Facultad de Economía,
Empresa y Turismo
Universidad de La Laguna

Práctica de Laboratorio #14.

Análisis Forense:

Seguridad de Sistemas Informáticos.

Cheuk Kelly Ng Pante alu0101364544@ull.edu.es
Carlos Pérez Fino alu0101340333@ull.edu.es

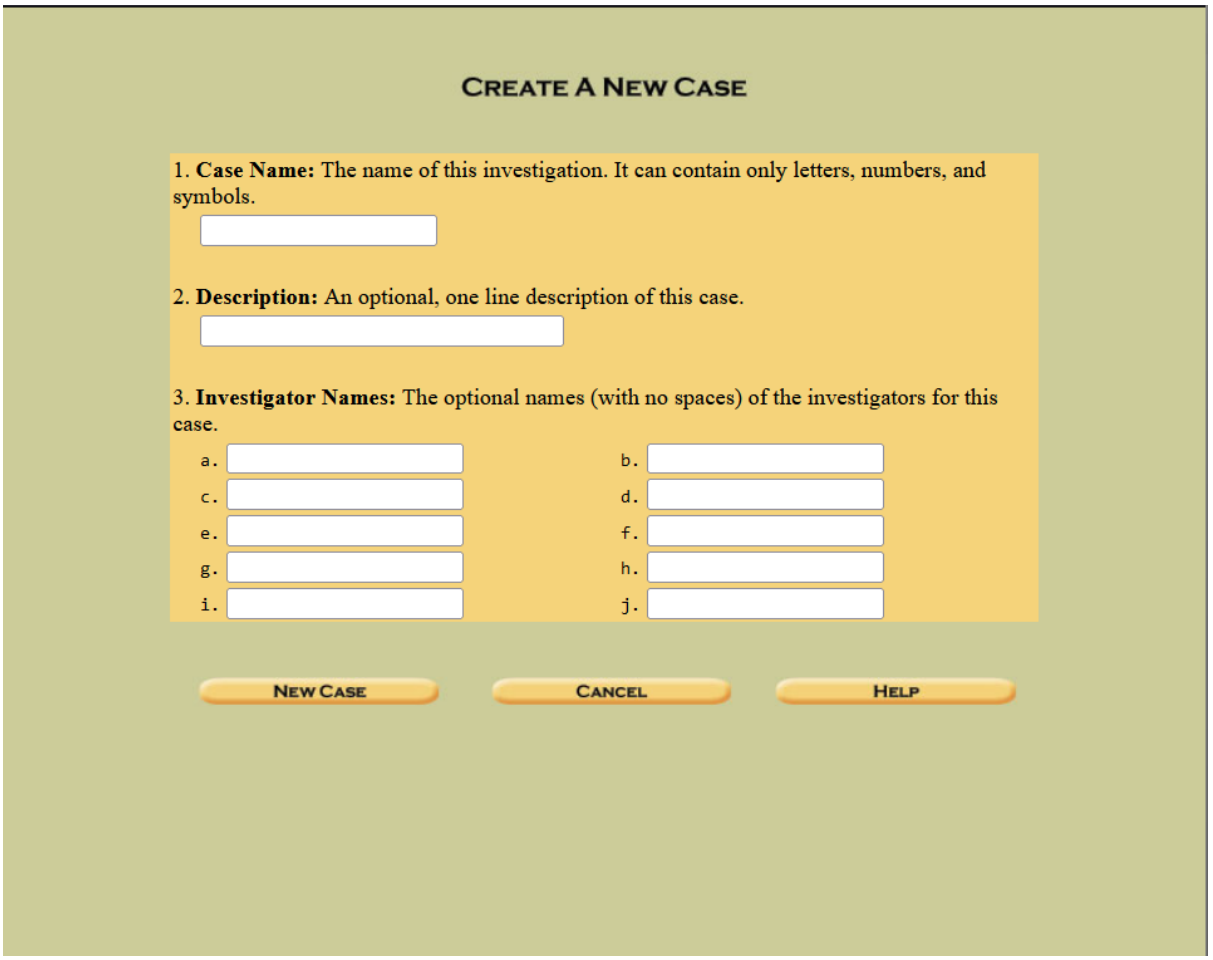
Reto 1:

Primero instalamos autopsy:

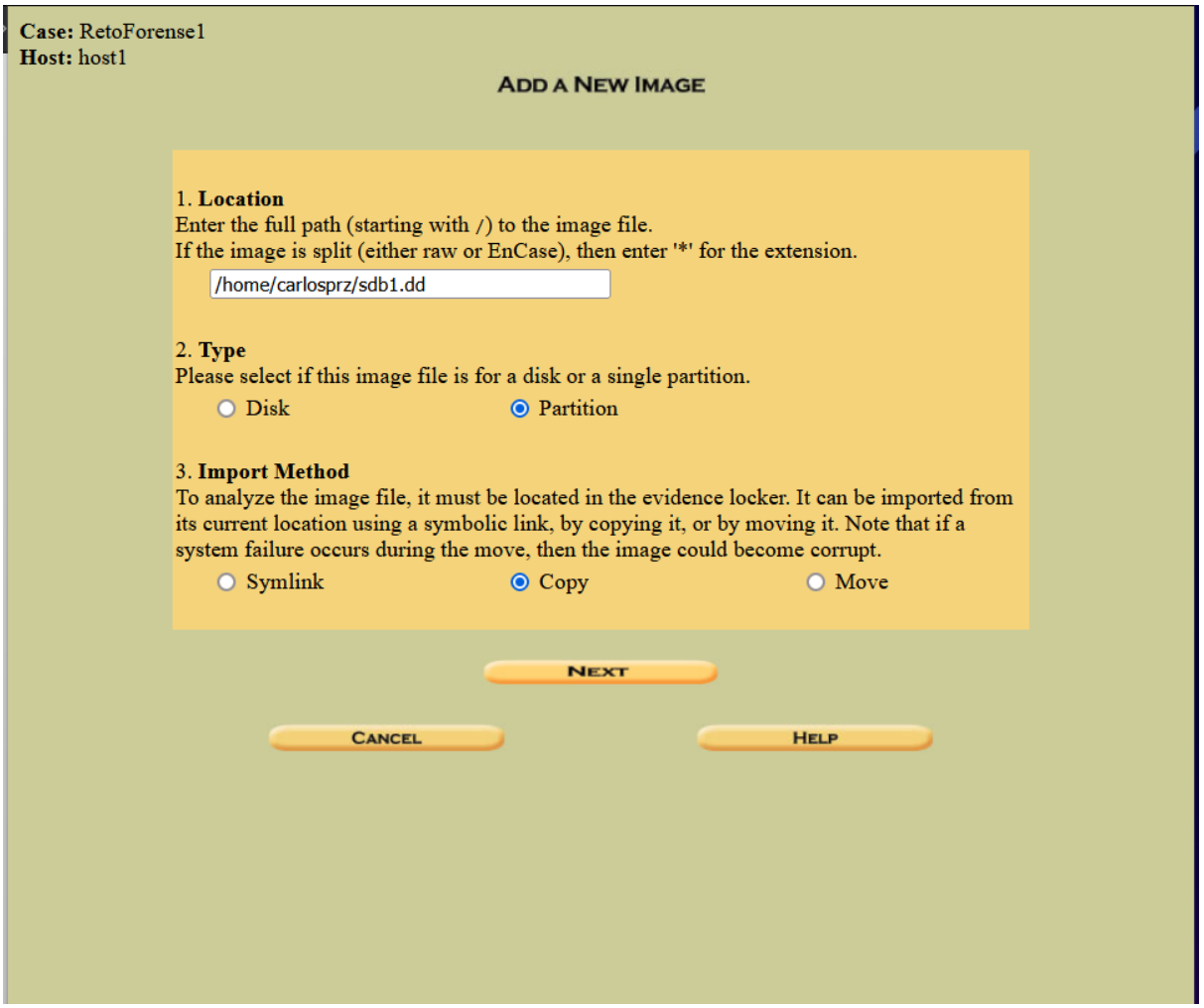
```
carlosprz@ROGStrix-Carlos:~$ sudo apt  install autopsy  # version 2.24-5
[sudo] password for carlosprz:
```

```
carlosprz@ROGStrix-Carlos:~$ sudo autopsy

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

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

================================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Fri Jan  5 20:25:37 2024
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
```

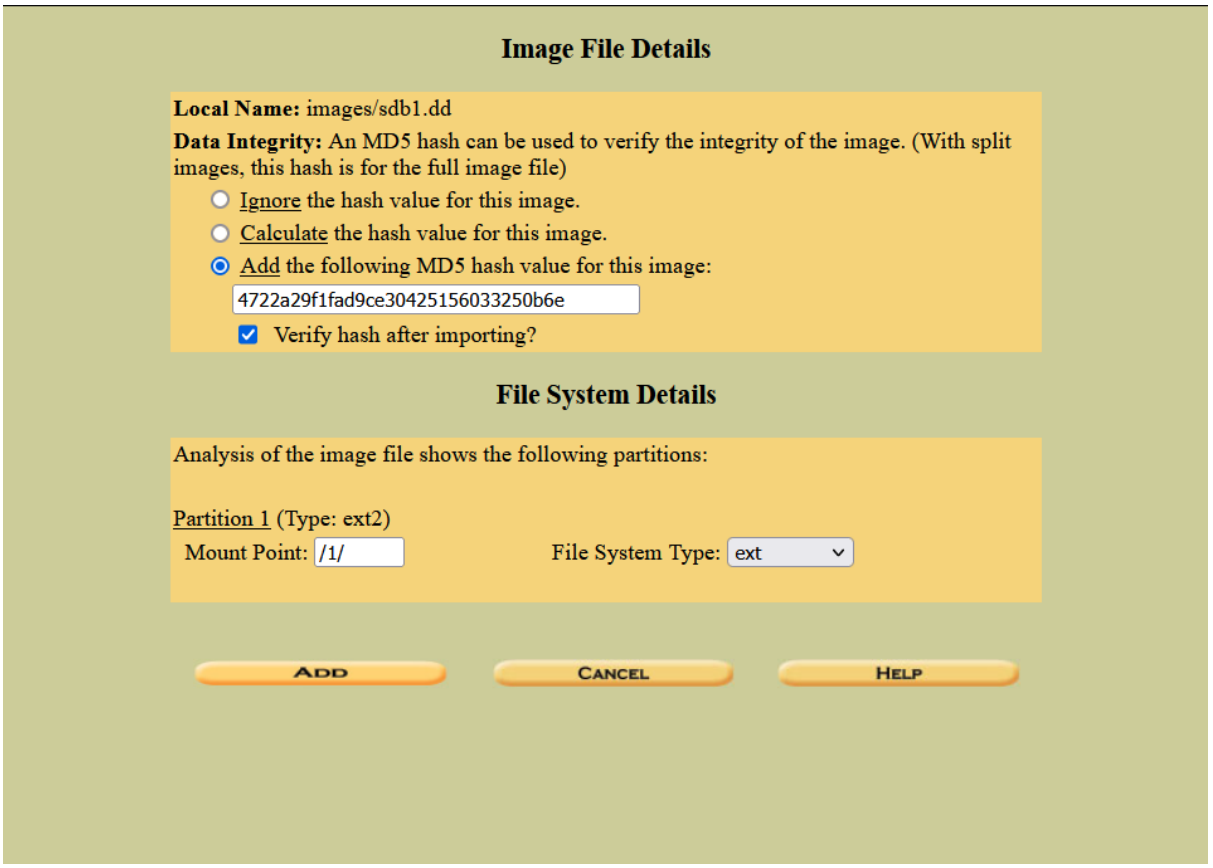
Creamos un nuevo caso:

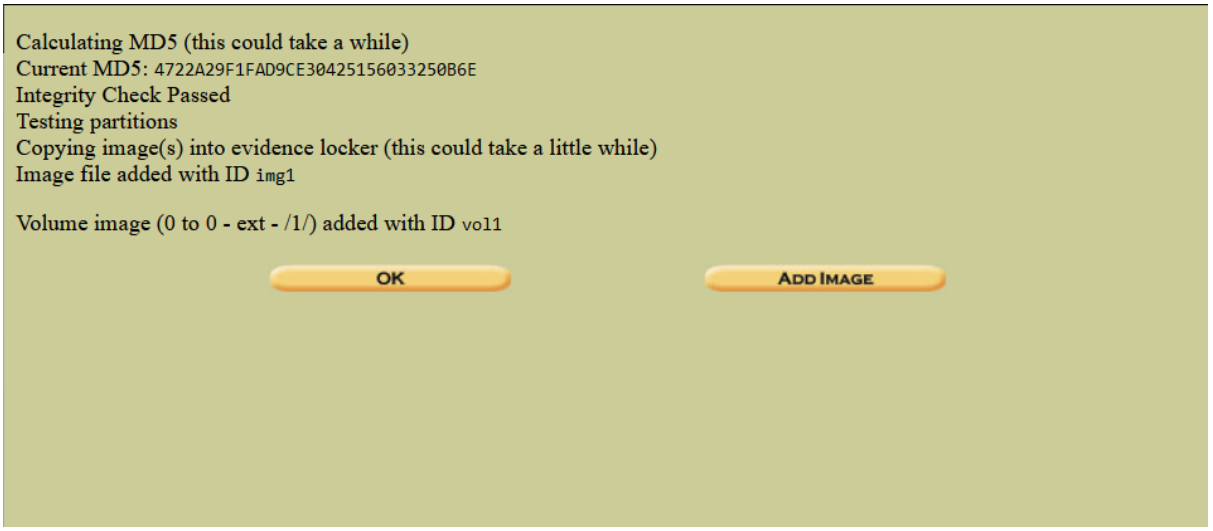


El programa nos pide a continuación la imagen a incorporar al caso y el método de importación que preferimos:

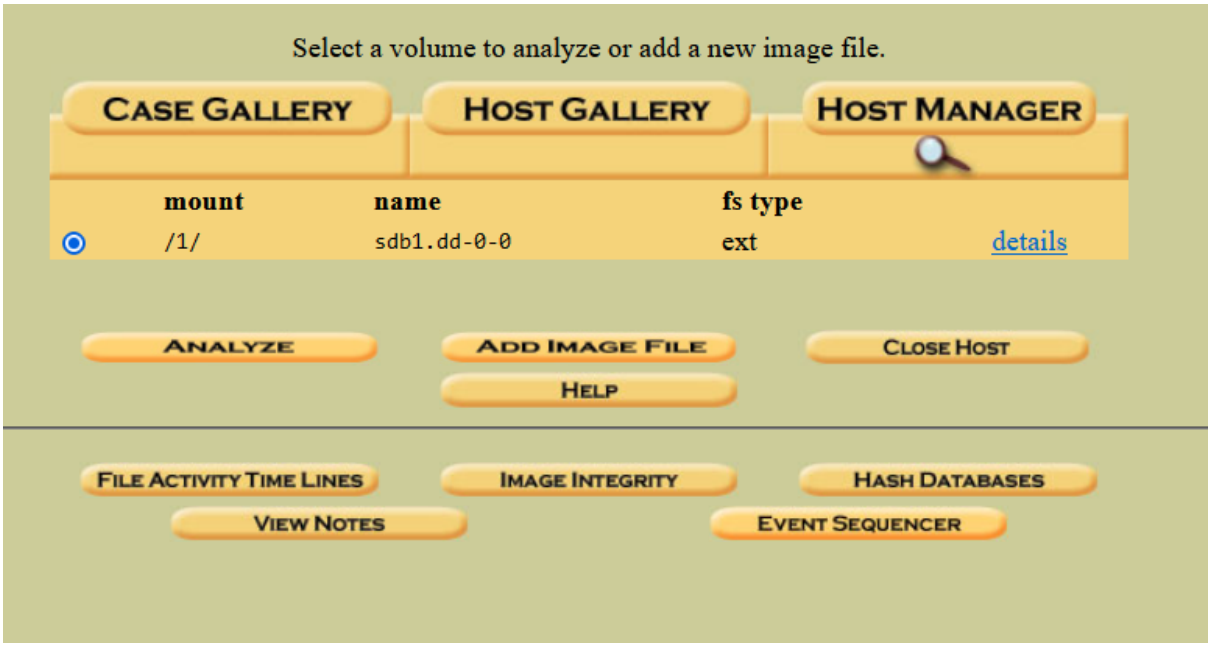


Nos solicita los detalles de la imagen. Como disponemos del hash md5 lo proporcionamos y le decimos que lo verifique después de importar la imagen:



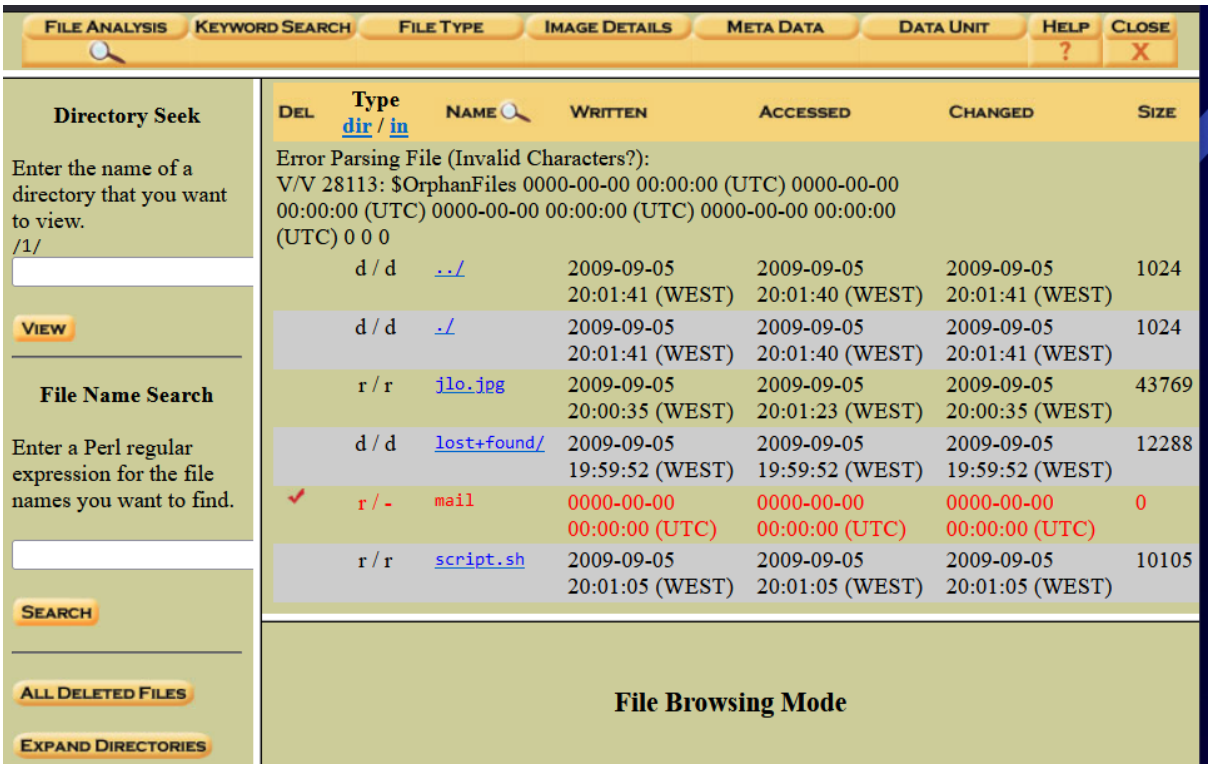


Después de verificar que la imagen ha sido importada correctamente ya podemos pulsar "OK" para ir a la ventana principal de gestión de casos "Host Manager" donde podemos comenzar con el análisis del pendrive:

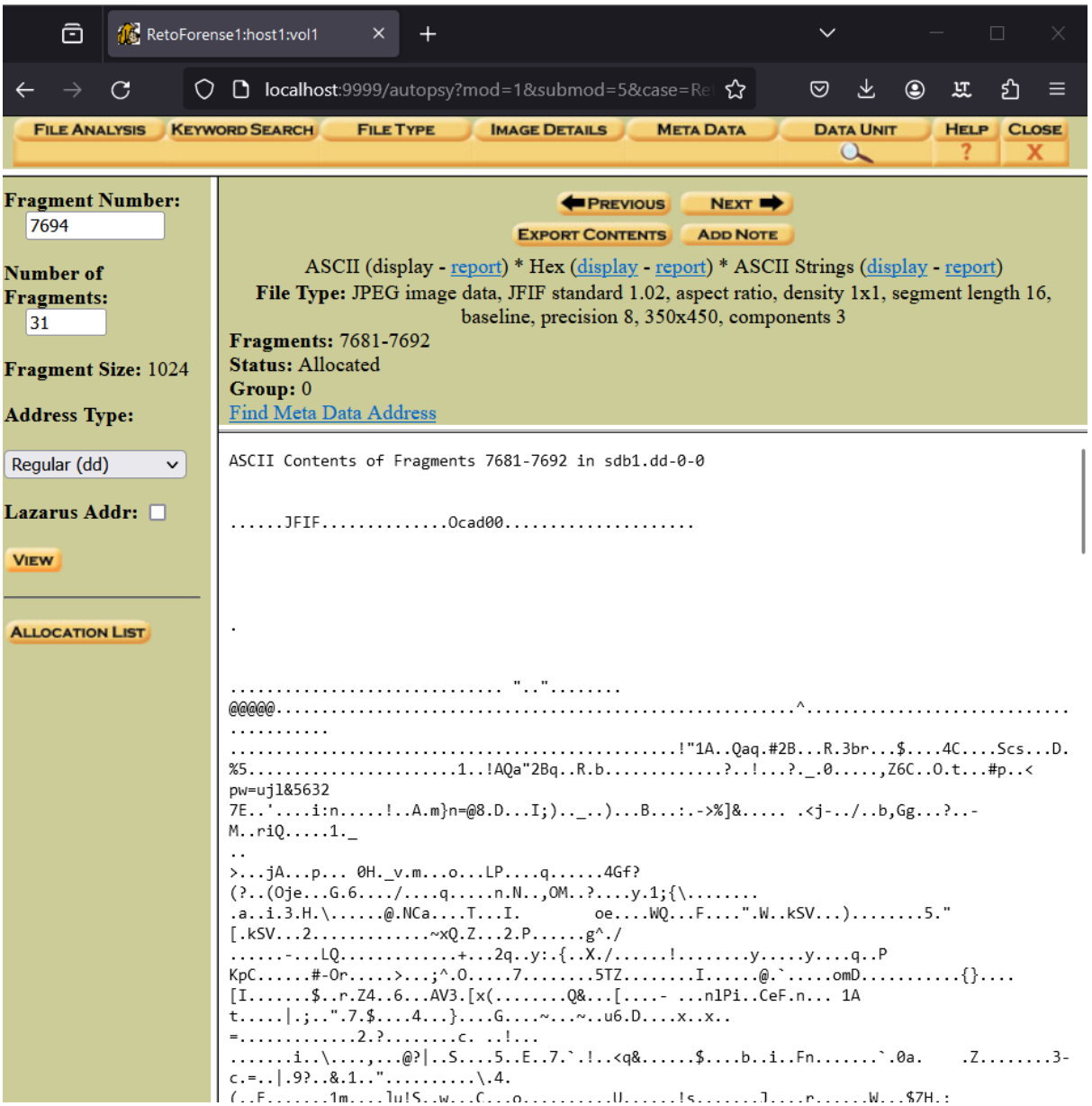


Seleccionamos ahora "File Analysis" del menú. Nos presenta el listado de los archivos y directorios encontrados en el volumen:

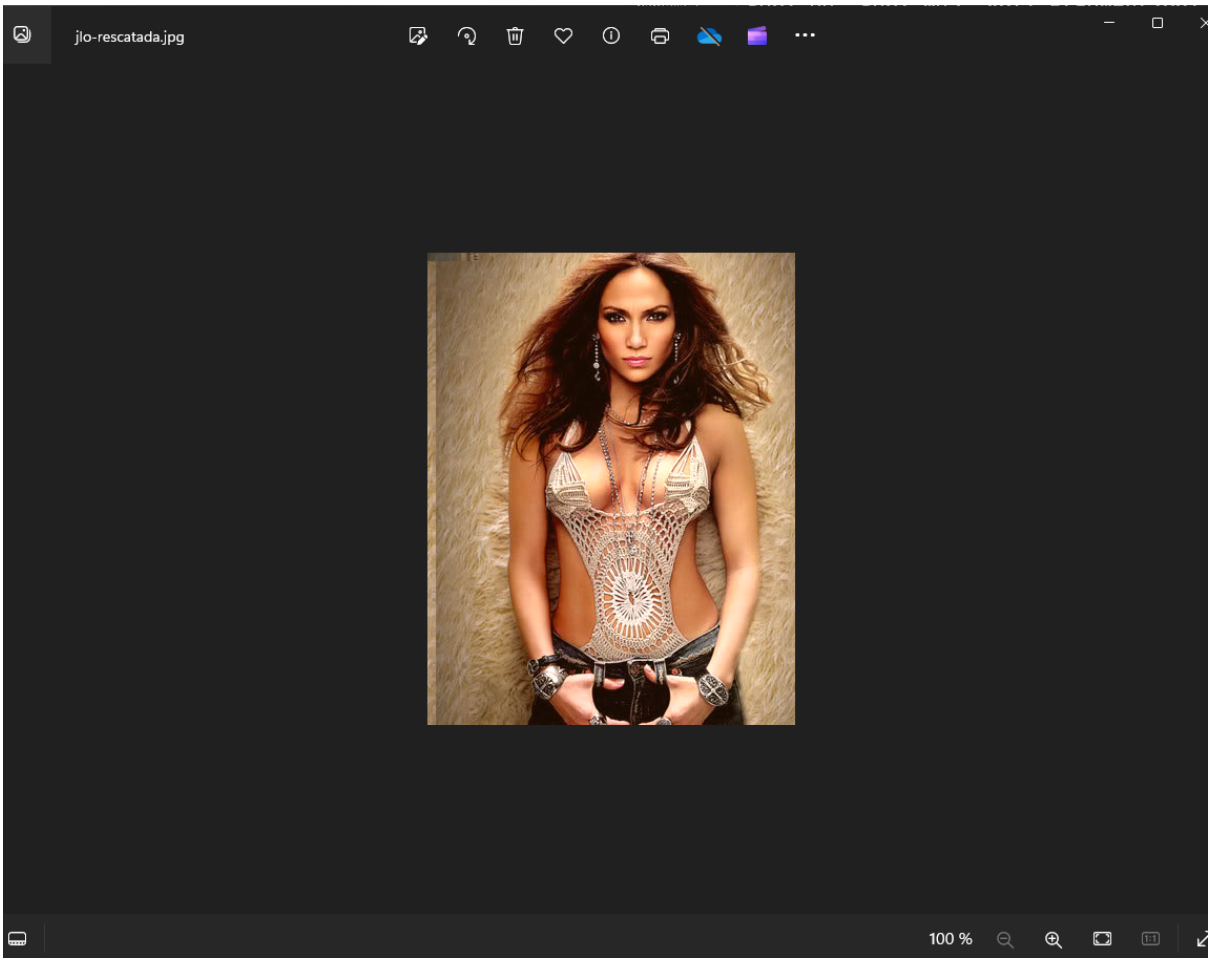
Empezaremos con el archivo .jpg.



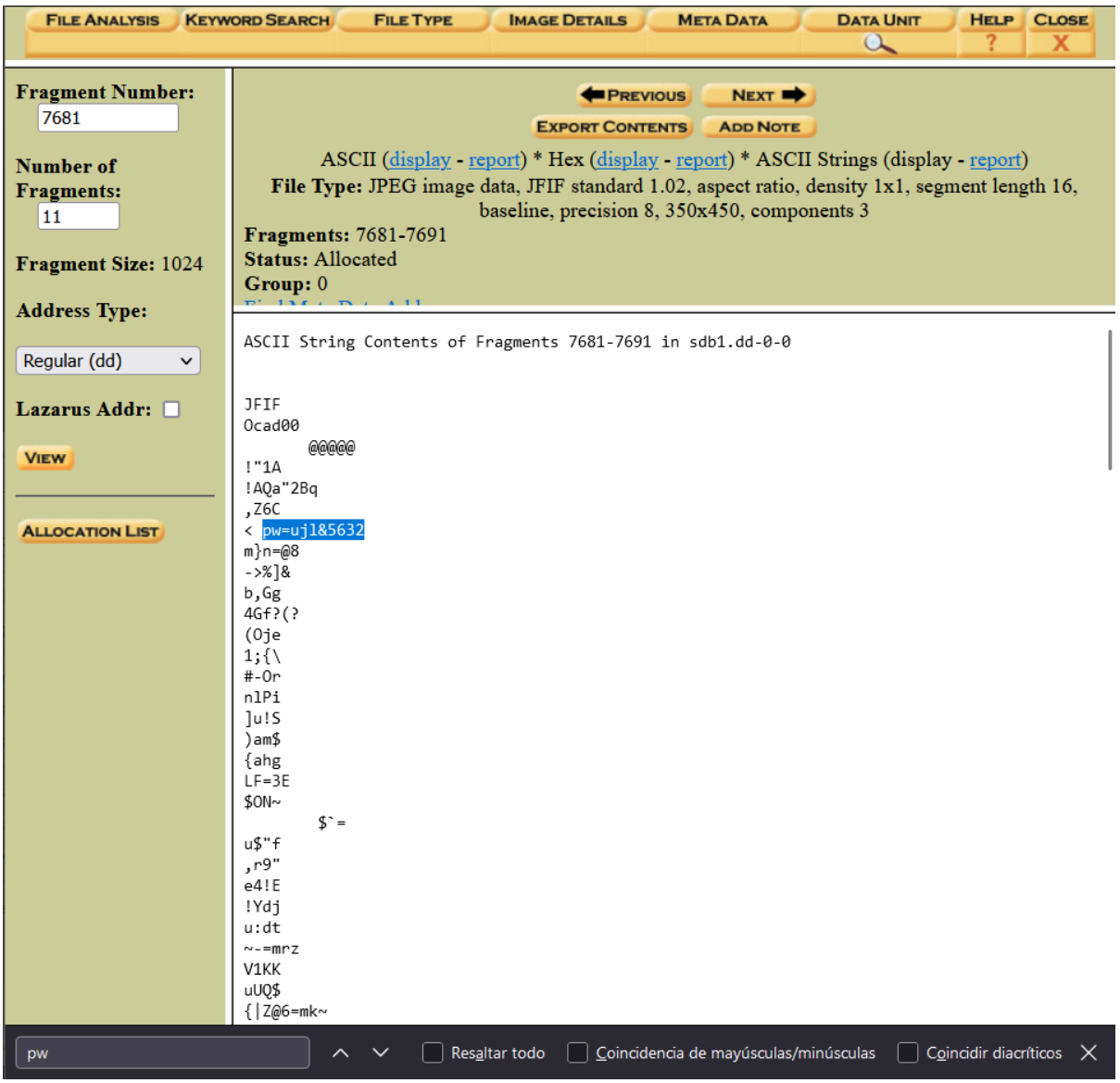
Separamos los bloques del archivo .jpg para quitar los que no son necesarios y luego unirlos para obtener la imagen que queremos recuperar:

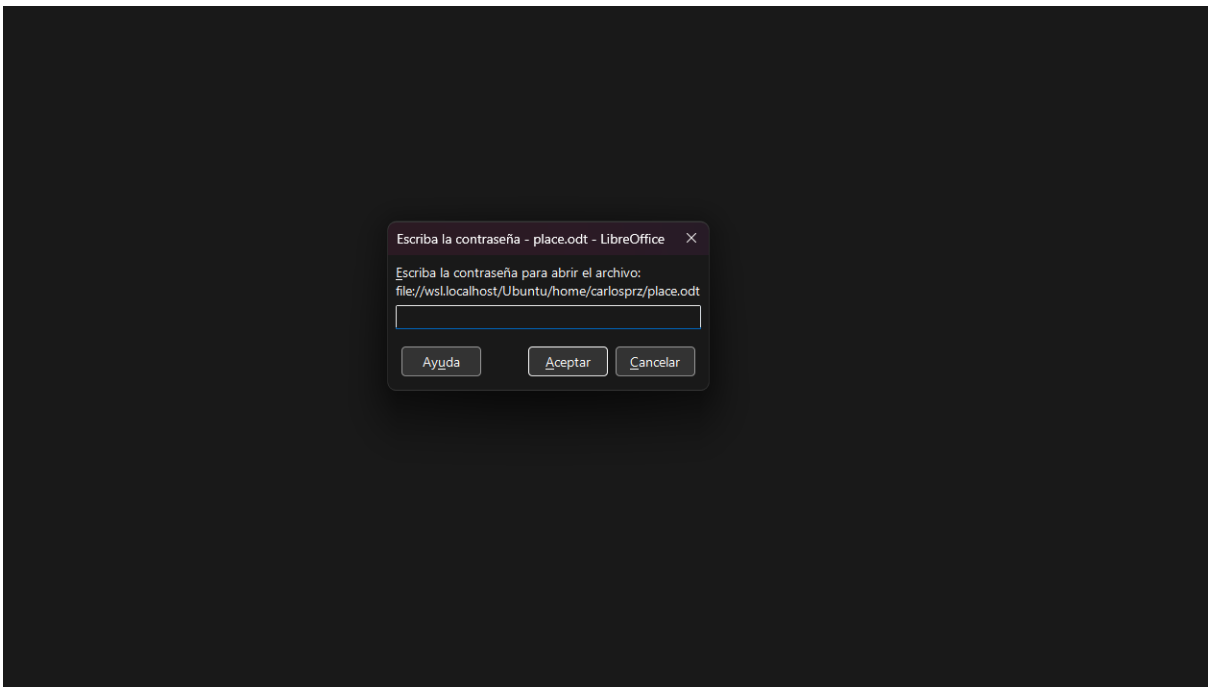


Obtenemos la imagen:



En esta parte accedemos al archivo script.sh, donde tenemos un archivo .odt en el cual tenemos que separar también sus bloques y volverlos a unir para entrar al documento, dicho documento nos pedirá una contraseña de acceso que la obtendremos mirando la información ASCII String de la imagen que extrajimos anterior:


FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Fragment Number:
7681
Number of Fragments:
11
Fragment Size: 1024
Address Type:
Regular (dd)
Lazarus Addr:
VIEW
ALLOCATION LIST
PREVIOUS
NEXT
EXPORT CONTENTS
ADD NOTE
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 350x450, components 3
Fragments: 7681-7691
Status: Allocated
Group: 0
ASCII String Contents of Fragments 7681-7691 in sdb1.dd-0-0
JFIF
Ocad00
@@@@@
!"1A
!AQa"2Bq
,Z6C
< pw=ujl&5632
m}n=@8
->%]&
b,Gg
4Gf?(?
(Oje
1;{\
#-Or
nlPi
]u!S
)am$
{ahg
LF=3E
$ON~
$`=
u$"f
,r9"
e4!E
!Ydj
u:dt
~-=mrz
V1KK
uUQ$
{|Z@6=mk~
pw
Resaltar todo
Coincidencia de mayúsculas/minúsculas
Coincidir diacríticos



Lugar de la entrega:

La entrega se hará en el garaje de la Calle Roma nº7

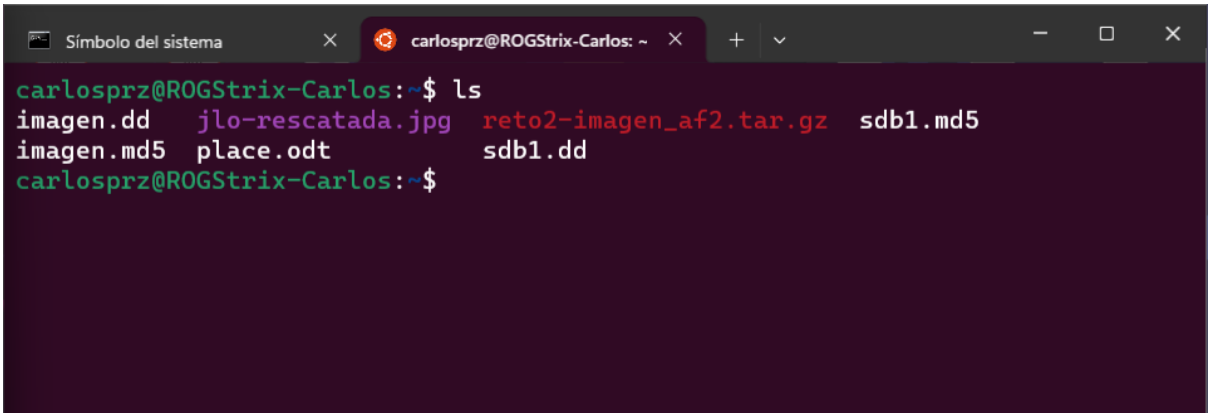
Es hora de mirar al resto del espacio de la unidad. Volvemos a la página principal de análisis y entramos en “Keyword Search”. Seleccionamos la búsqueda predefinida “Date” y obtenemos un resultado que parece corresponder con un mensaje ya borrado:

```
ASCII Contents of Fragment 526 in sdb1.dd-0-0


Que pasa Osvaldo, esto est.. calentito, no queda nada para el asunto...
Te adjunto un file con la info sobre el sitio de entrega.
No llegues tarde, a las 02:00 en punto.

nos vemos man, ya queda menos...
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
......
```

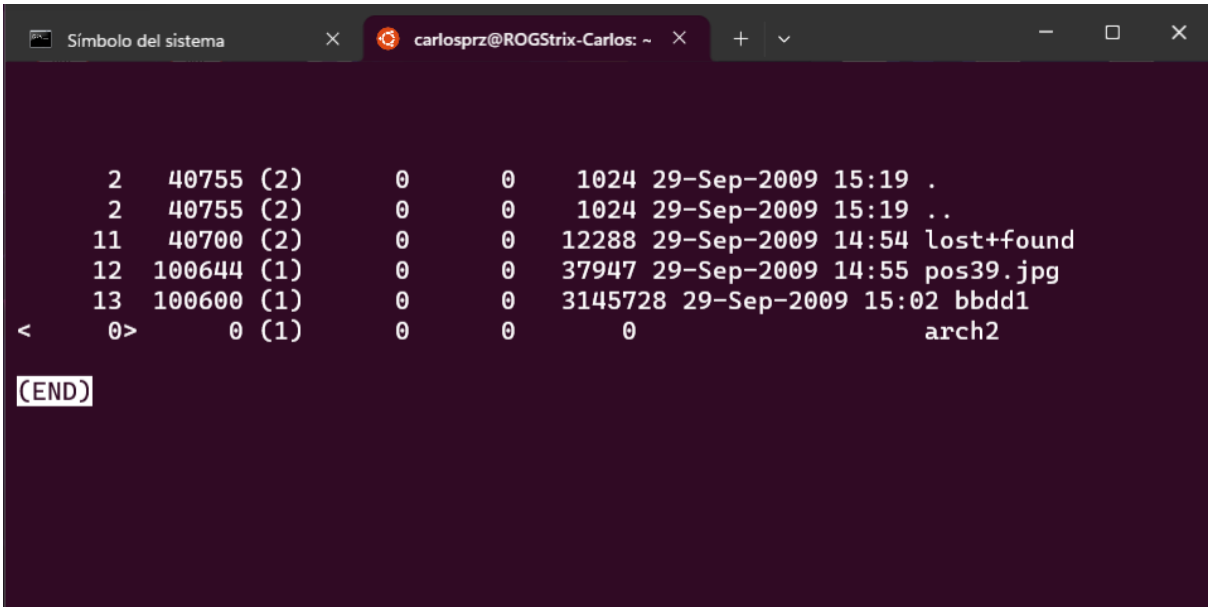
Y con la información obtenida sacamos las respuestas que se nos piden:
Hora de la entrega: 02:00
Nombre del jefe de la banda: Osvaldo.
Lugar del intercambio: En el garaje de la calle Roma nº 7

Reto 2:

Primero que hacemos es descomprimir el zip y comparar que coinciden los checksum:



A continuación procederemos a ver que hay dentro de este sistema de ficheros:
 # debugfs -w imagen.dd
Y una vez dentro, haciendo un simple ls -ld:



Problemas encontrados en la práctica:
Dada las pruebas, la práctica no se puede realizar ya que uno de los 3 archivos recuperados está vacío. Además, añadir que TrueCrypt ya no mantiene soporte y se encuentra desactualizado.

Se han realizado varias pruebas en distintas versiones de Linux(23.04 y 18.10), y en ninguna de ellas se ha podido ejecutar el programa. Por lo tanto, no se puede seguir realizando esta parte de la práctica.