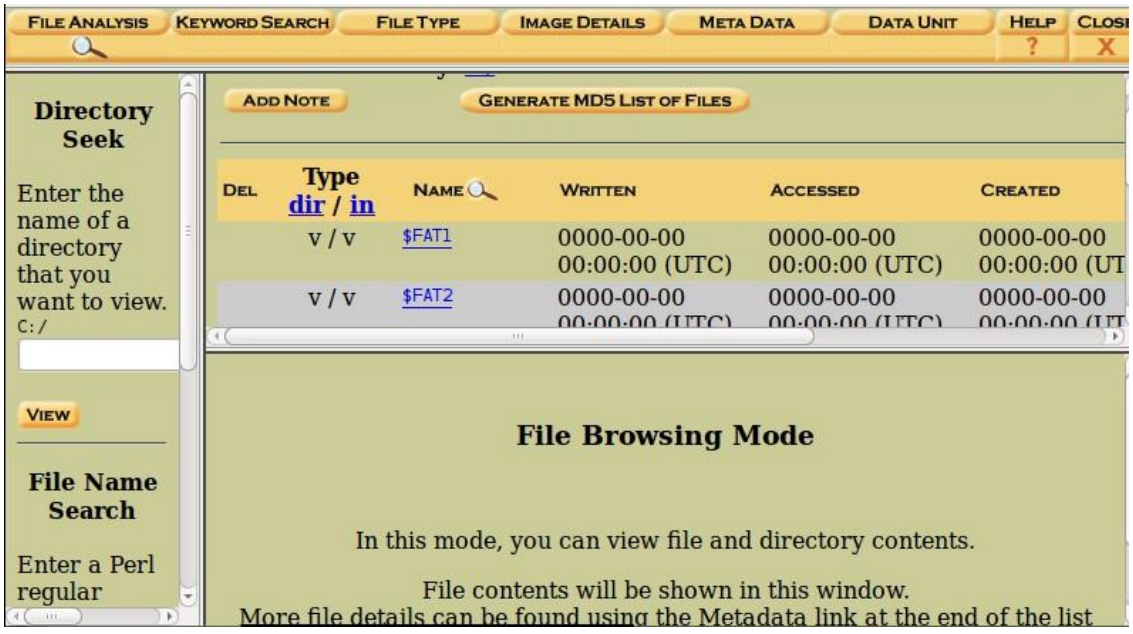


Extraer archivos para analizar

Antes del proceso.

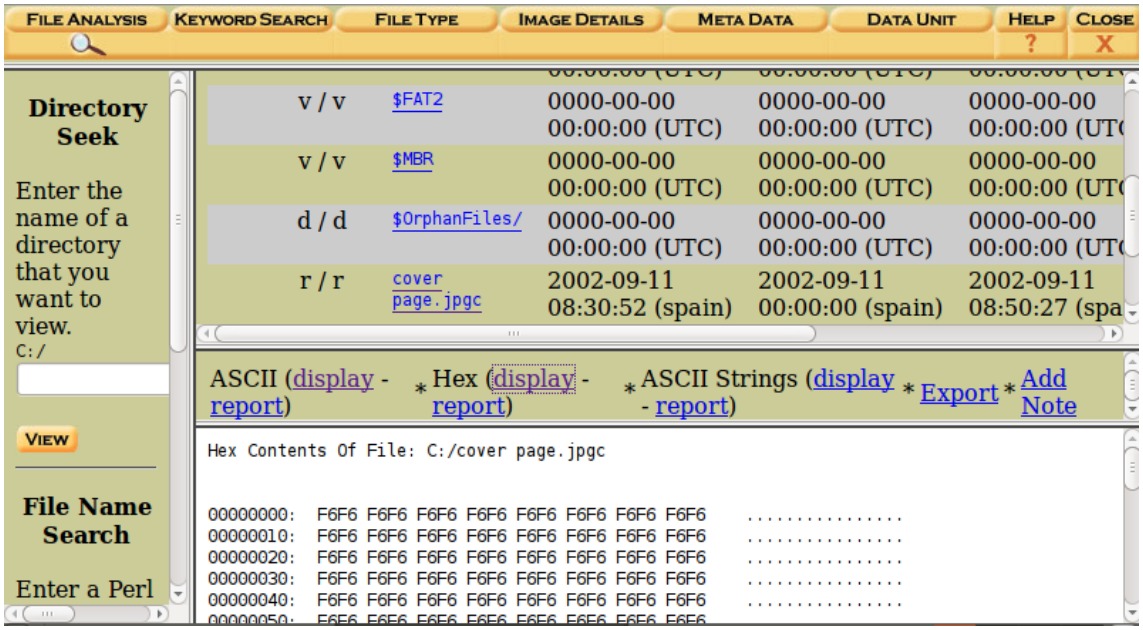


Extrae los dos hasta que queden los campos vacíos completamente rellenos. Luego File System.

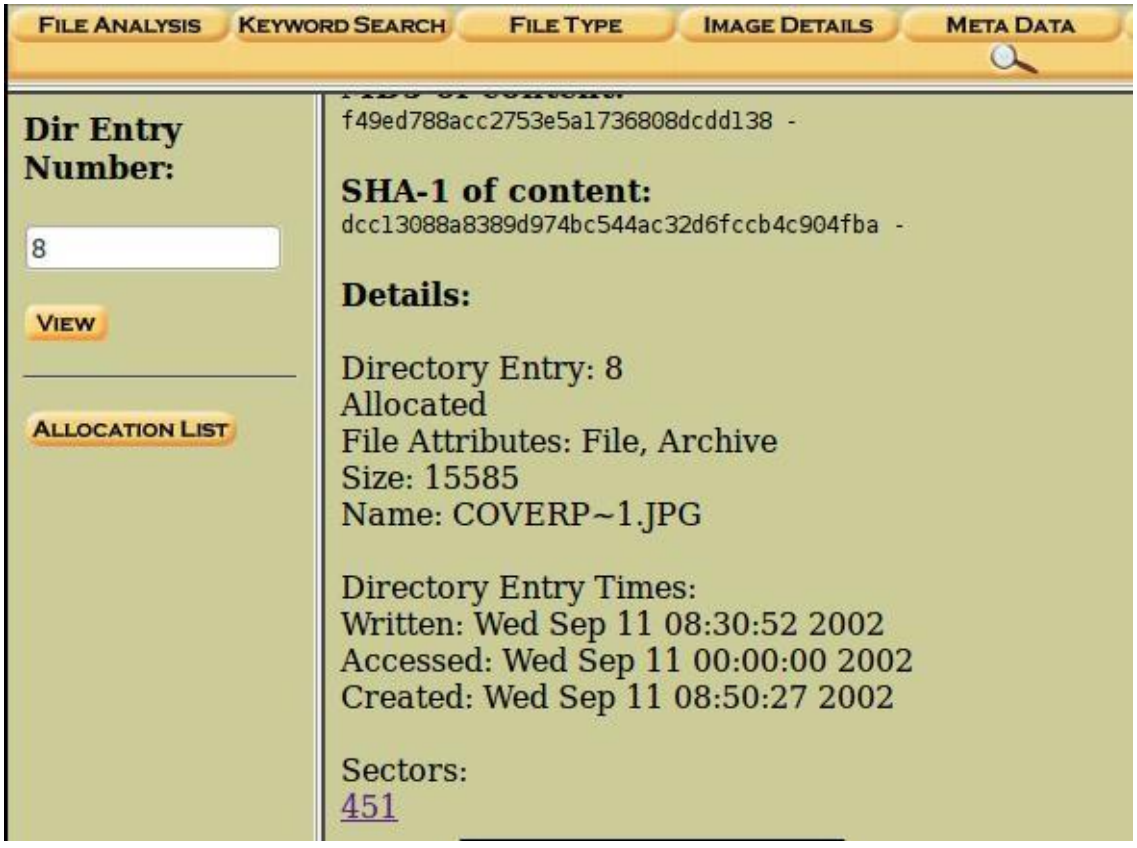


Empezamos analizar los archivos uno por uno

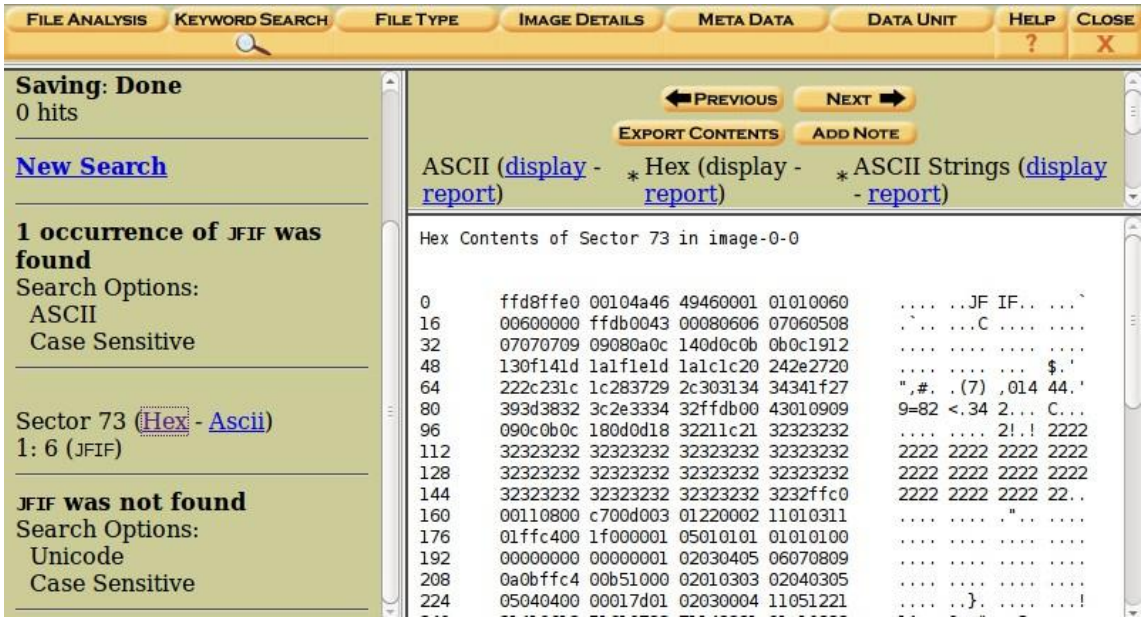
Archivo cover page.jpgc.



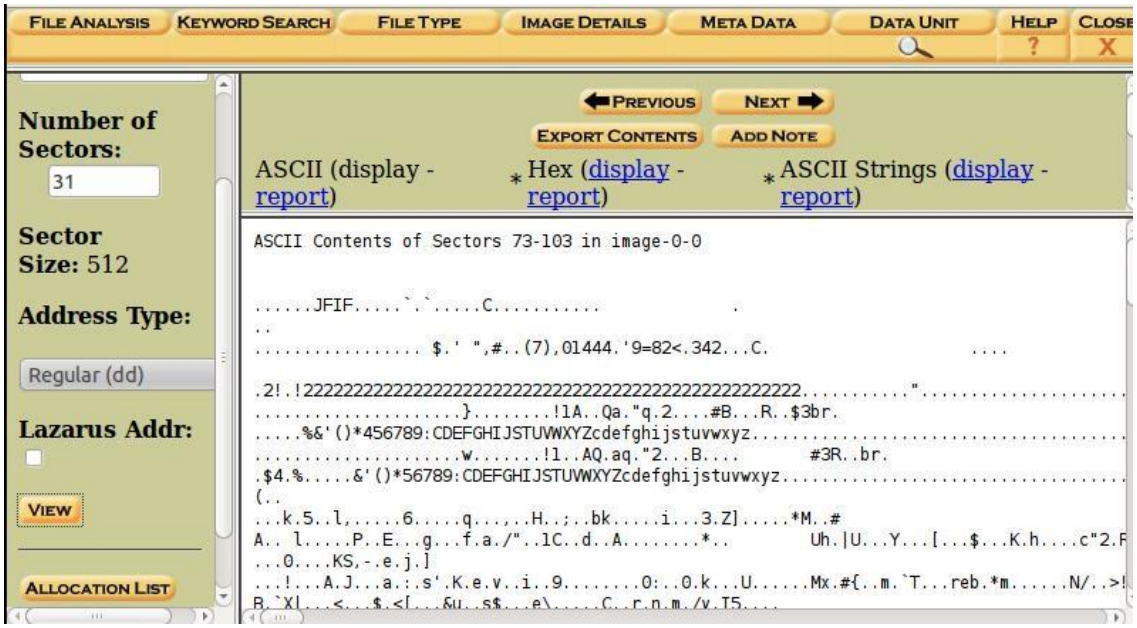
Visualizar los metadatos, en el directorio de entrada meter 8. Comprobamos la incoherencia en cuanto a tamaños comparando 15585 a un sector (512) 451.



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



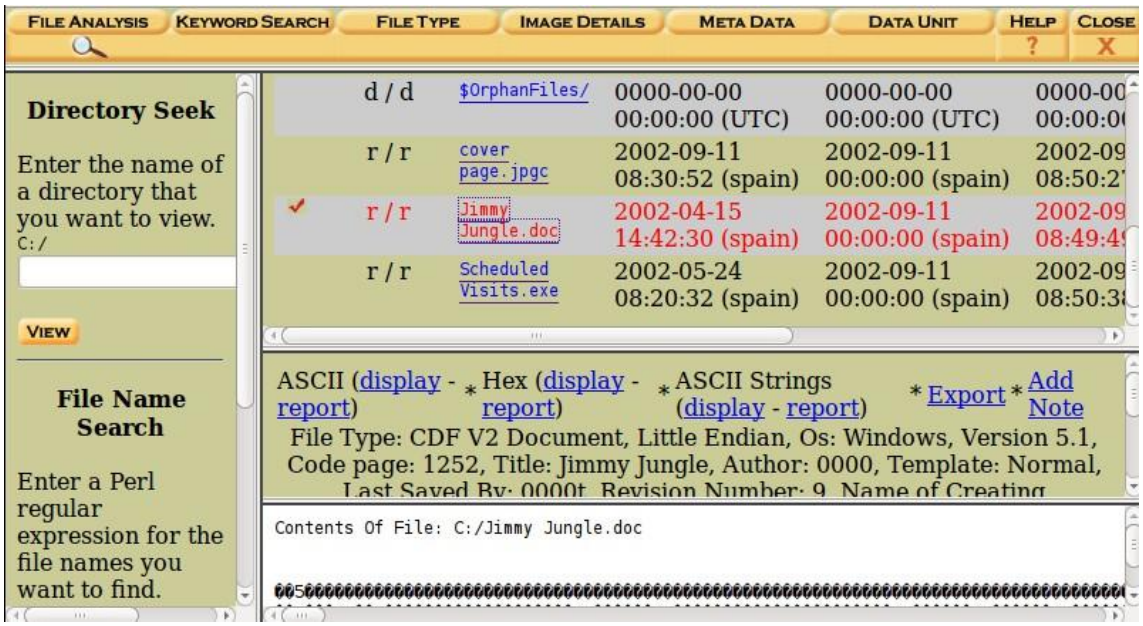
Se necesitan 31 sectores para almacenar 15585 bytes. Pero están asignados (36 sectores) del 73 hasta el 108. Pero solo 31 están asociados con el archivo; como se verifica más adelante; dado que la 104 y 105 están asignados a otro archivo.



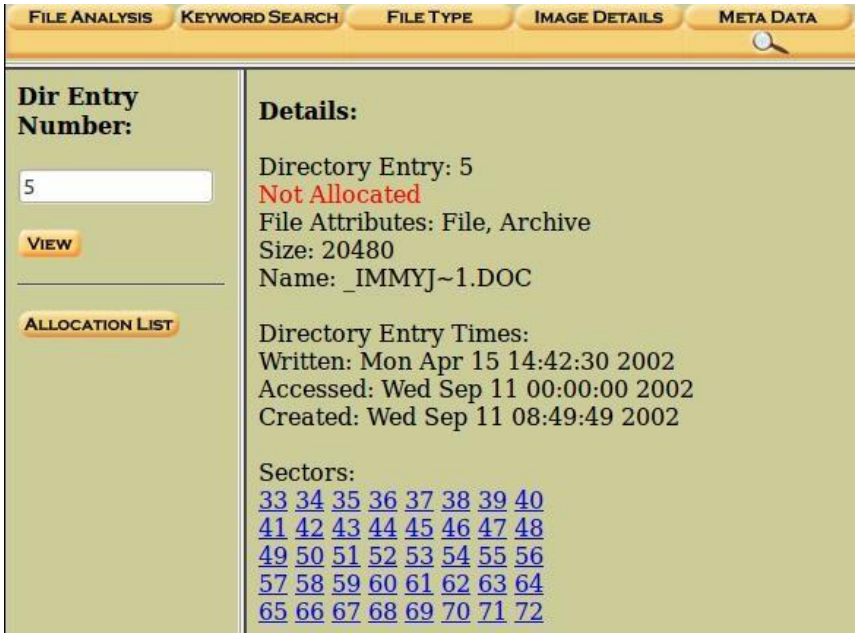
Exportamos el contenido con la opción Export Contens. Y abrimos la imagen.

```
root@ubuntu:/home/usuario/Escritorio# dd skip=73 bs=512 count=31 if=/home/usuari
o/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#
```

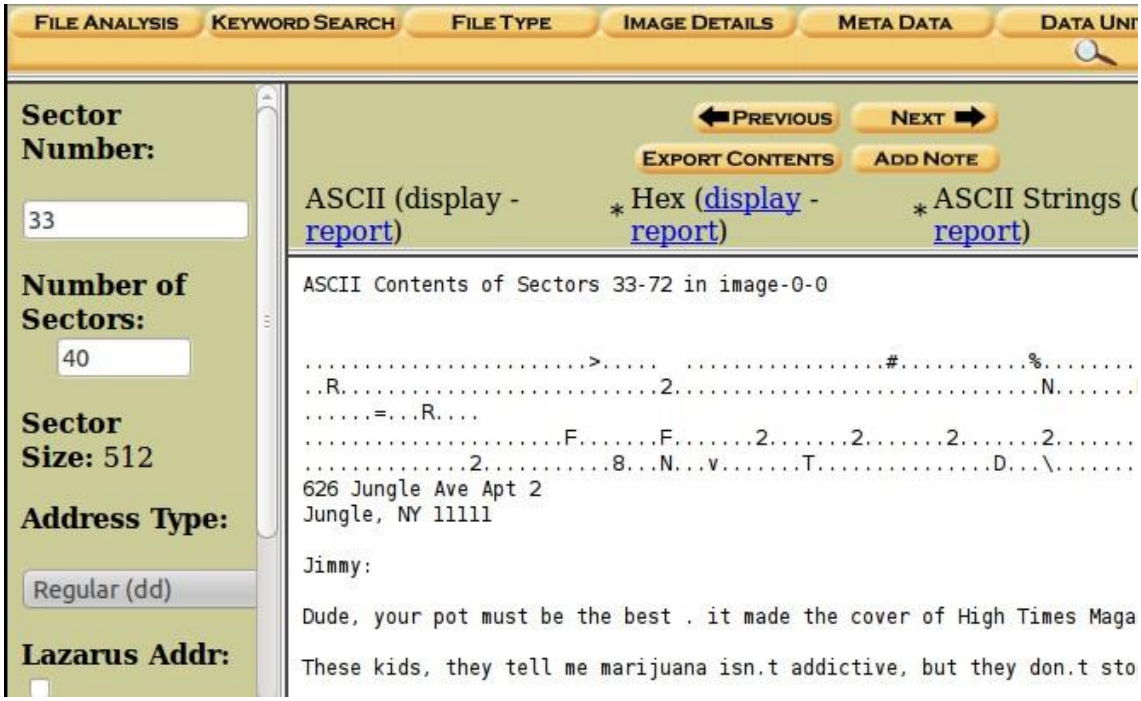
Archivo Jimmy Jungle.doc



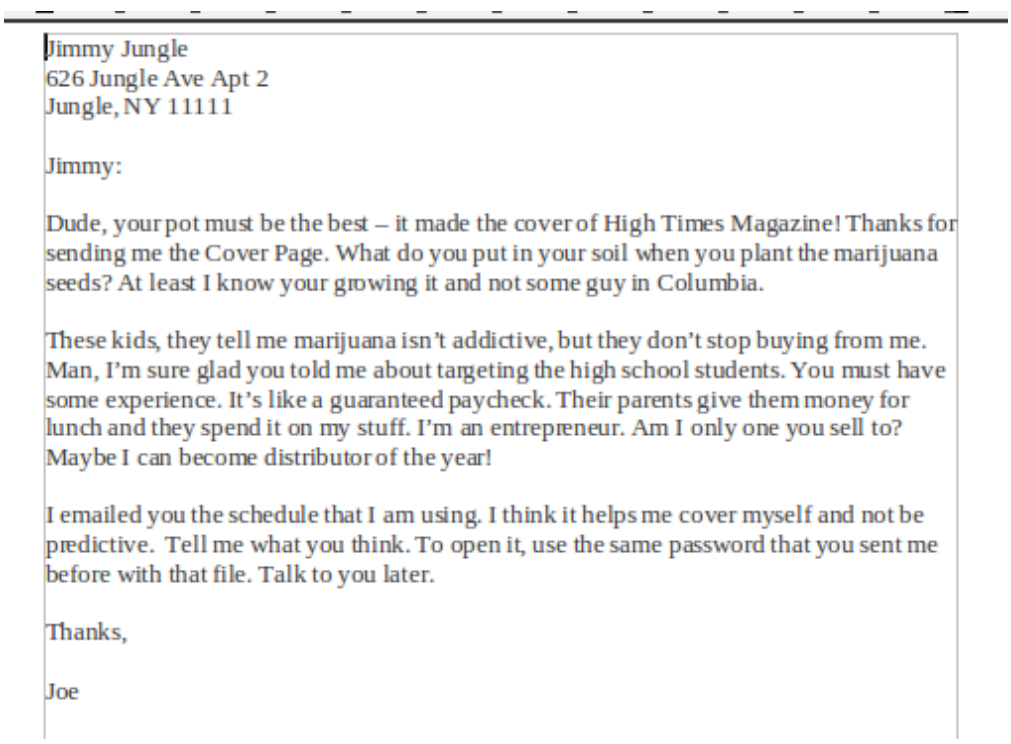
Visualicemos ahora los metadatos. El archivo tiene un tamaño de 20480 por lo tanto son necesarios 40 sectores.



Extraemos el archivo. Export contents.



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.

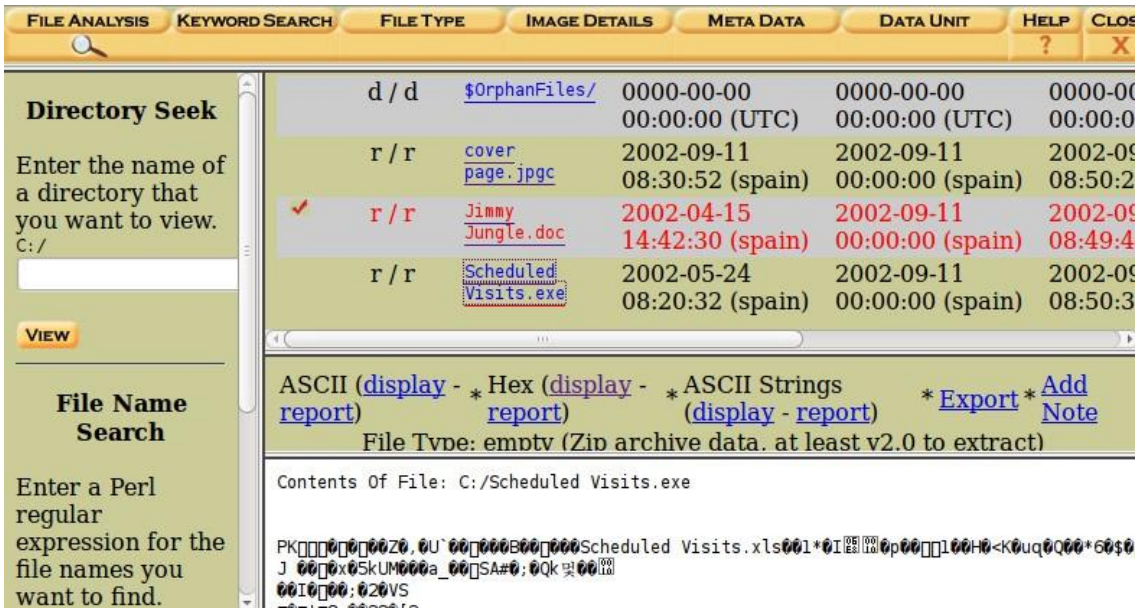
These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an 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.

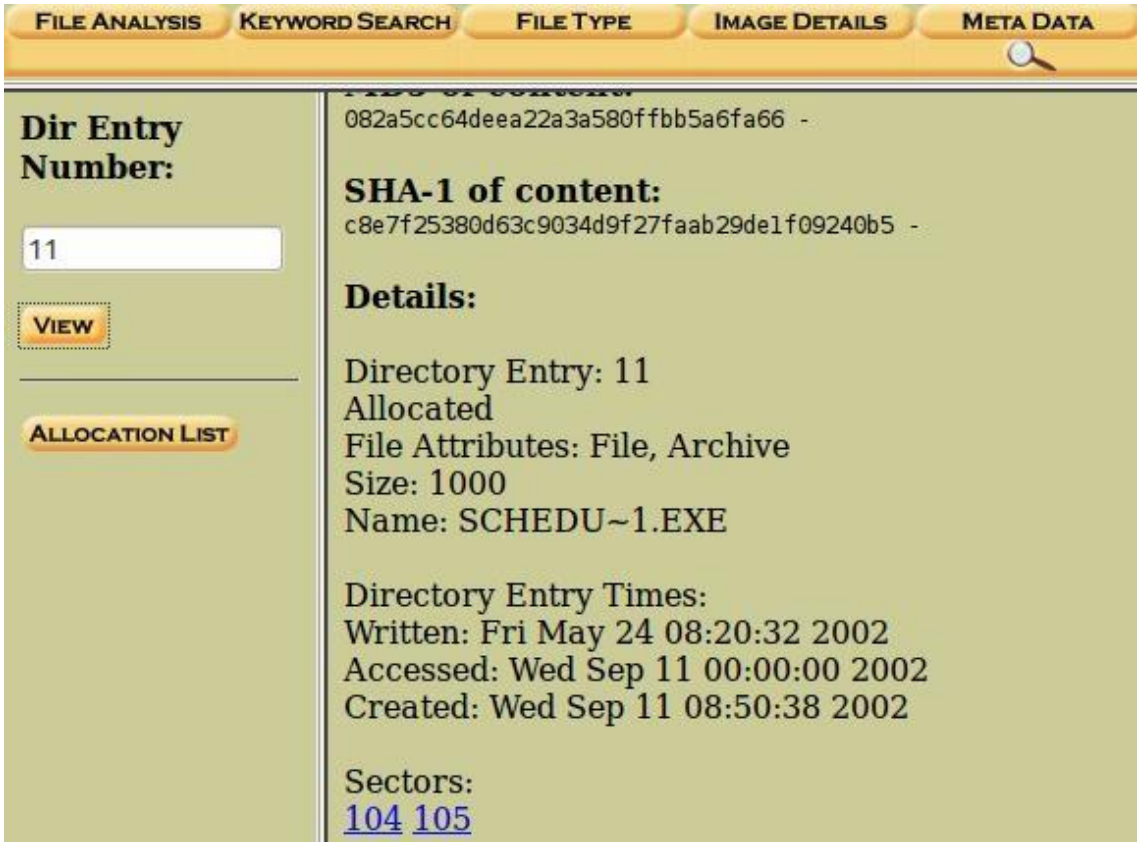
Thanks,

Joe

Archivo Scheluded Visists.exe



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



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 asignados los sectores desde el 73 hasta el 108. También se descubrió que cuando inicialmente se extraen los datos de la imagen

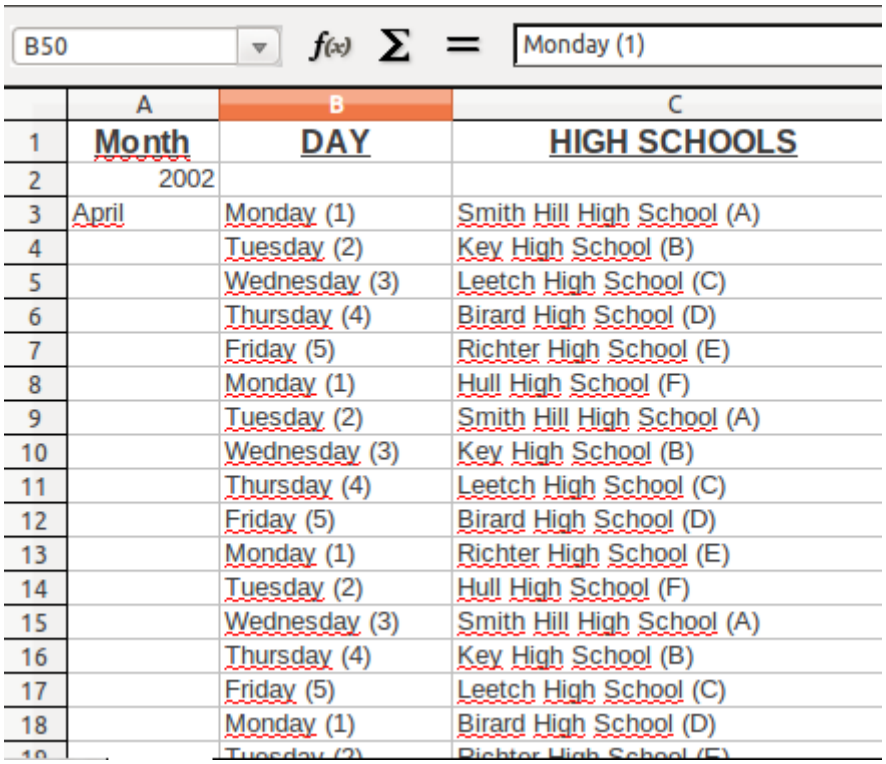
JPG desde el sector 73 hasta el 108 se encuentra en el último sector el texto “Scheduled Visits.xls”.

```
root@ubuntu:/home/usuario# dd skip=104 bs=512 count=5 if=/home/usuario/Escritori
o/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  vol1-Sector105.raw  vol1-Sector73.raw
image.zip   vol1-Sector104.raw   vol1-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 | Monday (1)

	A	B	C
1	**Month**	**DAY**	**HIGH SCHOOLS**
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)

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?