

# Prácticas de Laboratorio

Informática Forense y Auditoría

**Hugo Fonseca Díaz**

UO258318

[uo258318@uniovi.es](mailto:uo258318@uniovi.es)

Convocatoria Junio-Julio 2021.



Universidad de Oviedo

*Universidá d'Uviéu*

*University of Oviedo*

Escuela de Ingeniería Informática

Universidad de Oviedo

España

28 de junio de 2021

# Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Práctica 02</b>	<b>3</b>
2.1. Ejercicio 27 . . . . .	3
2.2. Ejercicio 31 . . . . .	6
<b>3. Práctica 03</b>	<b>15</b>
3.1. Ejercicio 8 . . . . .	15
3.2. Ejercicio 13 . . . . .	22
3.3. Ejercicio 14 . . . . .	34
3.4. Ejercicio 19 . . . . .	43
3.4.1. Imagen 1 . . . . .	44
3.4.2. Imagen 2 . . . . .	48
3.4.3. Imagen 3 . . . . .	50
3.4.4. Imagen 4 . . . . .	52
3.4.5. Imagen 5 . . . . .	54
<b>4. Práctica 04</b>	<b>56</b>
4.1. Ejercicio 7 . . . . .	56
<b>5. Práctica 05</b>	<b>72</b>
5.1. Ejercicio 5 . . . . .	72
5.2. Ejercicio 25 . . . . .	79
5.3. Ejercicio 31 . . . . .	83
<b>6. Índice de figuras</b>	<b>90</b>

# 1. Introducción

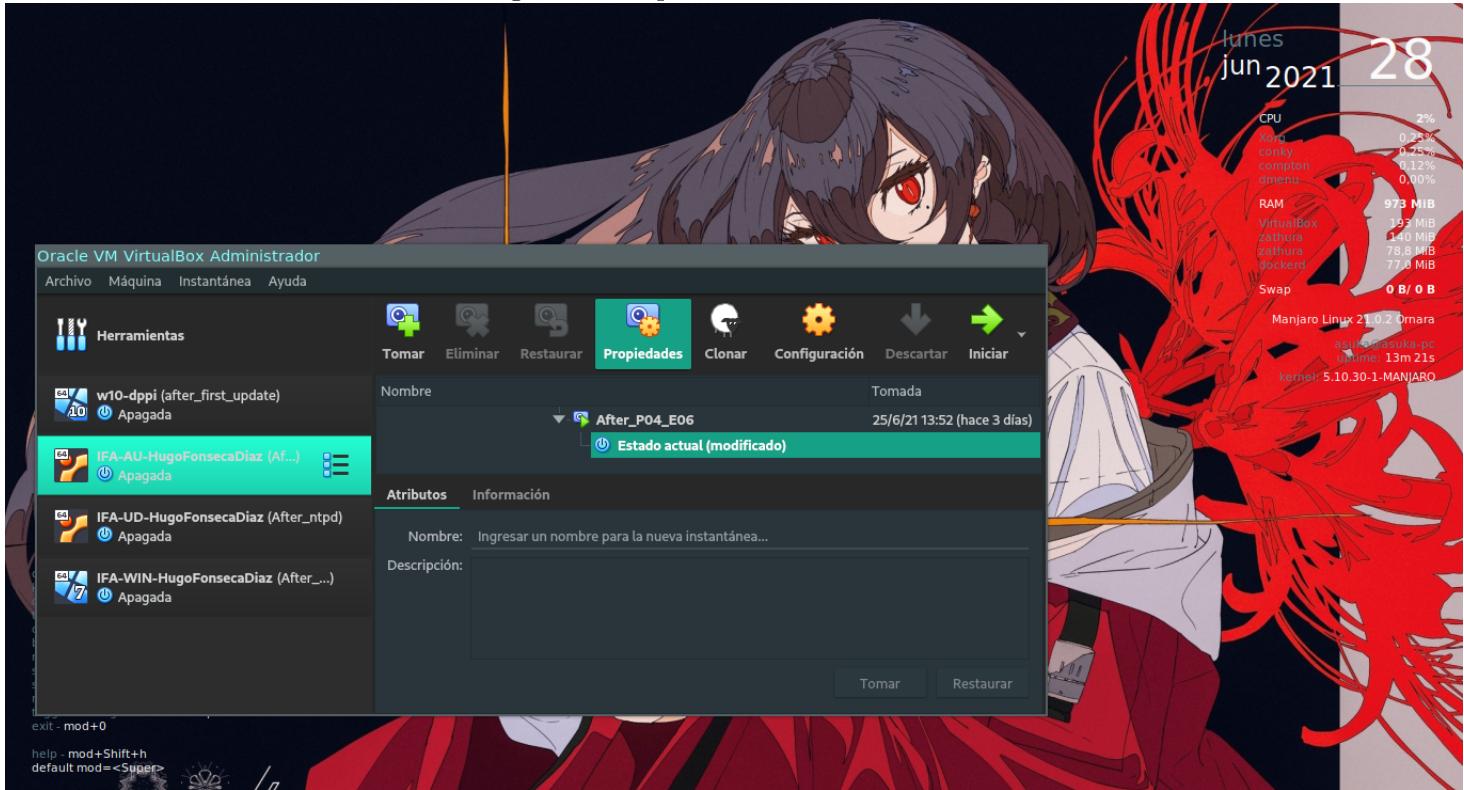
Los ejercicios de este documento se han realizado en una máquina cuyas características se muestran en la siguiente captura.

Figura 1: Sistema del alumno Hugo Fonseca Díaz.



Las máquinas virtuales utilizadas pueden verse en la siguiente imagen.

Figura 2: Máquinas virtuales.



## 2. Práctica 02

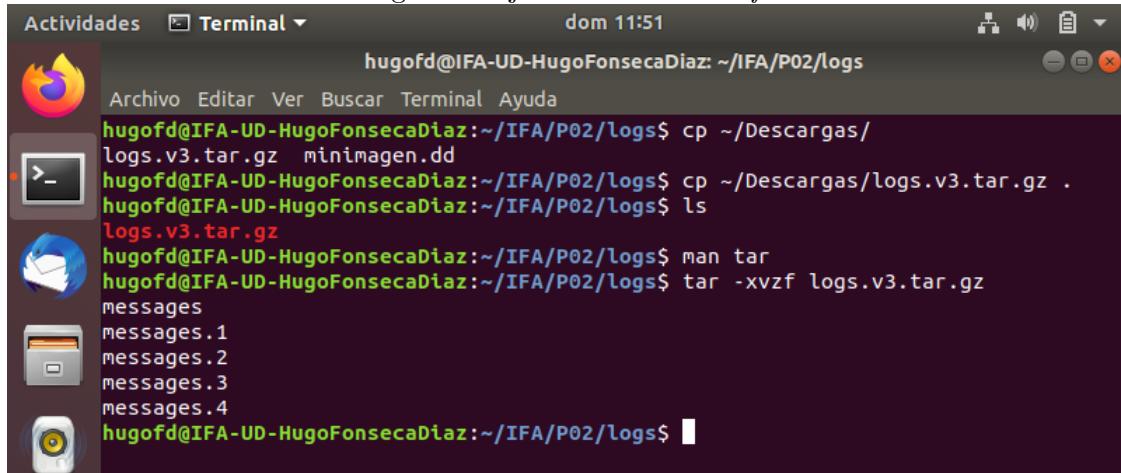
### 2.1. Ejercicio 27

Figura 3: Ejercicio 27: Enunciado.

Descargue del campus virtual el fichero denominado **Recursos de Prácticas->Práctica 2->logs.v3.tar.gz**. Destarea y descomprima el anterior archivo en una carpeta denominada logs. Deberás ver 5 ficheros de log de diferentes sistemas Unix. Estos ficheros de log contienen entradas correspondientes a una gran variedad de fuentes, incluyendo el kernel y otras aplicaciones. Crea un pipeline que muestre las fechas (mes y día) en las que ha habido apuntes en los respectivos logs de forma descendente (de más reciente a menos reciente) y que elimine las entradas múltiples (las repetidas para una misma fecha).

Se descomprime el archivo con el comando `tar` y las flags *xvzf*, siendo *x* una indicación de que se quiere extraer los contenidos del archivo comprimido, *v* para que lo haga de manera verbosa, *z* para indicarle al comando que el archivo es un zip y *f* para pasarle el fichero que se desea extraer al comando.

Figura 4: Ejercicio 27: `tar -xvzf`.



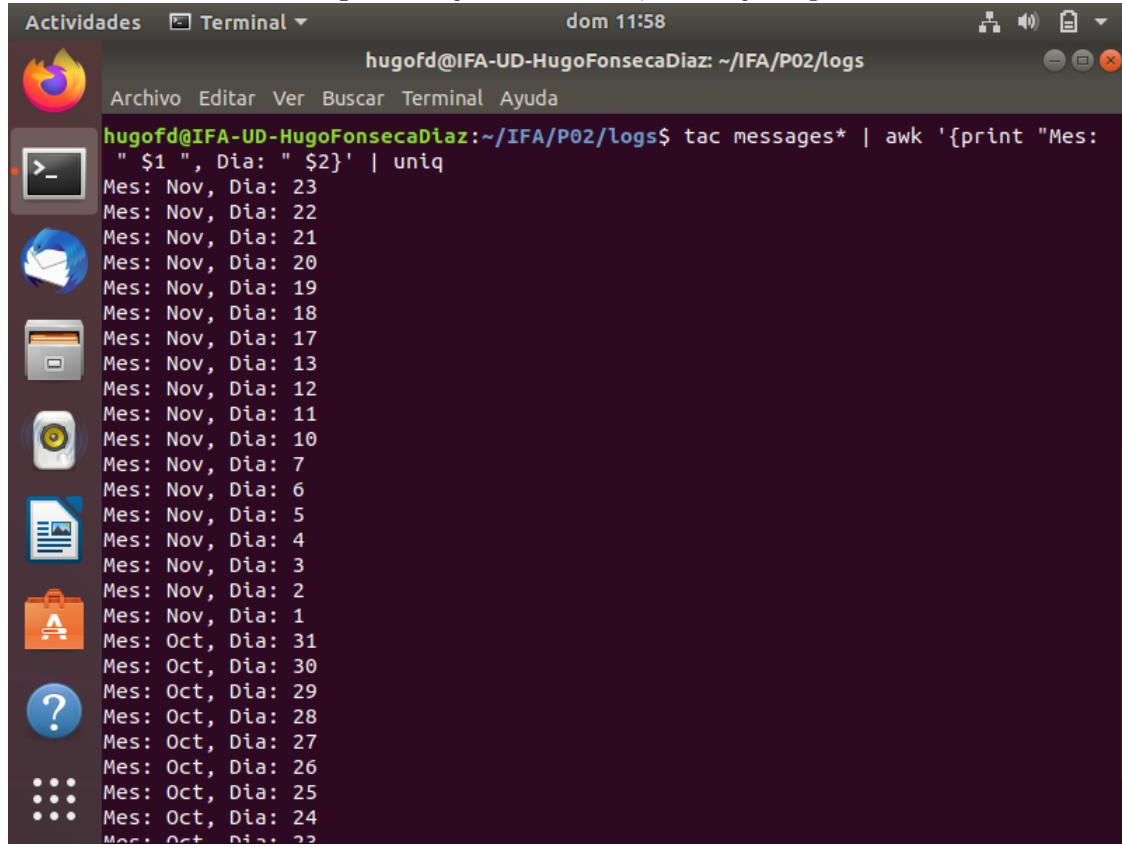
The screenshot shows a terminal window titled "Terminal" with the command line interface. The terminal window has a dark background with light-colored text. It displays the following sequence of commands and their output:

```
Actividades Terminal dom 11:51
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ cp ~/Descargas/
logs.v3.tar.gz minImagen.dd
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ cp ~/Descargas/logs.v3.tar.gz .
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ ls
logs.v3.tar.gz
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ man tar
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ tar -xvzf logs.v3.tar.gz
messages
messages.1
messages.2
messages.3
messages.4
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$
```

The terminal window also shows a sidebar with various application icons, including a browser, terminal, file manager, and others.

Una vez descomprimidos los ficheros de texto, se procede a utilizar tres nuevas herramientas. Se usa `tac` para concatenar ficheros de forma inversa (es el comando `cat` invertido), el lenguaje de programación AWK para procesar texto y el comando `uniq` para omitir líneas repetidas.

Figura 5: Ejercicio 27: *tac*, *AWK* y *uniq*.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title bar reads "Actividades Terminal" and "dom 11:58". The command entered is "hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs\$ tac messages\* | awk '{print \"Mes: \" \$1 \" , Dia: \" \$2}' | uniq". The output of the command is displayed in the terminal window, showing unique pairs of month and day from 1 to 23.

```
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ tac messages* | awk '{print "Mes: " $1 " , Dia: " $2}' | uniq
Mes: Nov, Dia: 23
Mes: Nov, Dia: 22
Mes: Nov, Dia: 21
Mes: Nov, Dia: 20
Mes: Nov, Dia: 19
Mes: Nov, Dia: 18
Mes: Nov, Dia: 17
Mes: Nov, Dia: 13
Mes: Nov, Dia: 12
Mes: Nov, Dia: 11
Mes: Nov, Dia: 10
Mes: Nov, Dia: 7
Mes: Nov, Dia: 6
Mes: Nov, Dia: 5
Mes: Nov, Dia: 4
Mes: Nov, Dia: 3
Mes: Nov, Dia: 2
Mes: Nov, Dia: 1
Mes: Oct, Dia: 31
Mes: Oct, Dia: 30
Mes: Oct, Dia: 29
Mes: Oct, Dia: 28
Mes: Oct, Dia: 27
Mes: Oct, Dia: 26
Mes: Oct, Dia: 25
Mes: Oct, Dia: 24
Mes: Oct, Dia: 23
```

## 2.2. Ejercicio 31

Figura 6: Ejercicio 31: Enunciado (I).

Descarga del campus virtual **Recursos de Prácticas->Práctica 2->RTR.E01**. Se trata de una imagen de un disco duro Western Digital realizada con el software forense EnCASE. Almacénelo en una carpeta de Evidencias. Abra la utilidad Autopsy desde **Menú->Forensic Tools->Autopsy**. Cree un nuevo caso desde el interfaz de Autopsy. Llame al nuevo caso de la siguiente manera: **EjercicioXX\_StringSearch\_Apellidos\_Nombre**, donde XX es el número del ejercicio que está realizando en este momento. En el número de caso ponga DDMMAAAA-XX donde DD es el día en el que realiza el ejercicio, MM es el número del mes actual y AAAA es el año actual, siendo XX el número del ejercicio que está realizando. Ponga su nombre y sus datos en la información del examinador (ponga en el correo su dirección de email de uniovi). Añada al caso la evidencia RTR.E01 como Imagen de Disco o fichero VM.

Investigue qué posibilidades ofrecen los módulos de ingestión de Autopsy siguientes: **File Type Identification, Keyword Search** y añádalos como módulos de ingestión de evidencia asociados al proyecto. En el módulo de ingestión **Keyword Search** cree una nueva lista de palabras denominada **RTR**. El caso que se está investigando es el robo y la destrucción de la nueva carta de menú de un conocido restaurante ruso. Lo único que recuerda el personal del restaurante son las secciones que contendría dicho menú, pero desconoce el contenido de cada una de ellas. Las cadenas a buscar son expresiones en inglés codificadas en Unicode UTF16BE y son las siguientes:

Figura 7: Ejercicio 31: Enunciado (II).

- Appetizers
- Soup
- Pancakes
- Meat pies and dumplings
- Meat and fish
- Cheese and milk products
- Beverages
- Dessert

Configure, en función de la información aportada, el módulo de ingestión de búsqueda de cadenas de Autopsy e intente reconstruir el menú robado tanto en inglés como los nombres de las diferentes entradas en ruso. Averigüe la fecha en la que fue confeccionado el documento del menú robado.

Se crea el caso en Autopsy con los datos solicitados.

Figura 8: Ejercicio 31: Creación del caso

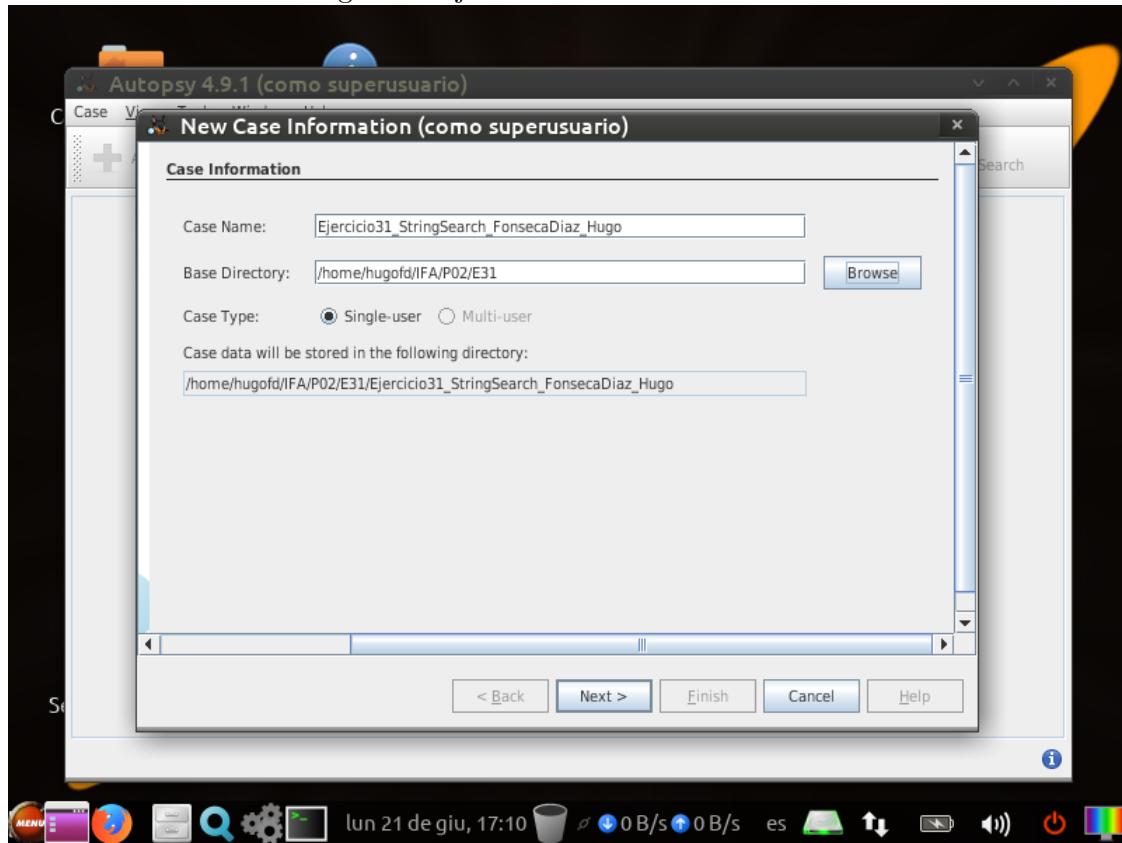
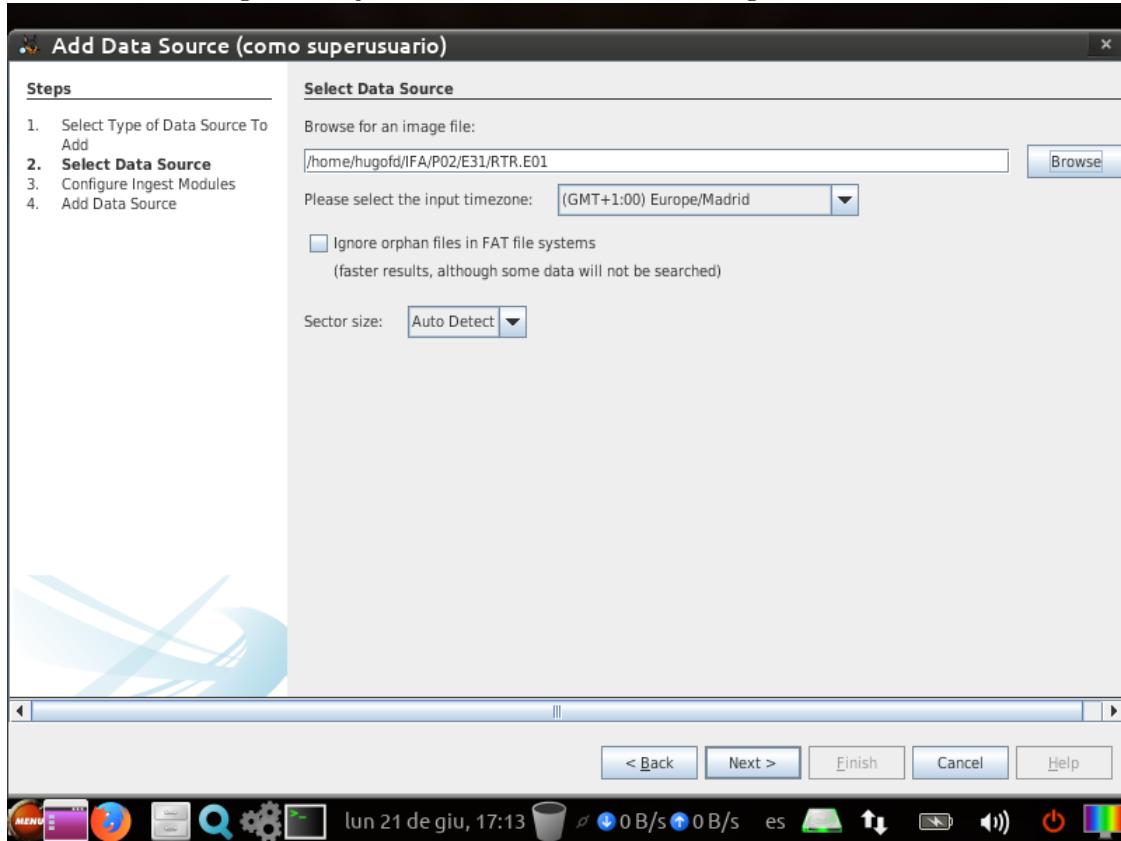


Figura 9: Ejercicio 31: Selección de la imagen a analizar



Se seleccionan los módulos y se configura el módulo de búsqueda de palabras clave.

Figura 10: Ejercicio 31: Palabras clave

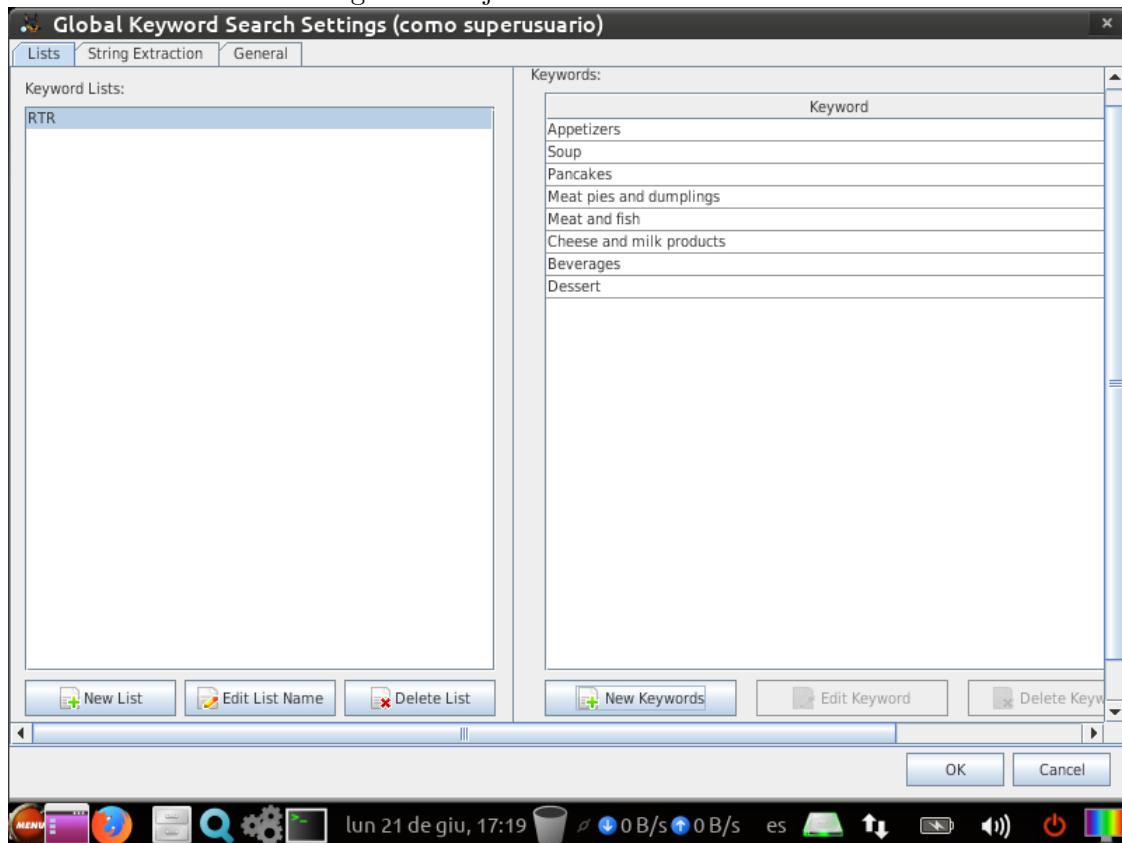


Figura 11: Ejercicio 31: Módulos seleccionados

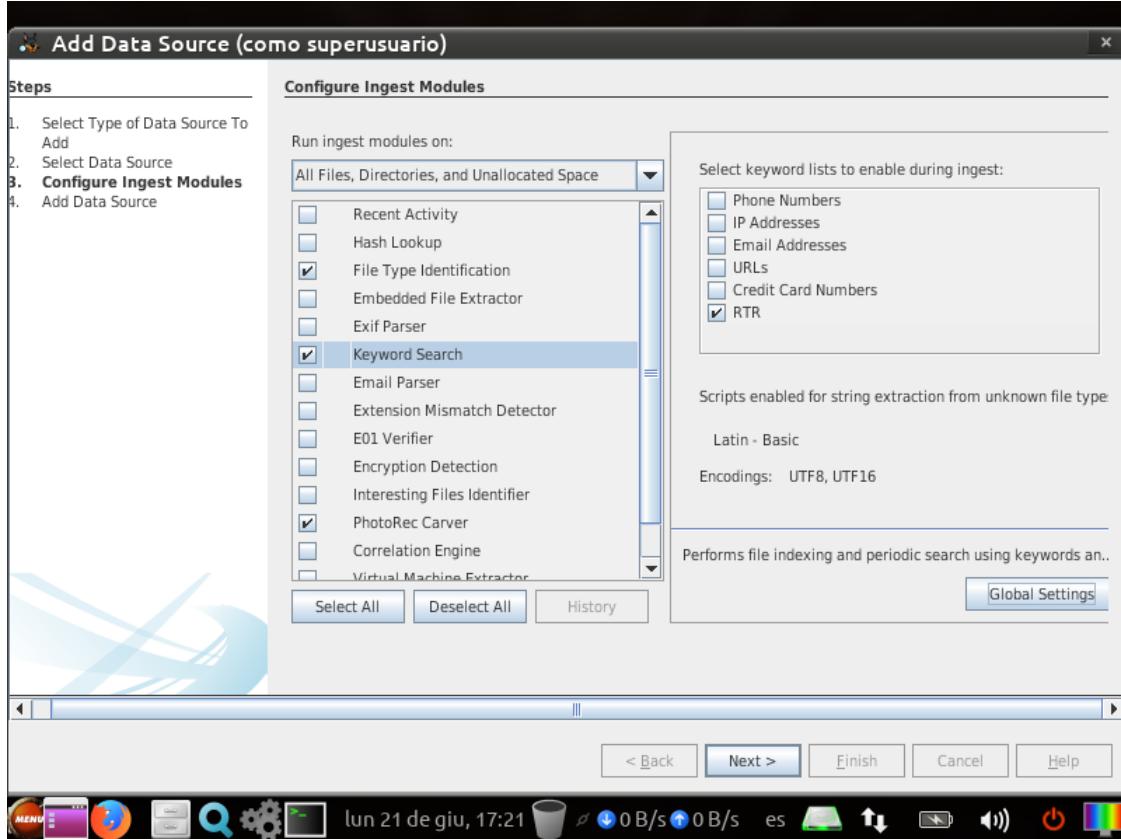
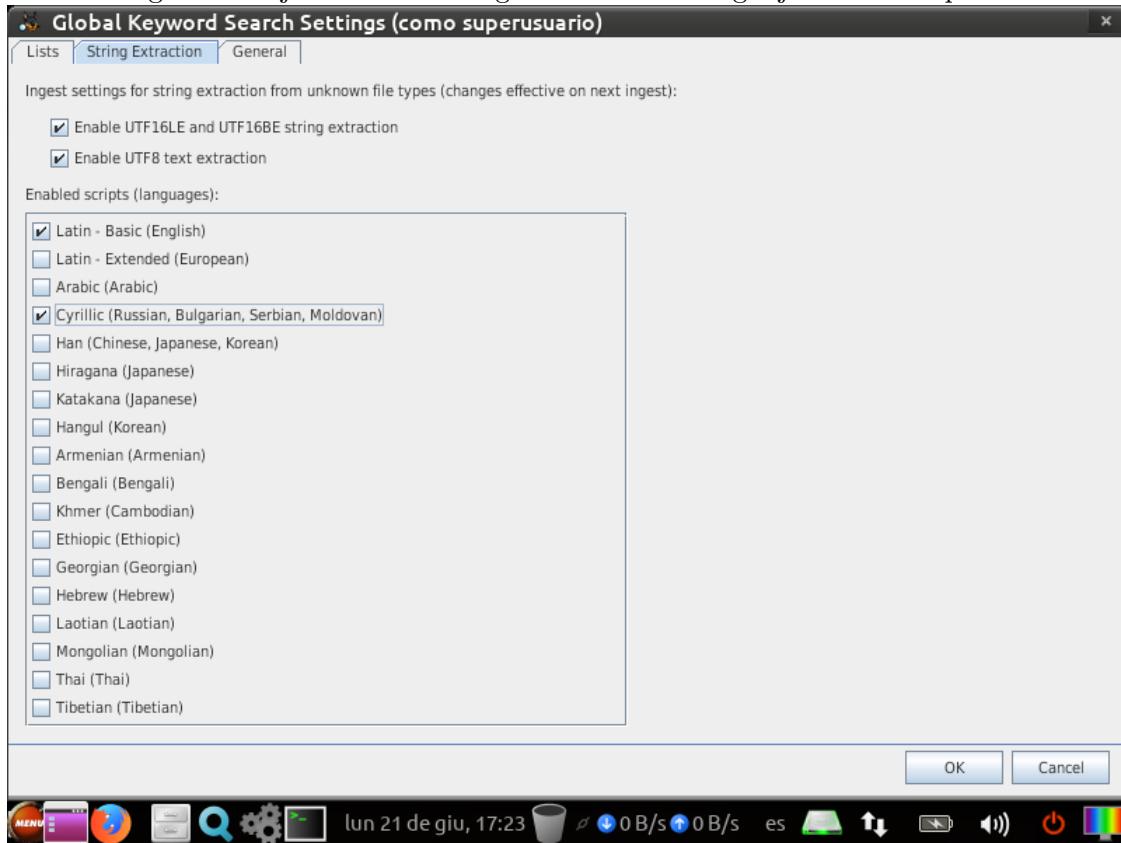
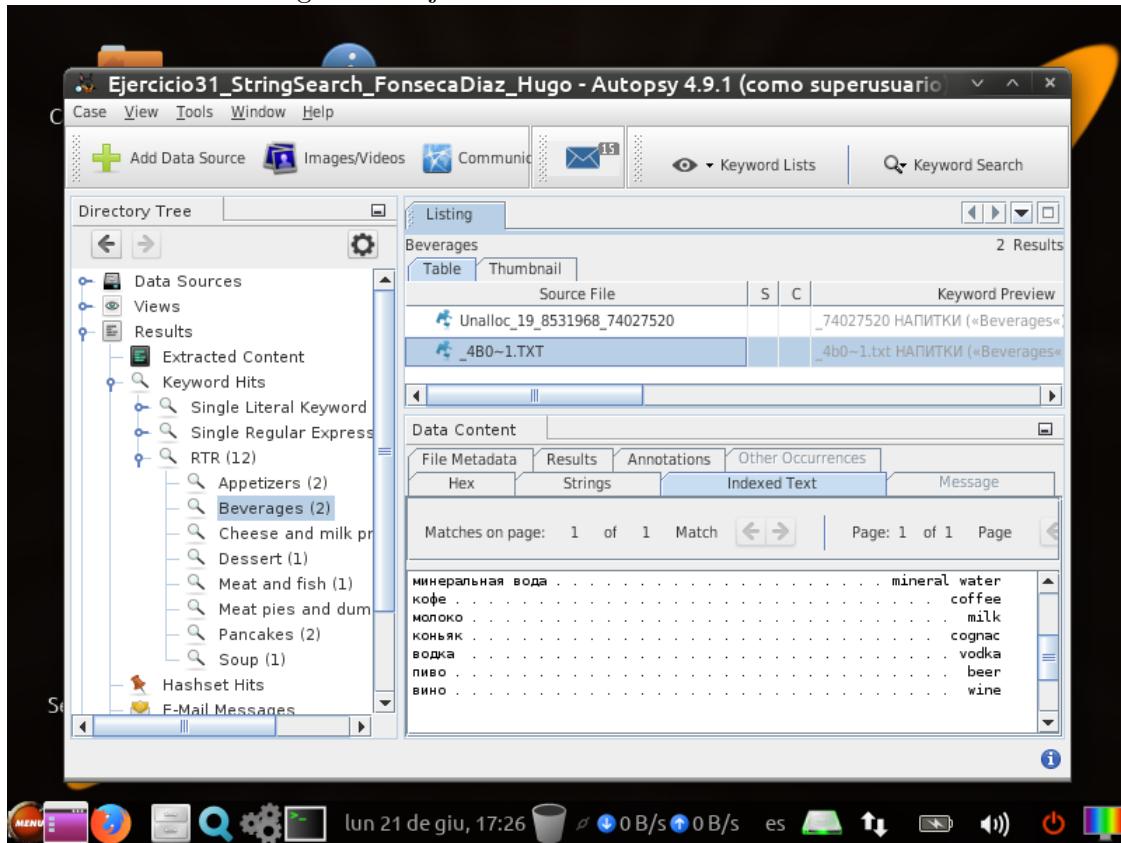


Figura 12: Ejercicio 31: Configuración de los lenguajes de la búsqueda



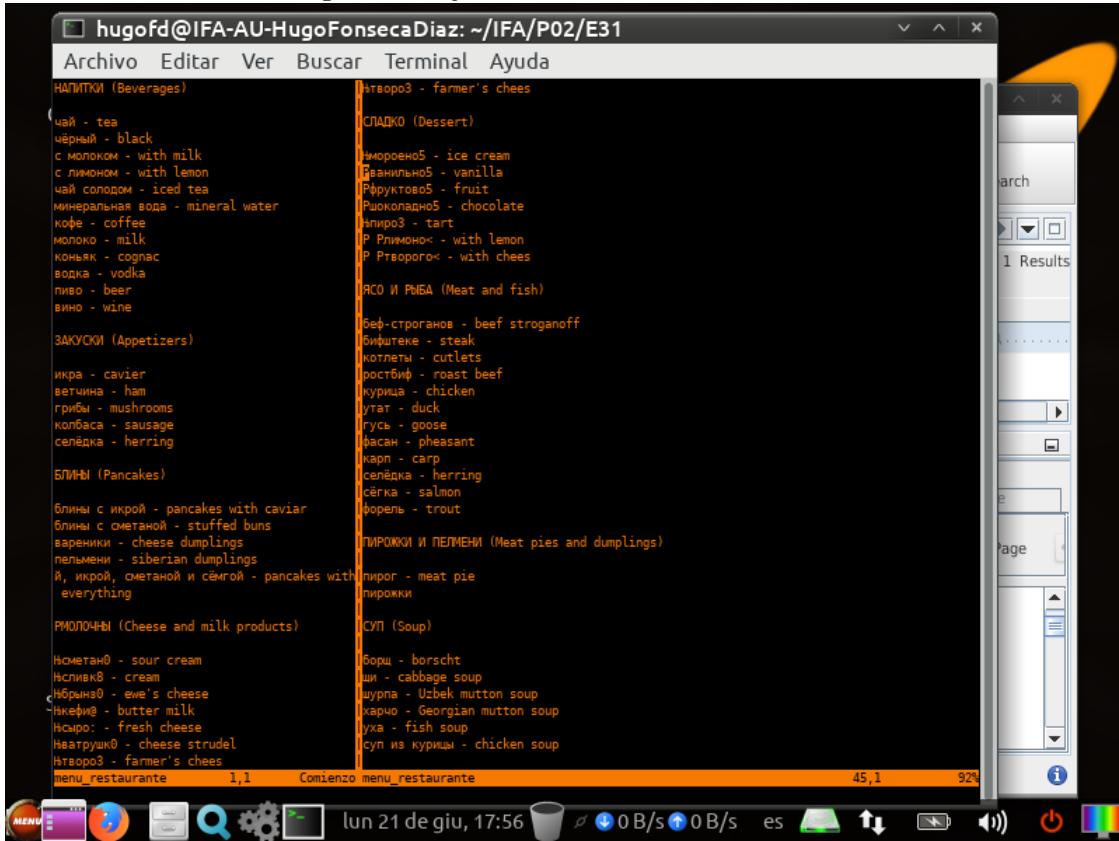
Una vez finalizado el análisis, se pueden observar los ficheros encontrados.

Figura 13: Ejercicio 31: Resultados del análisis



Se reconstruye el menú del restaurante, creado inicialmente el 3 de noviembre de 2004.

Figura 14: Ejercicio 31: Menú reconstruido



### 3. Práctica 03

#### 3.1. Ejercicio 8

Figura 15: Ejercicio 8: Enunciado.

8. En este ejercicio aplicaremos técnicas de carving sobre ficheros de formatos de audio (MP3, WAV, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L0\_Audio.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada además al caso los módulos de ingestión que ha utilizado en los ejercicios anteriores (en este caso ya no es necesario el módulo Embedded File Extractor). Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para llenar la siguiente tabla.

Indique por cada fichero carreado la siguiente información.

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	Autor	Género	Duración	Tasa Muestreo

Se crea el caso en Autopsy con los datos solicitados.

Figura 16: Ejercicio 8: Creación del caso

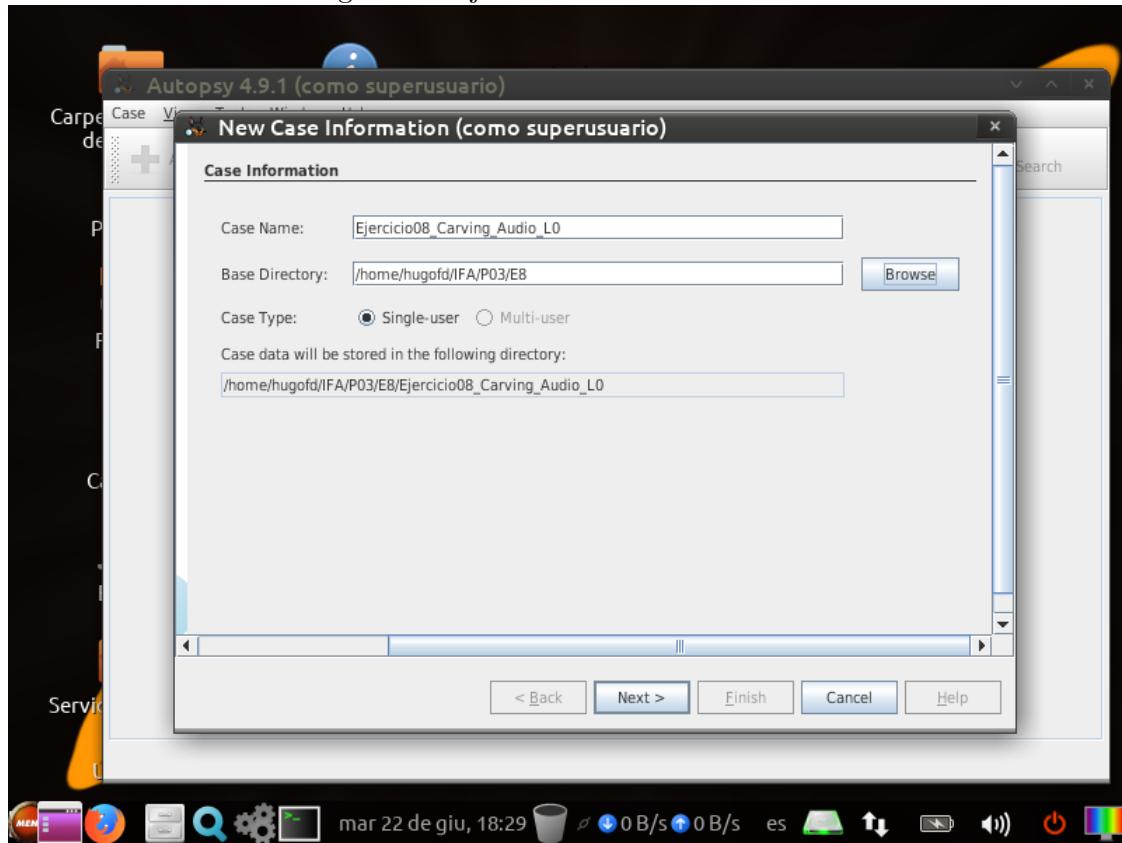
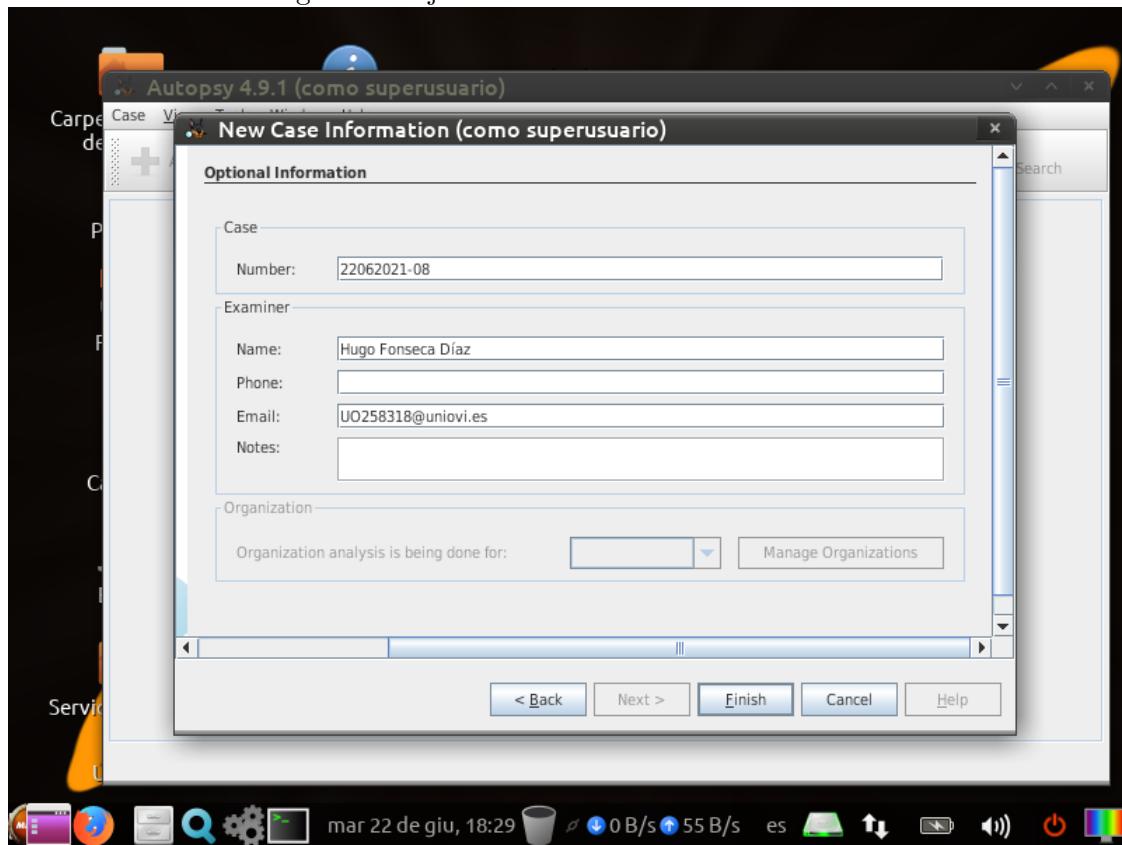
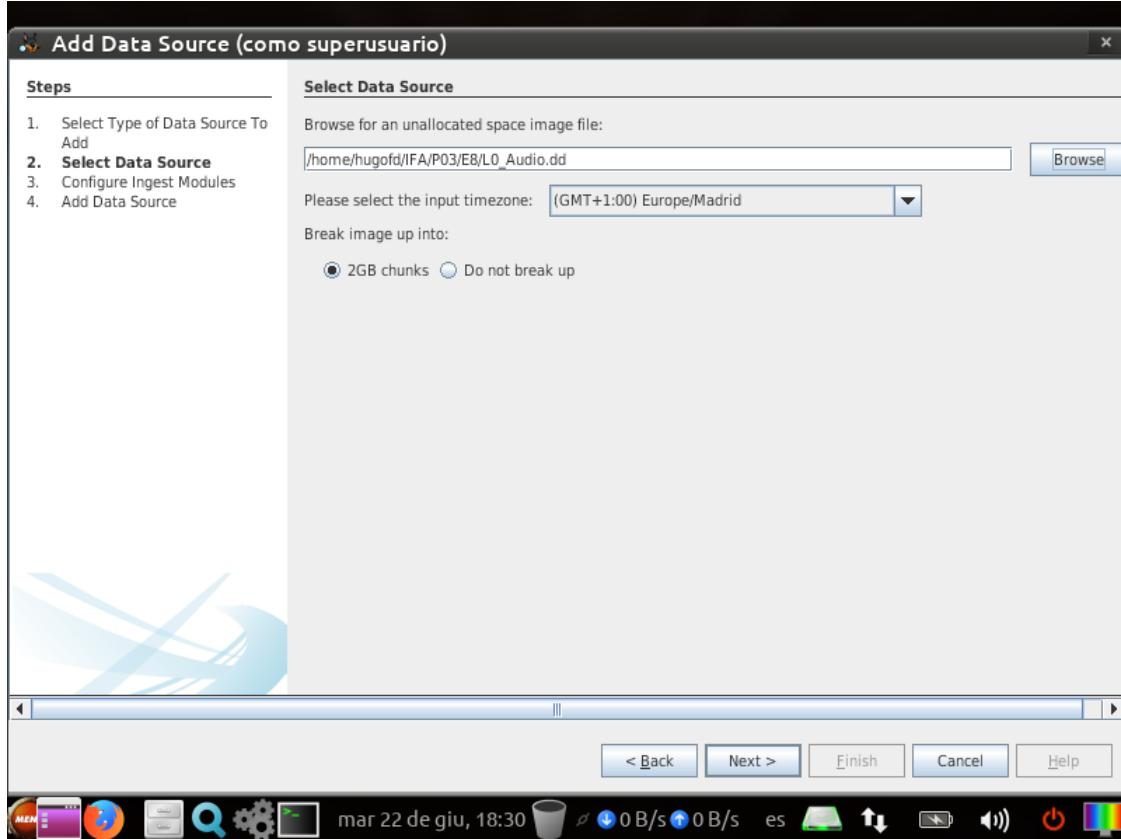


Figura 17: Ejercicio 8: Detalles del examinador



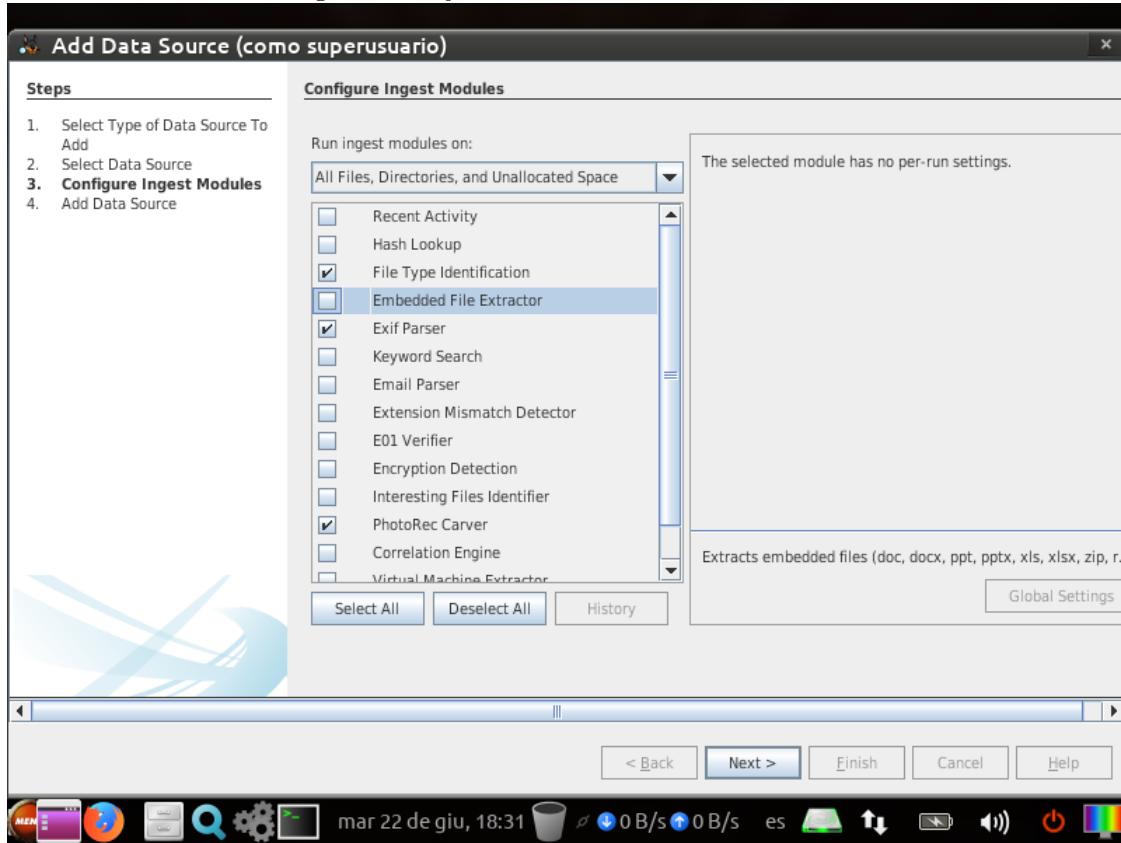
Añadimos la imagen a analizar.

Figura 18: Ejercicio 8: Selección de la imagen



Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

Figura 19: Ejercicio 8: Selección de módulos



Para llenar la tabla se usarán los datos obtenidos al ejecutar el análisis de Autopsy y mediante el uso de la herramienta *MediaInfo*.

Figura 20: Ejercicio 8: Resultados del análisis

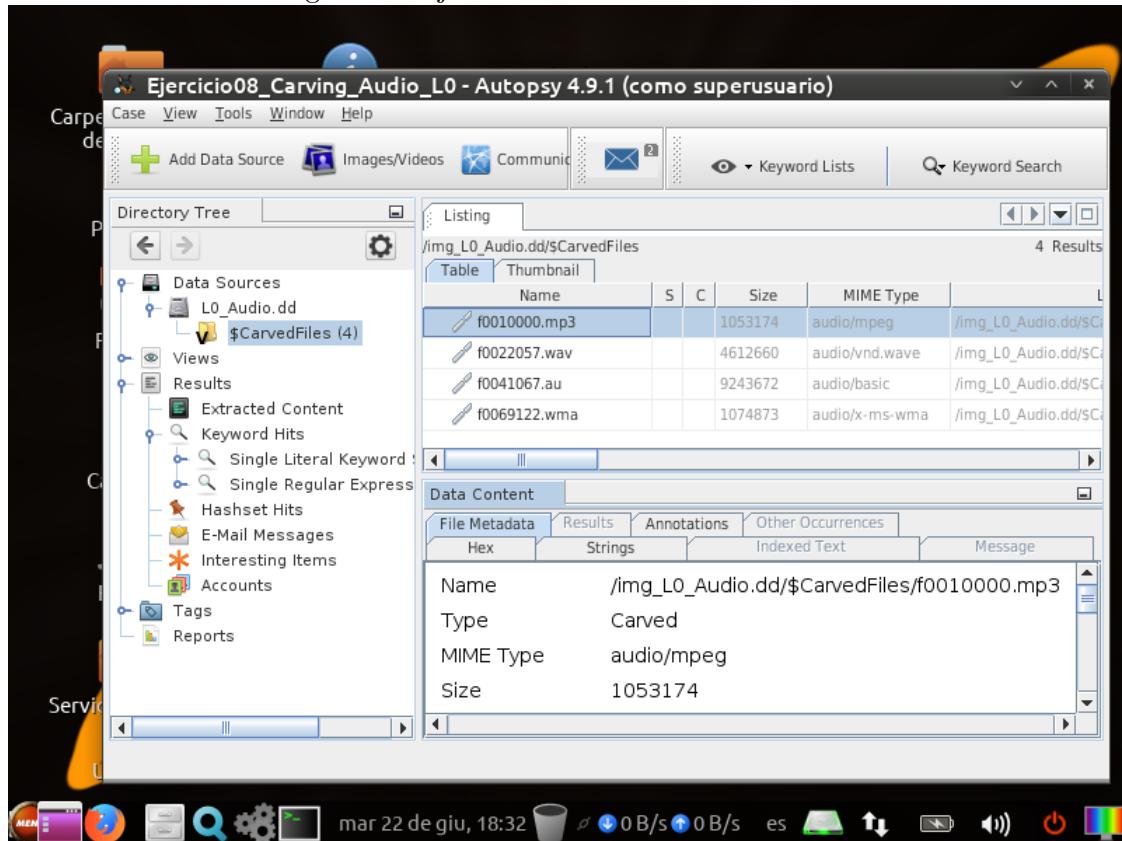
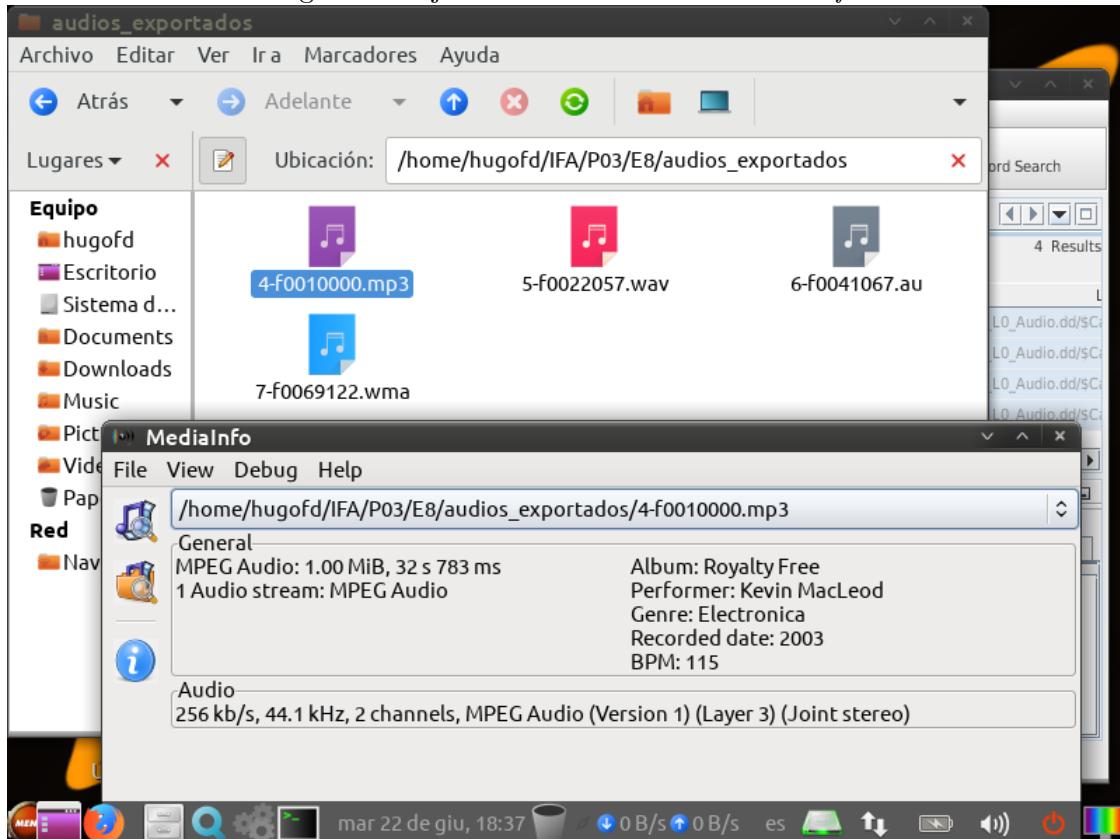


Figura 21: Ejercicio 8: Herramienta *MediaInfo*



Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	Autor	Género	Duración	Tasa de Muestreo
f0010000.mp3	1053174	audio/mpeg	Kevin McLeod	Electronica	32s 783ms	44.1kHz
f0022057.wav	4612660	audio/vnd.wave	-	-	26s 148ms	44.1kHz
f0041067.au	9243672	audio/basic	-	-	3min 29s	44.1kHz
f0069122.wma	1074873	audio/x-ms-wma	-	(80)	1min 5s	44.1kHz

### 3.2. Ejercicio 13

Figura 22: Ejercicio 13: Enunciado (I).

Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el **dfr-02-fyu.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada como módulos de ingestión de evidencia asociados al proyecto los módulos siguientes: **File Type Identification**, **PhotorecCarver**. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para llenar la siguiente tabla.

- a) Rellene la información correspondiente a cada partición identificada:

Número de Partición	Sector de Comienzo	Sector de Finalización	Tipo Sistema de Ficheros

- b) ¿Cuantos ficheros de texto plano (borrados o no) se encuentran en las particiones detectadas en la imagen?

Figura 23: Ejercicio 13: Enunciado (II).

- c) Por cada fichero borrado indique la siguiente información:

MAC times por cada fichero antes del borrado (hora GMT)					
Nombre	Tamaño	Partición	Acceso	Modificación	Cambio

- d) Muestre la línea temporal de cada uno de los ficheros borrados localizados por la herramienta.

Se crea el caso en Autopsy con los datos solicitados.

Figura 24: Ejercicio 13: Creación del caso

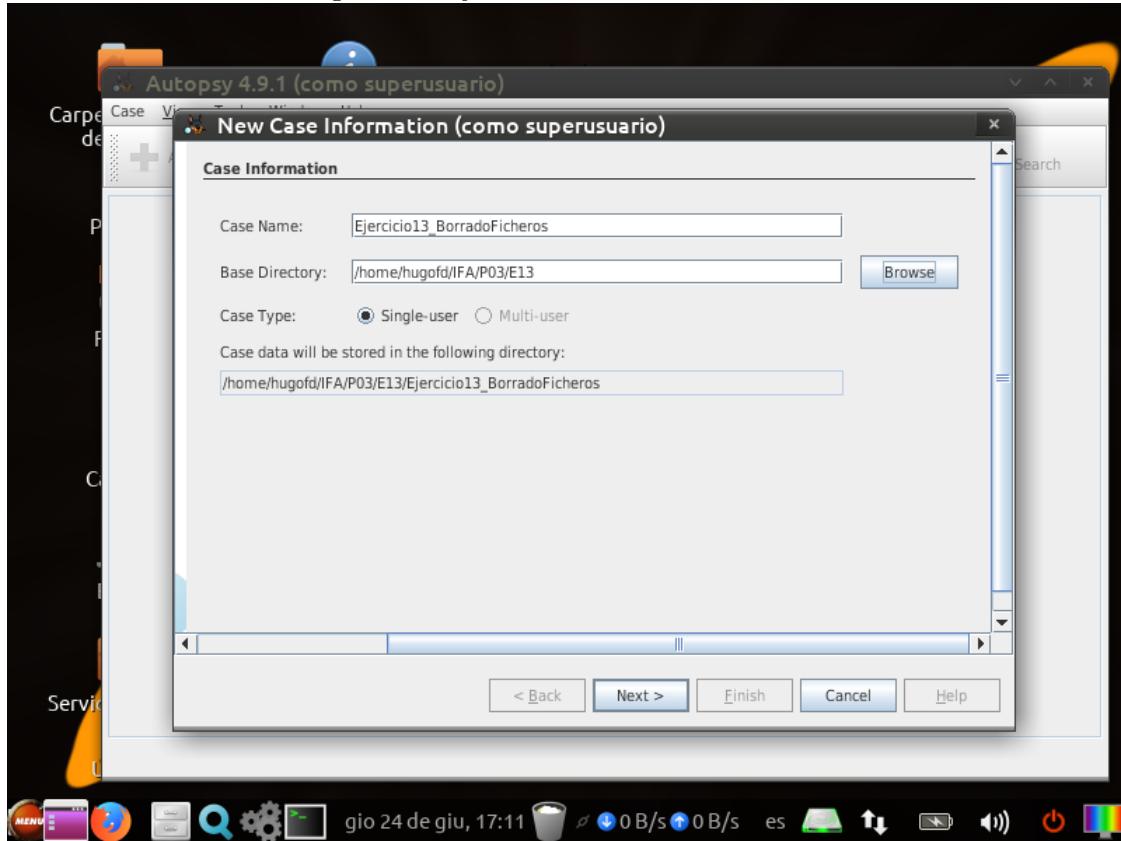
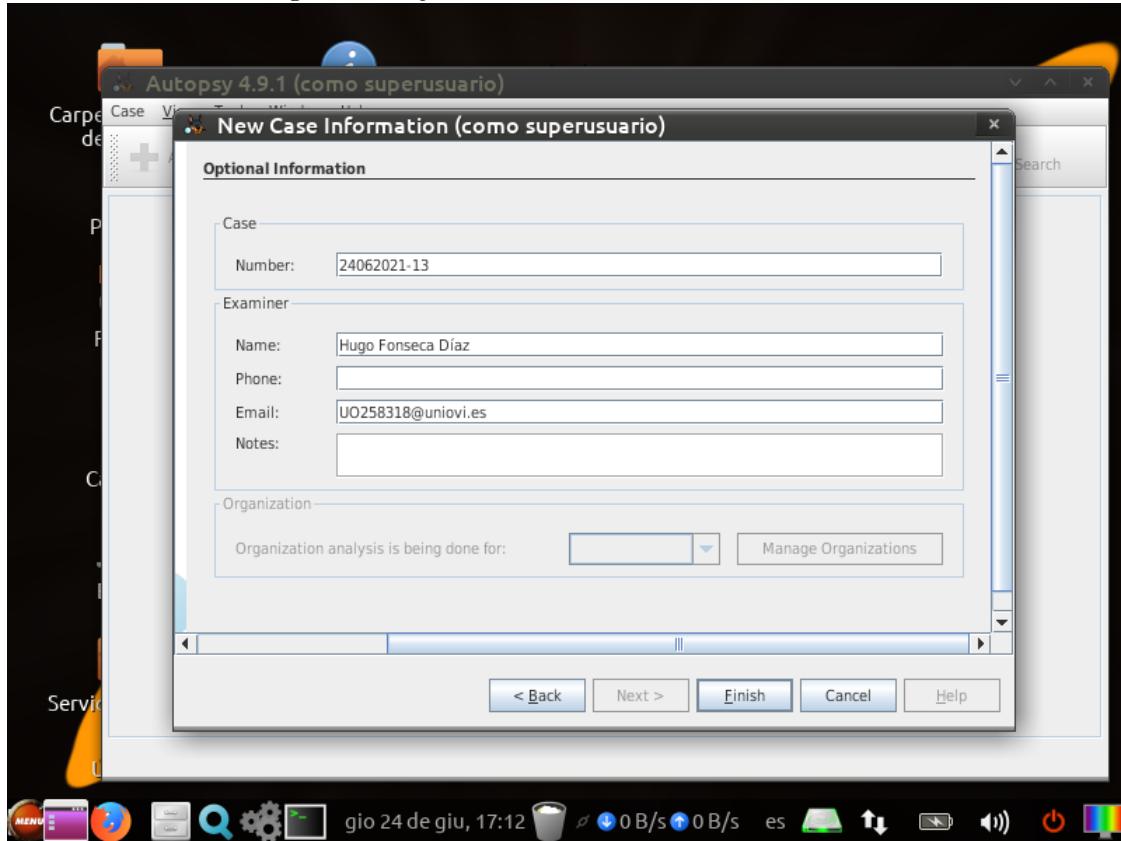
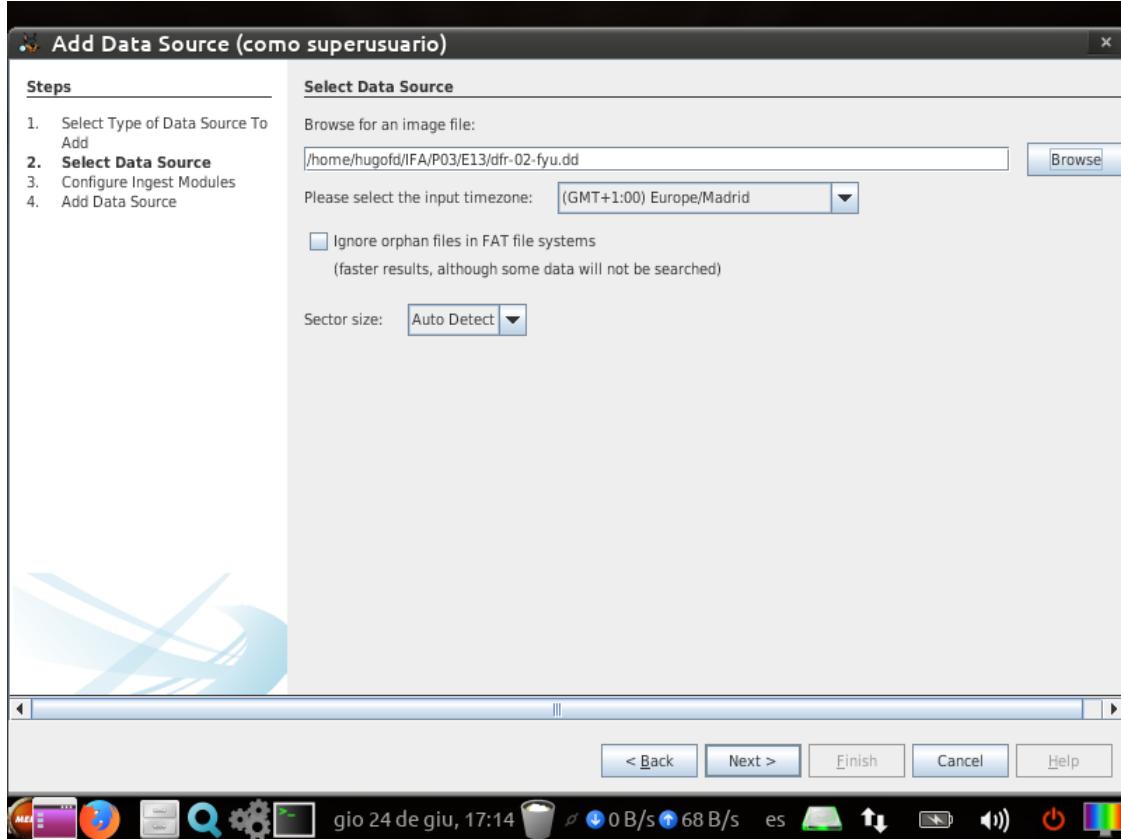


Figura 25: Ejercicio 13: Detalles del examinador



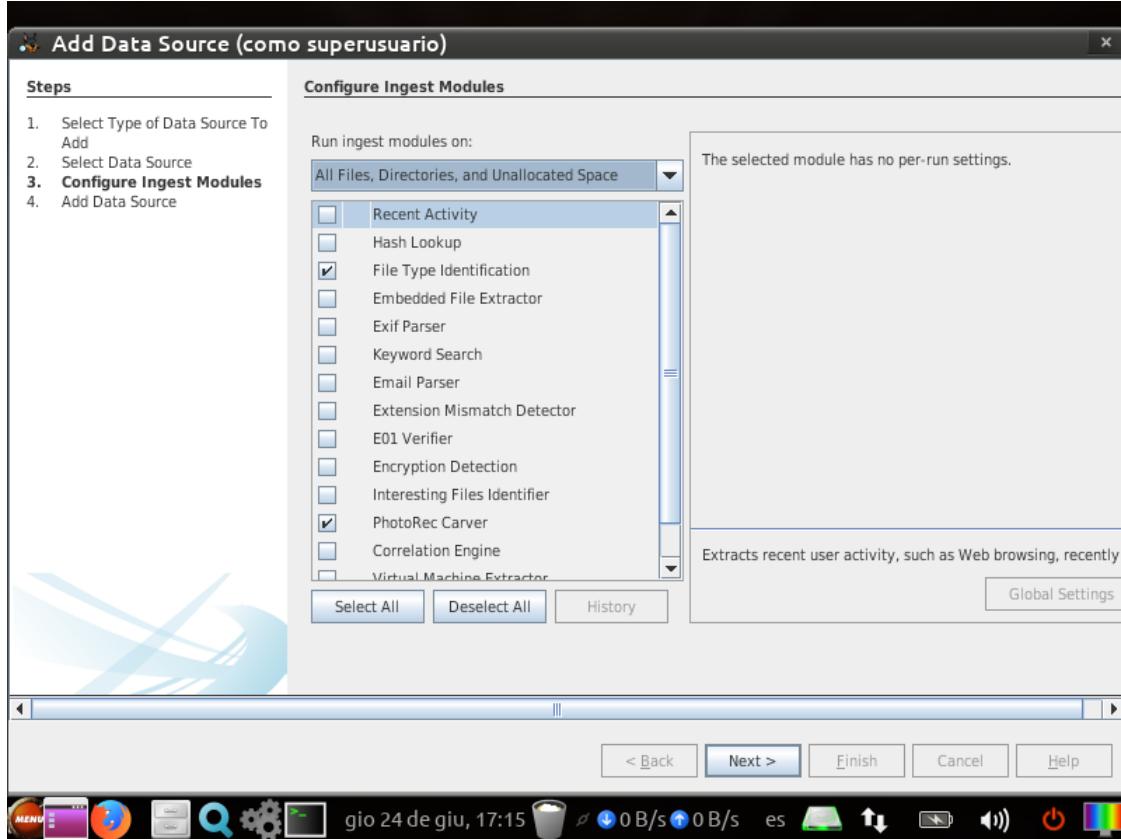
Añadimos la imagen a analizar.

Figura 26: Ejercicio 13: Selección de la imagen



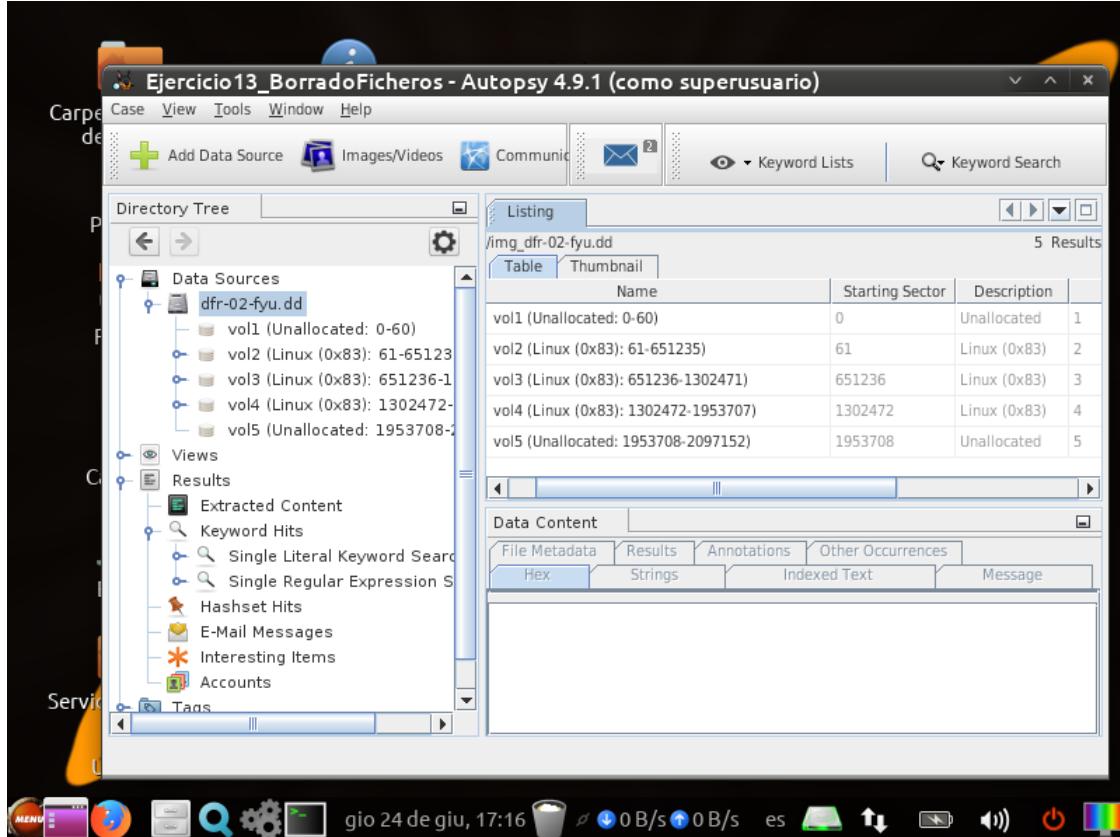
Se seleccionan los módulos de identificación de tipos de fichero y *PhotoRec Carver*.

Figura 27: Ejercicio 13: Selección de módulos



Se obtienen los resultados del análisis con los que se responderán a las diferentes cuestiones del ejercicio.

Figura 28: Ejercicio 13: Resultados del análisis

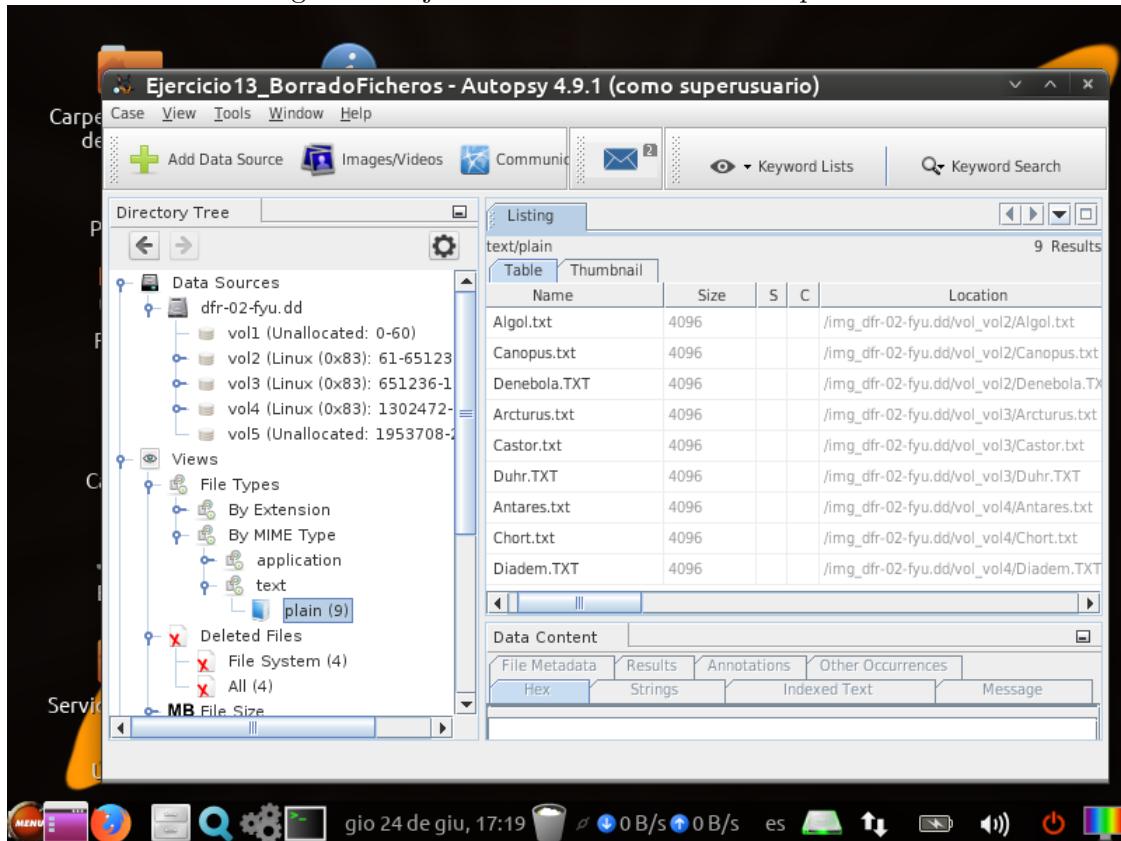


a)

Número partición	Sector comienzo	Sector finalización	Tipo Sistema de Ficheros
1	0	60	Unallocated
2	61	651235	Linux
3	651236	1302471	Linux
4	1302472	1953707	Linux
5	1953708	2097152	Unallocated

b) Para responder a esta cuestión se observan los resultados de la pestaña 'Views'.

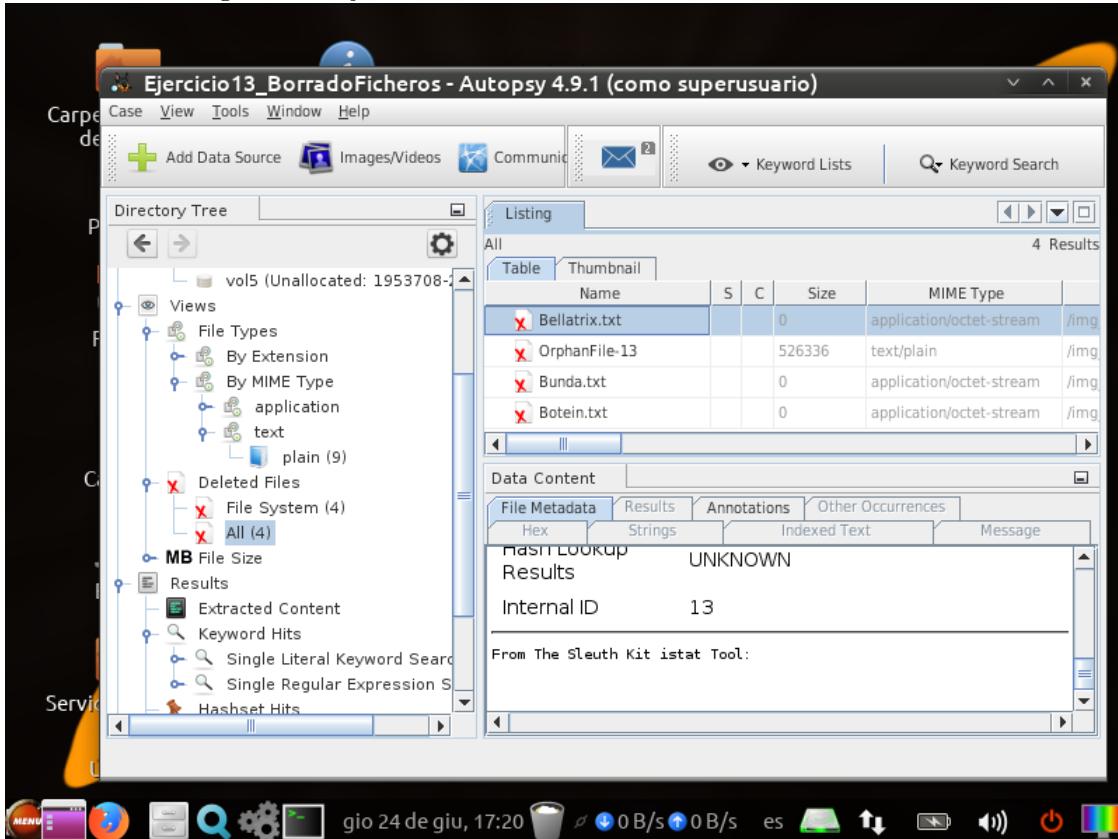
Figura 29: Ejercicio 13: Ficheros de texto plano



Se puede ver que hay 9 ficheros de texto plano. Hay 4 ficheros adicionales borrados, uno llamado Orphan-Files, el cual es autogenerado por Autopsy, y tres ficheros con extensión txt pero cuyos tipos MIME no son texto plano.

c) Para llenar esta tabla se miran los metadatos que muestra Autopsy de cada archivo borrado.

Figura 30: Ejercicio 13: Metadatos de los ficheros borrados

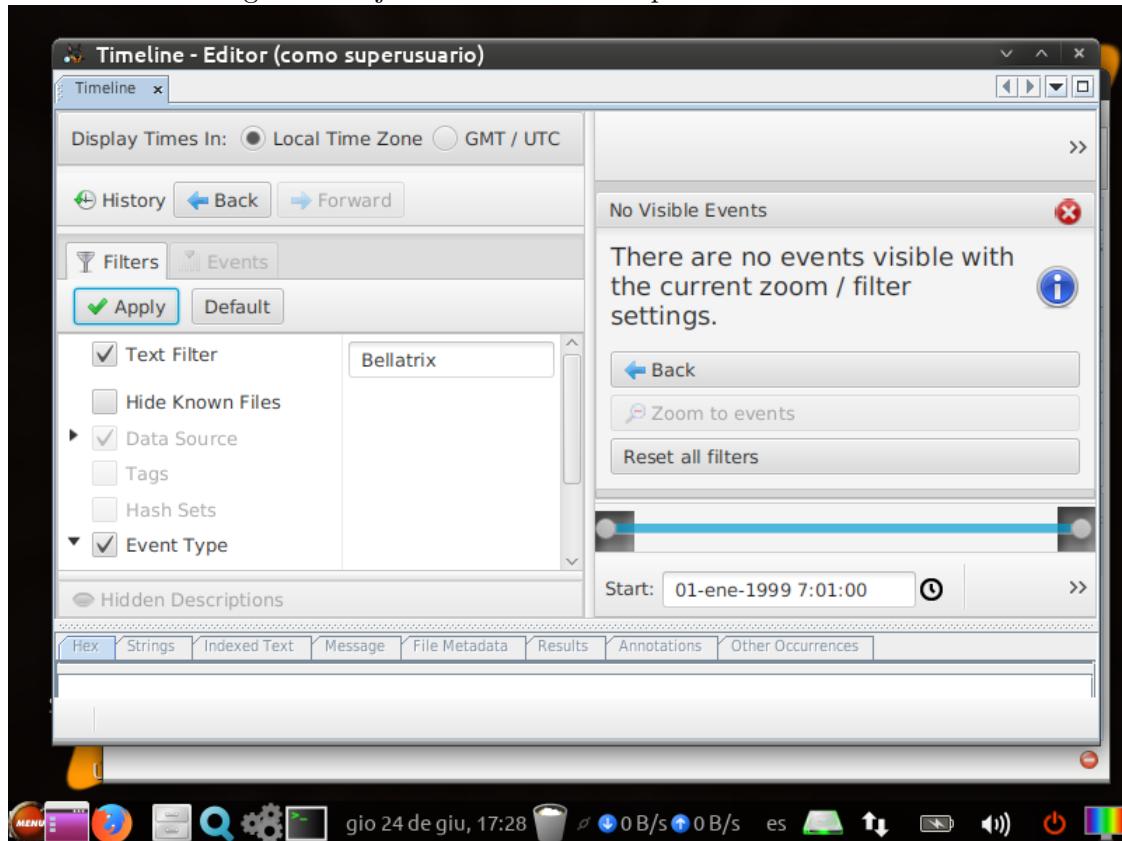


Como se puede observar hay menos metadatos sobre los ficheros borrados que en el ejercicio anterior, por lo que habrá secciones de la tabla sin rellenar.

Nombre	Tamaño	Partición	Sector relativo	Acceso (GMT)	Modificación (GMT)	Creación (GMT)
Bellatrix.txt	0	vol 2	-	-	-	-
Bunda.txt	0	vol 3	-	1999/01/02 08:04:00	2011/10/16 18:52:31	2011/10/16 18:52:31
Botein.txt	0	vol 4	-	1999/01/02 08:05:00	2011/10/16 18:52:31	2011/10/16 18:52:31

- d) Se muestran a continuación las líneas de tiempo de los tres ficheros borrados, en el filtro de la parte izquierda de la captura se observa el fichero actual.

Figura 31: Ejercicio 13: Línea temporal de *Bellatrix.txt*



Se observa que no hay datos para *Bellatrix.txt*

Figura 32: Ejercicio 13: Línea temporal de *Bunda.txt*

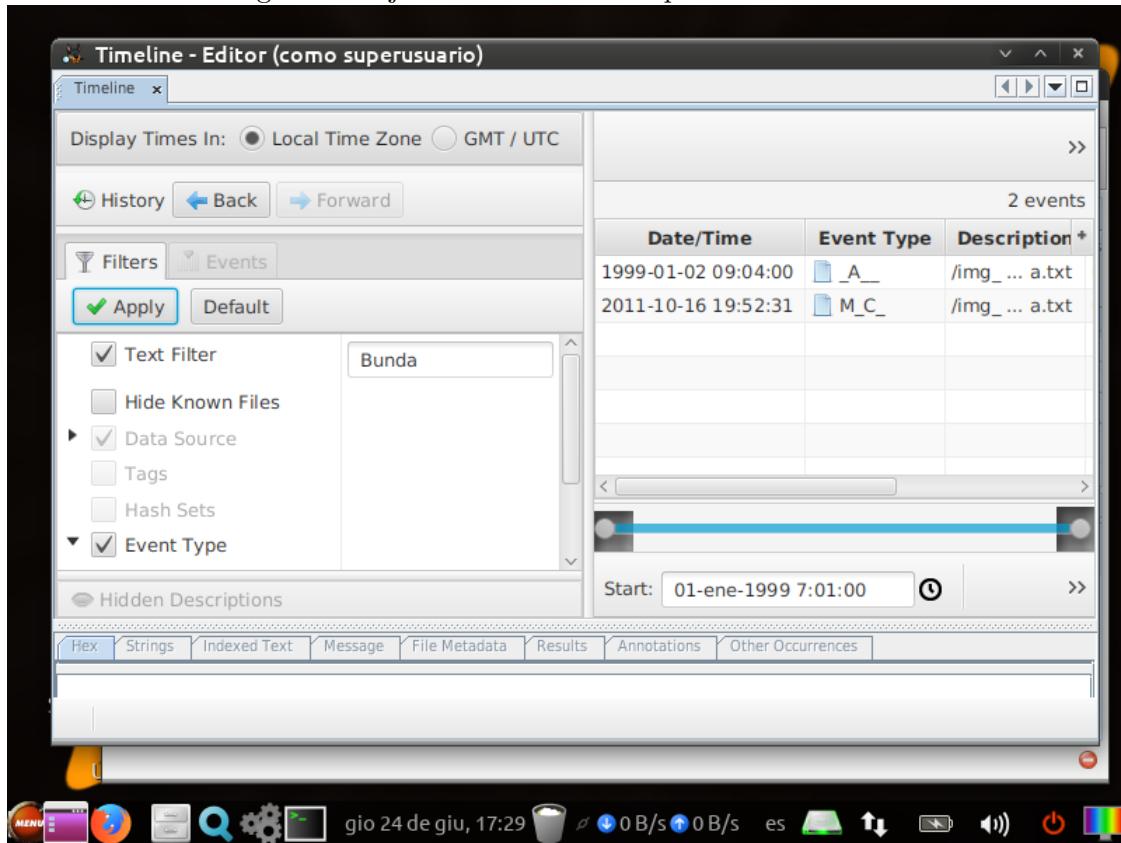
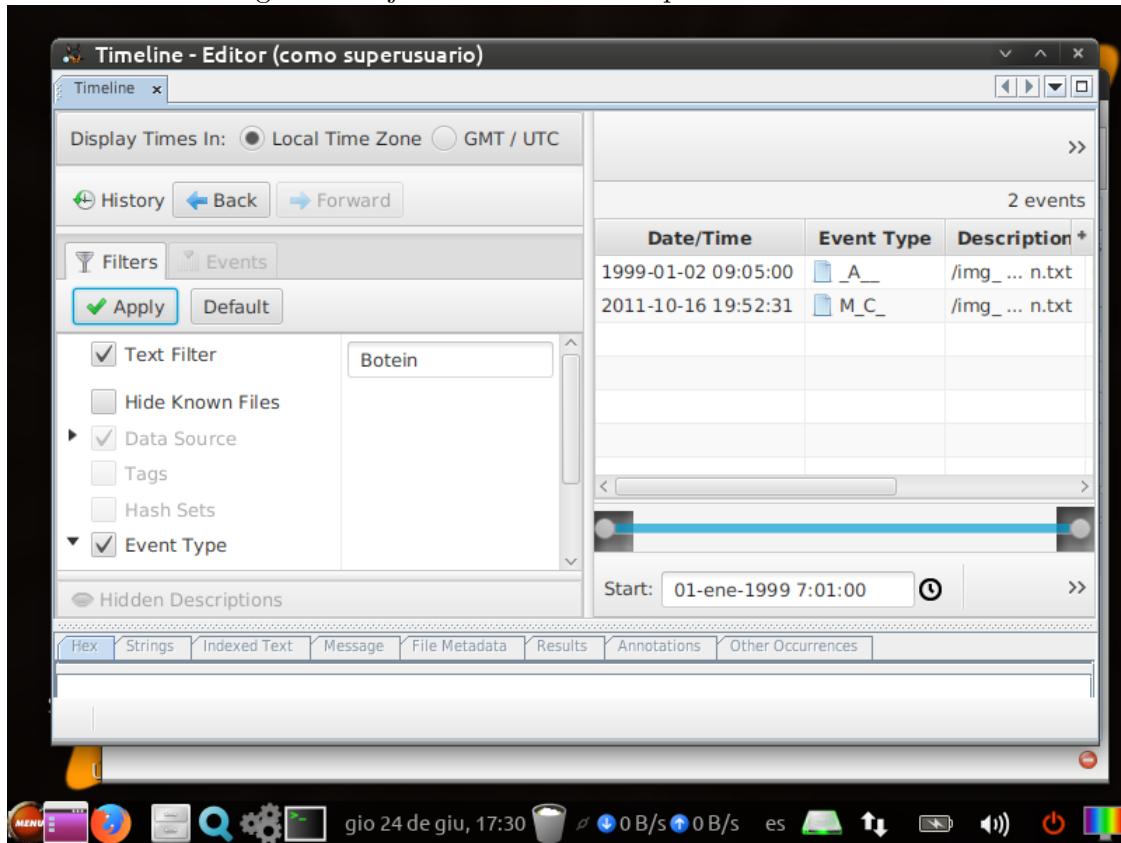


Figura 33: Ejercicio 13: Línea temporal de *Botein.txt*



Para *Bunda.txt* y *Botein.txt* sí que se recuperan datos.

### 3.3. Ejercicio 14

Figura 34: Ejercicio 14: Enunciado (I).

Sleuthkit es un conjunto de herramientas de investigación forense de código libre que puede ejecutarse tanto en plataformas Windows, Linux, OSX y Unix. Puede utilizarse para analizar imágenes de discos y realizar un análisis en profundidad de los sistemas de archivo. Soporta NTFS, FAT32, HFS+, Ext3, Ext4 y UFS entre otros. Tiene un sinfín de herramientas de línea de comando que permiten conducir una investigación forense. Revise la documentación de Sleuthkit y busque el comando que muestra información sobre un fichero de imagen. Para probar su funcionamiento aplíquelo a la imagen **dfr-02-fyu.dd** del ejercicio anterior.

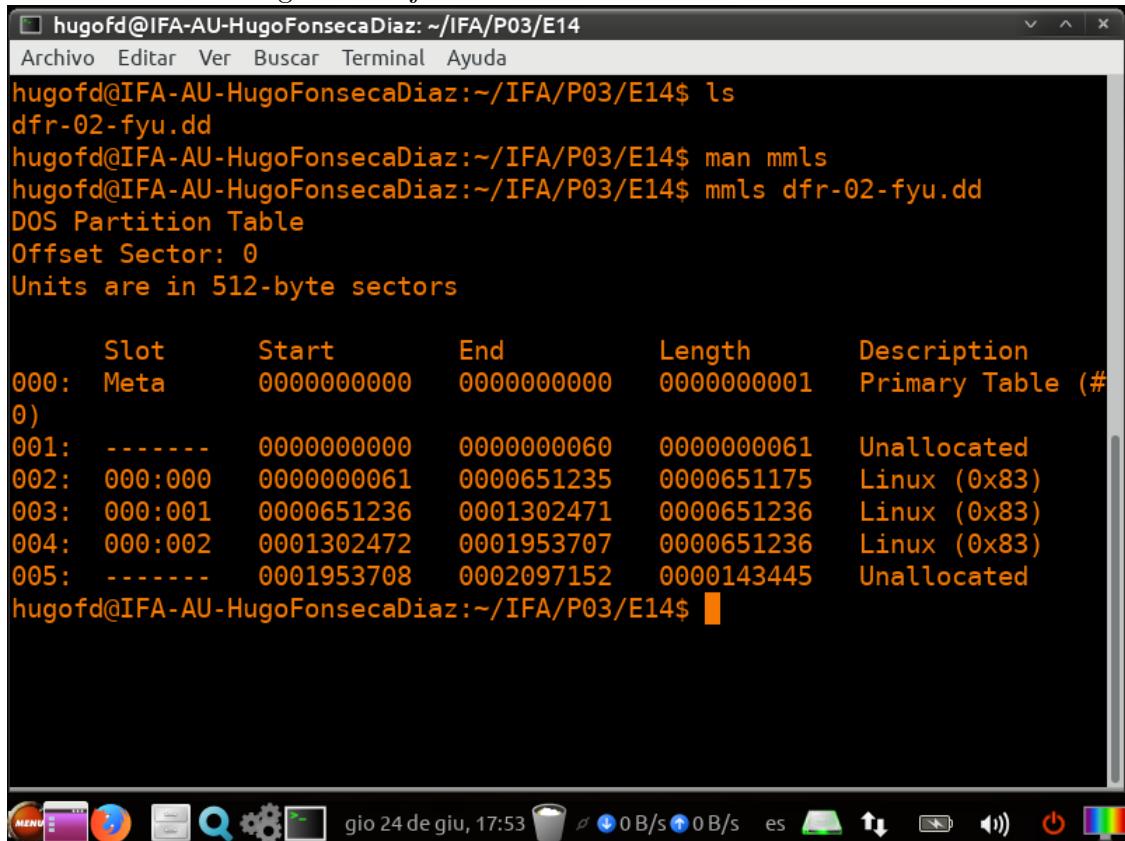
Figura 35: Ejercicio 14: Enunciado (II).

- a) Aplique el comando de Sleuthkit que permite acceder a la tabla de particiones dentro de una imagen y permite obtener los offsets de cada partición en sectores.
- b) Compruebe si la información obtenida sobre el sector de comienzo, de finalización y el tipo de partición coincide con la proporcionada por Autopsy.
- c) Aplique el comando de Sleuthkit que permite obtener información sobre los sistemas de archivos de las particiones contenidas en la imagen anterior. Para obtener información sobre el sistema de archivo de una partición deberemos indicar el offset del sector de comienzo de la partición dentro de la imagen.
- d) Utilice el comando de Sleuthkit apropiado para listar los ficheros y directorios contenidos en el sistema de ficheros de la cuarta partición utilizando el comando **fls**. Investigue qué opciones ofrece el comando anterior.
- e) Aplique el mismo comando para encontrar en la cuarta partición las entradas de directorio borradas correspondientes a ficheros y que el listado sea recursivo. Los ficheros que la herramienta menciona como borrados, ¿son los mismos que los indicados por Autopsy para esa partición?
- f) Utilice el comando **ffind** para encontrar todos los ficheros asociados con la entrada borrada del listado producido por el comando anterior en la partición 4.
- g) Utilice el comando **istat** y explore sus posibilidades para encontrar los metadatos asociados con el inodo del fichero borrado en la partición 4.
- h) Explora el comando **istat** para que te muestre la lista de sistemas de archivos soportados.

Se responde a continuación a las diferentes cuestiones planteadas por el ejercicio.

- a) Se utiliza el comando **mmls**, que lista las particiones con sus sectores de inicio y fin, entre otros datos.

Figura 36: Ejercicio 14: Salida del comando *mmls*



The screenshot shows a terminal window with the following content:

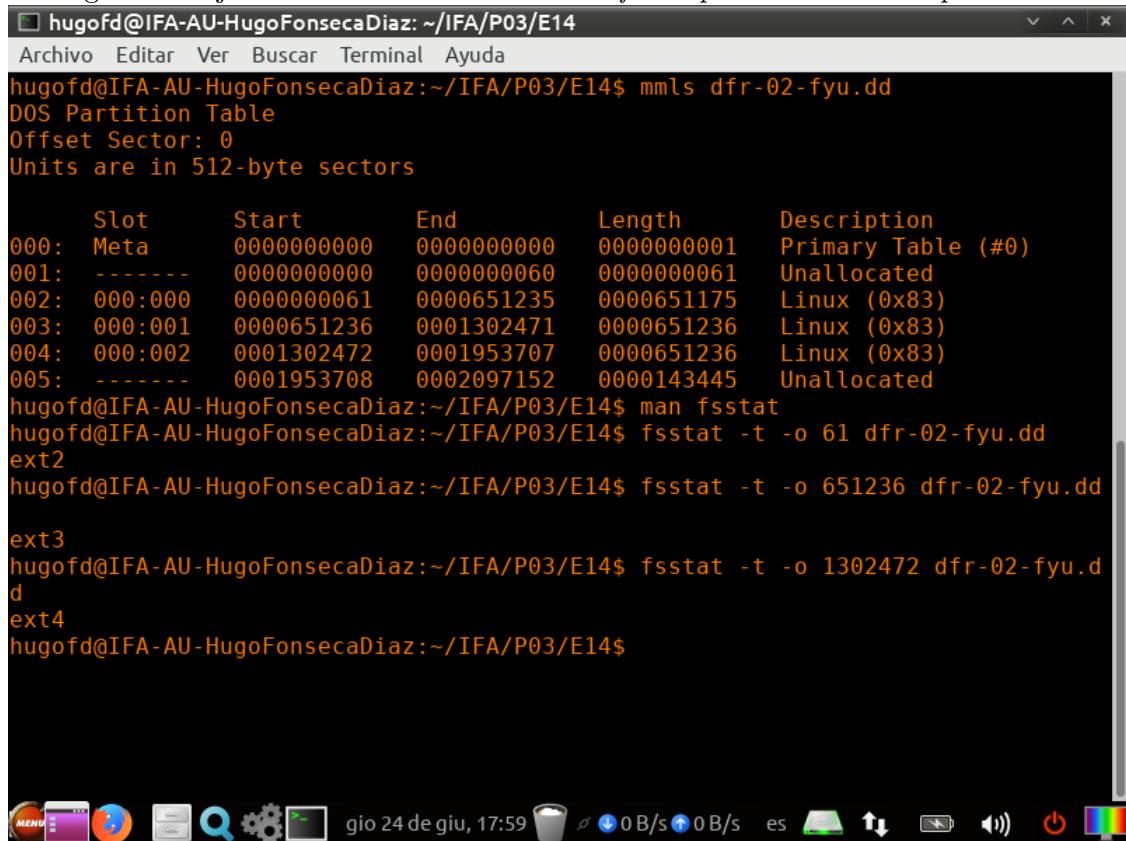
```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ ls
dfr-02-fyu.dd
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man mmls
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ mmls dfr-02-fyu.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End        Length     Description
000: Meta    0000000000  0000000000  0000000001  Primary Table (#0)
001: -----  0000000000  0000000060  0000000061  Unallocated
002: 000:000  0000000061  0000651235  0000651175  Linux (0x83)
003: 000:001  0000651236  0001302471  0000651236  Linux (0x83)
004: 000:002  0001302472  0001953707  0000651236  Linux (0x83)
005: -----  0001953708  0002097152  0000143445  Unallocated
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$
```

The terminal window has a menu bar with Archivo, Editar, Ver, Buscar, Terminal, Ayuda. The desktop environment icons at the bottom include MENU, a purple folder, a red circular icon, a file manager, a search icon, a gear icon, and a terminal icon.

- b) Sí, la información es consistente entre ambas herramientas.
- c) Se usa el comando **fsstat**, con la flag *t* para mostrar solo el tipo de partición y la flag *o* para pasarle al comando el sector donde comienza la partición.

Figura 37: Ejercicio 14: Salida del comando *fsstat* para las diferentes particiones



The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P03/E14". The window contains the following text:

```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ mmls dfr-02-fyu.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot      Start        End        Length     Description
000: Meta    0000000000  0000000000  0000000001 Primary Table (#0)
001: -----  0000000000  0000000060  0000000061 Unallocated
002: 000:000  0000000061  0000651235  0000651175 Linux (0x83)
003: 000:001  0000651236  0001302471  0000651236 Linux (0x83)
004: 000:002  0001302472  0001953707  0000651236 Linux (0x83)
005: -----  0001953708  0002097152  0000143445 Unallocated

hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man fsstat
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ fsstat -t -o 61 dfr-02-fyu.dd
ext2
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ fsstat -t -o 651236 dfr-02-fyu.dd
ext3
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ fsstat -t -o 1302472 dfr-02-fyu.dd
ext4
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$
```

The terminal window has a dark background with white text. The bottom of the window shows a standard Linux desktop interface with icons for menu, file manager, browser, terminal, search, and system settings. The system tray displays the date and time (gio 24 de giu, 17:59), battery status (0 B/s), network (0 B/s), signal strength, volume, and power management.

- d) Se utiliza el comando **f1s** que recibe como argumentos, entre otros, el comienzo del sector de la partición que se quiere analizar.

Figura 38: Ejercicio 14: Salida del comando `f1s` con las flags *ro*

The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P03/E14". The window contains the following text:

```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man f1s
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ mm1s dfr-02-fyu.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End        Length     Description
000: Meta    0000000000  0000000000  0000000001 Primary Table (#0)
001: -----  0000000000  0000000060  0000000061 Unallocated
002: 000:000  0000000061  0000651235  0000651175 Linux (0x83)
003: 000:001  0000651236  0001302471  0000651236 Linux (0x83)
004: 000:002  0001302472  0001953707  0000651236 Linux (0x83)
005: -----  0001953708  0002097152  0000143445 Unallocated
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ f1s -o 1302472 -r dfr-02-fyu.dd
d/d 11: lost+found
r/r 12: Antares.txt
r/r * 13:      Botein.txt
r/r 14: Chort.txt
r/r 15: Diadem.TXT
V/V 81601:      $OrphanFiles
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$
```

The terminal window has a dark background and light-colored text. Below the window is a dock with various icons, and at the bottom is a system tray with icons for battery, signal, and other system status.

- e) Se usa ahora el comando `f1s` con las flags *dFrO*, *d* muestra solo elementos borrados, *F* muestra solo ficheros, *r* es para que la búsqueda sea recursiva y *o* para introducir el comienzo del sector de la partición.

Figura 39: Ejercicio 14: Salida del comando *fls* con las flags *dFrO*

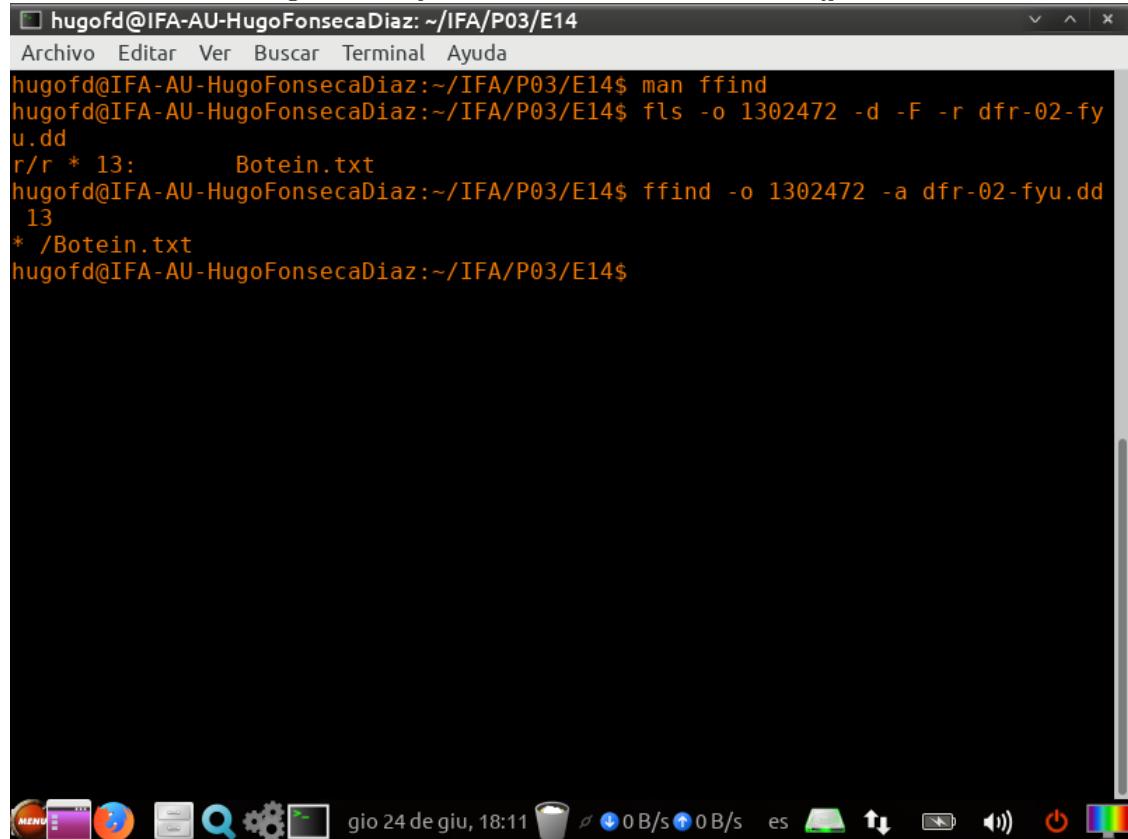
The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14". The window contains the following text:

```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man fls
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ fls -o 1302472 -d -F -r dfr-02-fy
u.dd
r/r * 13:      Botein.txt
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ █
```

The terminal is running on a desktop environment, as evidenced by the dock icons at the bottom, which include a menu, a file manager, a browser, a terminal, a search icon, system settings, and a window manager. The desktop environment is Unity.

- f) Se utiliza el comando **ffind** con las flags *oa*, *o* para introducir el comienzo del sector de la partición y *a* para buscar todos los ficheros asociados. Se le pasa al comando el inodo del elemento que se está buscando, en este caso el 13.

Figura 40: Ejercicio 14: Salida del comando *ffind*



The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P03/E14". The window contains the following text:

```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man ffind
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ fls -o 1302472 -d -F -r dfr-02-fy
u.dd
r/r * 13:      Botein.txt
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ ffind -o 1302472 -a dfr-02-fyu.dd
 13
* /Botein.txt
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$
```

The terminal window has a dark background and light-colored text. At the bottom, there is a dock with various icons, including a trash can, a search bar, and system status indicators like battery level and signal strength.

g) Se usa el comando *istat* pasandole como argumento el comienzo del sector de la partición y el inodo a buscar.

Figura 41: Ejercicio 14: Salida del comando *istat* para el inodo 13

The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P03/E14". The window contains the following text:

```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man istat
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ fls -o 1302472 -d -F -r dfr-02-fy
u.dd
r/r * 13:      Botein.txt
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ istat -o 1302472 dfr-02-fyu.dd 13
inode: 13
Not Allocated
Group: 0
Generation Id: 2392951179
uid / gid: 0 / 0
mode: rrw-----
Flags: Extents,
size: 0
num of links: 0

Extended Attributes (Block: 4386)
security.selinux=unconfined_u:object_r:file_t:s0

Inode Times:
Accessed: 1999-01-02 09:05:00 (CET)
File Modified: 2011-10-16 19:52:31 (CEST)
Inode Modified: 2011-10-16 19:52:31 (CEST)
Deleted: 2011-10-16 19:52:31 (CEST)

Direct Blocks:
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$
```

The terminal window has a dark background with white text. At the bottom, there is a standard Linux desktop dock with icons for various applications like a menu, file manager, browser, terminal, and system settings. The date and time "gio 24 de giu, 18:13" are also visible at the bottom.

h) Se usa el comando *istat* con la flag *f* y el argumento *list*.

Figura 42: Ejercicio 14: Salida del comando *istat -f list*

The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P03/E14". The window contains the following text:

```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man istat
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ istat -f list
Supported file system types:
    ntfs (NTFS)
    fat (FAT (Auto Detection))
    ext (ExtX (Auto Detection))
    iso9660 (ISO9660 CD)
    hfs (HFS+)
    ufs (UFS (Auto Detection))
    raw (Raw Data)
    swap (Swap Space)
    fat12 (FAT12)
    fat16 (FAT16)
    fat32 (FAT32)
    exfat (exFAT)
    ext2 (Ext2)
    ext3 (Ext3)
    ext4 (Ext4)
    ufs1 (UFS1)
    ufs2 (UFS2)
    yaffs2 (YAFFS2)
```

At the bottom of the terminal window, there is a standard Linux desktop status bar with icons for network, battery, volume, and system status.

### 3.4. Ejercicio 19

Figura 43: Ejercicio 19: Enunciado.

Descarga del campus virtual (Recursos Prácticas- Práctica 3), el fichero **imagenesEXIF.zip**. Almacénalo en una carpeta de Evidencias. Descomprime dicho

12



archivo y, ayudado por las herramientas instaladas en los dos ejercicios anteriores, obtén para cada archivo la siguiente información a partir de sus etiquetas:

- Fecha en la que fue tomada la imagen
- Marca de la cámara.
- Modelo de la cámara.
- Características de la imagen:
  - Ancho y alto de la imagen en pixels.
  - Resolución.
  - Bits de color por pixel.
- Tamaño del archivo.
- Ubicación GPS (si disponible)

Para este ejercicio se pueden realizar dos aproximaciones, una es mediante la interfaz gráfica de `exiftool` para el sistema operativo Windows y la otra mediante el propio comando de consola `exiftool`. Se probarán las dos para la primera imagen y se realizará el resto de imágenes con el comando de consola.

### 3.4.1. Imagen 1

Figura 44: Ejercicio 19: Metadatos de la imagen 1 con la interfaz gráfica de *exiftool* (I)

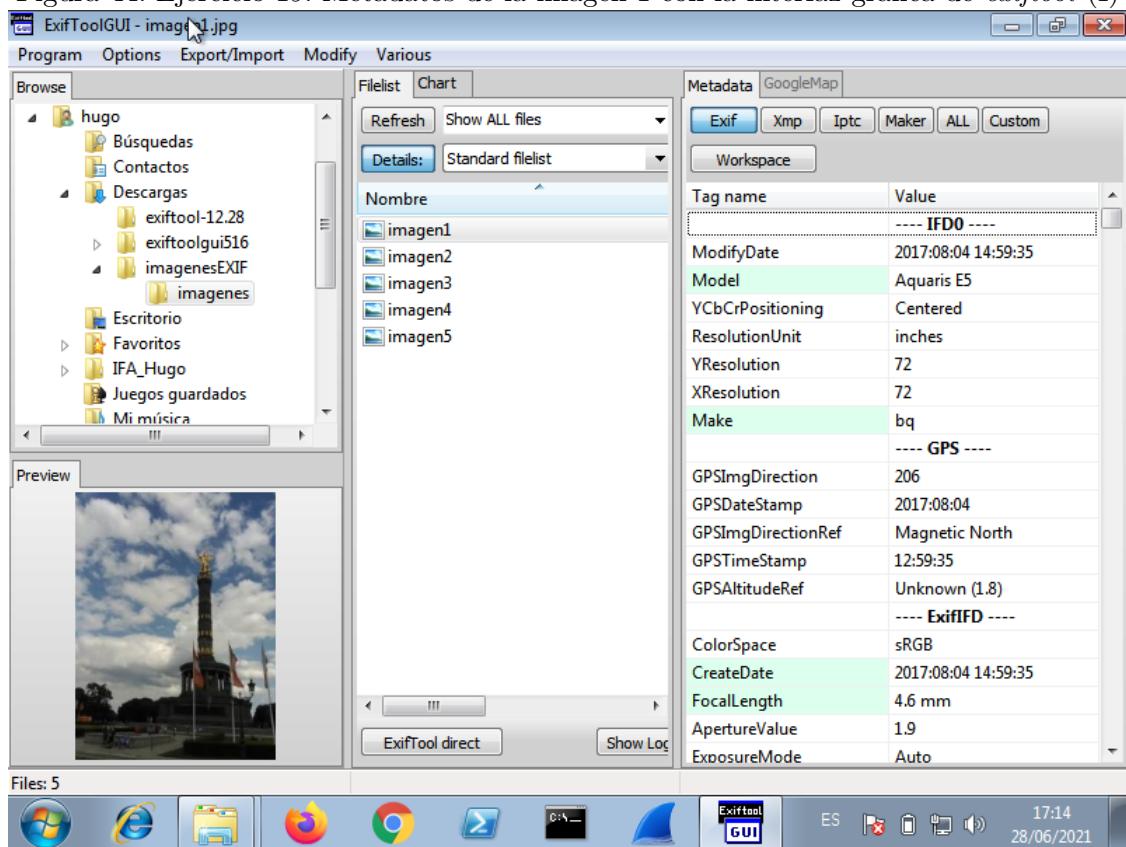


Figura 45: Ejercicio 19: Metadatos de la imagen 1 con la interfaz gráfica de *exiftool* (II)

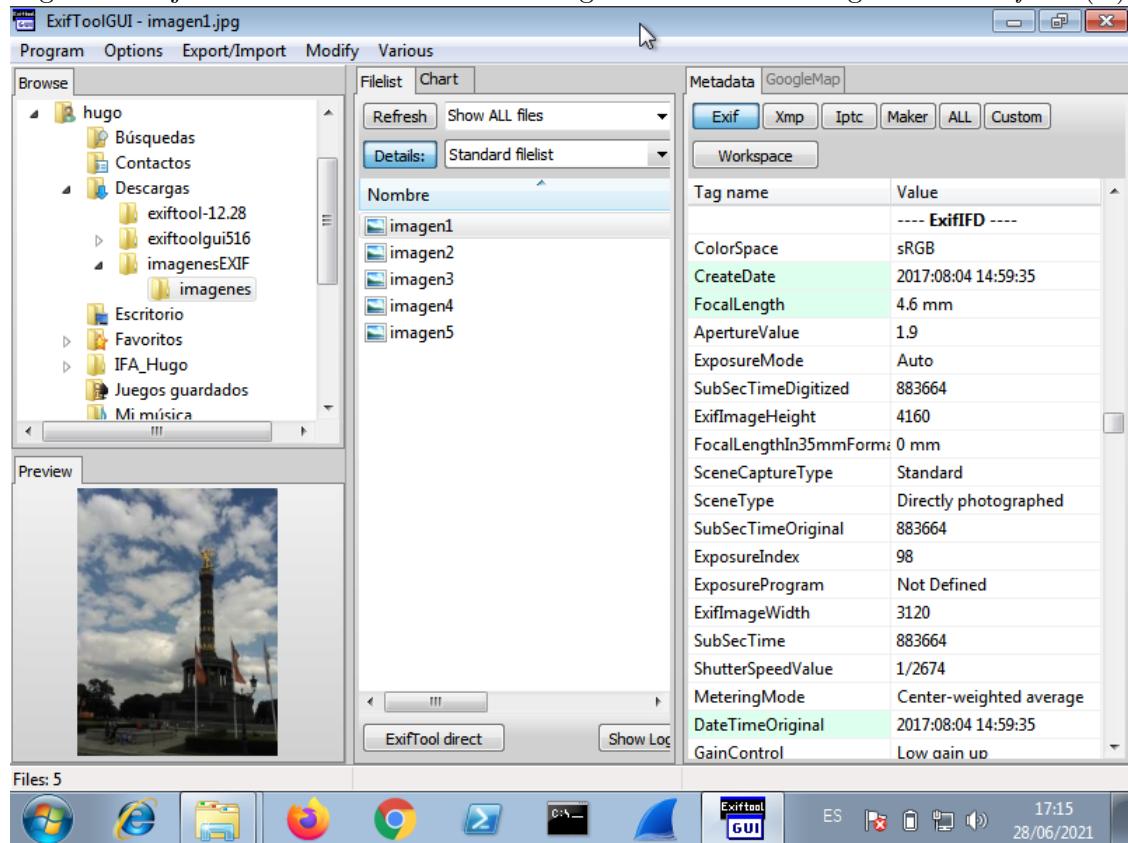
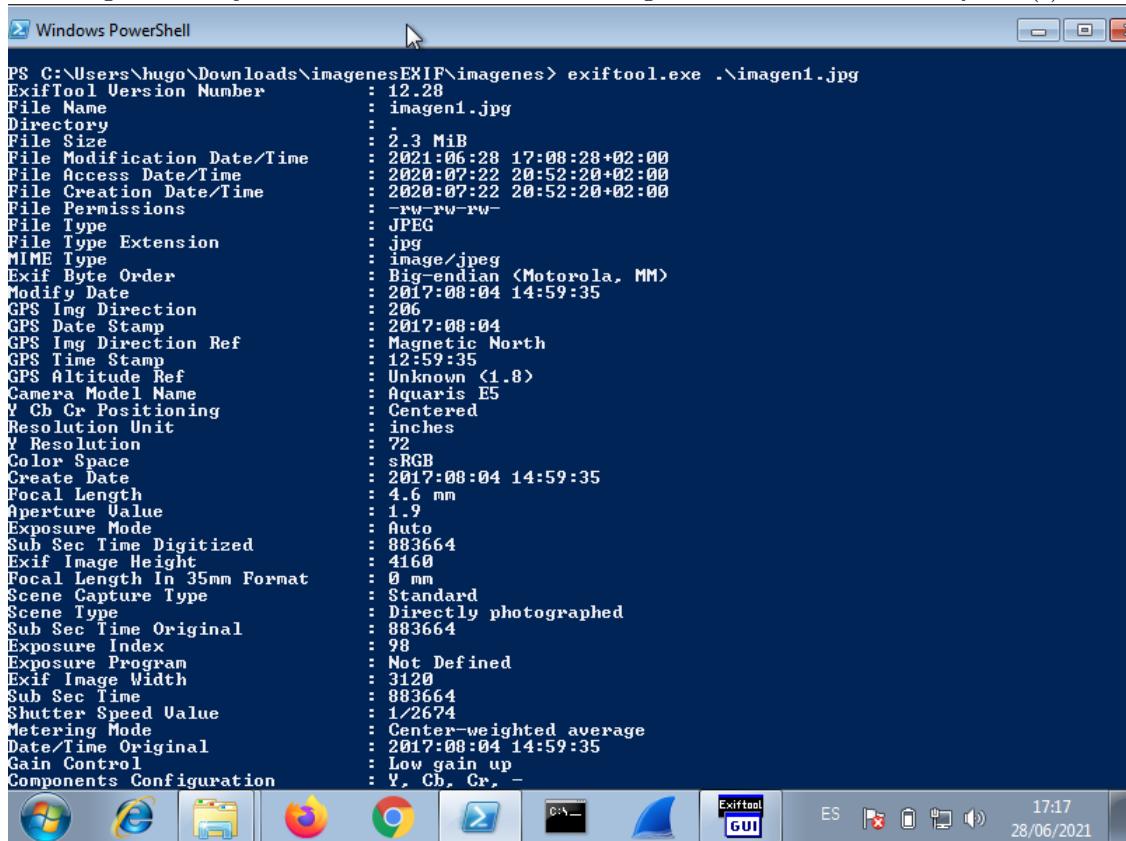


Figura 46: Ejercicio 19: Metadatos de la imagen 1 con el comando *exiftool* (I)



```
PS C:\Users\hugo\Downloads\imagenes\EXIF\imagenes> exiftool.exe .\imagen1.jpg
ExifTool Version Number      : 12.28
File Name                   : imagen1.jpg
Directory                   :
File Size                    : 2.3 MiB
File Modification Date/Time : 2021:06:28 17:08:28+02:00
File Access Date/Time       : 2020:07:22 20:52:20+02:00
File Creation Date/Time    : 2020:07:22 20:52:20+02:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension        : jpg
MIME Type                   : image/jpeg
Exif Byte Order             : Big-endian <Motorola, MM>
Modify Date                 : 2017:08:04 14:59:35
GPS Img Direction          : 206
GPS Date Stamp              : 2017:08:04
GPS Img Direction Ref     : Magnetic North
GPS Time Stamp              : 12:59:35
GPS Altitude Ref           : Unknown <1.8>
Camera Model Name          : Aquaris E5
Y Cr Cb Positioning       : Centered
Resolution Unit            : inches
Y Resolution               : 72
Color Space                 : sRGB
Create Date                 : 2017:08:04 14:59:35
Focal Length                : 4.6 mm
Aperture Value              : 1.9
Exposure Mode               : Auto
Sub Sec Time Digitized     : 883664
Exif Image Height           : 4160
Focal Length In 35mm Format: 0 mm
Scene Capture Type          : Standard
Scene Type                  : Directly photographed
Sub Sec Time Original      : 883664
Exposure Index              : 98
Exposure Program            : Not Defined
Exif Image Width             : 3120
Sub Sec Time                : 883664
Shutter Speed Value         : 1/2674
Metering Mode                : Center-weighted average
Date/Time Original          : 2017:08:04 14:59:35
Gain Control                 : Low gain up
Components Configuration     : Y, Cr, Cb, -
```

Figura 47: Ejercicio 19: Metadatos de la imagen 1 con el comando *exiftool* (II)

```

Windows PowerShell
Sub Sec Time Original      : 883664
Exposure Index              : 98
Exposure Program            : Not Defined
Exif Image Width            : 3120
Sub Sec Time                : 883664
Shutter Speed Value         : 1/2674
Metering Mode               : Center-weighted average
Date/Time Original          : 2017:08:04 14:59:35
Gain Control                : Low gain up
Components Configuration    : Y, Cb, Cr, -
Flash                        : Off, Did not fire
Exif Version                : 0220
Interoperability Index      : R98 - DCF basic file <sRGB>
Interoperability Version    : 0100
Brightness Value             : 0
ISO                           : 101
Sensing Method              : Unknown <0>
Flashpix Version             : 0100
Warning                      : [minor] Unrecognized MakerNotes
Exposure Time                : 1/2675
X Resolution                 : 72
Make                          : bq
Thumbnail Length             : 12796
Thumbnail Offset              : 899
Compression                  : JPEG <old-style>
Image Width                   : 3120
Image Height                  : 4160
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y_Cb_Cr Sub Sampling        : YCbCr4:2:0 <2 2>
Aperture                     : 1.9
Image Size                    : 3120x4160
Megapixels                    : 13.0
Shutter Speed                 : 1/2675
Create Date                   : 2017:08:04 14:59:35.883664
Date/Time Original            : 2017:08:04 14:59:35.883664
Modify Date                   : 2017:08:04 14:59:35.883664
Thumbnail Image               : <Binary data 12796 bytes, use -b option to extract>
GPS Date/Time                 : 2017:08:04 12:59:35Z
Focal Length                  : 4.6 mm
Light Value                   : 13.2
PS C:\Users\hugo\Downloads\imagenes\EXIF\imagenes1.jpg - 

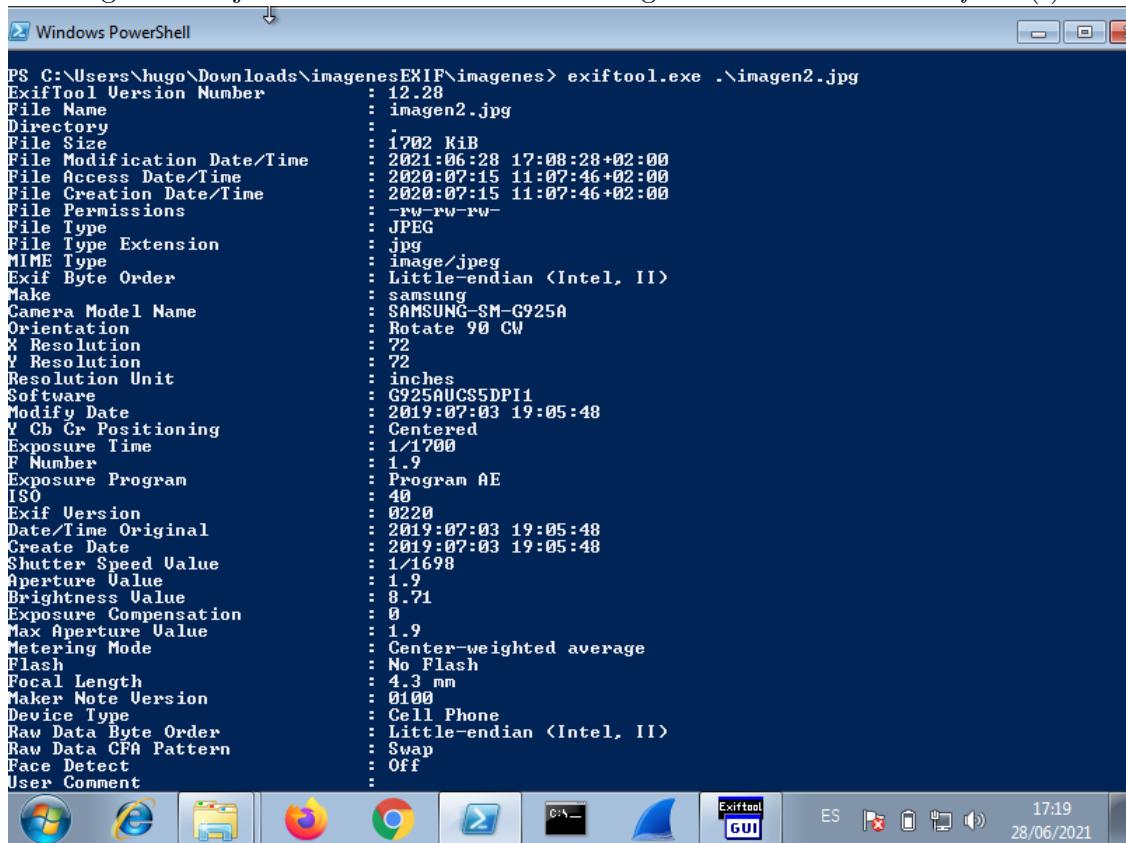
```

Con lo anterior visto, se procede a llenar la lista de datos requeridos:

- **Fecha en la que fue tomada la imagen:** 2017/08/04 14:59:35
- **Marca de la cámara:** bq
- **Modelo de la cámara:** Aquaris E5
- **Características de la imagen:**
  - **Ancho y alto en píxeles:** Ancho 3120, alto 4160
  - **Resolución:** 3120x4160
  - **Bits de color por pixel:** 8 bits y 3 canales, así que 24 bits de color por pixel
- **Tamaño del archivo:** 2.3MiB
- **Ubicación GPS:** No está presente

### 3.4.2. Imagen 2

Figura 48: Ejercicio 19: Metadatos de la imagen 2 con el comando *exiftool* (I)



```
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes> exiftool.exe .\imagen2.jpg
ExifTool Version Number      : 12.28
File Name                   : imagen2.jpg
Directory                   :
File Size                    : 1702 KiB
File Modification Date/Time : 2021:06:28 17:08:28+02:00
File Access Date/Time       : 2020:07:15 11:07:46+02:00
File Creation Date/Time    : 2020:07:15 11:07:46+02:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension        : jpg
MIME Type                   : image/jpeg
Exif Byte Order             :
Make                         : samsung
Camera Model Name           : SAMSUNG-SM-G925A
Orientation                  : Little-endian (Intel, II)
X Resolution                : Rotate 90 CW
Y Resolution                : 72
V Resolution                : 22
Resolution Unit             : inches
Software                     : G925AUCS5DP1I
Modify Date                 : 2019:07:03 19:05:48
YCbCr Positioning          : Centered
Exposure Time               : 1/1700
F Number                     : 1.9
Exposure Program            : Program AE
ISO                          : 40
Exif Version                : 0220
Date/Time Original          : 2019:07:03 19:05:48
Create Date                 : 2019:07:03 19:05:48
Shutter Speed Value         : 1/1698
Aperture Value              : 1.9
Brightness Value            : 8.71
Exposure Compensation       : 0
Max Aperture Value          : 1.9
Metering Mode               : Center-weighted average
Flash                        : No Flash
Focal Length                : 4.3 mm
Marker Note Version          : 0100
Device Type                 : Cell Phone
Raw Data Byte Order          : Little-endian (Intel, II)
Raw Data CFA Pattern        : Swap
Face Detect                 : Off
User Comment                 :
```

Figura 49: Ejercicio 19: Metadatos de la imagen 2 con el comando *exiftool* (II)

```

Face Detect : Off
User Comment :
Flashpix Version : 0100
Color Space : sRGB
Exif Image Width : 3264
Exif Image Height : 1836
Exposure Mode : Auto
White Balance : Auto
Focal Length In 35mm Format : 28 mm
Scene Capture Type : Standard
Image Unique ID : A16LSIA00SM A16LSJG01SM.
GPS Version ID : 2.2.0.0
GPS Latitude Ref : North
GPS Longitude Ref : West
GPS Altitude Ref : Below Sea Level
GPS Time Stamp : 18:00:41
GPS Date Stamp : 2019:07:03
Compression : JPEG (old-style)
Thumbnail Offset : 1166
Thumbnail Length : 8986
Image Width : 3264
Image Height : 1836
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y_Cb_Cr Sub Sampling : YCbCr4:2:2 <2 1>
Time Stamp : 2019:07:03 20:05:48+02:00
Aperture : 1.9
Image Size : 3264x1836
Megapixels : 6.0
Scale Factor To 35 mm Equivalent : 6.5
Shutter Speed : 1/1700
Thumbnail Image : <Binary data 8986 bytes, use -b option to extract>
GPS Altitude : 0 m Above Sea Level
GPS Date/Time : 2019:07:03 18:00:41Z
GPS Latitude : 53 deg 21' 8.00" N
GPS Longitude : 6 deg 18' 17.00" W
GPS Circle Of Confusion : 0.005 mm
Field Of View : 65.5 deg
Focal Length : 4.3 mm <35 mm equivalent: 28.0 mm>
GPS Position : 53 deg 21' 8.00" N, 6 deg 18' 17.00" W
Hyperfocal Distance : 2.11 m
Light Value : 13.9
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes2.jpg>

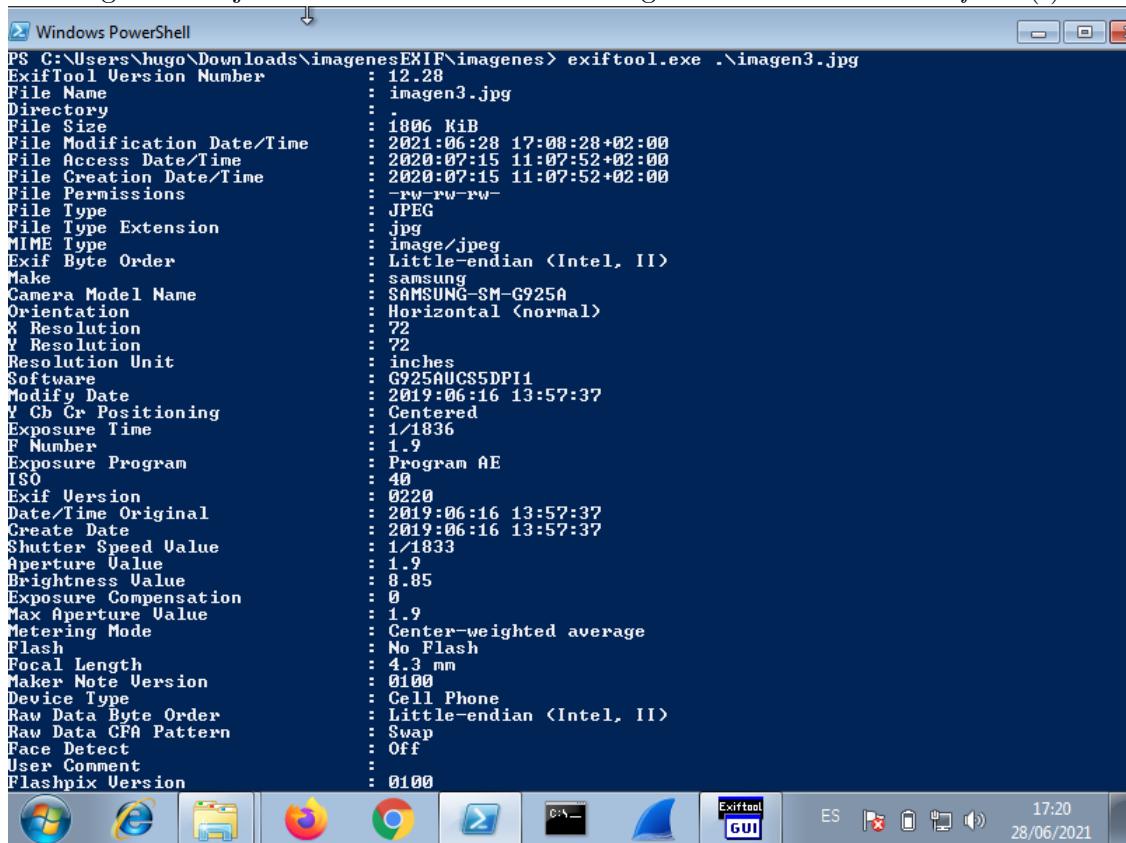
```

Con lo anterior visto, se procede a llenar la lista de datos requeridos:

- **Fecha en la que fue tomada la imagen:** 2019/07/03 19:05:48
- **Marca de la cámara:** Samsung
- **Modelo de la cámara:** SAMSUNG-SM-G925A
- **Características de la imagen:**
  - **Ancho y alto en píxeles:** Ancho 3264, alto 1836
  - **Resolución:** 3264x1836
  - **Bits de color por pixel:** 8 bits y 3 canales, así que 24 bits de color por pixel
- **Tamaño del archivo:** 1702 KiB
- **Ubicación GPS:** Latitud 53 deg 21' 8.00"North, longitud 6 deg 18' 17.00"West

### 3.4.3. Imagen 3

Figura 50: Ejercicio 19: Metadatos de la imagen 3 con el comando *exiftool* (I)



```
Windows PowerShell
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes> exiftool.exe .\imagen3.jpg
ExifTool Version Number : 12.28
File Name : imagen3.jpg
Directory :
File Size : 1806 KiB
File Modification Date/Time : 2021:06:28 17:08:28+02:00
File Access Date/Time : 2020:07:15 11:07:52+02:00
File Creation Date/Time : 2020:07:15 11:07:52+02:00
File Permissions : -rw-rw-rw-
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
Exif Byte Order : Little-endian (Intel, II)
Make : samsung
Camera Model Name : SAMSUNG-SM-G925A
Orientation : Horizontal (normal)
X Resolution : 72
Y Resolution : 72
Resolution Unit : inches
Software : G925AUCSS5DPI1
Modify Date : 2019:06:16 13:57:37
YCbCr Positioning : Centered
Exposure Time : 1/1836
F Number : 1.9
Exposure Program : Program AE
ISO : 40
Exif Version : 0220
Date/Time Original : 2019:06:16 13:57:37
Create Date : 2019:06:16 13:57:37
Shutter Speed Value : 1/1833
Aperture Value : 1.9
Brightness Value : 8.85
Exposure Compensation : 0
Max Aperture Value : 1.9
Metering Mode : Center-weighted average
Flash : No Flash
Focal Length : 4.3 mm
Marker Note Version : 0100
Device Type : Cell Phone
Raw Data Byte Order : Little-endian (Intel, II)
Raw Data CFA Pattern : Swap
Face Detect : Off
User Comment :
Flashpix Version : 0100
Exiftool GUI
```

Figura 51: Ejercicio 19: Metadatos de la imagen 3 con el comando *exiftool* (II)

```

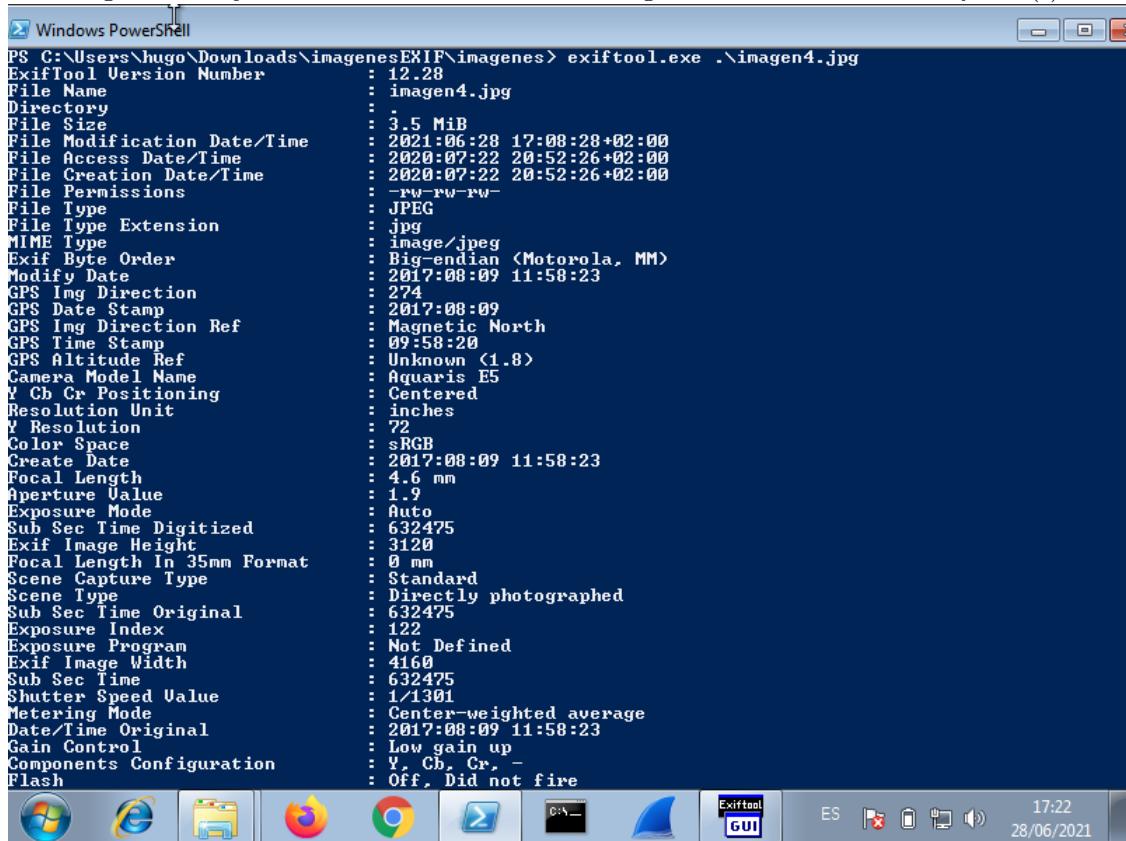
Windows PowerShell
User Comment          : 0100
Flashpix Version     : sRGB
Color Space           : 3264
Exif Image Width     : 1836
Exif Image Height    : Auto
Exposure Mode        : Auto
White Balance         : Auto
Focal Length In 35mm Format : 28 mm
Scene Capture Type   : Standard
Image Unique ID      : A16LSIA00SM A16LSJG01SM.
GPS Version ID       : 2.2.0.0
GPS Latitude Ref     : North
GPS Longitude Ref    : West
GPS Altitude Ref     : Above Sea Level
GPS Time Stamp       : 12:57:36
GPS Date Stamp       : 2019:06:16
Compression          : JPEG <old-style>
Thumbnail Offset     : 1166
Thumbnail Length     : 14630
Image Width          : 3264
Image Height         : 1836
Encoding Process     : Baseline DCT, Huffman coding
Bits Per Sample      : 8
Color Components     : 3
Y Cb Cr Sub Sampling: YCbCr4:2:2 <2 1>
Time Stamp           : 2019:06:16 14:57:37+02:00
Aperture             : 1.9
Image Size           : 3264x1836
Megapixels           : 6.0
Scale Factor To 35 mm Equivalent: 6.5
Shutter Speed        : 1/1836
Thumbnail Image      : <Binary data 14630 bytes, use -b option to extract>
GPS Altitude         : 77 m Above Sea Level
GPS Date/Time        : 2019:06:16 12:57:36Z
GPS Latitude          : 38 deg 42' 51.00" N
GPS Longitude         : 9 deg 8' 23.00" W
Circle Of Confusion   : 0.005 mm
Field Of View         : 65.5 deg
Focal Length          : 4.3 mm <35 mm equivalent: 28.0 mm>
GPS Position          : 38 deg 42' 51.00" N, 9 deg 8' 23.00" W
Hyperfocal Distance   : 2.11 m
Light Value           : 14.0
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes>
```

Con lo anterior visto, se procede a llenar la lista de datos requeridos:

- **Fecha en la que fue tomada la imagen:** 2019/06/16 13:57:37
- **Marca de la cámara:** Samsung
- **Modelo de la cámara:** SAMSUNG-SM-G925A
- **Características de la imagen:**
  - **Ancho y alto en píxeles:** Ancho 3264, alto 1836
  - **Resolución:** 3264x1836
  - **Bits de color por pixel:** 8 bits y 3 canales, así que 24 bits de color por pixel
- **Tamaño del archivo:** 1806 KiB
- **Ubicación GPS:** Latitud 38 deg 42' 51.00"North, longitud 9 deg 8' 23.00"West

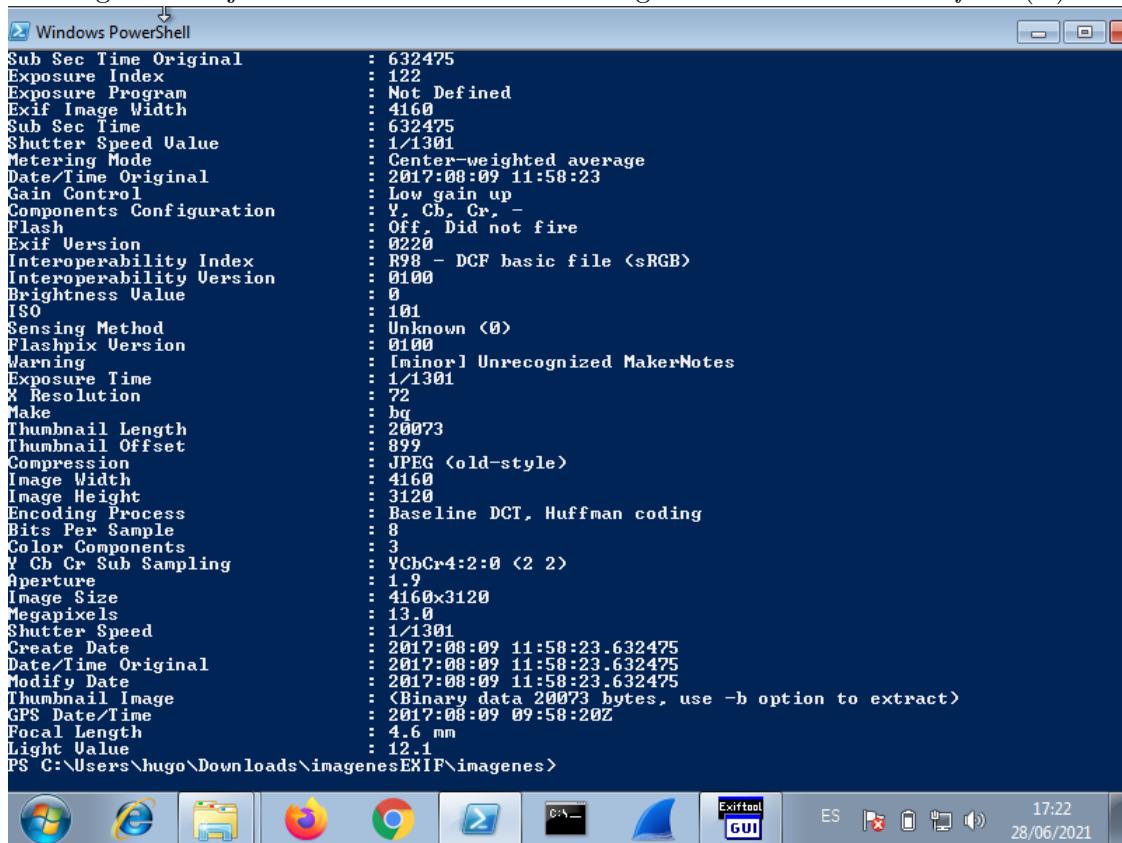
### 3.4.4. Imagen 4

Figura 52: Ejercicio 19: Metadatos de la imagen 4 con el comando *exiftool* (I)



```
Windows PowerShell
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes> exiftool.exe .\image4.jpg
ExifTool Version Number      : 12.28
File Name                   : image4.jpg
Directory                   :
File Size                   : 3.5 MiB
File Modification Date/Time : 2021:06:28 17:08:28+02:00
File Access Date/Time       : 2020:07:22 20:52:26+02:00
File Creation Date/Time    : 2020:07:22 20:52:26+02:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Big-endian <Motorola, MM>
Modify Date                 : 2017:08:09 11:58:23
GPS Img Direction           : 274
GPS Date Stamp               : 2017:08:09
GPS Img Direction Ref       : Magnetic North
GPS Time Stamp               : 09:58:20
GPS Altitude Ref             : Unknown <1.8>
Camera Model Name            : Aquaris E5
Y_Cb_Cr Positioning         : Centered
Resolution Unit              : inches
Y Resolution                : 72
Color Space                  : sRGB
Create Date                  : 2017:08:09 11:58:23
Focal Length                 : 4.6 mm
Aperture Value               : 1.9
Exposure Mode                : Auto
Sub Sec Time Digitized       : 632475
Exif Image Height             : 3120
Focal Length In 35mm Format   : 0 mm
Scene Capture Type            : Standard
Scene Type                   : Directly photographed
Sub Sec Time Original        : 632475
Exposure Index                : 122
Exposure Program              : Not Defined
Exif Image Width              : 4160
Sub Sec Time                 : 632475
Shutter Speed Value           : 1/1301
Metering Mode                 : Center-weighted average
Date/Time Original            : 2017:08:09 11:58:23
Gain Control                  : Low gain up
Components Configuration       : Y, Cb, Cr, -
Flash                         : Off, Did not fire
```

Figura 53: Ejercicio 19: Metadatos de la imagen 4 con el comando *exiftool* (II)



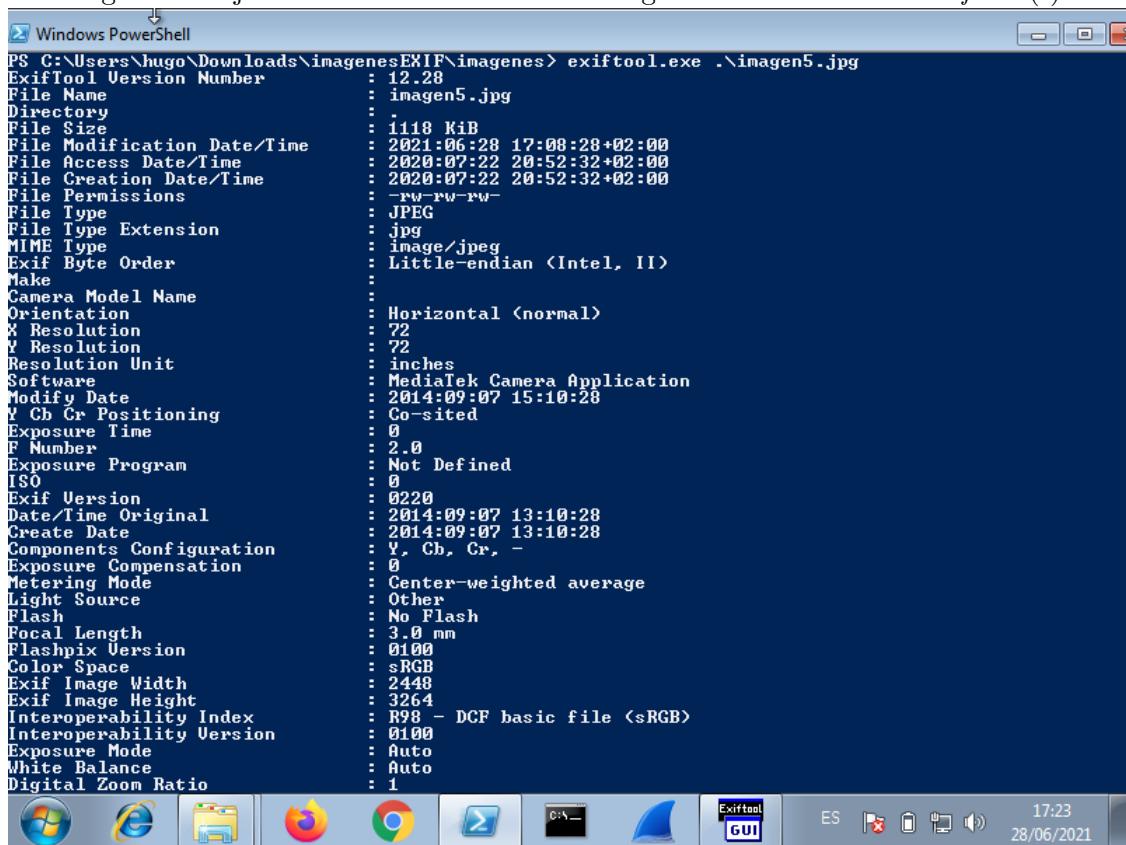
```
Windows PowerShell
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes> exiftool -v
Sub Sec Time Original      : 632475
Exposure Index              : 122
Exposure Program             : Not Defined
Exif Image Width             : 4160
Sub Sec Time                 : 632475
Shutter Speed Value          : 1/1301
Metering Mode                : Center-weighted average
Date/Time Original            : 2017:08:09 11:58:23
Gain Control                  : Low gain up
Components Configuration       : Y, Cb, Cr, -
Flash                         : Off, Did not fire
Exif Version                  : 0220
Interoperability Index        : R98 - DCF basic file <sRGB>
Interoperability Version       : 0100
Brightness Value               : 0
ISO                            : 101
Sensing Method                : Unknown <0>
Flashpix Version              : 0100
Warning                        : [minor] Unrecognized MakerNotes
Exposure Time                  : 1/1301
X Resolution                   : 72
Make                           : bq
Thumbnail Length               : 20073
Thumbnail Offset                : 899
Compression                     : JPEG <old-style>
Image Width                      : 4160
Image Height                     : 3120
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                  : 8
Color Components                  : 3
Y Ch Cr Sub Sampling           : YCbCr4:2:0 <2 2>
Aperture                         : 1.9
Image Size                        : 4160x3120
Megapixels                         : 13.0
Shutter Speed                     : 1/1301
Create Date                      : 2017:08:09 11:58:23.632475
Date/Time Original                : 2017:08:09 11:58:23.632475
Modify Date                       : 2017:08:09 11:58:23.632475
Thumbnail Image                  : <Binary data 20073 bytes, use -b option to extract>
GPS Date/Time                    : 2017:08:09 09:58:20Z
Focal Length                      : 4.6 mm
Light Value                        : 12.1
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes>
```

Con lo anterior visto, se procede a llenar la lista de datos requeridos:

- **Fecha en la que fue tomada la imagen:** 2017/08/09 11:58:23
- **Marca de la cámara:** bq
- **Modelo de la cámara:** Aquaris E5
- **Características de la imagen:**
  - **Ancho y alto en píxeles:** Ancho 4160, alto 3120
  - **Resolución:** 4160x3120
  - **Bits de color por pixel:** 8 bits y 3 canales, así que 24 bits de color por pixel
- **Tamaño del archivo:** 3.5 MiB
- **Ubicación GPS:** No está presente

### 3.4.5. Imagen 5

Figura 54: Ejercicio 19: Metadatos de la imagen 5 con el comando *exiftool* (I)



```
Windows PowerShell
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes> exiftool.exe .\imagen5.jpg
ExifTool Version Number      : 12.28
File Name                   : imagen5.jpg
Directory                   :
File Size                   : 1110 KiB
File Modification Date/Time : 2021:06:28 17:08:28+02:00
File Access Date/Time       : 2020:07:22 20:52:32+02:00
File Creation Date/Time    : 2020:07:22 20:52:32+02:00
File Permissions            : -rw-rw-rw-
File Type                  : JPEG
File Type Extension        : jpg
MIME Type                  : image/jpeg
Exif Byte Order             : Little-endian (Intel, II)
Make                         :
Camera Model Name          :
Orientation                 : Horizontal (normal)
X Resolution                : 72
Y Resolution                : 72
Resolution Unit             : inches
Software                     : MediaTek Camera Application
Modify Date                 : 2014:09:07 15:10:28
YCbCr Positioning          : Co-sited
Exposure Time               : 0
F Number                    : 2.0
Exposure Program            : Not Defined
ISO                          : 0
Exif Version                : 0220
Date/Time Original          : 2014:09:07 13:10:28
Create Date                 : 2014:09:07 13:10:28
Components Configuration    : Y, Cb, Cr, -
Exposure Compensation       : 0
Metering Mode               : Center-weighted average
Light Source                 : Other
Flash                        : No Flash
Focal Length                : 3.0 mm
Flashpix Version            : 0100
Color Space                 : sRGB
Exif Image Width            : 2448
Exif Image Height           : 3264
Interoperability Index      : R98 - DCF basic file (sRGB)
Interoperability Version    : 0100
Exposure Mode               : Auto
White Balance                : Auto
Digital Zoom Ratio          : 1
```

Figura 55: Ejercicio 19: Metadatos de la imagen 5 con el comando *exiftool* (II)

```
Resolution Unit : inches
Software       : MediaTek Camera Application
Modify Date    : 2014:09:07 13:10:28
YCbCr Positioning : Co-sited
Exposure Time   : 0
F Number        : 2.0
Exposure Program : Not Defined
ISO             : 0
Exif Version    : 0220
Date/Time Original : 2014:09:07 13:10:28
Create Date     : 2014:09:07 13:10:28
Components Configuration : Y, Cb, Cr, -
Exposure Compensation : 0
Metering Mode   : Center-weighted average
Light Source     : Other
Flash            : No Flash
Focal Length    : 3.0 mm
Flashpix Version: 0100
Color Space      : sRGB
Exif Image Width: 2448
Exif Image Height: 3264
Interoperability Index: R98 - DCF basic file <sRGB>
Interoperability Version: 0100
Exposure Mode   : Auto
White Balance   : Auto
Digital Zoom Ratio: 1
Scene Capture Type: Standard
Compression     : JPEG (old-style)
Thumbnail Offset: 276
Thumbnail Length: 10131
JFIF Version    : 1.01
Image Width     : 2448
Image Height    : 3264
Encoding Process: Baseline DCT, Huffman coding
Bits Per Sample: 8
Color Components: 3
YCbCr Sub Sampling: YCbCr4:2:2 (2 1)
Aperture        : 2.0
Image Size       : 2448x3264
Megapixels      : 8.0
Shutter Speed   : 0
Thumbnail Image: <Binary data 10131 bytes, use -b option to extract>
Focal Length    : 3.0 mm
PS C:\Users\hugo\Downloads\imagenes\EXIF\imagenes>
```

Con lo anterior visto, se procede a llenar la lista de datos requeridos:

- **Fecha en la que fue tomada la imagen:** 2014/09/07 13:10:28
- **Marca de la cámara:** No está presente
- **Modelo de la cámara:** No está presente
- **Características de la imagen:**
  - **Ancho y alto en píxeles:** Ancho 2448, alto 3264
  - **Resolución:** 2448x3264
  - **Bits de color por pixel:** 8 bits y 3 canales, así que 24 bits de color por pixel
- **Tamaño del archivo:** 1118 KiB
- **Ubicación GPS:** No está presente

## 4. Práctica 04

### 4.1. Ejercicio 7

Figura 56: Ejercicio 7: Enunciado (I).

Las diferentes herramientas forenses tienen diferentes capacidades y características. Es normal que la información que no podemos obtener fácilmente con una herramienta, sea más fácil de obtener desde otra. Descargue de la página web <https://belkasoft.com/get> la herramienta BelkaSoft Evidence Center en su versión de Evaluación (trial-version). En dicha página introduzca un email válido. Al cabo de 24 horas, si tu solicitud es admitida por correo, recibirás un correo para descargar la copia de evaluación de BelkaSoft Evidence Center. Descomprime la carpeta comprimida **bec-trial.zip**. Una vez descomprimida, lanza la aplicación **becu.cm.trial.x64** que te permitirá instalar dicho software (hazlo en un equipo de tu propiedad). Una vez instalada la aplicación, debes activarla (realiza la activación On line). Una vez actives la aplicación deberás reiniciarla y estará lista para poder usarse en modo prueba durante los próximos 30 días. A continuación, crea un nuevo caso desde el interfaz de BelKasoft. En el nombre del caso pon DDMMAAAA-XX donde DD es el día en el que realiza el ejercicio, MM es el número del mes actual y AAAA es el año actual, siendo XX el número del ejercicio que está realizando. Ponga su nombre y sus datos en la información del Investigador (también su dirección de email de uniovi). Añada al caso la evidencia (Recursos Prácticas-P4-ChipoffLGK7.raw) como imagen de disco. Al igual que en el caso de Autopsy, Belkasoft tiene varios módulos de ingestión. Seleccione y configure los siguientes:

- Aplicaciones móviles estándar.
- Archivos (SQLite Databases).
- Archivos del sistema (solo los relativos a conexiones Wifi de Android).
- Correos (sólo los relativos al SO Android).
- Chats (sólo los relativos al SO Android).
- Datos de geolocalización (sólo los relativos al SO Android).
- Documentos (a excepción del SO Mac OS).
- Imágenes.
- Miniaturas (sólo los relativos al SO Android).
- Navegadores (sólo los más comunes en el SO Android).
- Redes sociales (Facebook, Facebook Messenger, Google Plus y Twitter).
- Servicios en la nube (sólo los relativos al SO Android).
- Videos.

Figura 57: Ejercicio 7: Enunciado (II).

Además, configure en la misma ventana las opciones de Análisis para que solamente se analice la partición userdata y system. En cuanto a las opciones de Carving,

9

---

configure para que se apliquen tanto al espacio asignado como al espacio sin asignar en las particiones userdata y system.

Pulse Terminar y comenzará el proceso de ingestión y análisis de las evidencias. Cuando haya finalizado, conteste a las siguientes preguntas:

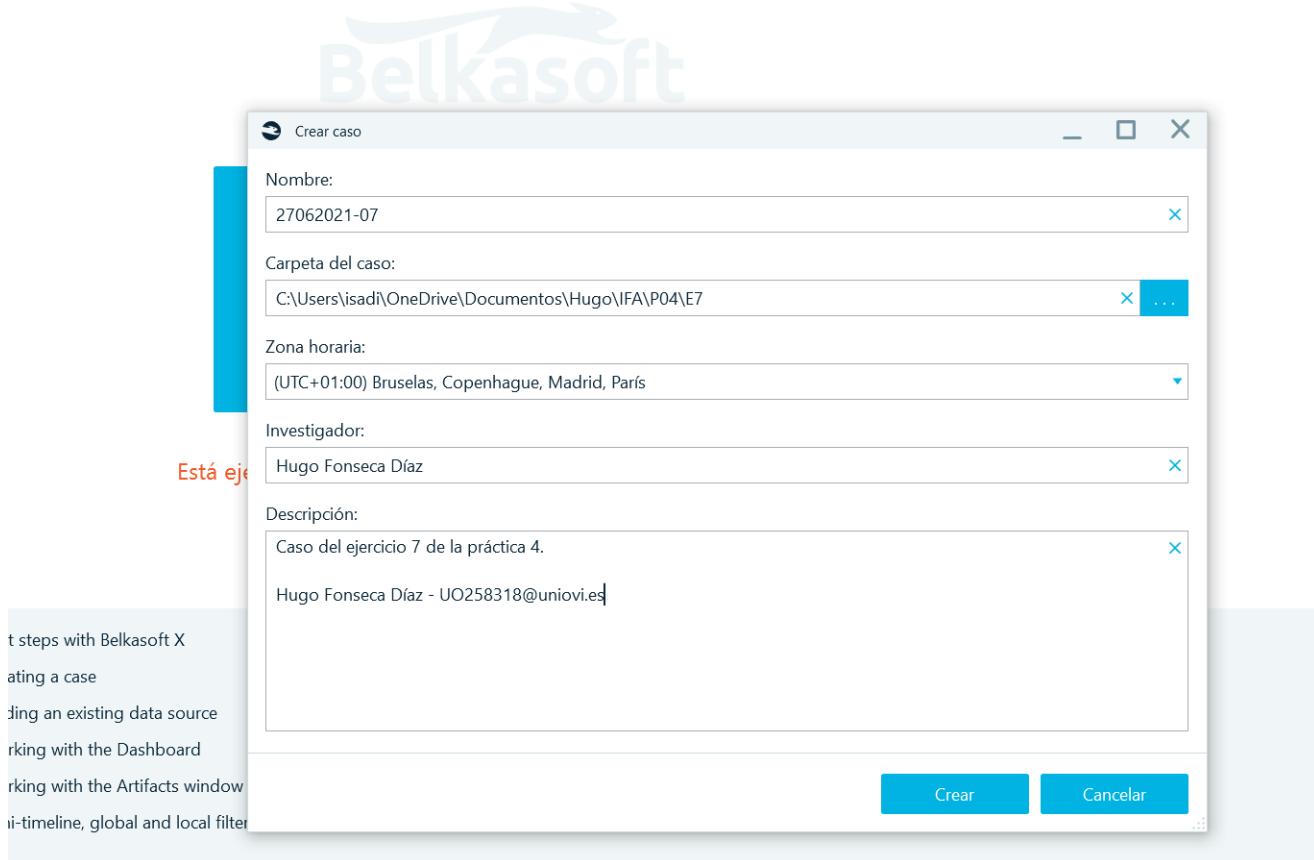
Figura 58: Ejercicio 7: Enunciado (III).

- rr) ¿Cuántos documentos han sido identificados en el teléfono intervenido?
- ss) De los documentos identificados, ¿cuántos son pdfs?
- tt) De las URLs visitadas, ¿cuántas corresponden a Facebook?
- uu) ¿Cuál fue la hora de la última visita a <http://www.facebook.com>?
- vv) ¿Cuántos ficheros con imágenes fueron encontrados en el teléfono?
- ww) ¿Cuántos de los ficheros que contienen imágenes están en formato jpg?
- xx) Aplique el filtro de análisis sobre el conjunto de imágenes para detectar en cuántas de ellas se detecta un rostro e indique el número de rostros detectados.
- yy) Indique cuántos eventos de calendario se han identificado.
- zz) De los eventos de calendario, ¿cuántos se desarrollan en Los Ángeles?
- aaa) ¿Cuál es la fecha de comienzo del primer evento de los desarrollados en Los Ángeles?

Debido a que la máquina que se utiliza para hacer los ejercicios tiene un sistema operativo Linux, el ejercicio 7 se realizó en el ordenador de un familiar. Se han incluído datos personales en las capturas para asegurar la autoría de las mismas.

Lo primero que se debe hacer en este ejercicio es crear un caso en la herramienta *Belkasoft Evidence Center X*.

Figura 59: Ejercicio 4: Creación del caso

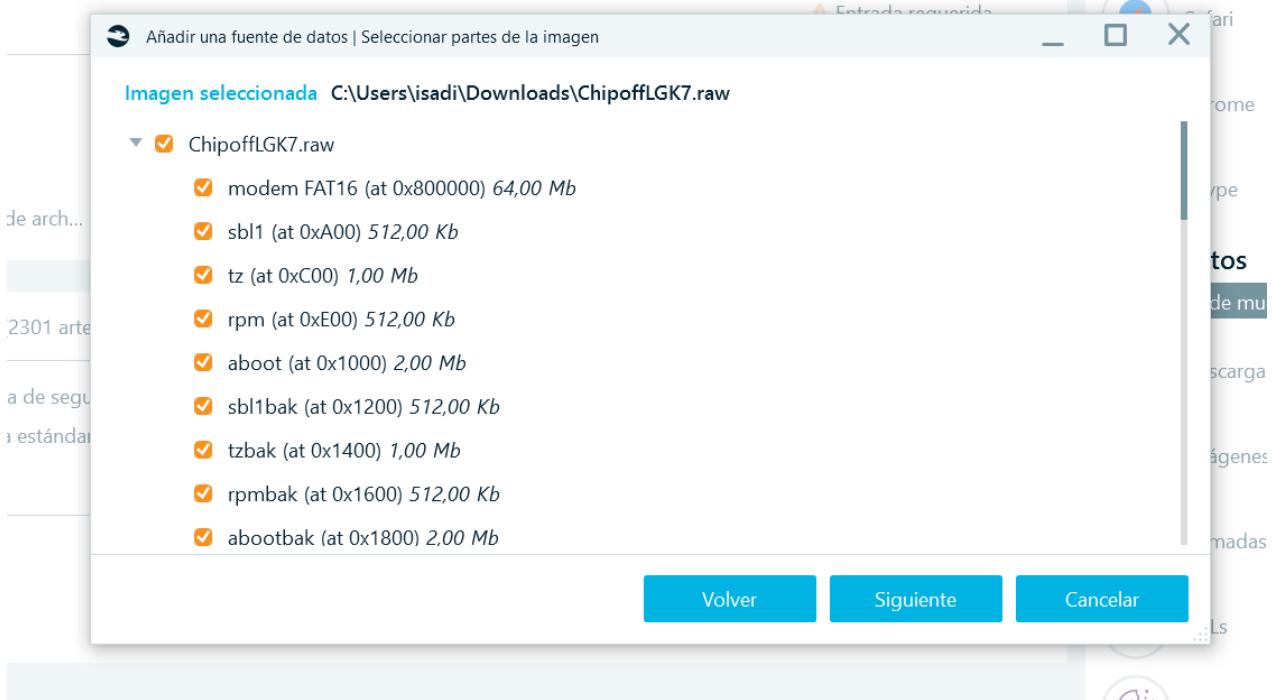


Se selecciona la imagen.

Figura 60: Ejercicio 4: Selección de la imagen

a de seguridad de iTunes

› estándar romance



Se eligen las opciones que pide el enunciado.

Figura 61: Ejercicio 4: Tipo de análisis

Parte	Tipo de análisis	Tipo de carving
factory	No aplicable	No carving
mpt Ext4	Ningún análisis seleccionado	No carving
system Ext4	Archivos existentes, Nested data sour...	Carve all space
cache Ext4	Ningún análisis seleccionado	No carving
userdata Ext4	Archivos existentes, Nested data sour...	Carve all space
grow	No aplicable	No carving
Espacio sin asignar	No aplicable	No carving

Volver Siguiente Cancelar

Se configuran las opciones de análisis avanzadas.

Figura 62: Ejercicio 4: Opciones de análisis avanzadas

Perfil: Custom

**Tipos de artefactos**

- Todos
- Aplicaciones móviles estándar
- Archivos
- Archivos de sistema
- Audios
- Chats
- Correos
- Datos de geolocalización
- Documentos
- Imágenes
- Juegos en línea multiusuario
- Miniaturas
- Navegadores
- Otras aplicaciones móviles
- P2P
- Redes sociales
- Servicios en la nube
- Sistemas de pago
- Videos

**Aplicaciones y formatos**

- Ventanas
- Bebo
- Facebook
- Facebook Messenger
- Google Plus
- Myspace
- Odnoklassniki
- Orkut
- Twitter
- VKontakte

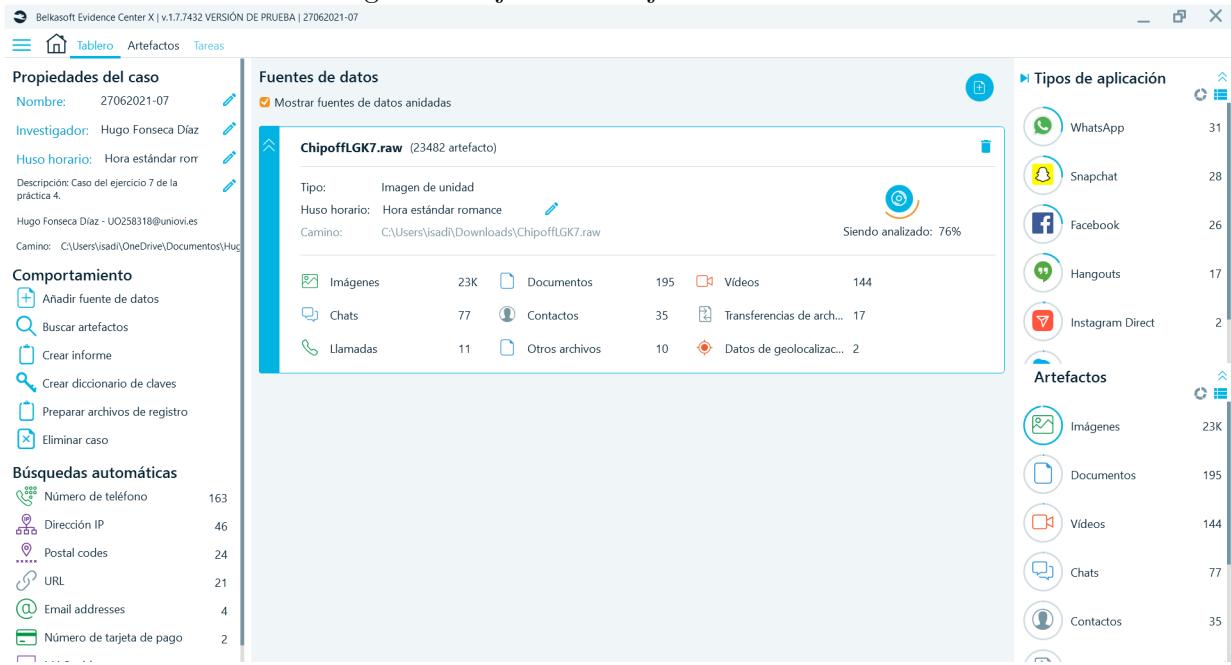
No extraer datos, realice solamente una búsqueda de perfil  
(Utilice esta opción para triaje)

Filtro: [ ]

Volver Siguiente Cancelar

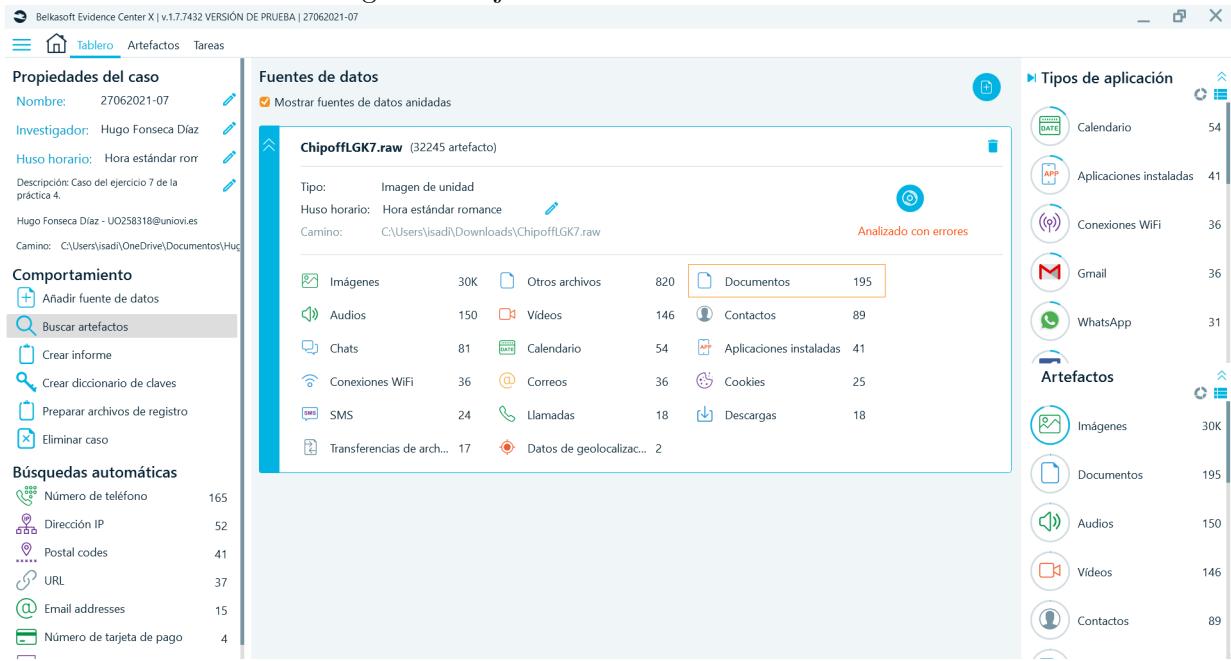
Se ejecuta el análisis, nótese que el tiempo de ejecución es bastante superior al que se obtuvo al analizar la misma imagen con Autopsy, aunque los resultados son más completos.

Figura 63: Ejercicio 4: Ejecución del análisis



Finalizado el análisis, se comienza a responder a las preguntas del ejercicio. Cabe mencionar que el análisis ha finalizado con errores, pero considerando los resultados obtenidos y viendo el tiempo de ejecución, no se cree conveniente reintentar el análisis.

Figura 64: Ejercicio 4: Resultado del análisis



rr) Como se puede observar en la anterior captura, hay 195 documentos identificados.

ss)

Figura 65: Ejercicio 4: Documentos de tipo *pdf*

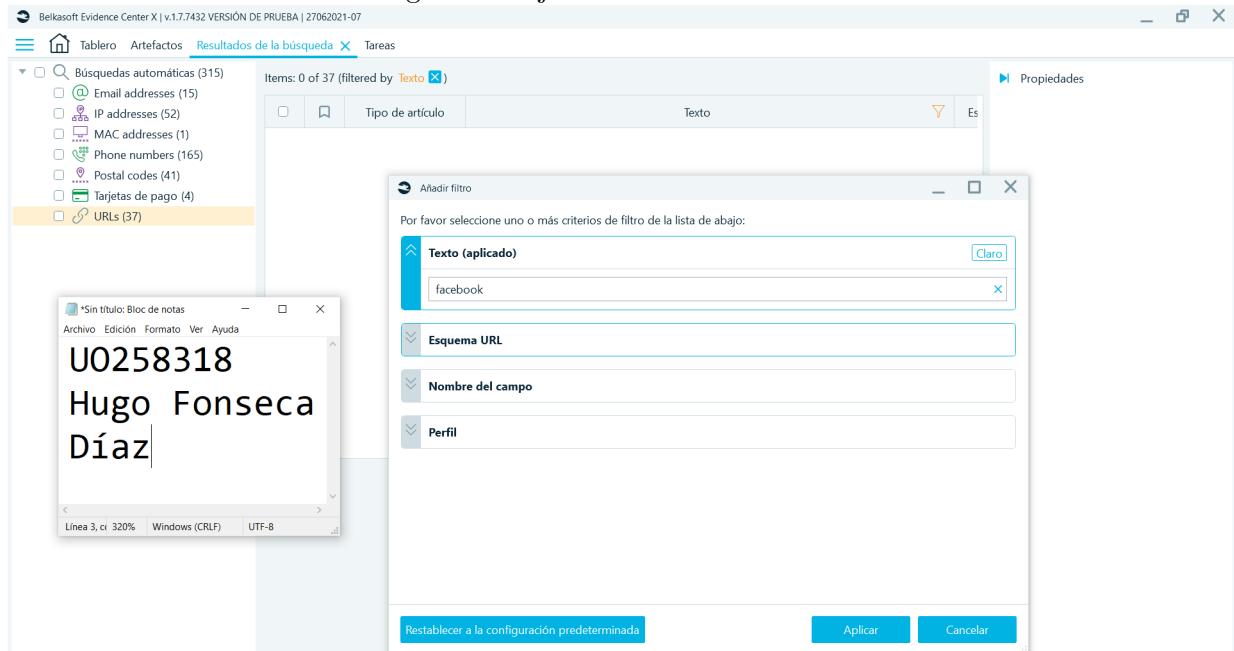
The screenshot shows the Belkasoft Evidence Center X interface. The top navigation bar includes 'Belkasoft Evidence Center X | v.1.7.7432 VERSIÓN DE PRUEBA | 27/06/2021-07' and tabs for 'Reporte', 'Tablero', 'Artefactos' (selected), and 'Tareas'. Below the tabs is a timeline from 2003 to 2020. The left sidebar shows a tree view of artifacts: 'Aplicaciones instaladas (41)', 'Audios (150)', 'Calendario (54)', 'Chats (81)', 'Conexiones WiFi (36)', 'Contactos (89)', 'Correos (36)', 'Datos de geolocalización (2)', 'Documentos (195)' (selected), 'Imágenes (30493)', 'Llamadas (18)', 'Navegadores (43)', 'Otros archivos (820)', 'SMS (24)', 'Transferencias de archivos (17)', and 'Videos (146)'. The main area displays a table with columns: 'Tipo de archivo', 'Vista preliminar...', 'Estado', 'Nombre del a...', and 'Archivos emp...'. One item is listed: 'Forensics is an emerg' with 'Valid' status and file 'forensics.pdf'. A preview window shows the PDF content: 'U0258318', 'Hugo Fonseca', and 'Díaz'. The properties panel on the right provides detailed information:

General	
Vista preliminar del texto	Forensics is an emerging technology that is branching off into many different avenues (e.g., PDA Forensics, Cell Phone Forensics, Network Forensics, and Stand Alone machine Forensics.)
Estado	Valid
Está eliminado	No
Archivo	
Nombre del archivo	forensics.pdf
Ruta	image:\8\vol_2961178624\media\0\Download\forensics.pdf
Desplazamiento (bytes)	2347466752
Tamaño del archivo (bytes)	24143
Creado (UTC)	06/11/2018 19:52:56

Hay un solo documento de tipo *pdf*, llamado *forensics.pdf*.

tt)

Figura 66: Ejercicio 4: URLs visitadas



No hay ninguna url correspondiente a *Facebook*.

uu)

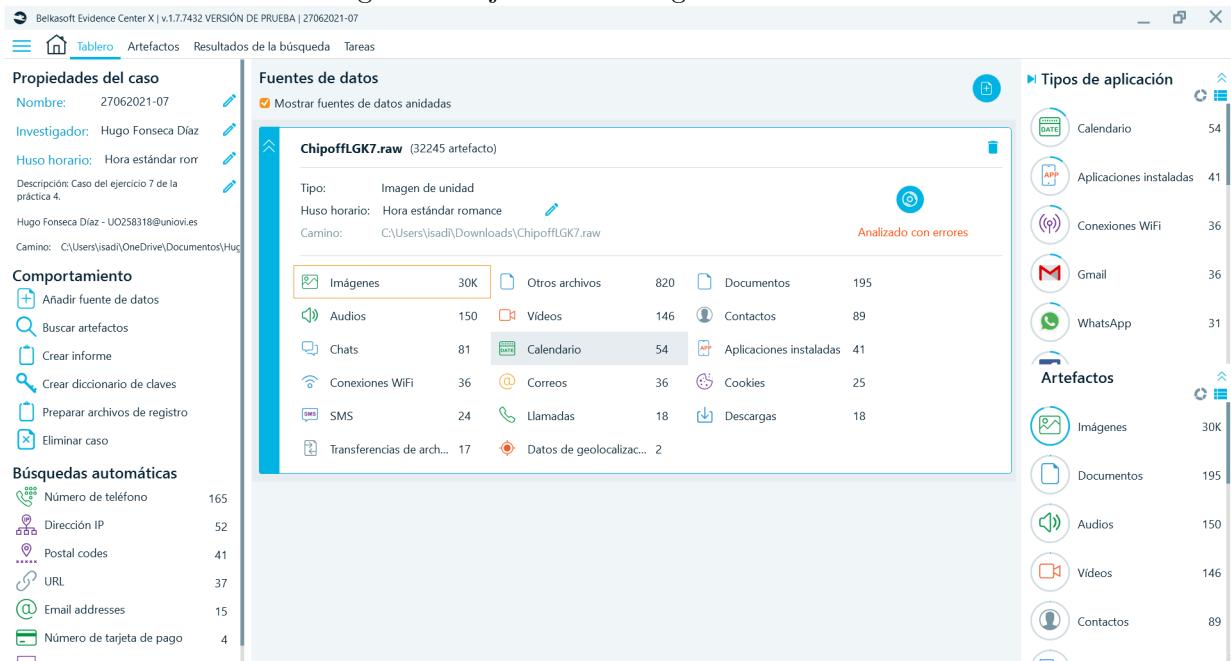
Figura 67: Ejercicio 4: Cookies relativas a *Facebook*

The screenshot shows the Belkasoft Evidence Center X interface. The top navigation bar includes 'Belkasoft Evidence Center X | v.1.7.7432 VERSIÓN DE PRUEBA | 27/06/2021-07', 'Tablero', 'Artefactos' (selected), 'Resultados de la búsqueda', and 'Tareas'. A timeline at the top right spans from 2003 to 2020. The left sidebar has 'Reporte' selected, followed by 'Estructura' and 'Visión general'. Under 'Visión general', there's a tree view of artifacts: Aplicaciones instaladas (41), Audios (150), Calendario (54), Chats (81), Conexiones WiFi (36), Contactos (89), Correos (36), Datos de geolocalización (2), Documentos (195), Imágenes (30493), Llamadas (18), Navegadores (43), Cookies (25) (selected), Descargas (18), Otros archivos (820), SMS (24), Transferencias de archivos (17), and Videos (146). The main pane shows a table titled '425 Anfitrión' with columns: #, Ficha, Tipo, Host, Fecha de v..., Fecha de venc..., Fecha de mod..., Fecha. One row is highlighted for a cookie from '.facebook.com' with a value of 'fr' and a long alphanumeric string. To the right, a 'Propiedades' panel is open for this cookie, showing details like Host (.facebook.com), Clave (fr), Valor (long string), and various dates/times. Below the table, a note window titled 'Sin título: Bloc de notas' contains the text: 'U0258318', 'Hugo Fonseca', and 'Díaz'. The bottom status bar shows '.facebook.com', 'Línea 3, cr 320%', 'Windows (CRLF)', and 'UTF-8'.

Aunque no haya ninguna url visitada correspondiente a *Facebook*, inspeccionando las cookies se puede observar que la hora de la última visita a *Facebook* fue a las 13:42:23 del día 2019/11/09.

vv)

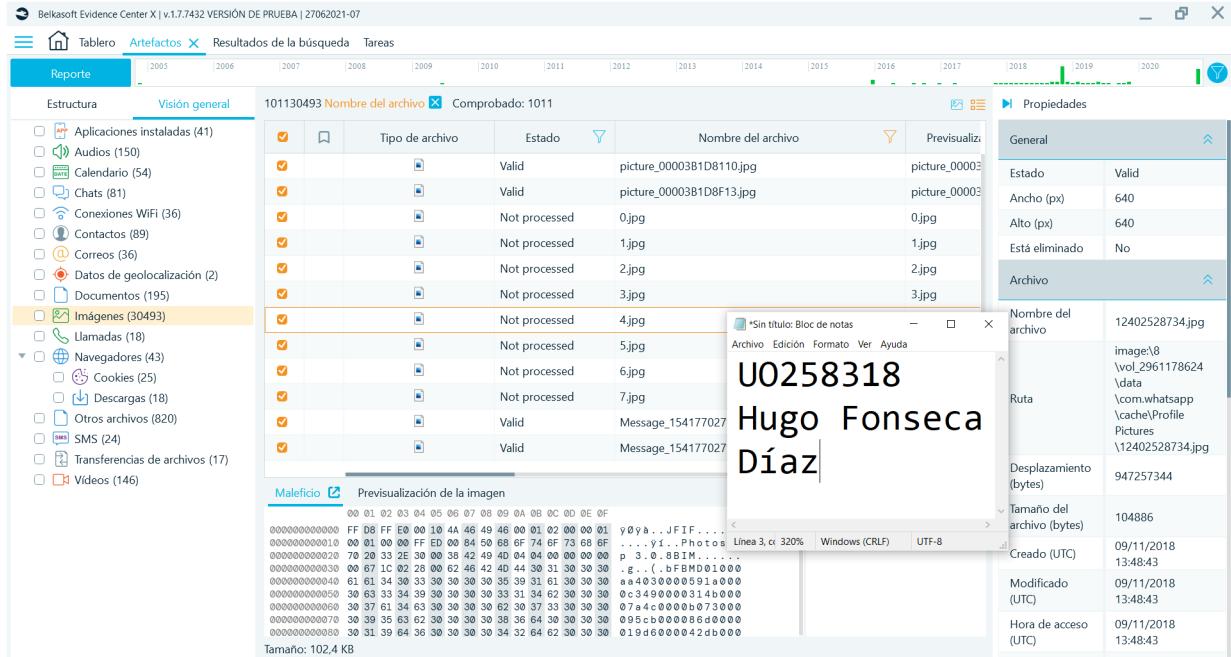
Figura 68: Ejercicio 4: Imágenes identificadas



Como se observa en la figura, se identificaron algo más de 30.000 imágenes.

ww)

Figura 69: Ejercicio 4: Imágenes en formato *jpg*



Se han encontrado 1011 imágenes en formato *jpg*. Sin embargo, se han buscado mediante el nombre del fichero, lo que no es la mejor aproximación (ya que podría haber imágenes con tipo MIME *jpg* que no tuvieran extensión), pero como no se encontró ningún filtro por tipo MIME se deja esta solución. Sería una funcionalidad interesante para el programa (a menos que ya exista, en cuyo caso no pudo encontrarse).

xx)

Figura 70: Ejercicio 4: Reconocimiento de rostros

The screenshot shows the Belkasoft Evidence Center X interface. The top navigation bar includes 'Belkasoft Evidence Center X | v.1.7.7432 VERSIÓN DE PRUEBA | 27/06/2021-07' and tabs for 'Tablero', 'Artefactos' (selected), 'Resultados de la búsqueda', and 'Tareas'. A timeline from 2003 to 2020 is visible above the search results.

The left sidebar shows a tree view of artifacts: 'Aplicaciones instaladas (41)', 'Audios (150)', 'Calendario (54)', 'Chats (81)', 'Conexiones WiFi (36)', 'Contactos (89)', 'Correos (36)', 'Datos de geolocalización (2)', 'Documentos (195)', 'Imagenes (30493)' (selected), 'Caras (100)' (selected), 'Llamadas (18)', 'Navegadores (43)', 'Cookies (25)', 'Descargas (18)', 'Otros archivos (820)', 'SMS (24)', 'Transferencias de archivos (17)', and 'Vídeos (146)'.

The main area displays a table titled 'Elementos: 100' with columns: 'Ti...', 'Estado', 'Nombre del a...', 'Previsualización', 'Faces', and 'Nombre de la...'. The table lists 100 entries, all marked as 'Valid' and showing 'Faces' counts ranging from 0 to 1. A preview window shows a smiling emoji face.

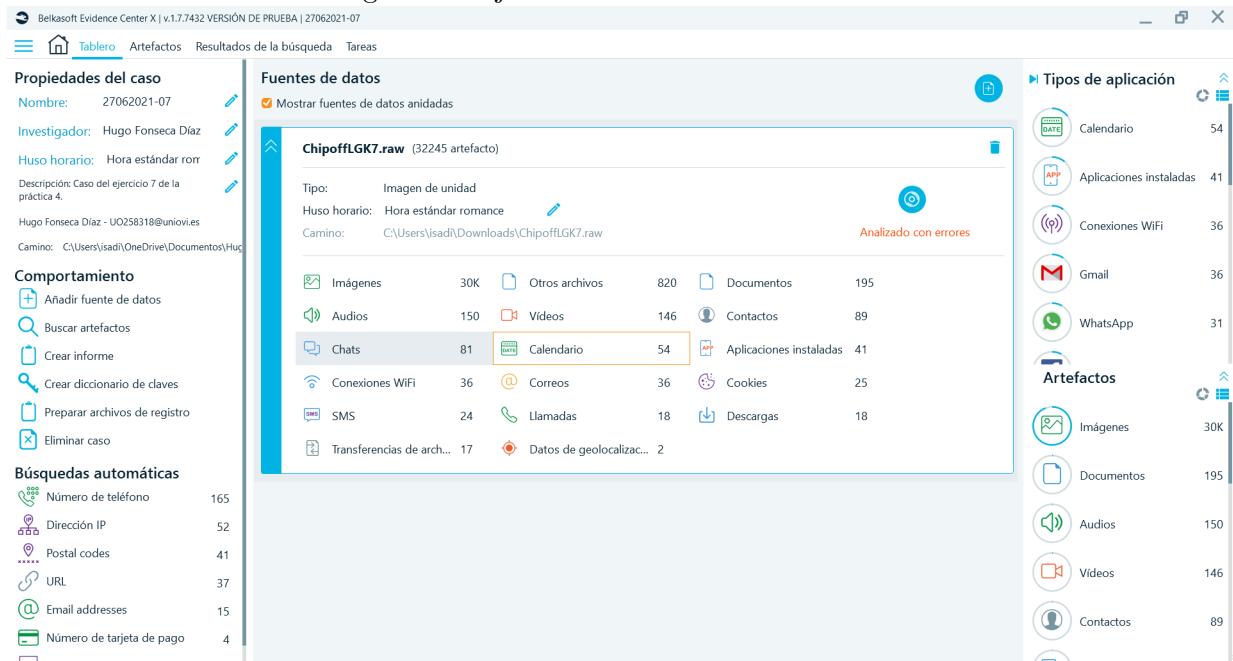
A context menu is open over one of the table rows, showing options like 'Archivo', 'Edición', 'Formato', 'Ver', and 'Ayuda'. The 'Archivo' option is highlighted.

The right side features a 'Propiedades' panel with two tabs: 'General' and 'Archivo'. The 'General' tab shows details like 'Estado: Valid', 'Faces: Rostro 0', 'Ancho (px): 60', 'Alto (px): 60', and 'Está eliminado: No'. The 'Archivo' tab shows the file path: 'bitmoji-ifrowny-preview-normal.png' located at 'image\8\vol\_2961178624\data\com.snapchat.android\files\category\_icons\bitmoji-geopack-en-bitmoji-hometab-preview-hometab\_exp2\1\drawable-hdpi\bitmoji-ifrowny-preview-normal.png'.

Hay 100 imágenes con rostros detectados, aunque en su mayoría se trata de *emojis*, y muchos de ellos ni siquiera son rostros.

yy)

Figura 71: Ejercicio 4: Eventos de calendario



Se han identificado 54 eventos de calendario.

zz)

Figura 72: Ejercicio 4: Eventos en Los Ángeles

The screenshot shows the Belkasoft Evidence Center X interface. The top navigation bar includes 'Belkasoft Evidence Center X | v1.7.7432 VERSIÓN DE PRUEBA | 27062021-0' and tabs for 'Tablero', 'Artefactos' (selected), 'Resultados de la búsqueda', and 'Tareas'. Below the tabs is a timeline from 2005 to 2020. A search bar indicates '154 Ubicación' results. The left sidebar has a tree view of artifacts, with 'Calendario (54)' selected. The main pane displays a table with columns: Organizador..., Lugar del eve..., Descripción, Comentarios, Hora de in..., and Hora. One row is highlighted for 'cfttmobile1@gmail.com' at 'Los angeles' on '23/04/2016 8:00:00'. A preview window shows a note titled 'U0258318' containing the text 'Hugo Fonseca Diaz'. On the right, the 'Propiedades' panel is open, showing details like 'Recurrencia del evento: FREQ=YEARLY;WKS T=MO', 'Organizador del evento: cfttmobile1@gmail.com', and 'Lugar del evento: Los Angeles'. The bottom pane shows a hex dump of a SQLite database file, specifically the 'Maleficio' SQLite database, with a size of 160 KB and position 147184:272.

Solo uno se desarrolla en Los Ángeles.

aaa) La fecha de comienzo del evento puede verse en la anterior captura, es el 2016/04/23 a las 8:00:00.

## 5. Práctica 05

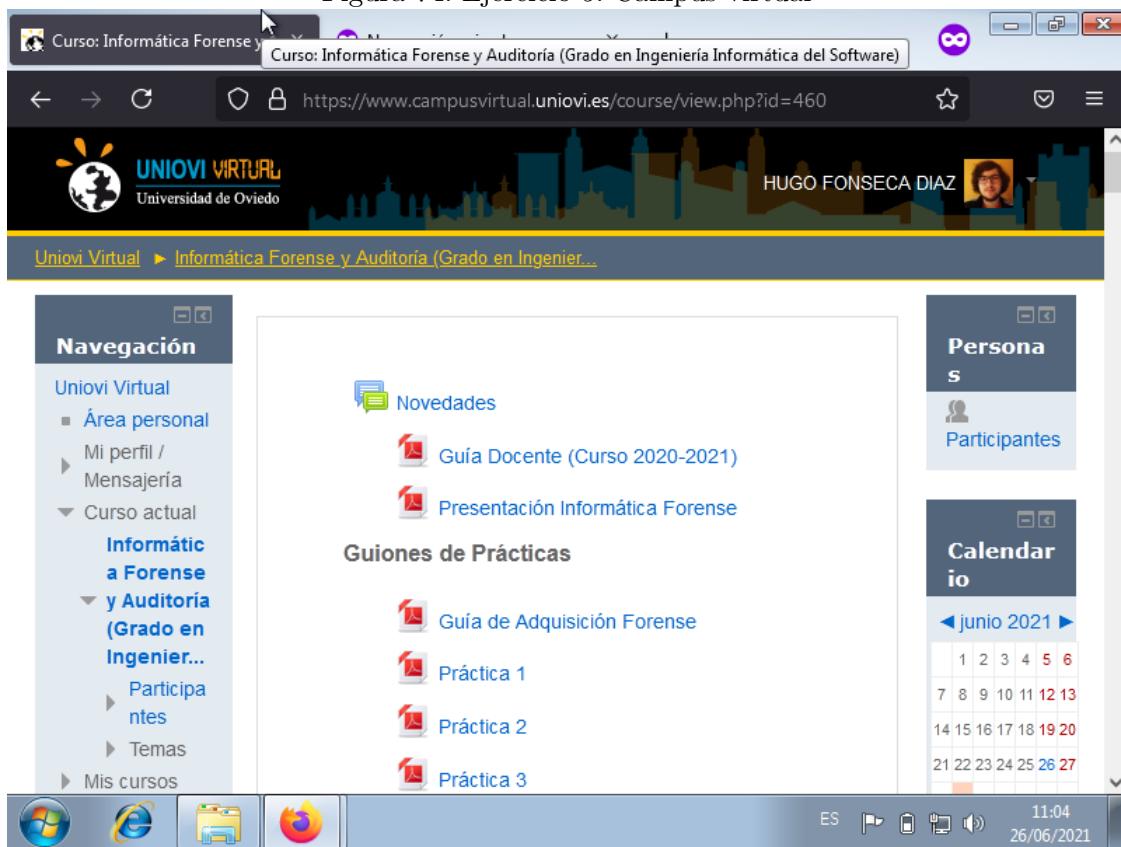
### 5.1. Ejercicio 5

Figura 73: Ejercicio 5: Enunciado.

Antes de realizar el ejercicio, abre una ventana y conéctate desde ella a la página web del campus virtual de la asignatura y no cierre dicha ventana. Busca entre las utilidades que proporciona Nirsoft aquellas que te permiten obtener las conexiones de red existentes con los puertos de red abiertos y los ejecutables a la escucha en dichos puertos. Almacene dicha lista en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia. Compruebe que en dicho listado aparece el ejecutable del navegador en el que tiene abierta la conexión al campus virtual y realice una captura de pantalla donde se pueda apreciar el puerto local y el puerto remoto para dicha conexión, así como la dirección IP o el FQDN del destino. Realice de nuevo el ejercicio, pero esta vez utilizando el comando del sistema con las opciones adecuadas que permite averiguar dicha información.

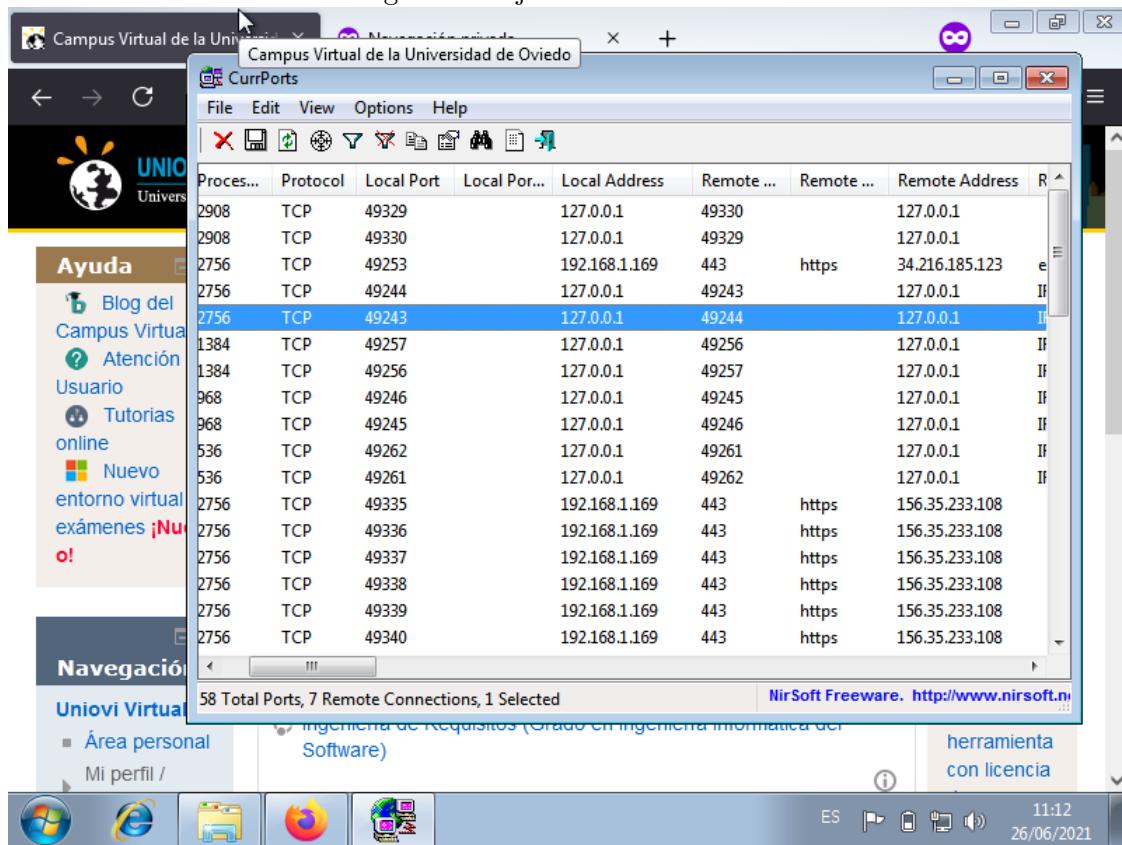
Se realiza una conexión al campus virtual con el navegador Firefox en navegación privada.

Figura 74: Ejercicio 5: Campus virtual



Se utiliza la aplicación de Nirsoft llamada *CurrPorts*.

Figura 75: Ejercicio 5: *CurrPorts*



Se ordena la salida de la aplicación por nombre de proceso para poder visualizar todos los procesos de Firefox.

Figura 76: Ejercicio 5: *CurrPorts* - Firefox

The screenshot shows the CurrPorts application interface. The title bar reads "CurrPorts". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu is a toolbar with icons for search, file operations, and filtering. The main window is a grid table with the following columns: Process Name, Process ID, Protocol, Local Port, Local Port Range, Local Address, Remote Port, Remote Port Range, Remote Address, and Remote Host. The table lists numerous connections, primarily from Firefox processes (firefox.exe) running under various process IDs (e.g., 2908, 2756, 1384). Other entries include svchost.exe (process IDs 2032, 1208) and services.exe (process ID 428). Most connections are TCP, with some UDP entries. Local ports range from 49243 down to 1208, and remote ports range from 49330 down to 1900. Local addresses are mostly 127.0.0.1 or 192.168.1.169, while remote addresses include 127.0.0.1, 34.216.185.123, and ec2-34-21. The status bar at the bottom indicates "52 Total Ports, 1 Remote Connections, 1 Selected" and "NirSoft Freeware. http://www.nirsoft.net". The taskbar at the bottom shows icons for the Start button, Internet Explorer, File Explorer, Firefox, and Task View, along with system tray icons for battery, signal, volume, and date/time (11:14, 26/06/2021).

Process Name	Process ID	Protocol	Local Port	Local Port Range	Local Address	Remote Port	Remote Port Range	Remote Address	Remote Host
firefox.exe	2908	TCP	49329		127.0.0.1	49330		127.0.0.1	
firefox.exe	2908	TCP	49330		127.0.0.1	49329		127.0.0.1	
firefox.exe	2756	TCP	49253		192.168.1.169	443	https	34.216.185.123	ec2-34-21
firefox.exe	2756	TCP	49244		127.0.0.1	49243		127.0.0.1	IFA-WIN-1
firefox.exe	2756	TCP	49243		127.0.0.1	49244		127.0.0.1	IFA-WIN-1
firefox.exe	1384	TCP	49257		127.0.0.1	49256		127.0.0.1	IFA-WIN-1
firefox.exe	1384	TCP	49256		127.0.0.1	49257		127.0.0.1	IFA-WIN-1
firefox.exe	968	TCP	49246		127.0.0.1	49245		127.0.0.1	IFA-WIN-1
firefox.exe	968	TCP	49245		127.0.0.1	49246		127.0.0.1	IFA-WIN-1
firefox.exe	536	TCP	49262		127.0.0.1	49261		127.0.0.1	IFA-WIN-1
firefox.exe	536	TCP	49261		127.0.0.1	49262		127.0.0.1	IFA-WIN-1
lsass.exe	444	TCP	49157		0.0.0.0			0.0.0.0	
lsass.exe	444	TCP	49157		::			::	IFA-WIN-1
services.exe	428	TCP	49155		0.0.0.0			0.0.0.0	
services.exe	428	TCP	49155		::			::	IFA-WIN-1
svchost.exe	2032	UDP	3540	pnrr-port	::				IFA-WIN-1
svchost.exe	2032	TCP	3587	p2pgroup	::			::	IFA-WIN-1
svchost.exe	1208	UDP	1900	ssdp	127.0.0.1				
svchost.exe	1208	UDP	1900	ssdp	192.168.1.169				
svchost.exe	1208	UDP	3702	ws-disc...	0.0.0.0				
svchost.exe	1208	UDP	61458		0.0.0.0				
svchost.exe	1208	UDP	64443		192.168.1.169				

Curiosamente, no sale ninguna conexión con el campus virtual. Se prueba ahora con una ventana de navegación privada del navegador Chrome.

Figura 77: Ejercicio 5: *CurrPorts* - Chrome (I)

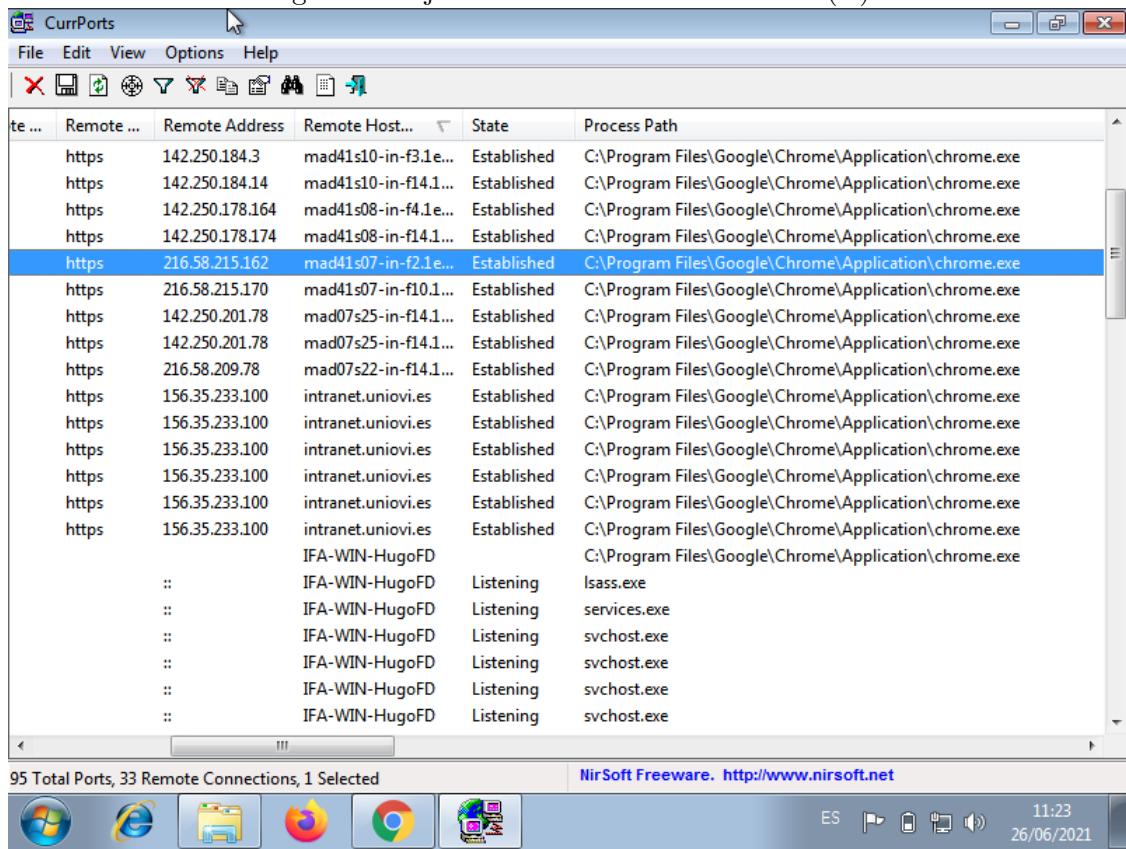
The screenshot shows the CurrPorts application interface. The main window displays a table of network connections. The columns are: Process Name, Proces..., Protocol, Local Port, L..., Local Address, Remote ..., Remote ..., Remote Address, and Remote Host... . The table contains numerous entries, primarily for chrome.exe processes, showing various local ports (e.g., 1320, 61129, 60873, 61224, 58059, 49346) connecting to remote hosts like 142.250.184.3, 142.250.184.14, 142.250.178.164, and 216.58.215.162. Other entries include Unknown processes and svchost.exe. The status bar at the bottom indicates 104 Total Ports, 33 Remote Connections, and 1 Selected.

Process Name	Proces...	Protocol	Local Port	L...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host...
chrome.exe	1320	TCP	55095		192.168.1.169	443	https	142.250.184.3	mad41s10-in-f3.1.e.
Unknown	0	TCP	61129		192.168.1.169	443	https	142.250.184.3	mad41s10-in-f3.1.e.
chrome.exe	1320	TCP	60873		192.168.1.169	443	https	142.250.184.14	mad41s10-in-f14.1.
chrome.exe	1320	TCP	61224		192.168.1.169	443	https	142.250.178.164	mad41s08-in-f4.1.e.
chrome.exe	1320	TCP	58059		192.168.1.169	443	https	142.250.178.174	mad41s08-in-f14.1.
chrome.exe	1320	TCP	49346		192.168.1.169	443	https	216.58.215.162	mad41s07-in-f2.1.e.
chrome.exe	1320	TCP	62806		192.168.1.169	443	https	216.58.215.170	mad41s07-in-f10.1.
chrome.exe	1320	TCP	58184		192.168.1.169	443	https	142.250.201.78	mad07s25-in-f14.1.
chrome.exe	1320	TCP	59054		192.168.1.169	443	https	142.250.201.78	mad07s25-in-f14.1.
Unknown	0	TCP	58927		192.168.1.169	443	https	142.250.200.77	mad07s24-in-f13.1.
chrome.exe	1320	TCP	59679		192.168.1.169	443	https	216.58.209.78	mad07s22-in-f14.1.
chrome.exe	1320	TCP	54110		192.168.1.169	443	https	156.35.233.100	intranet.uniovi.es
chrome.exe	1320	TCP	54834		192.168.1.169	443	https	156.35.233.100	intranet.uniovi.es
chrome.exe	1320	TCP	59230		192.168.1.169	443	https	156.35.233.100	intranet.uniovi.es
chrome.exe	1320	TCP	59565		192.168.1.169	443	https	156.35.233.100	intranet.uniovi.es
chrome.exe	1320	TCP	62909		192.168.1.169	443	https	156.35.233.100	intranet.uniovi.es
chrome.exe	1320	TCP	63405		192.168.1.169	443	https	156.35.233.100	intranet.uniovi.es
chrome.exe	1280	UDP	5353		::				IFA-WIN-HugoFD
lsass.exe	444	TCP	49157		::			::	IFA-WIN-HugoFD
services.exe	428	TCP	49155		::			::	IFA-WIN-HugoFD
svchost.exe	624	TCP	135	e...	::			::	IFA-WIN-HugoFD
svchost.exe	2032	TCP	3587	p...	::			::	IFA-WIN-HugoFD

104 Total Ports, 33 Remote Connections, 1 Selected      NirSoft Freeware. <http://www.nirsoft.net>

Windows Taskbar icons: Internet Explorer, File Explorer, Firefox, Google Chrome, and a system monitor icon. System tray icons: ES, battery, volume, and date/time (11:21, 26/06/2021).

Figura 78: Ejercicio 5: *CurrPorts* - Chrome (II)



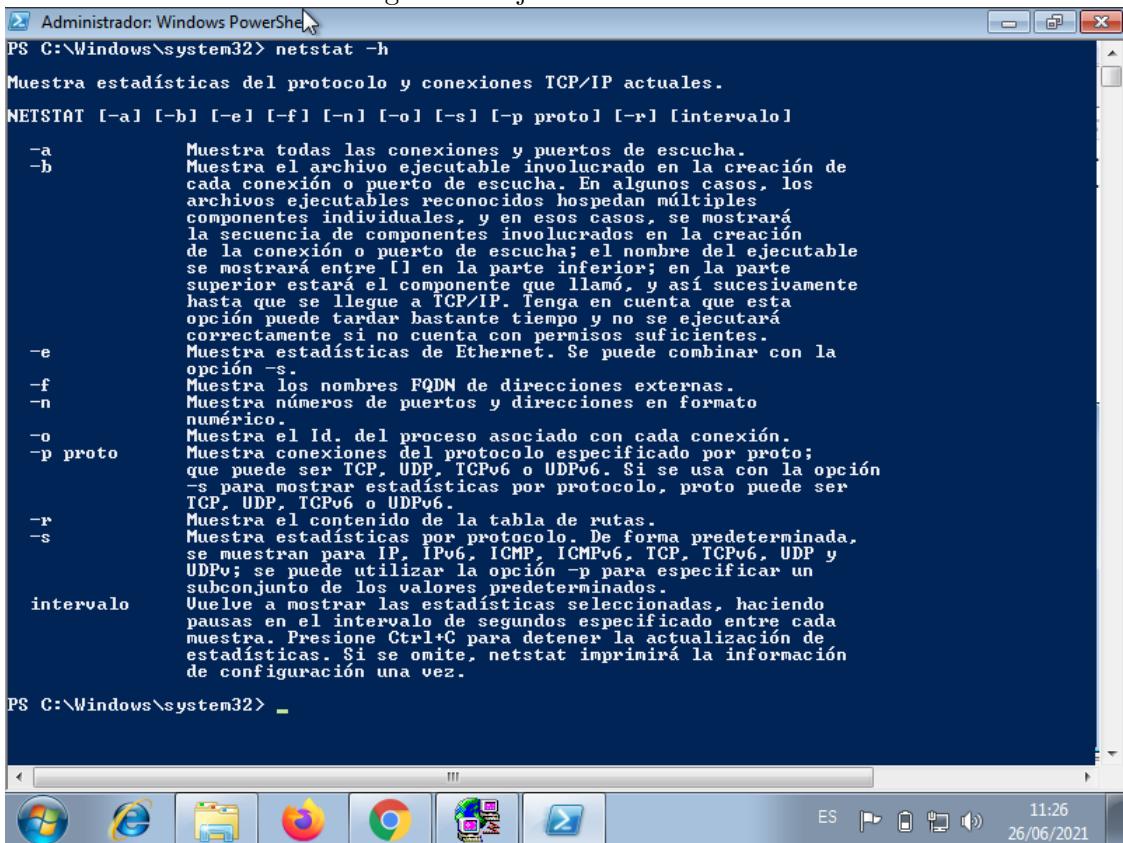
The screenshot shows the CurrPorts application interface. The main window displays a list of network connections. The columns are labeled: Remote Port, Remote Address, Remote Host..., State, and Process Path. The process path for most entries is C:\Program Files\Google\Chrome\Application\chrome.exe. There are also several listening ports listed under the host ::, including IFA-WIN-HugoFD, lsass.exe, services.exe, svchost.exe, and svhost.exe. At the bottom of the application window, there is a status bar showing "95 Total Ports, 33 Remote Connections, 1 Selected" and the developer information "NirSoft Freeware. http://www.nirsoft.net". Below the application window, the Windows taskbar is visible, featuring icons for the Start button, Internet Explorer, File Explorer, Firefox, Google Chrome, and Task View.

Remote Port	Remote Address	Remote Host...	State	Process Path
https	142.250.184.3	mad41s10-in-f3.1e...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	142.250.184.14	mad41s10-in-f14.1...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	142.250.178.164	mad41s08-in-f4.1e...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	142.250.178.174	mad41s08-in-f14.1...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	216.58.215.162	mad41s07-in-f2.1e...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	216.58.215.170	mad41s07-in-f10.1...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	142.250.201.78	mad07s25-in-f14.1...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	142.250.201.78	mad07s25-in-f14.1...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	216.58.209.78	mad07s22-in-f14.1...	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	156.35.233.100	intranet.uniovi.es	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	156.35.233.100	intranet.uniovi.es	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	156.35.233.100	intranet.uniovi.es	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	156.35.233.100	intranet.uniovi.es	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
https	156.35.233.100	intranet.uniovi.es	Established	C:\Program Files\Google\Chrome\Application\chrome.exe
	IFA-WIN-HugoFD			C:\Program Files\Google\Chrome\Application\chrome.exe
::	IFA-WIN-HugoFD	Listening	lsass.exe	
::	IFA-WIN-HugoFD	Listening	services.exe	
::	IFA-WIN-HugoFD	Listening	svchost.exe	
::	IFA-WIN-HugoFD	Listening	svchost.exe	
::	IFA-WIN-HugoFD	Listening	svchost.exe	
::	IFA-WIN-HugoFD	Listening	svchost.exe	

Ahora sí que se visualizan las conexiones con la intranet de uniovi. Se ha podido comprobar por casualidad que Firefox ofrece menos información sobre sus conexiones que Chrome, quizás por su mayor enfoque en la privacidad de los usuarios. Se desconoce si esto solo ocurre al usar navegación privada.

Si se quisiera obtener esta información por consola, lo primero habría que tener cuidado porque los comandos del equipo intervenido pueden no dar información confiable, pero suponiendo que es una operación segura, se deberá usar el comando `netstat`. Se listan a continuación sus opciones.

Figura 79: Ejercicio 5: *netstat -h*



Administrador: Windows PowerShell

```
PS C:\Windows\system32> netstat -h
Muestra estadísticas del protocolo y conexiones TCP/IP actuales.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-s] [-p proto] [-r] [intervalo]

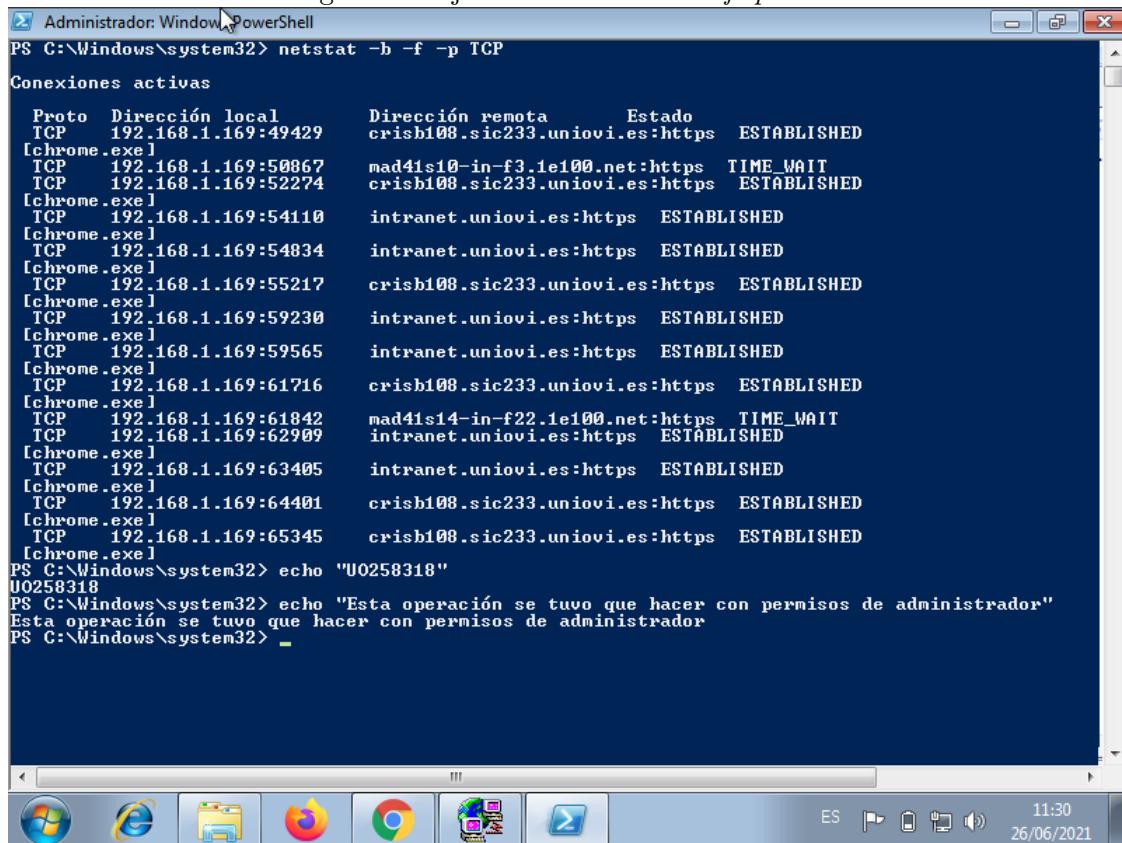
-a      Muestra todas las conexiones y puertos de escucha.
-b      Muestra el archivo ejecutable involucrado en la creación de
       cada conexión o puerto de escucha. En algunos casos, los
       archivos ejecutables reconocidos hospedan múltiples
       componentes individuales, y en esos casos, se mostrará
       la secuencia de componentes involucrados en la creación
       de la conexión o puerto de escucha; el nombre del ejecutable
       se mostrará entre [] en la parte inferior; en la parte
       superior estará el componente que llamó, y así sucesivamente
       hasta que se llegue a TCP/IP. Tenga en cuenta que esta
       opción puede tardar bastante tiempo y no se ejecutará
       correctamente si no cuenta con permisos suficientes.
-e      Muestra estadísticas de Ethernet. Se puede combinar con la
       opción -s.
-f      Muestra los nombres FQDN de direcciones externas.
-n      Muestra números de puertos y direcciones en formato
       numérico.
-o      Muestra el Id. del proceso asociado con cada conexión.
-p proto  Muestra conexiones del protocolo especificado por proto;
       que puede ser TCP, UDP, TCPv6 o UDPv6. Si se usa con la opción
       -s para mostrar estadísticas por protocolo, proto puede ser
       TCP, UDP, TCPv6 o UDPv6.
-r      Muestra el contenido de la tabla de rutas.
-s      Muestra estadísticas por protocolo. De forma predeterminada,
       se muestran para IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP y
       UDPv6; se puede utilizar la opción -p para especificar un
       subconjunto de los valores predeterminados.
intervalo  Vuelve a mostrar las estadísticas seleccionadas, haciendo
       pausas en el intervalo de segundos especificado entre cada
       muestra. Presione Ctrl+C para detener la actualización de
       estadísticas. Si se omite, netstat imprimirá la información
       de configuración una vez.

PS C:\Windows\system32> _
```

The screenshot shows a Windows PowerShell window titled "Administrador: Windows PowerShell". The command "netstat -h" is run, displaying the help text for the "netstat" command. The help text includes descriptions for various options: -a (show all connections and ports), -b (show executable involved in creation of connection or port), -e (show Ethernet statistics), -f (show fully qualified domain names of external addresses), -n (show numbers of ports and addresses in numeric format), -o (show process ID associated with each connection), -p (show connections for specified protocol: TCP, UDP, TCPv6, UDPv6), -r (show routing table), and -s (show statistics for specified protocol: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, UDPv6). It also describes the "-r" option for showing the routing table and the "-s" option for showing statistics by protocol. The bottom of the window shows the Windows taskbar with icons for Start, Internet Explorer, File Explorer, Firefox, Google Chrome, Control Panel, Task View, and Task Manager, along with system status icons like battery level, signal strength, and volume, and the date and time (11:26, 26/06/2021).

Lo que pide el ejercicio puede obtenerse mediante las flags *bfp*, cuyas funcionalidades fueron listadas en la anterior captura. La opción *p* requiere como argumento el nombre del protocolo que se está buscando, siendo en este caso TCP.

Figura 80: Ejercicio 5: `netstat -b -f -p TCP`



The screenshot shows a Windows PowerShell window titled "Administrador: Windows PowerShell". The command `netstat -b -f -p TCP` is run, displaying a list of active connections. The output includes columns for Proto, Dirección local, Dirección remota, and Estado. Most connections are to "intranet.uniovi.es:https" or "crisb108.sic233.uniovi.es:https" and are in an ESTABLISHED state. Some connections are in TIME\_WAIT state. The process "chrome.exe" is listed multiple times. The session ends with the command `echo "U0258318"`, which outputs "U0258318" and then "Esta operación se tuvo que hacer con permisos de administrador". The taskbar at the bottom shows icons for Internet Explorer, File Explorer, Firefox, Google Chrome, and others.

```
PS C:\Windows\system32> netstat -b -f -p TCP
Conexiones activas
Proto  Dirección local        Dirección remota      Estado
TCP    192.168.1.169:49429  crisb108.sic233.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:50867  mad41s10-in-f3.1e100.net:https  TIME_WAIT
TCP    192.168.1.169:52274  crisb108.sic233.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:54110  intranet.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:54834  intranet.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:55217  crisb108.sic233.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:59230  intranet.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:59565  intranet.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:61716  crisb108.sic233.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:61842  mad41s14-in-f22.1e100.net:https  TIME_WAIT
TCP    192.168.1.169:62909  intranet.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:63405  intranet.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:64401  crisb108.sic233.uniovi.es:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.169:65345  crisb108.sic233.uniovi.es:https  ESTABLISHED
[chrome.exe]
PS C:\Windows\system32> echo "U0258318"
U0258318
PS C:\Windows\system32> echo "Esta operación se tuvo que hacer con permisos de administrador"
Esta operación se tuvo que hacer con permisos de administrador
PS C:\Windows\system32>
```

La operación debe realizarse con permisos de administrador.

## 5.2. Ejercicio 25

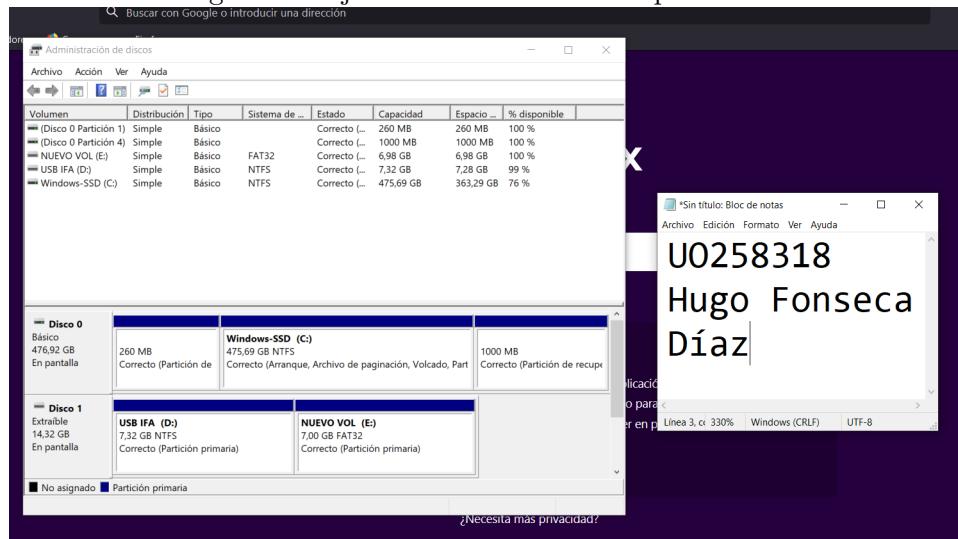
Figura 81: Ejercicio 25: Enunciado.

Para realizar el siguiente ejercicio deberá disponer de un lápiz de memoria o tarjeta SD. Borre las particiones que se encuentren en dicho lápiz. Una vez hecho esto, busque y ejecute la utilidad de Photorec que le permita recuperar particiones que han sido borradas. Compruebe y documente que las particiones borradas han sido convenientemente recuperadas y que los archivos que contenían dichas particiones siguen existiendo.

Este ejercicio, como el 7 de la práctica 4, fue realizado en el ordenador de un familiar, ya que Virtualbox en Linux no parece reconocer los USBs conectados a la máquina anfitriona, lo que impide realizar los filtros.

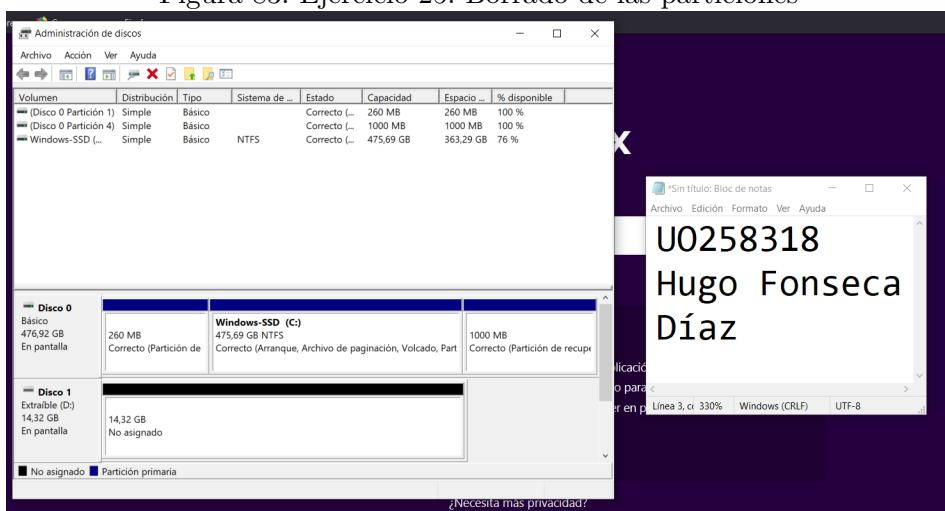
Lo primero que se va a hacer es formatear un USB con el sistema de archivos NTFS y posteriormente se van a crear dos particiones, una en NTFS y otra en FAT32.

Figura 82: Ejercicio 25: USB con las particiones



Ahora, se introducen ficheros de ejemplo en ambas particiones y posteriormente se borran dichas particiones.

Figura 83: Ejercicio 25: Borrado de las particiones



Se añade el filtro del usb y se conecta a la máquina virtual. Aquí se produce un problema inesperado, tanto la máquina anfitriona con Linux como la del familiar con Windows son el mismo modelo, y ambas cuentan solo con puertos USB 3.0. Como Windows 7 no tiene soporte para USB 3.0 se intentaron instalar los drivers necesarios, pero la operación no pudo ejecutarse.

Figura 84: Ejercicio 25: Fallo al instalar los drivers de los puertos de USB 3.0

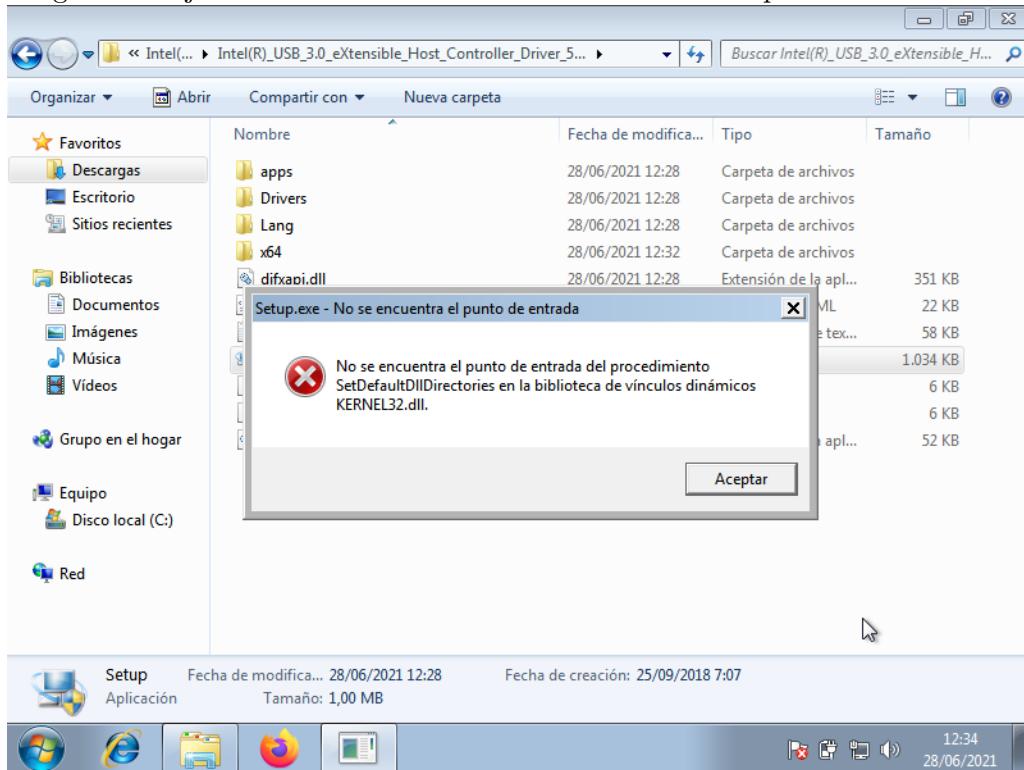
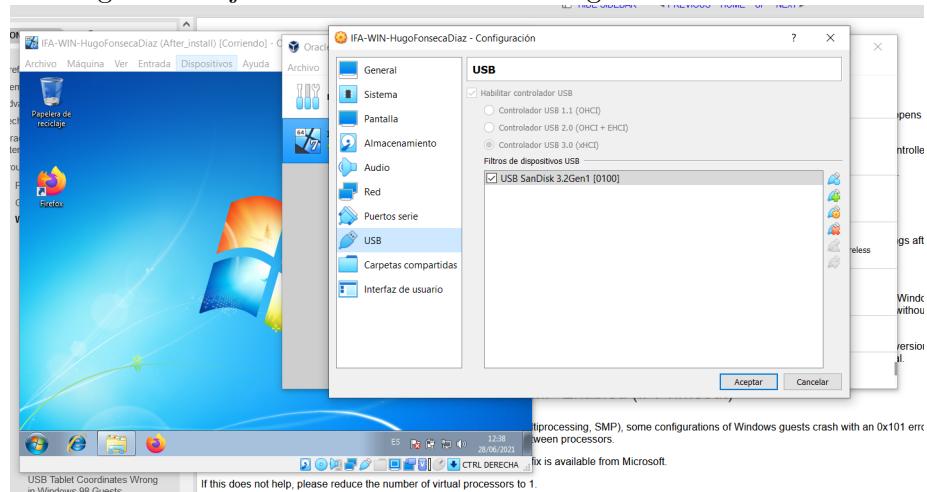
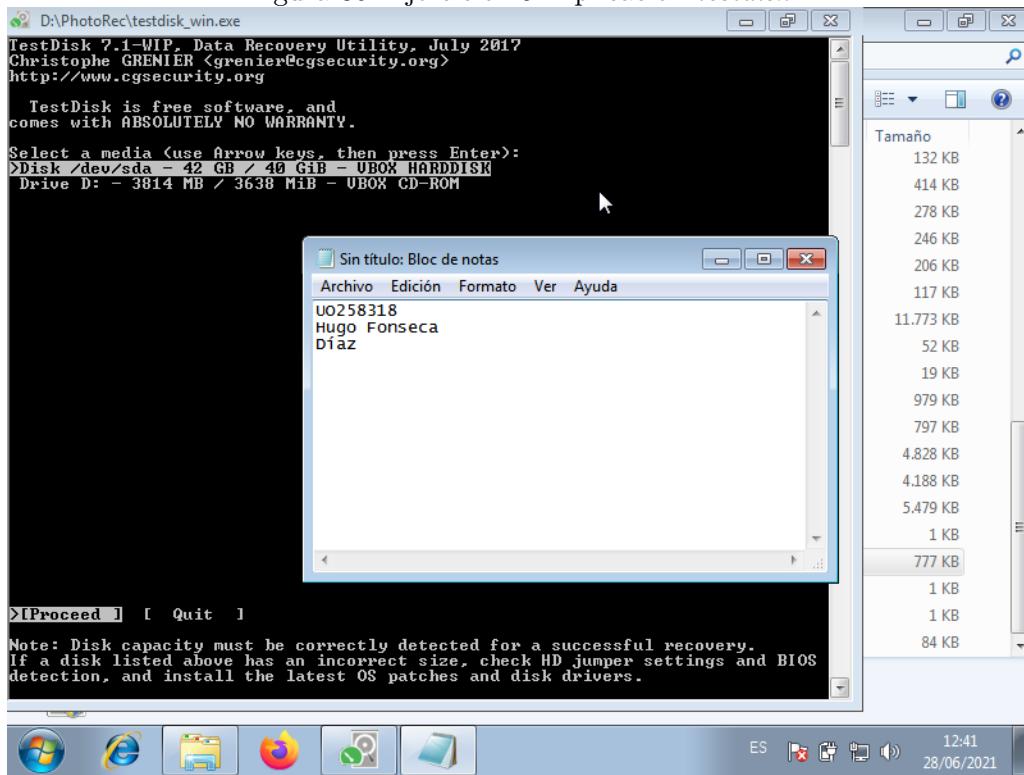


Figura 85: Ejercicio 25: Filtro USB configurado correctamente



Como no se puede conectar el USB al equipo virtual, se seguirá el ejercicio hasta donde sea posible. La aplicación que se usará para resolver el ejercicio se encuentra en la carpeta *PhotoRec*, y se llama *testdisk*.

Figura 86: Ejercicio 25: Aplicación *testdisk*



Aquí se debería seleccionar el USB correcto, elegir el tipo de la tabla de particiones, y realizar un análisis. Lamentablemente, debido a los problemas antes mencionados, no se ha podido continuar con el ejercicio.

### 5.3. Ejercicio 31

Figura 87: Ejercicio 31: Enunciado.

En el mes de junio de 2018, Donald Trump adoptó una serie de medidas frente a los menores indocumentados que cruzan la frontera con sus padres. Utilizando la técnica de búsqueda inversa de imágenes a través de Google Images, Yandex o TinEye, determinar la veracidad de la información publicada por el perfil de Twitter: **@PabloPardo1:** <https://twitter.com/pablopardo1>, concretamente el Tweet: <https://twitter.com/PabloPardo1/status/1008923855954567170> Investigar

10

---

la veracidad de la información asociada a la imagen que se encuentra asociada a dicho Tweet.

Se localiza el hilo de Twitter mencionado en el enunciado.

Figura 88: Ejercicio 31: Hilo de Twitter



Una vez obtenida la URL de la imagen del hilo, se realiza una búsqueda inversa de la misma mediante el buscador Google con las palabras clave 'trump' y 'niños'.

Figura 89: Ejercicio 31: Búsqueda inversa



Se entra a la noticia de la rama en español del medio estadounidense *CNN*, y se obtiene la información mostrada en la siguiente captura.

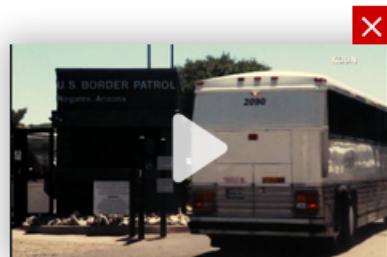
Figura 90: Ejercicio 31: Noticia *CNN en Español*

The screenshot shows a Microsoft Edge browser window. The address bar displays the URL <https://cnnespanol.cnn.com/2018/05/29/ninos-inmigrantes/>. A tooltip above the address bar says "DgBq5Y0WkAAzSSQ (Imagen JPEG, 520 x 390 pixels)". The main content area shows a news article from CNN in Spanish. The headline reads: "Para mejorar la calidad del video, puede que necesite instalar el Media Feature Pack de Microsoft. [Saber cómo](#)". Below the headline, the text discusses the context of the photo under the Trump administration, mentioning that the photo was taken in 2014 at a detention center in Arizona. The CNN logo and "Estados Unidos" are visible in the top left corner of the page.

Inicialmente, la imagen fue presentada bajo el contexto de la nueva política del gobierno Trump, insinuando que la foto era reciente que las niñas fueron separadas de sus familias. [Pero pronto fue claro que la fotografía se tomó en un centro de detención de Arizona... en 2014. Así que nada tenía que ver con la administración actual.](#)

Algunos partidarios del presidente Trump [están usando la imagen](#) ahora para reclamar que el gobierno del expresidente Barack Obama también separó a los niños inmigrantes de sus familias, bajo las mismas circunstancias.

De nuevo, aunque los niños han sido históricamente separados de sus familias en la frontera bajo ciertas condiciones, eso no es igual a la nueva medida de enjuiciamiento, que afecta incluso a los menores que lleguen con sus padres o tutores legales.



Según esta fuente, los niños de la imagen estaban detenidos en un centro de detención de Arizona en el año 2014. Como nunca conviene fiarce de lo que diga una única fuente, se va a investigar en mayor profundidad. Se hace una búsqueda inversa que ocupe el período entre el 1 de enero de 2014 y el 1 de enero de 2015, y se obtiene la siguiente información.

Figura 91: Ejercicio 31: Búsqueda inversa por rango de fechas

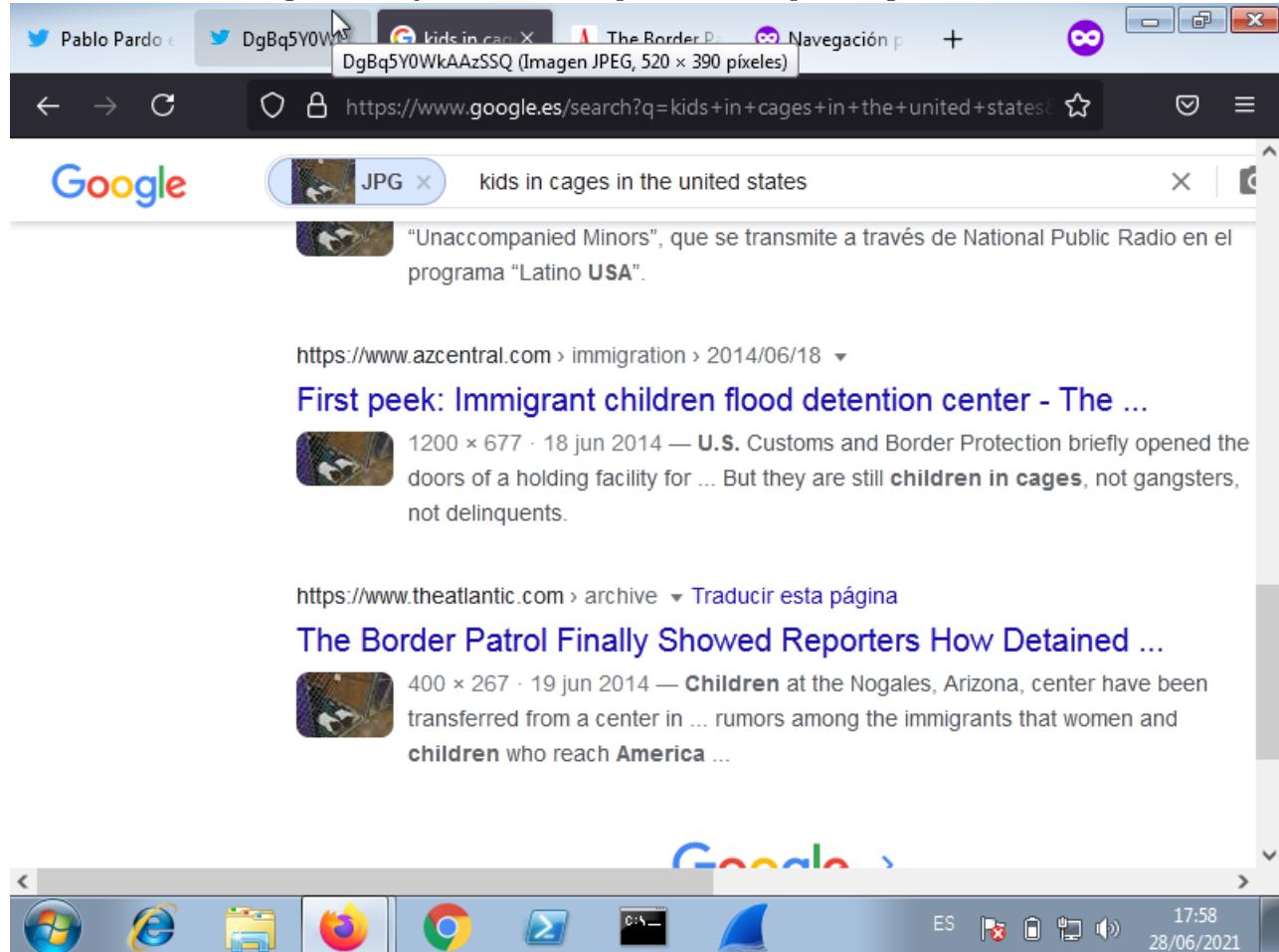


Figura 92: Ejercicio 31: Noticia de *azcentral*

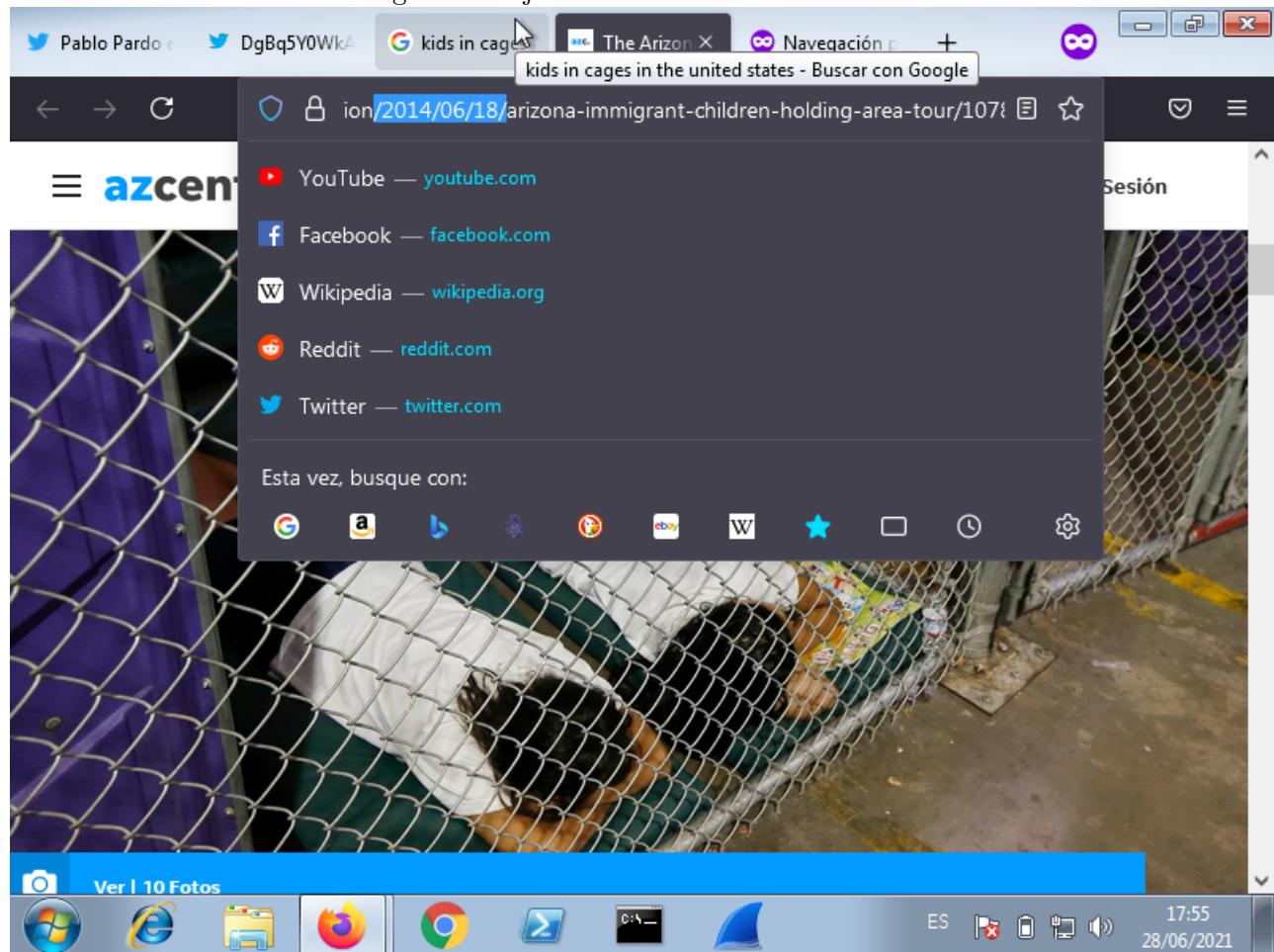


Figura 93: Ejercicio 31: Noticia de *The Atlantic*

A screenshot of a web browser displaying a news article from *The Atlantic*. The browser's address bar shows the URL <https://www.theatlantic.com/politics/archive/2014/06/the-border-pa>. The page content includes a headline and text about children held in cages, followed by a photograph of two detainees in a holding pen and a caption below it. The browser interface includes a navigation bar, a search bar, and various icons.

There are 900 children from El Salvador, Honduras, and Guatemala being held in nine holding pens, separated by age and gender. They sleep on mats on the floor and are clothed, fed and clean according to Fernanda Santos at *The New York*

Two female detainees in Nogales. (AP)

Enjoy unlimited access to The Atlantic. | [Sign in](#) [Subscribe Now](#)

ES 17:57 28/06/2021

Como se puede observar, la foto es verdaderamente del año 2014, en el período de la administración Obama, por lo que el hilo original usaba una imagen errónea. Esto refuerza más la idea de comprobar bien las fuentes de información a las que estamos sometidos cada día para no caer en la desinformación, y para que nuestros argumentos tengan una mayor base verídica que les de más peso.

## 6. Índice de figuras

### Índice de figuras

1.	Sistema del alumno Hugo Fonseca Díaz.	2
2.	Máquinas virtuales.	3
3.	Ejercicio 27: Enunciado.	3
4.	Ejercicio 27: <i>tar -xvzf</i> .	4
5.	Ejercicio 27: <i>tac, AWK y uniq</i> .	5
6.	Ejercicio 31: Enunciado (I).	6
7.	Ejercicio 31: Enunciado (II).	7
8.	Ejercicio 31: Creación del caso	8
9.	Ejercicio 31: Selección de la imagen a analizar	9
10.	Ejercicio 31: Palabras clave	10
11.	Ejercicio 31: Módulos seleccionados	11
12.	Ejercicio 31: Configuración de los lenguajes de la búsqueda	12
13.	Ejercicio 31: Resultados del análisis	13
14.	Ejercicio 31: Menú reconstruido	14
15.	Ejercicio 8: Enunciado.	15
16.	Ejercicio 8: Creación del caso	16
17.	Ejercicio 8: Detalles del examinador	17
18.	Ejercicio 8: Selección de la imagen	18
19.	Ejercicio 8: Selección de módulos	19
20.	Ejercicio 8: Resultados del análisis	20
21.	Ejercicio 8: Herramienta <i>MediaInfo</i>	21
22.	Ejercicio 13: Enunciado (I).	22
23.	Ejercicio 13: Enunciado (II).	23
24.	Ejercicio 13: Creación del caso	24
25.	Ejercicio 13: Detalles del examinador	25
26.	Ejercicio 13: Selección de la imagen	26
27.	Ejercicio 13: Selección de módulos	27
28.	Ejercicio 13: Resultados del análisis	28
29.	Ejercicio 13: Ficheros de texto plano	29
30.	Ejercicio 13: Metadatos de los ficheros borrados	30
31.	Ejercicio 13: Línea temporal de <i>Bellatrix.txt</i>	31
32.	Ejercicio 13: Línea temporal de <i>Bunda.txt</i>	32
33.	Ejercicio 13: Línea temporal de <i>Botein.txt</i>	33
34.	Ejercicio 14: Enunciado (I).	34
35.	Ejercicio 14: Enunciado (II).	35
36.	Ejercicio 14: Salida del comando <i>mmls</i>	36
37.	Ejercicio 14: Salida del comando <i>fsstat</i> para las diferentes particiones	37
38.	Ejercicio 14: Salida del comando <i>fls</i> con las flags <i>ro</i>	38
39.	Ejercicio 14: Salida del comando <i>fls</i> con las flags <i>dFro</i>	39

40.	Ejercicio 14: Salida del comando <i>ffind</i>	40
41.	Ejercicio 14: Salida del comando <i>istat</i> para el inodo 13	41
42.	Ejercicio 14: Salida del comando <i>istat -f list</i>	42
43.	Ejercicio 19: Enunciado	43
44.	Ejercicio 19: Metadatos de la imagen 1 con la interfaz gráfica de <i>exiftool</i> (I)	44
45.	Ejercicio 19: Metadatos de la imagen 1 con la interfaz gráfica de <i>exiftool</i> (II)	45
46.	Ejercicio 19: Metadatos de la imagen 1 con el comando <i>exiftool</i> (I)	46
47.	Ejercicio 19: Metadatos de la imagen 1 con el comando <i>exiftool</i> (II)	47
48.	Ejercicio 19: Metadatos de la imagen 2 con el comando <i>exiftool</i> (I)	48
49.	Ejercicio 19: Metadatos de la imagen 2 con el comando <i>exiftool</i> (II)	49
50.	Ejercicio 19: Metadatos de la imagen 3 con el comando <i>exiftool</i> (I)	50
51.	Ejercicio 19: Metadatos de la imagen 3 con el comando <i>exiftool</i> (II)	51
52.	Ejercicio 19: Metadatos de la imagen 4 con el comando <i>exiftool</i> (I)	52
53.	Ejercicio 19: Metadatos de la imagen 4 con el comando <i>exiftool</i> (II)	53
54.	Ejercicio 19: Metadatos de la imagen 5 con el comando <i>exiftool</i> (I)	54
55.	Ejercicio 19: Metadatos de la imagen 5 con el comando <i>exiftool</i> (II)	55
56.	Ejercicio 7: Enunciado (I)	56
57.	Ejercicio 7: Enunciado (II)	57
58.	Ejercicio 7: Enunciado (III)	58
59.	Ejercicio 4: Creación del caso	59
60.	Ejercicio 4: Selección de la imagen	60
61.	Ejercicio 4: Tipo de análisis	61
62.	Ejercicio 4: Opciones de análisis avanzadas	61
63.	Ejercicio 4: Ejecución del análisis	62
64.	Ejercicio 4: Resultado del análisis	63
65.	Ejercicio 4: Documentos de tipo <i>pdf</i>	64
66.	Ejercicio 4: URLs visitadas	65
67.	Ejercicio 4: Cookies relativas a <i>Facebook</i>	66
68.	Ejercicio 4: Imágenes identificadas	67
69.	Ejercicio 4: Imágenes en formato <i>jpg</i>	68
70.	Ejercicio 4: Reconocimiento de rostros	69
71.	Ejercicio 4: Eventos de calendario	70
72.	Ejercicio 4: Eventos en Los Ángeles	71
73.	Ejercicio 5: Enunciado	72
74.	Ejercicio 5: Campus virtual	73
75.	Ejercicio 5: <i>CurrPorts</i>	74
76.	Ejercicio 5: <i>CurrPorts</i> - Firefox	75
77.	Ejercicio 5: <i>CurrPorts</i> - Chrome (I)	76
78.	Ejercicio 5: <i>CurrPorts</i> - Chrome (II)	77
79.	Ejercicio 5: <i>netstat -h</i>	78
80.	Ejercicio 5: <i>netstat -b -f -p TCP</i>	79
81.	Ejercicio 25: Enunciado	79
82.	Ejercicio 25: USB con las particiones	80

83.	Ejercicio 25: Borrado de las particiones . . . . .	80
84.	Ejercicio 25: Fallo al instalar los drivers de los puertos de USB 3.0 . . . . .	81
85.	Ejercicio 25: Filtro USB configurado correctamente . . . . .	82
86.	Ejercicio 25: Aplicación <i>testdisk</i> . . . . .	82
87.	Ejercicio 31: Enunciado. . . . .	83
88.	Ejercicio 31: Hilo de Twitter . . . . .	84
89.	Ejercicio 31: Búsqueda inversa . . . . .	85
90.	Ejercicio 31: Noticia <i>CNN en Español</i> . . . . .	86
91.	Ejercicio 31: Búsqueda inversa por rango de fechas . . . . .	87
92.	Ejercicio 31: Noticia de <i>azcentral</i> . . . . .	88
93.	Ejercicio 31: Noticia de <i>The Atlantic</i> . . . . .	89