



**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:

1

Reto 2:

13



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:

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"/>	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"/>



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

Case: RetoForensel
Host: host1

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**



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:

Image File Details

Local Name: images/sdb1.dd

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: ext2)

Mount Point: File System Type:

Calculating MD5 (this could take a while)

Current MD5: 4722A29F1FAD9CE30425156033250B6E

Integrity Check Passed

Testing partitions

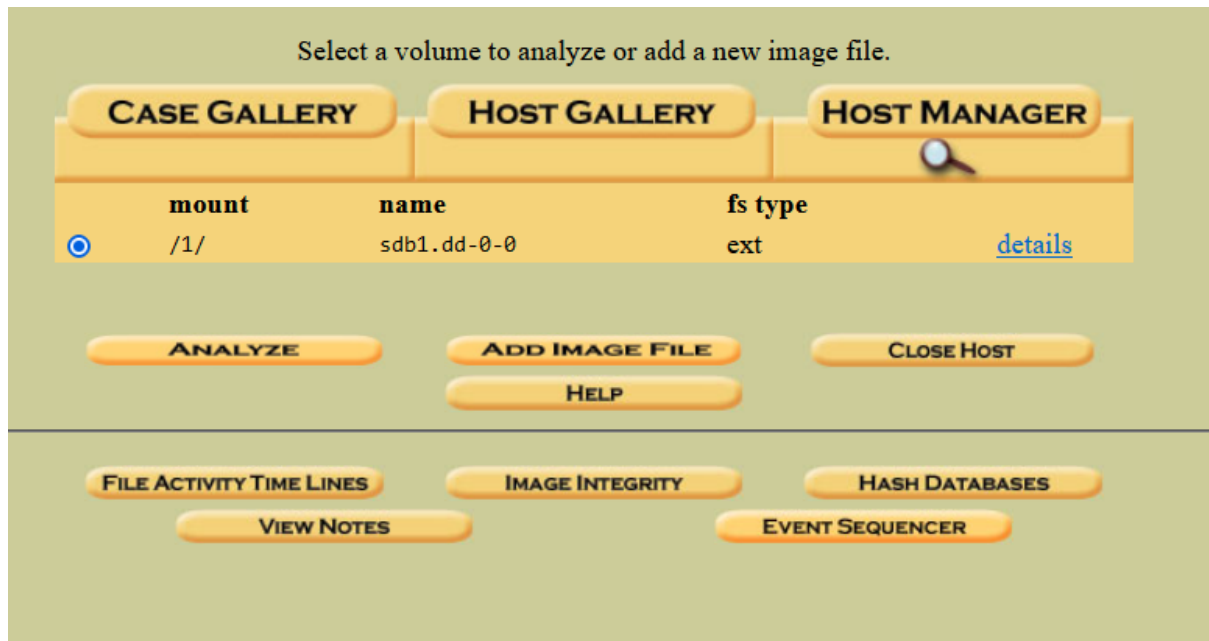
Copying image(s) into evidence locker (this could take a little while)

Image file added with ID img1

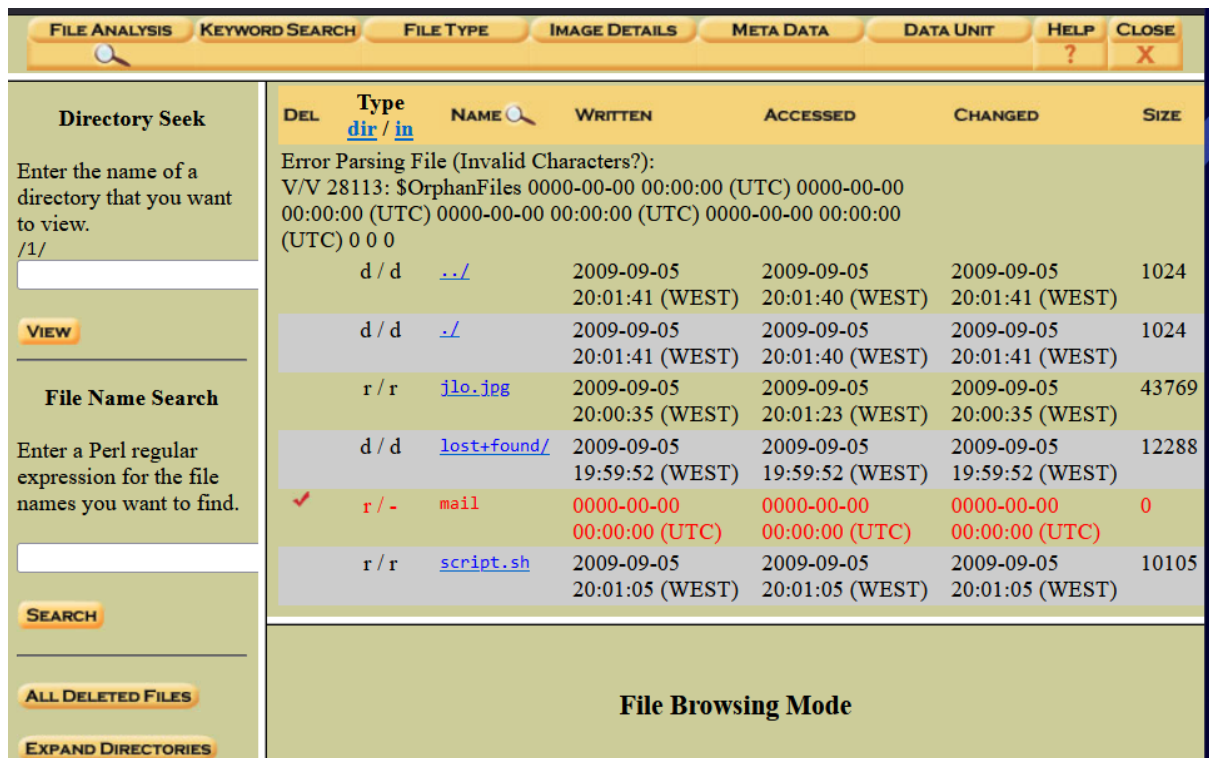
Volume image (0 to 0 - ext - /1/) added with ID vol1



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.



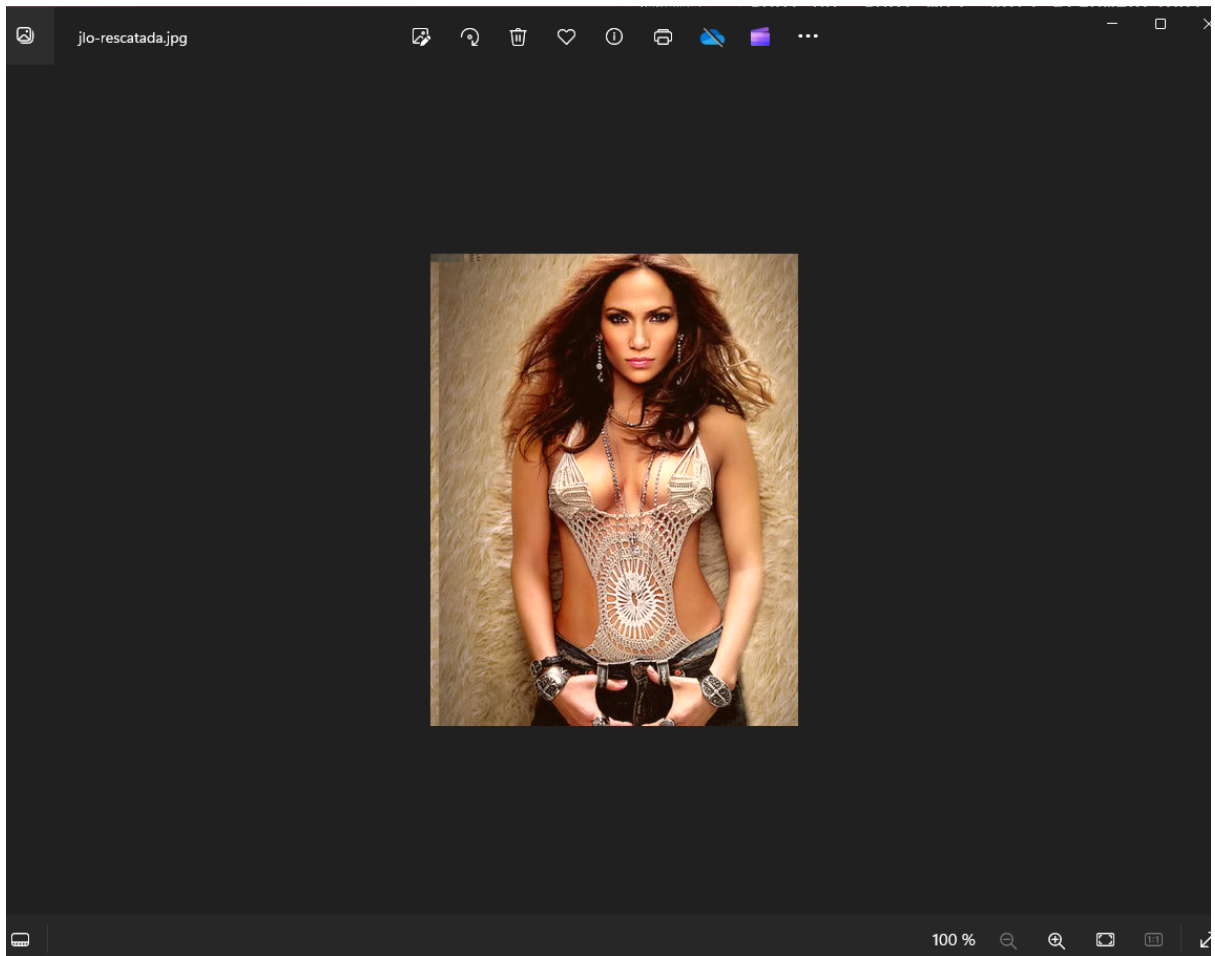


Separamos los bloques del archivo .jpg para quitar los que no son necesarios y luego unirlos para obtener la imagen que queremos recuperar:

The screenshot shows the RetoForensis web interface. The browser address bar displays `localhost:9999/autopsy?mod=1&submod=5&case=Re`. The interface has a top navigation bar with tabs: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. The left sidebar contains fields for: Fragment Number (7694), Number of Fragments (31), Fragment Size (1024), Address Type (Regular (dd)), and Lazarus Addr (unchecked). Below these is a VIEW button and an ALLOCATION LIST button. The main content area shows: PREVIOUS, NEXT, EXPORT CONTENTS, and ADD NOTE buttons. Text details include: 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: 7681-7692, Status: Allocated, Group: 0, and a link to Find Meta Data Address. The bottom section, titled 'ASCII Contents of Fragments 7681-7692 in sdb1.dd-0-0', displays a large block of ASCII text, which appears to be a corrupted or encoded image file header and metadata.



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=uj1&5632
m}n=@8
->%]&
b,Gg
4Gf?(?
(0je
1;{\n
#-0r
n1Pi
]u!S
)am\$
{ahg
LF=3E
\$ON~
\$`=
u\$"f
,r9"
e4!E
!Ydj
u:dt
~-mrz
V1KK
uUQ\$
{|Z@6=mk~

pw

^

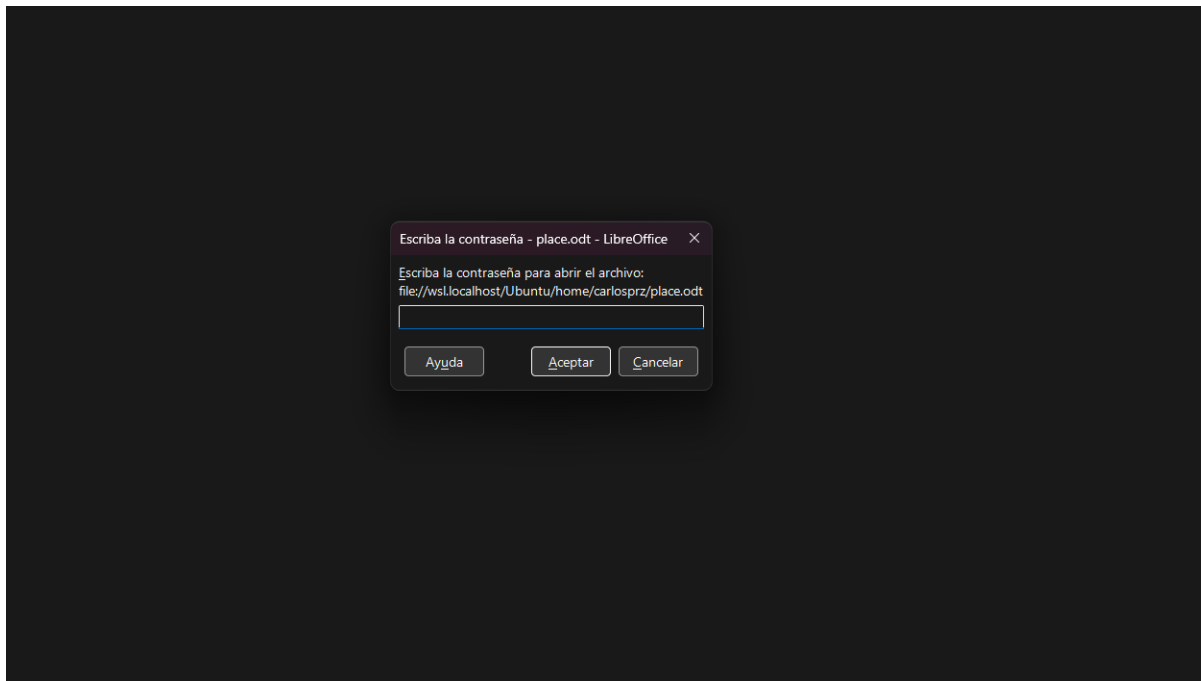
v

☐ Resaltar todo

☐ Coincidencia de mayúsculas/minúsculas

☐ Coincidir diacríticos

X



Lugar de la entrega:

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



Reto 2:

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

```
carlosprz@ROGStrix-Carlos: ~$ ls
imagen.dd      jlo-rescatada.jpg  reto2-imagen_af2.tar.gz  sdb1.md5
imagen.md5     place.odt          sdb1.dd
carlosprz@ROGStrix-Carlos: ~$

carlosprz@ROGStrix-Carlos: ~$ sudo cat imagen.md5
f266485f8a7f0efcb7c0cc1f93a0446a  imagen.dd
carlosprz@ROGStrix-Carlos: ~$ md5sum imagen.dd
f266485f8a7f0efcb7c0cc1f93a0446a  imagen.dd
carlosprz@ROGStrix-Carlos: ~$
```



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:

```
Símbolo del sistema  carlosprz@ROGStrix-Carlos: ~  
  
  2  40755 (2)      0      0    1024 29-Sep-2009 15:19 .  
  2  40755 (2)      0      0    1024 29-Sep-2009 15:19 ..  
 11  40700 (2)      0      0   12288 29-Sep-2009 14:54 lost+found  
 12 100644 (1)      0      0   37947 29-Sep-2009 14:55 pos39.jpg  
 13 100600 (1)      0      0  3145728 29-Sep-2009 15:02 bbdd1  
<  0>      0 (1)      0      0      0  
                                arch2  
  
(END)
```

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.