

Prácticas de Laboratorio

Informática Forense y Auditoría

Hugo Fonseca Díaz

UO258318

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

1. Introducción	2
2. Práctica 02	3
2.1. Ejercicio 27	3
2.2. Ejercicio 31	5
3. Práctica 03	12
3.1. Ejercicio 8	12
3.2. Ejercicio 13	18
3.3. Ejercicio 14	28
3.4. Ejercicio 19	35
3.4.1. Imagen 1	36
3.4.2. Imagen 2	40
3.4.3. Imagen 3	42
3.4.4. Imagen 4	44
3.4.5. Imagen 5	46
4. Práctica 04	48
4.1. Ejercicio 7	48
5. Práctica 05	60
5.1. Ejercicio 5	60
5.2. Ejercicio 25	67
5.3. Ejercicio 31	70

1. Introducción

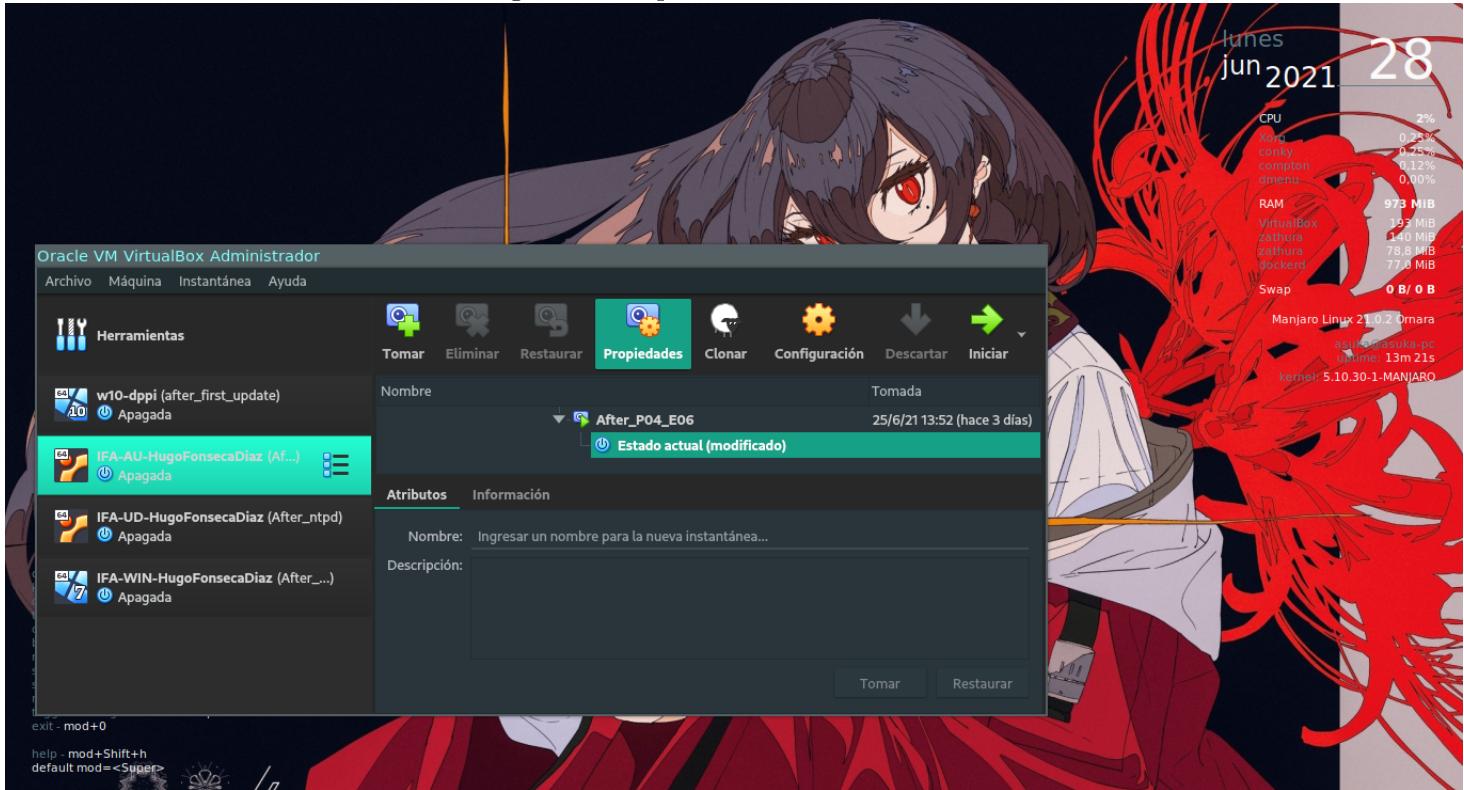
Los ejercicios de este documento se han realizado en una máquina cuyas características se muestran en la siguiente captura.

Figura 1: Sistema del alumno Hugo Fonseca Díaz.



Las máquinas virtuales utilizadas pueden verse en la siguiente imagen.

Figura 2: Máquinas virtuales.

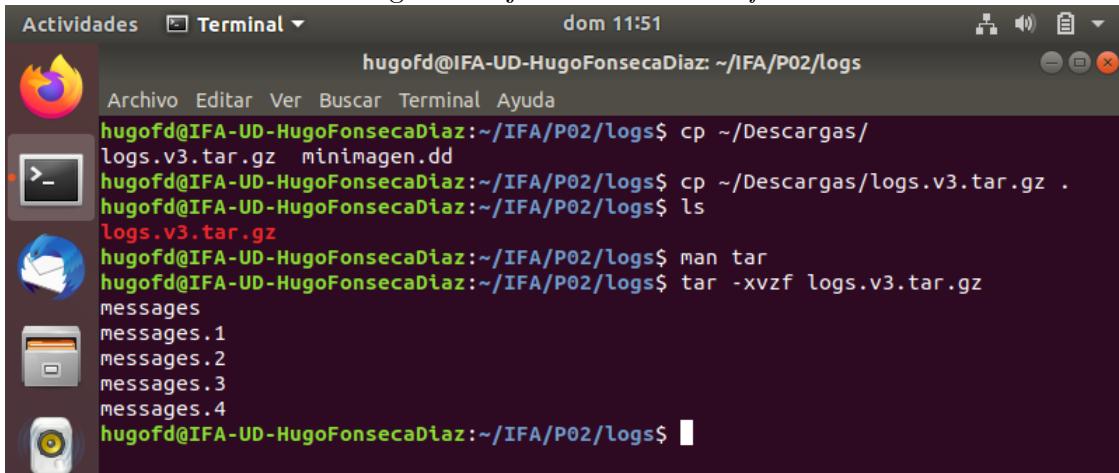


2. Práctica 02

2.1. Ejercicio 27

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

Figura 3: Ejercicio 27: *tar -xvzf*.

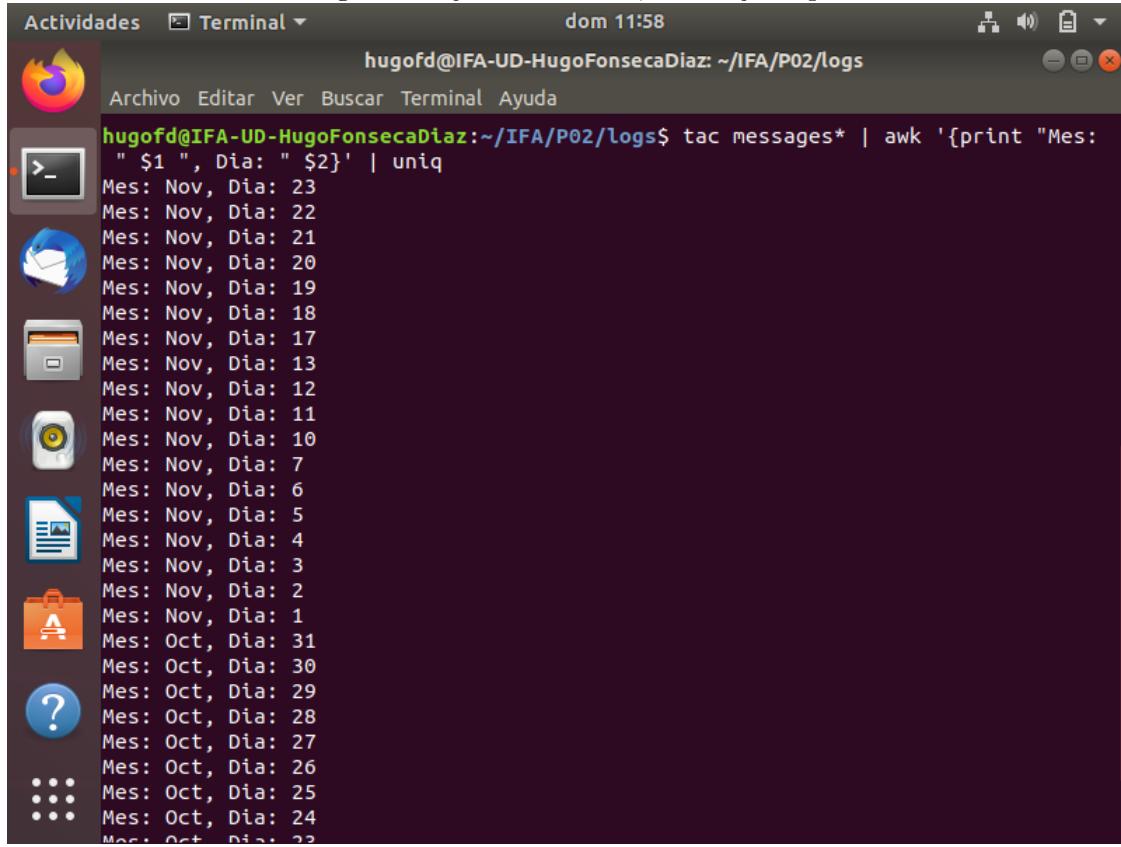


The screenshot shows a terminal window titled "Terminal" running on a Linux desktop. The terminal window has a dark background and contains the following text:

```
Actividades Terminal dom 11:51
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs
Archivo Editar Ver Buscar Terminal Ayuda
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$
```

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 4: Ejercicio 27: *tac*, *AWK* y *uniq*.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Actividades Terminal" and the status bar shows "dom 11:58" and the user "hugofd@IFA-UD-HugoFonsecaDiaz: ~/IFA/P02/logs". The terminal content displays the output of a command: "hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs\$ tac messages* | awk '{print \"Mes: \" \$1 \" , Dia: \" \$2}' | uniq". The output lists dates from November 23 down to October 23, with each date appearing once.

```
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

Se crea el caso en Autopsy con los datos solicitados.

Figura 5: Ejercicio 31: Creación del caso

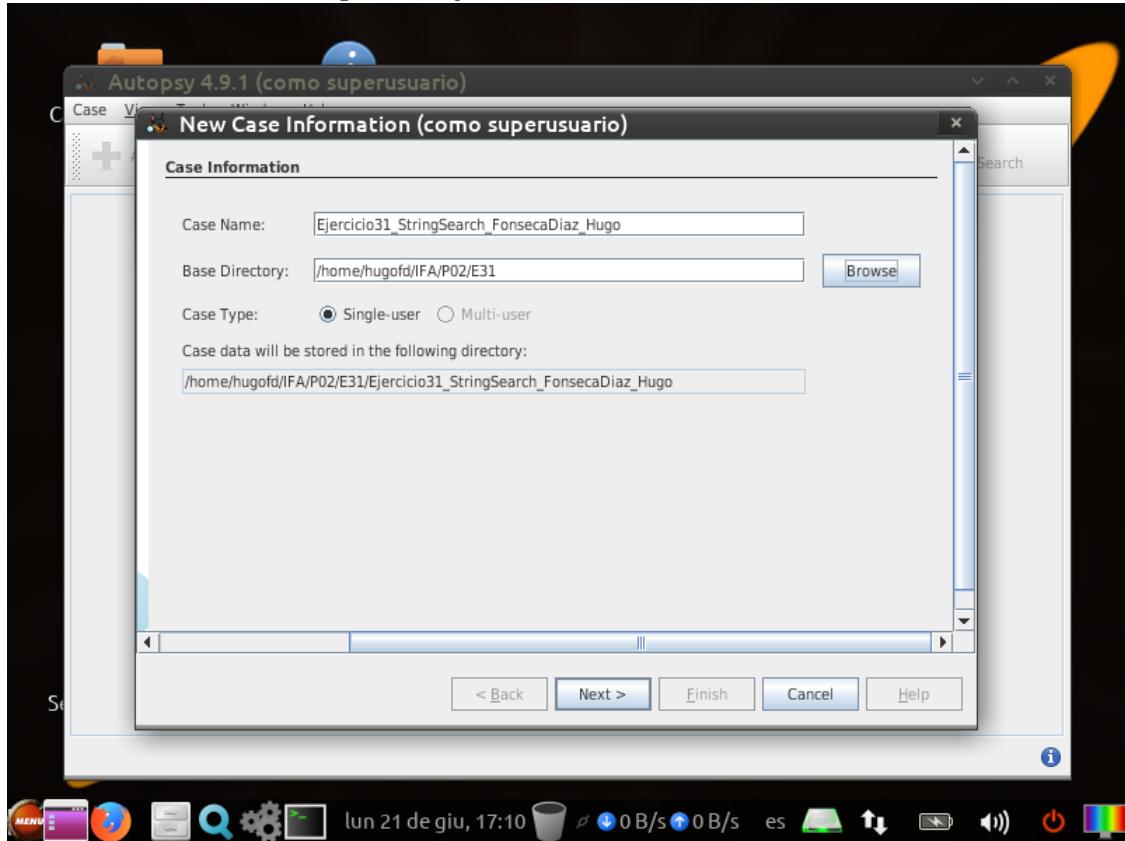
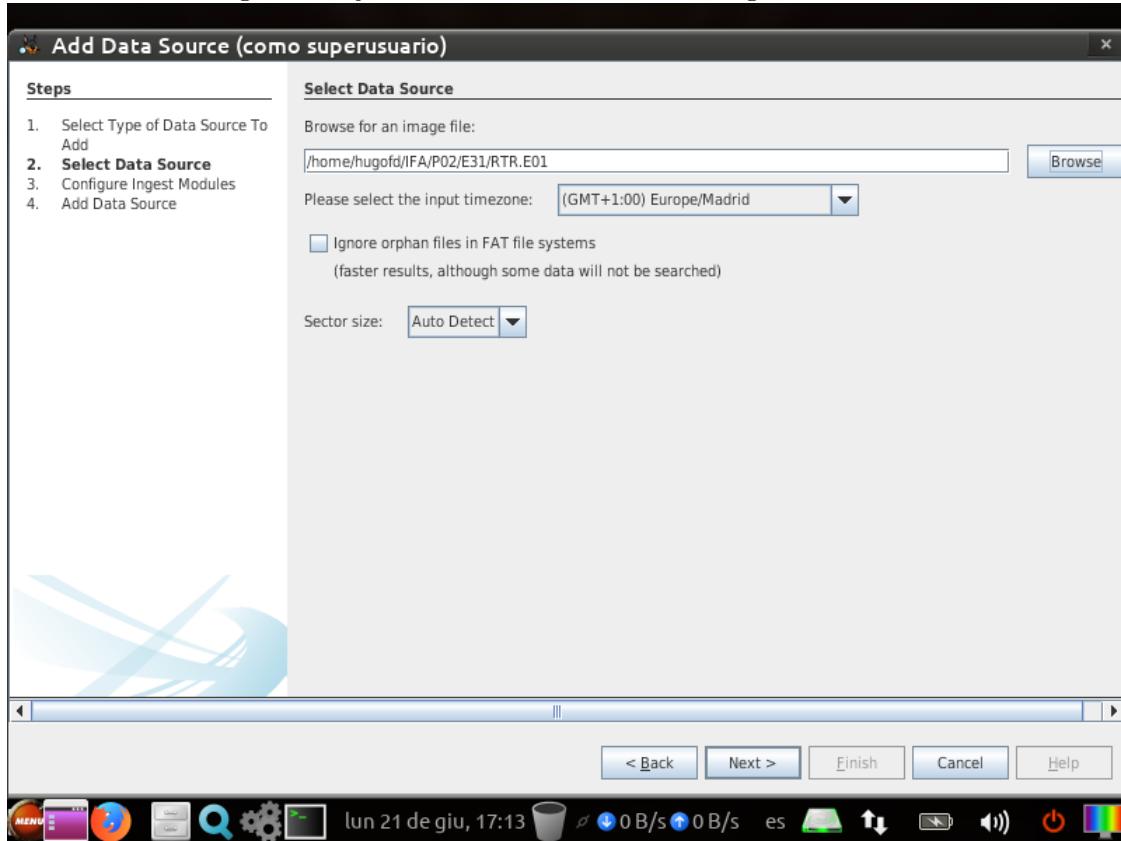


Figura 6: Ejercicio 31: Selección de la imagen a analizar



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

Figura 7: Ejercicio 31: Palabras clave

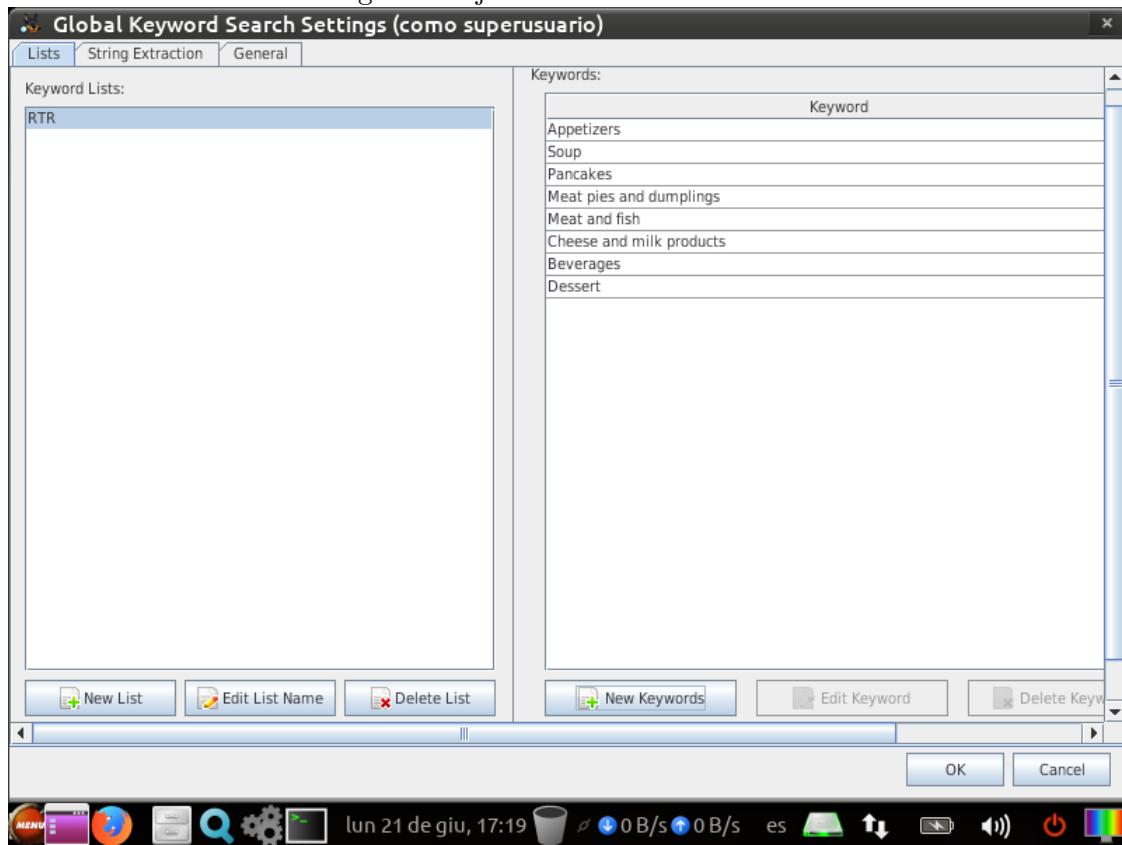


Figura 8: Ejercicio 31: Módulos seleccionados

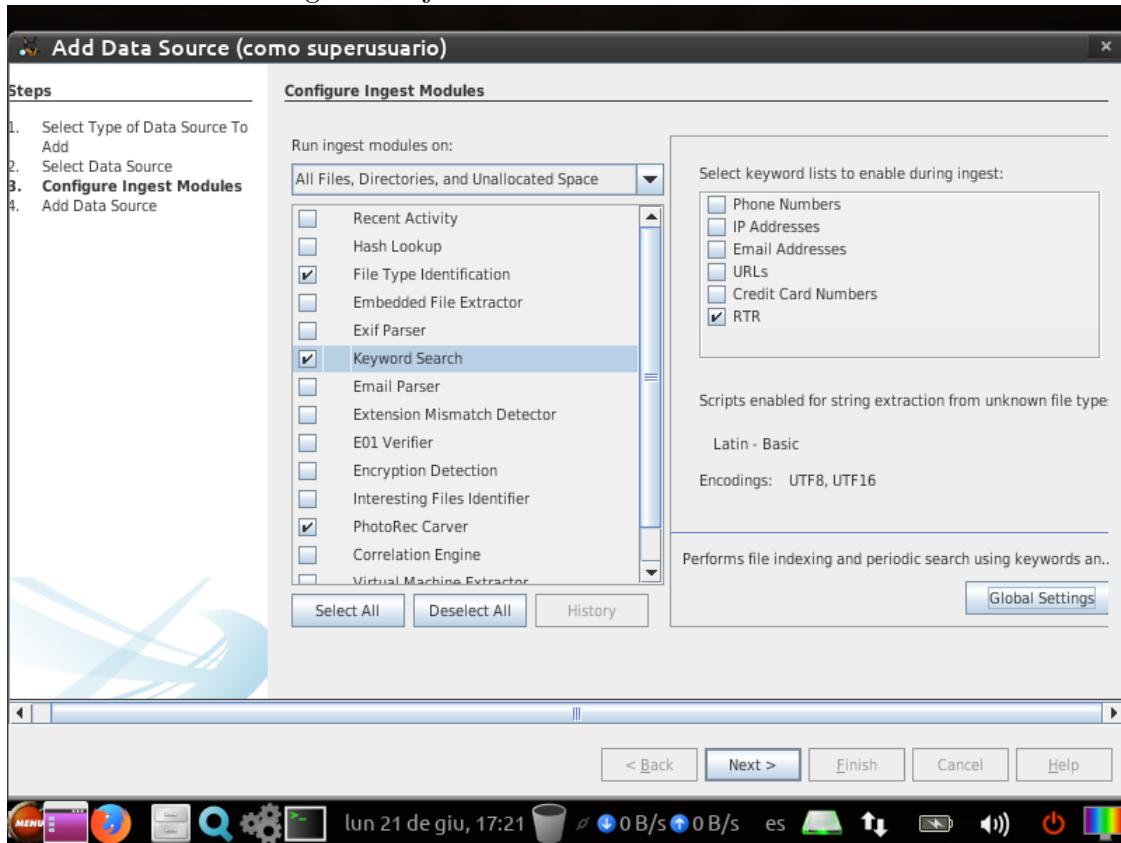
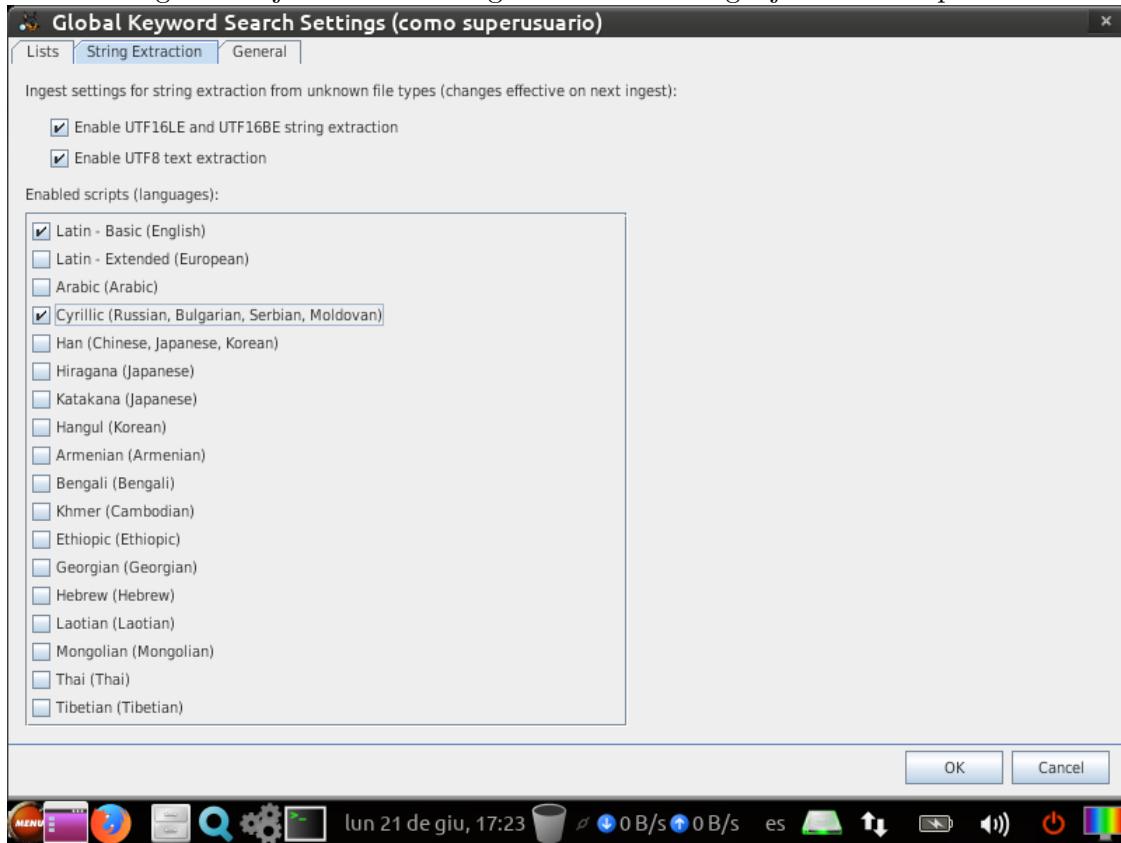
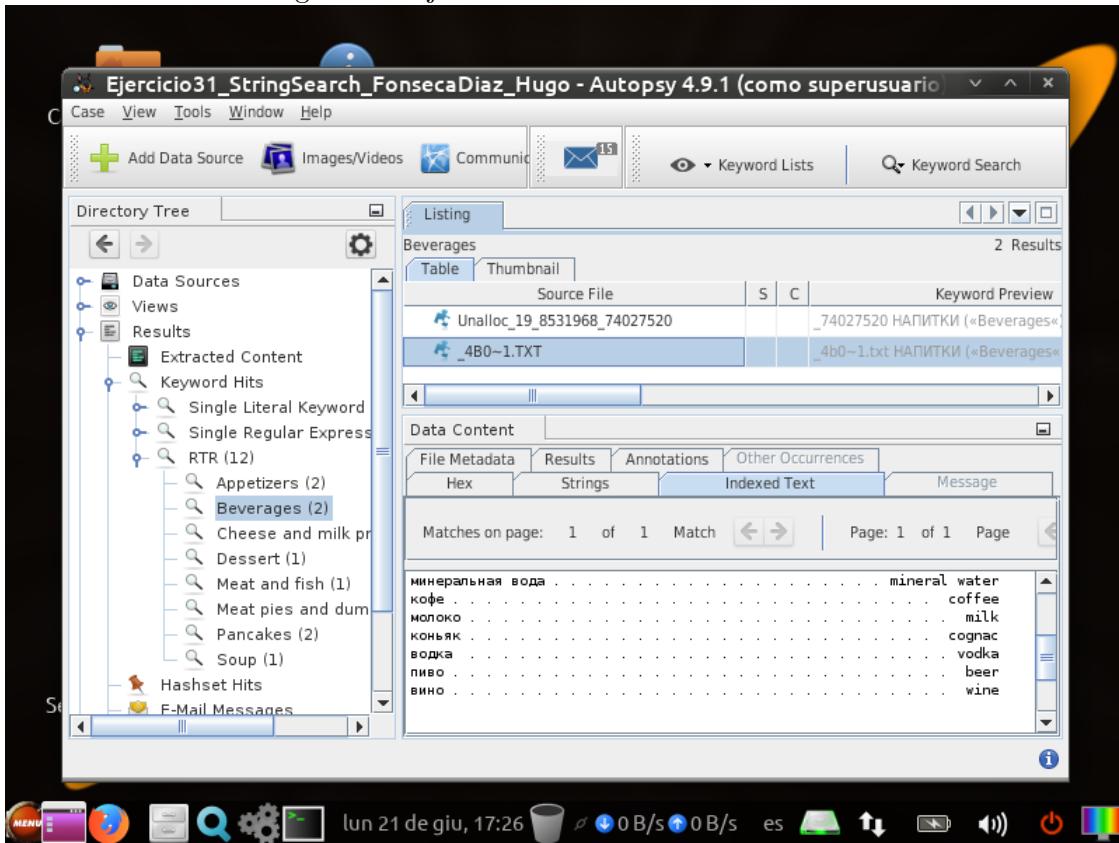


Figura 9: Ejercicio 31: Configuración de los lenguajes de la búsqueda



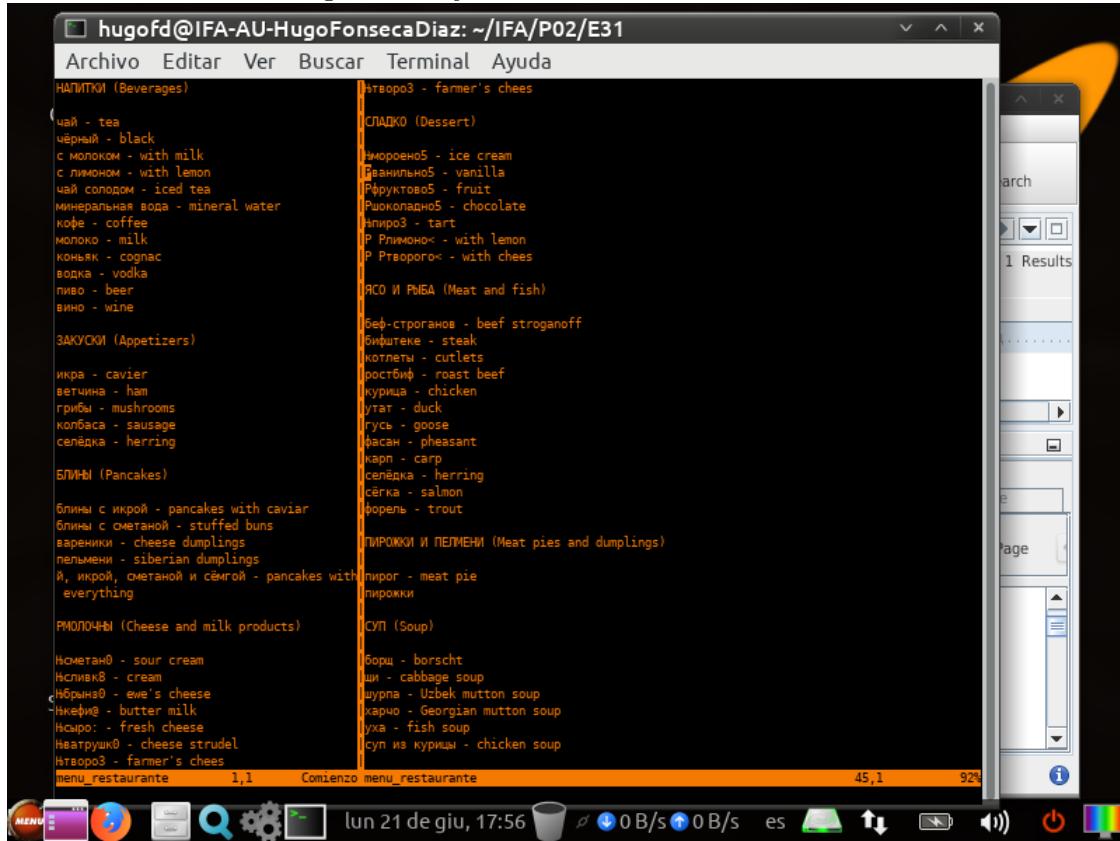
Una vez finalizado el análisis, se pueden observar los ficheros encontrados.

Figura 10: Ejercicio 31: Resultados del análisis



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

Figura 11: Ejercicio 31: Menú reconstruido



3. Práctica 03

3.1. Ejercicio 8

Se crea el caso en Autopsy con los datos solicitados.

Figura 12: Ejercicio 8: Creación del caso

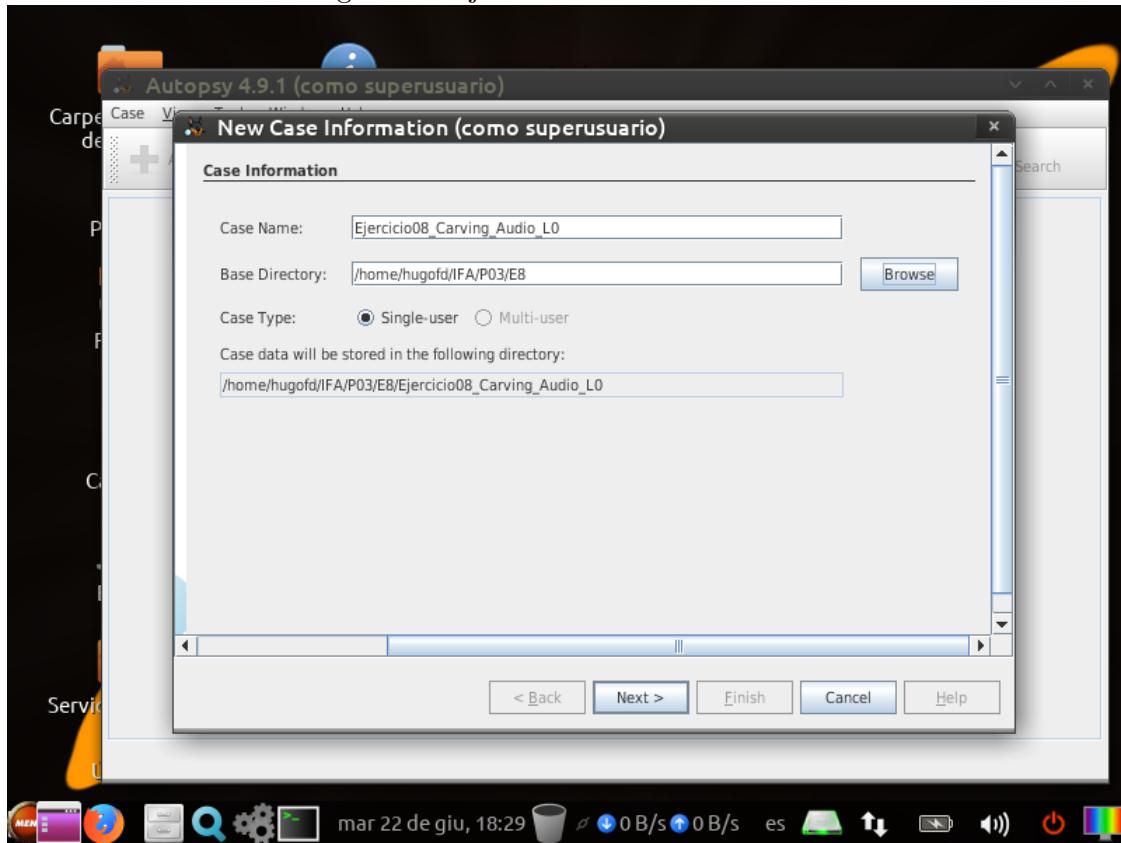
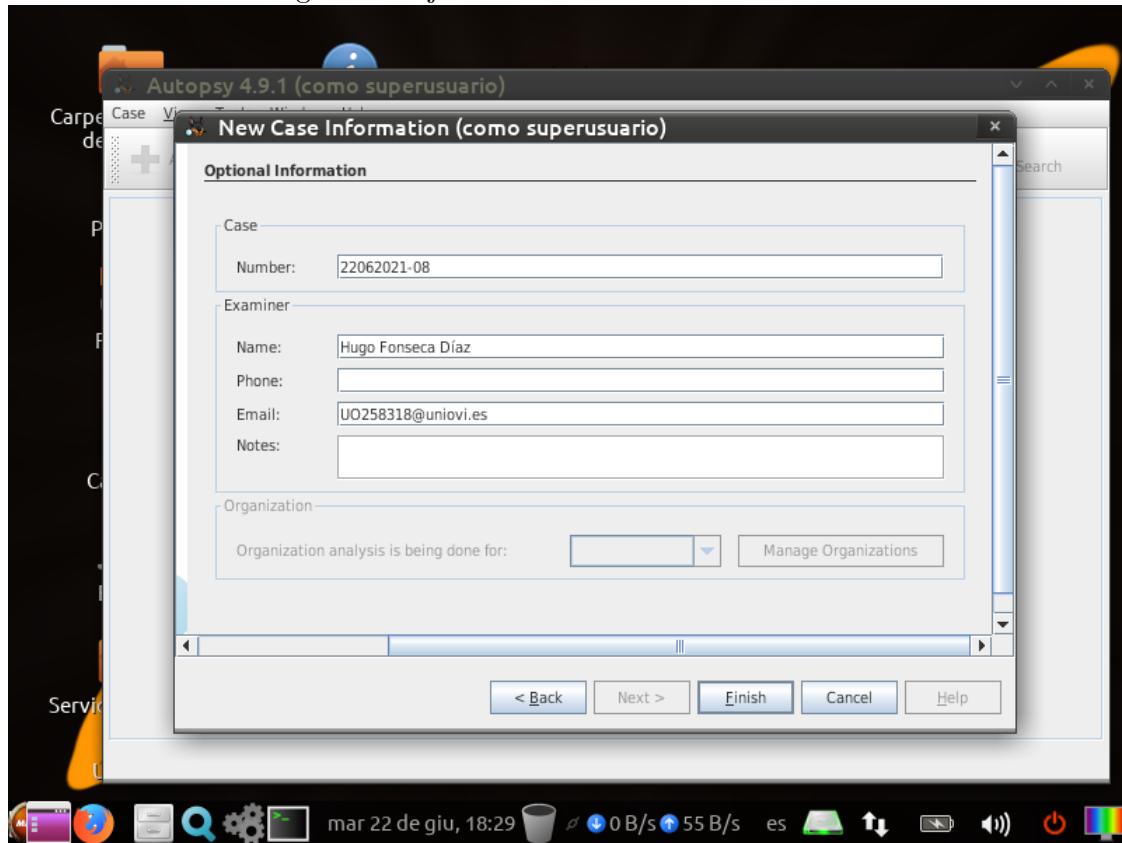
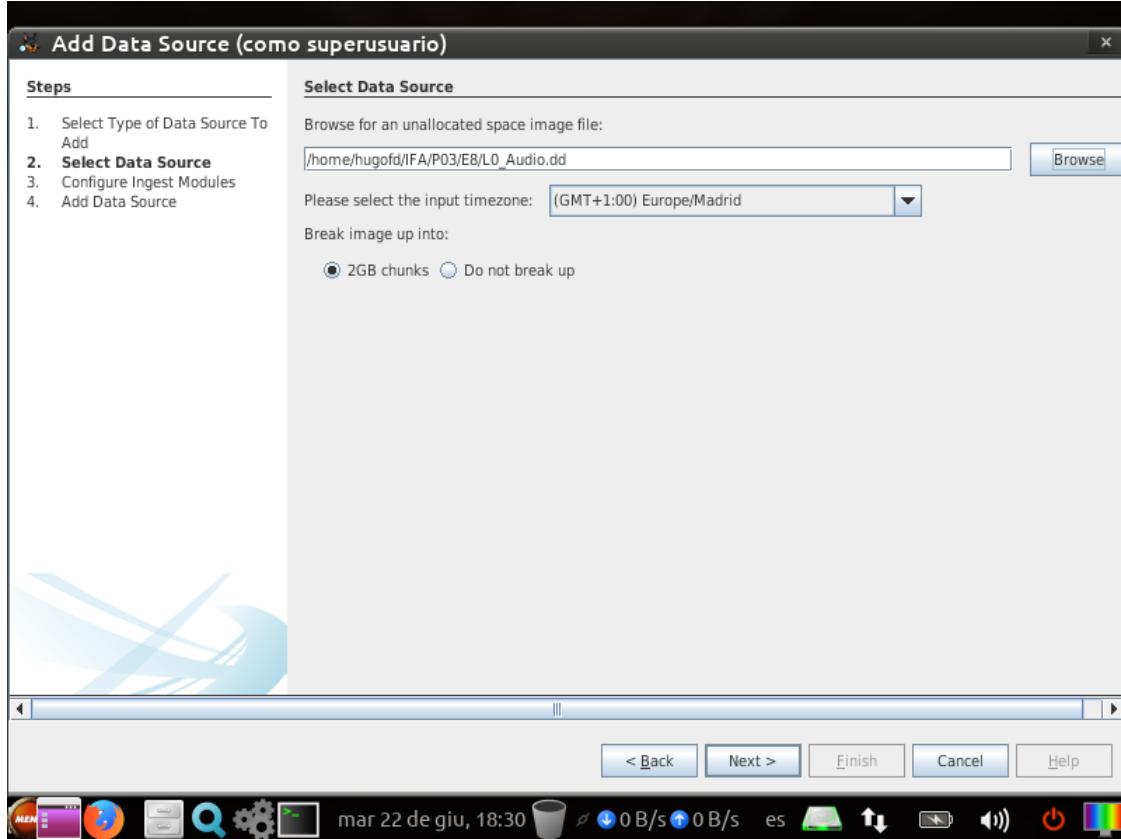


Figura 13: Ejercicio 8: Detalles del examinador



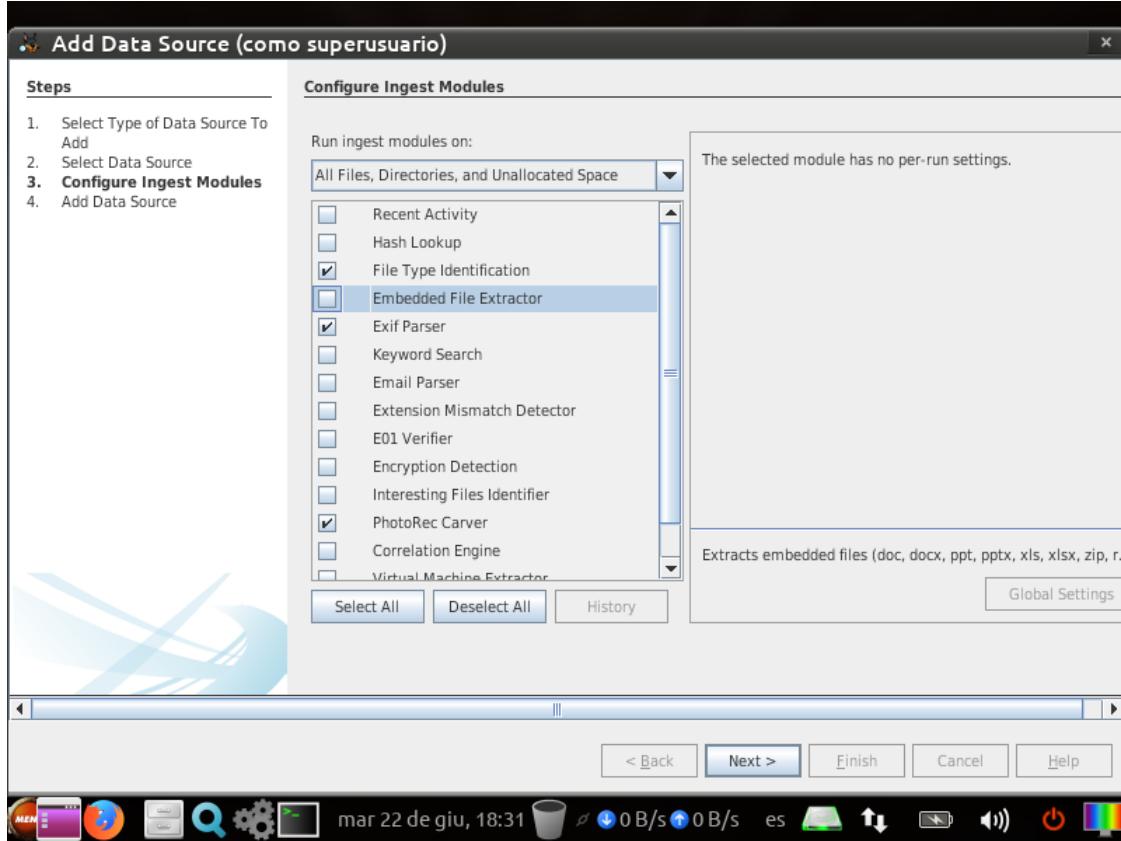
Añadimos la imagen a analizar.

Figura 14: Ejercicio 8: Selección de la imagen



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

Figura 15: 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 16: Ejercicio 8: Resultados del análisis

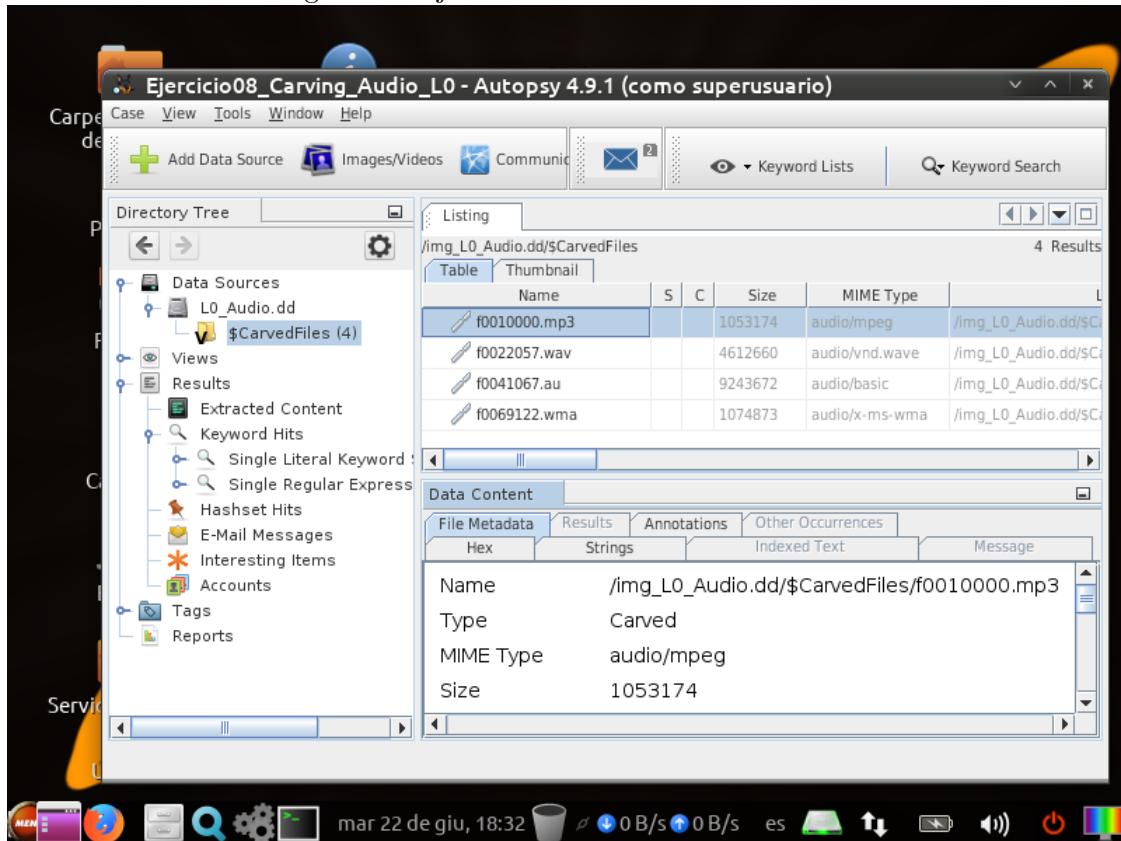
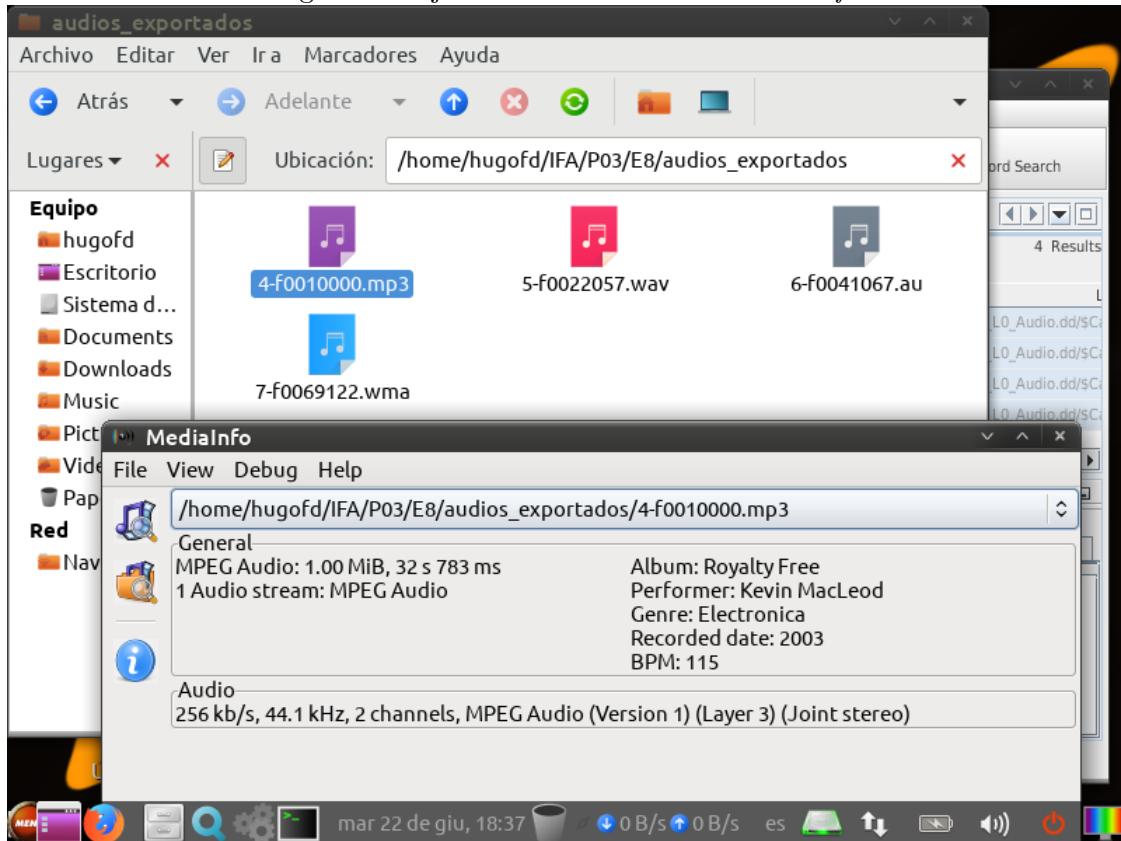


Figura 17: Ejercicio 8: Herramienta *MediaInfo*



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

Se crea el caso en Autopsy con los datos solicitados.

Figura 18: Ejercicio 13: Creación del caso

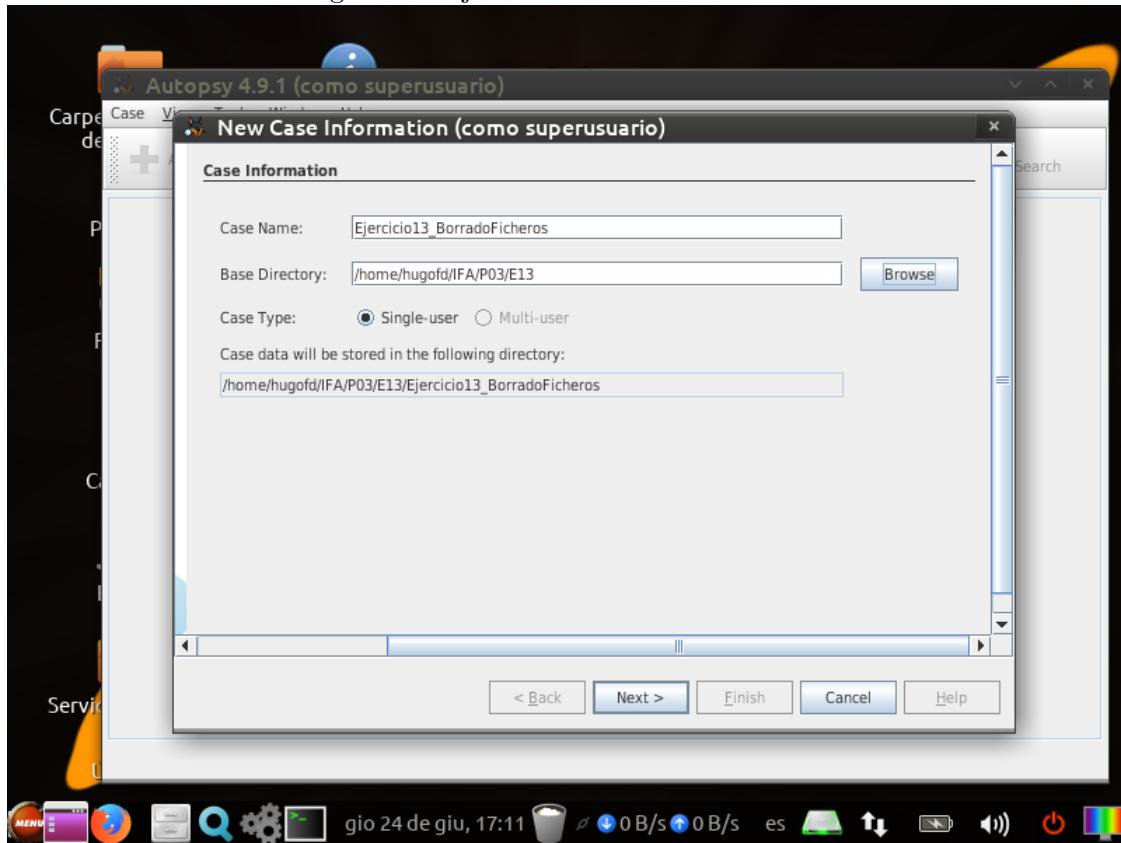
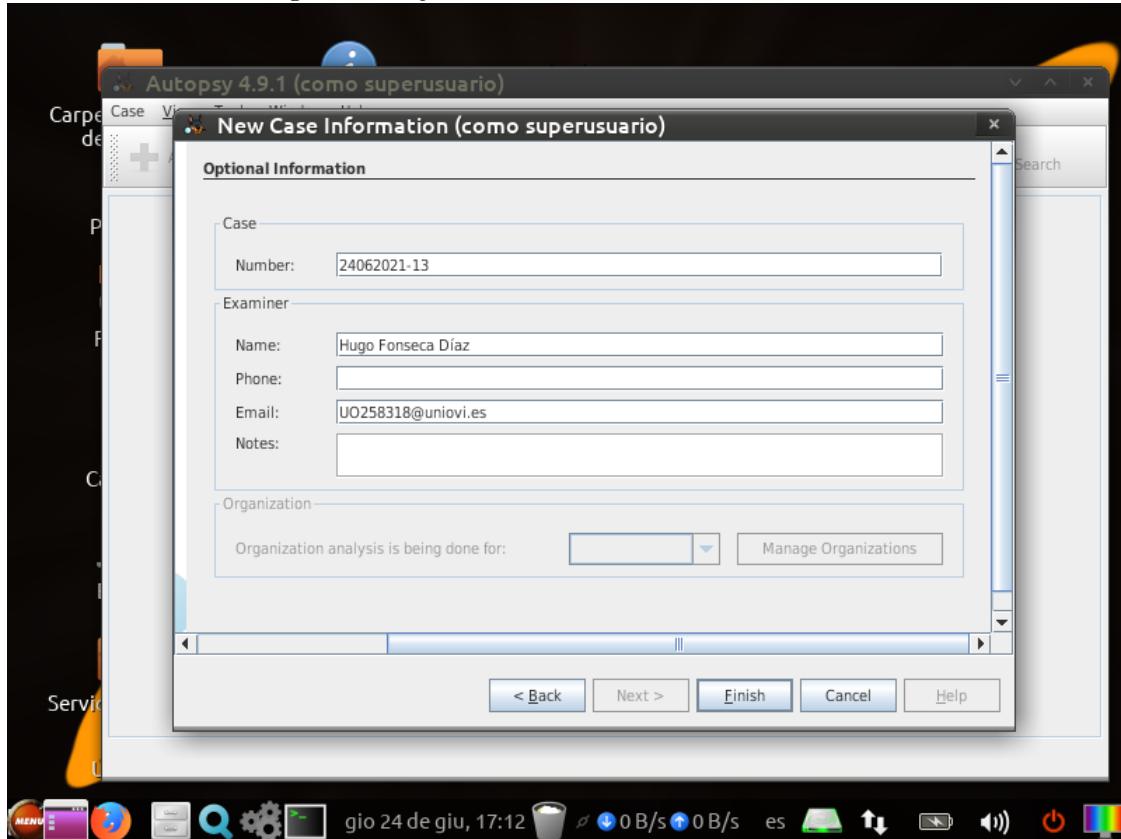
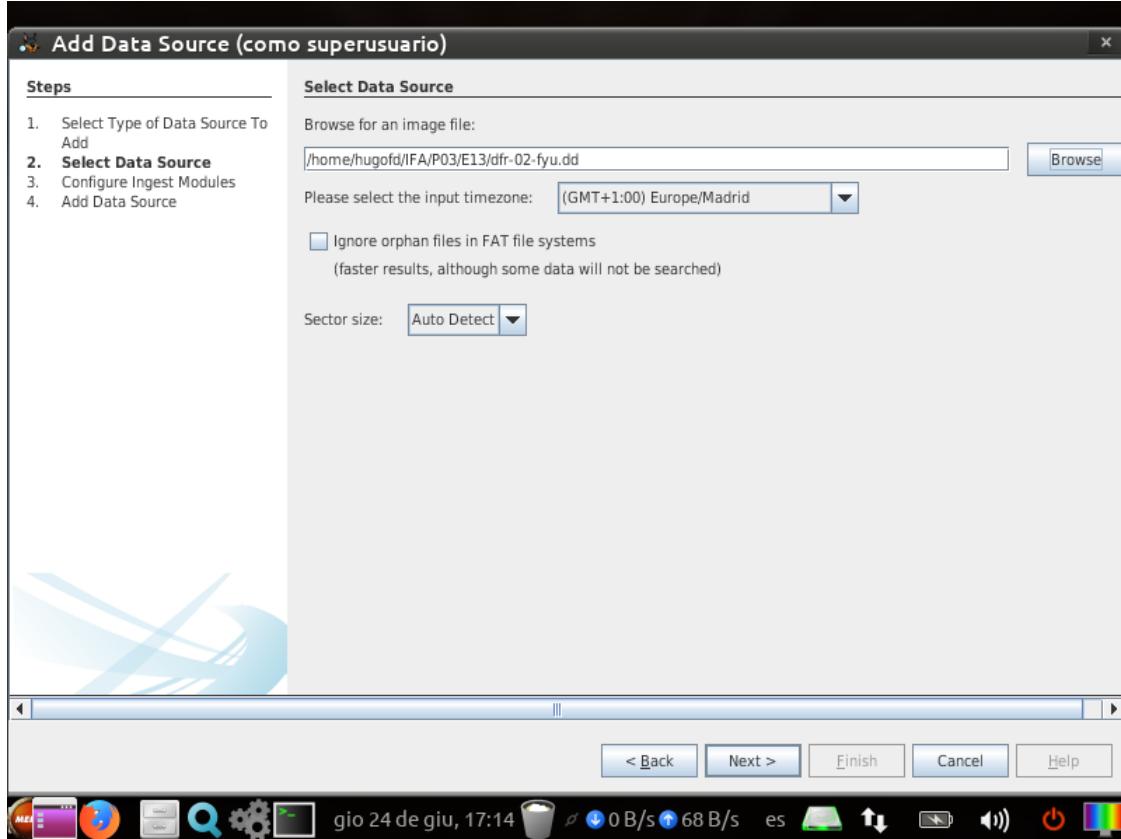


Figura 19: Ejercicio 13: Detalles del examinador



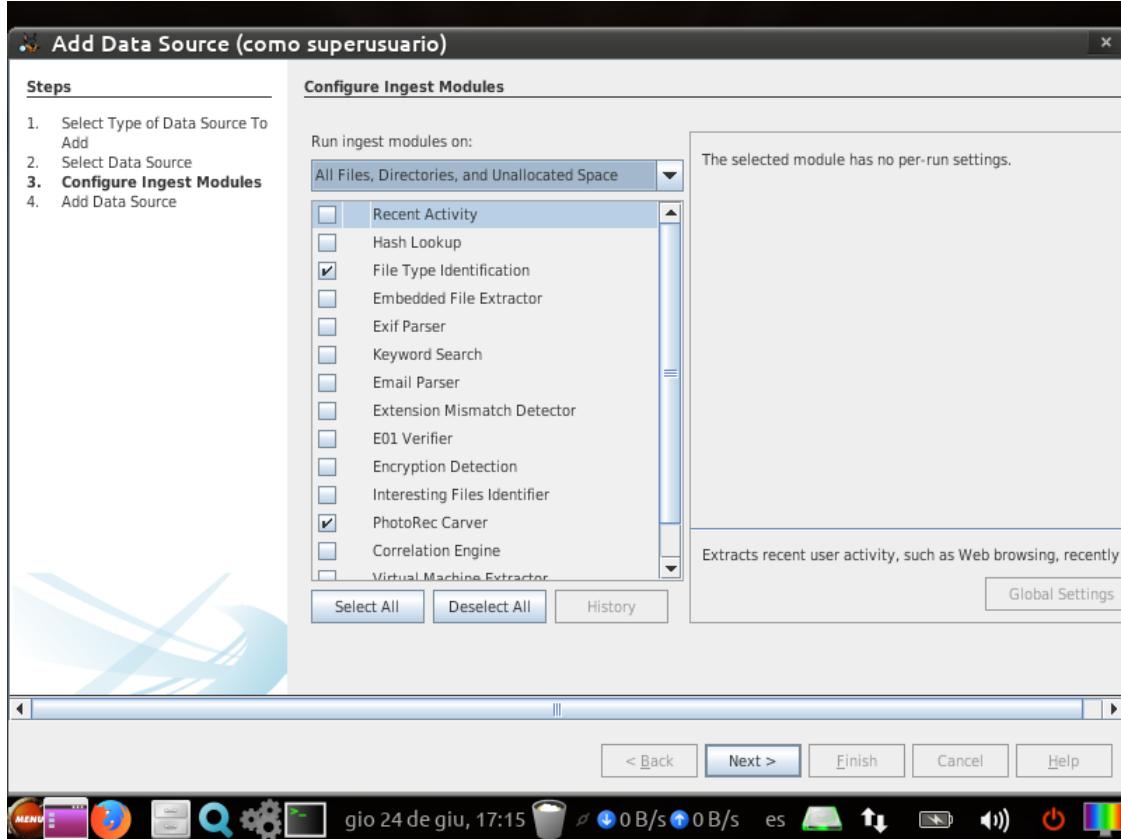
Añadimos la imagen a analizar.

Figura 20: Ejercicio 13: Selección de la imagen



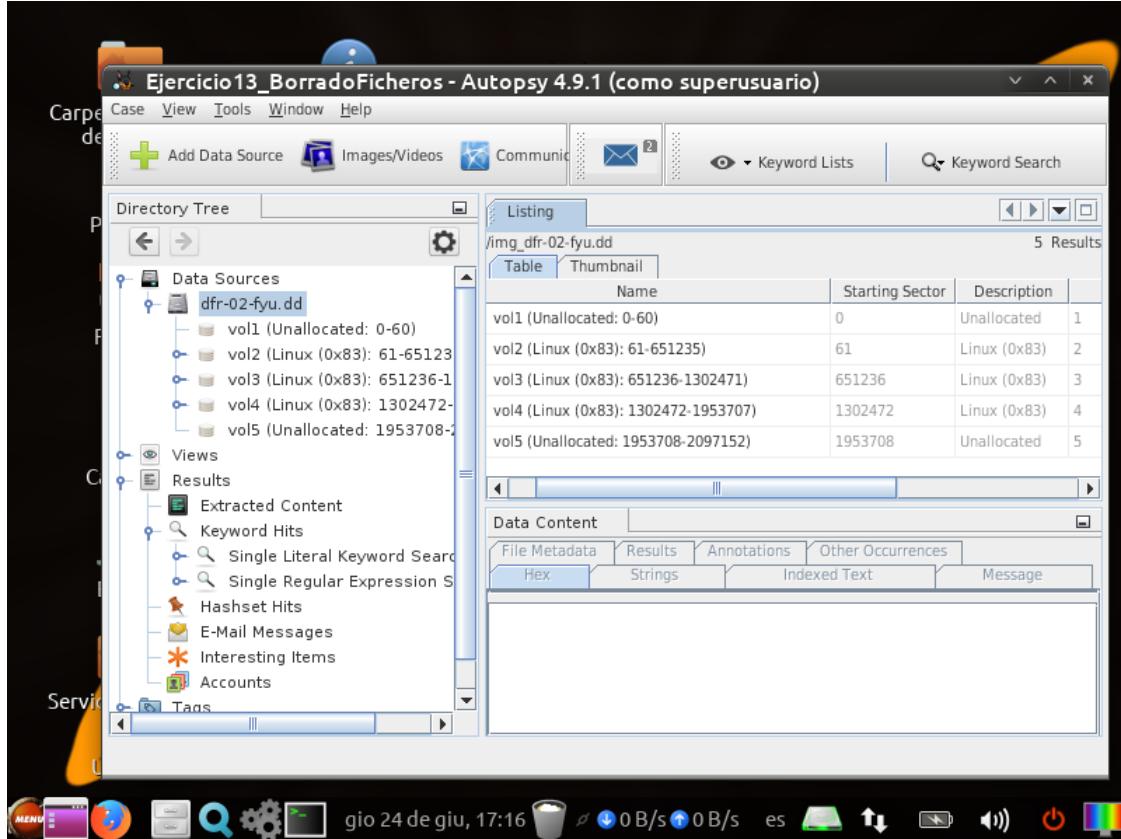
Se seleccionan los módulos de identificación de tipos de fichero y *PhotoRec Carver*.

Figura 21: Ejercicio 13: Selección de módulos



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

Figura 22: Ejercicio 13: Resultados del análisis

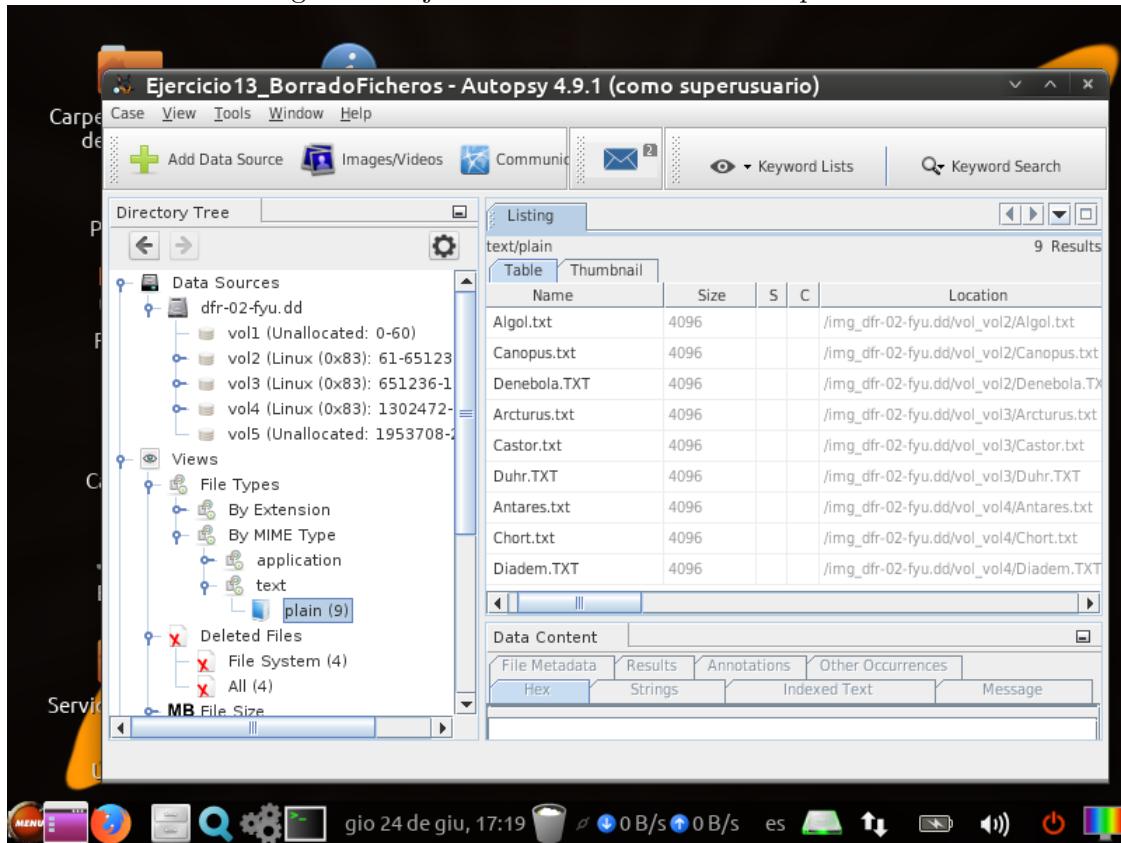


a)

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'.

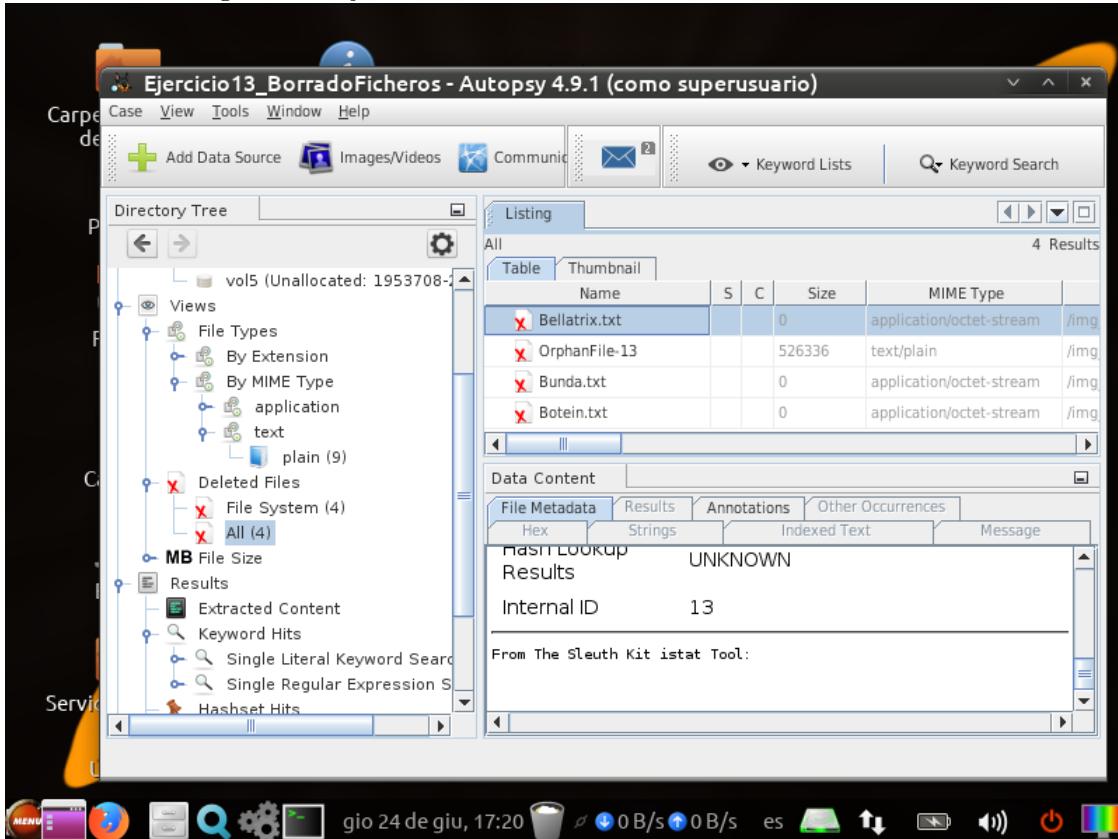
Figura 23: Ejercicio 13: Ficheros de texto plano



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 24: Ejercicio 13: Metadatos de los ficheros borrados

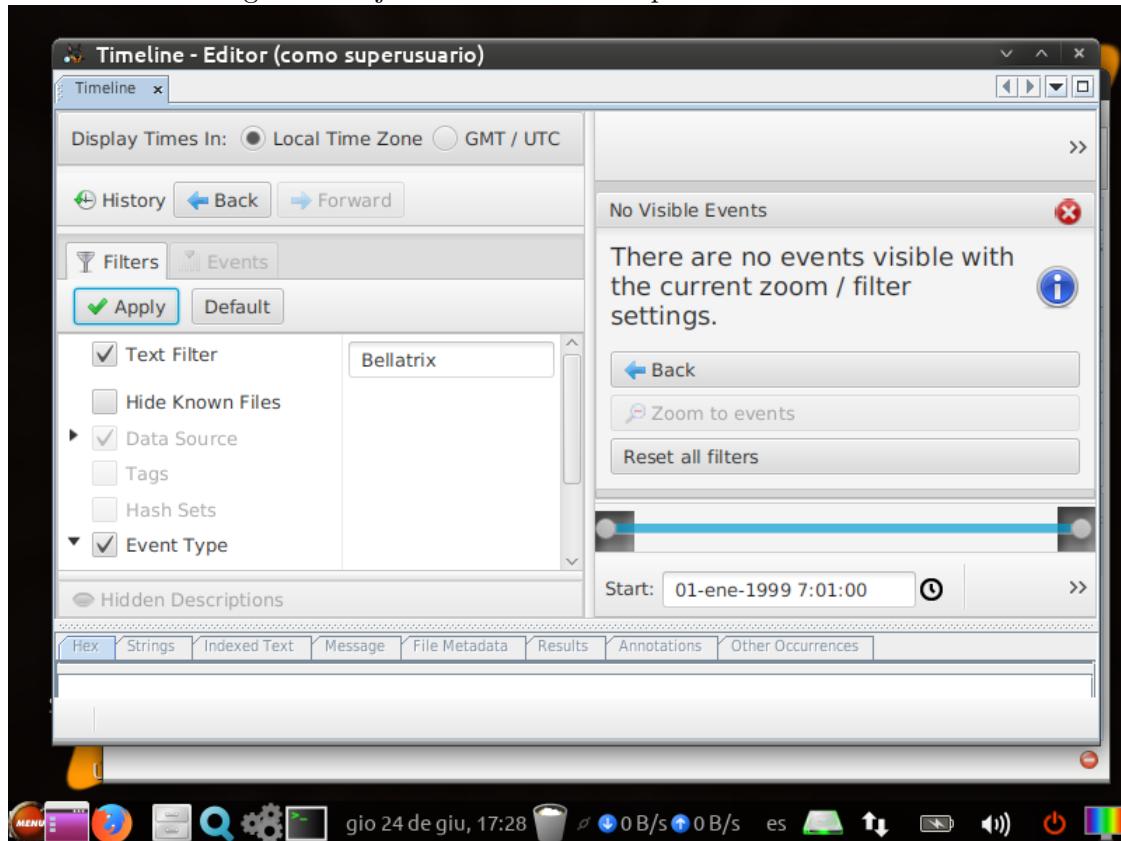


Como se puede observar hay menos metadatos sobre los ficheros borrados que en el ejercicio anterior, por lo que habrá secciones de la tabla sin rellenar.

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 25: Ejercicio 13: Línea temporal de *Bellatrix.txt*



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

Figura 26: Ejercicio 13: Línea temporal de *Bunda.txt*

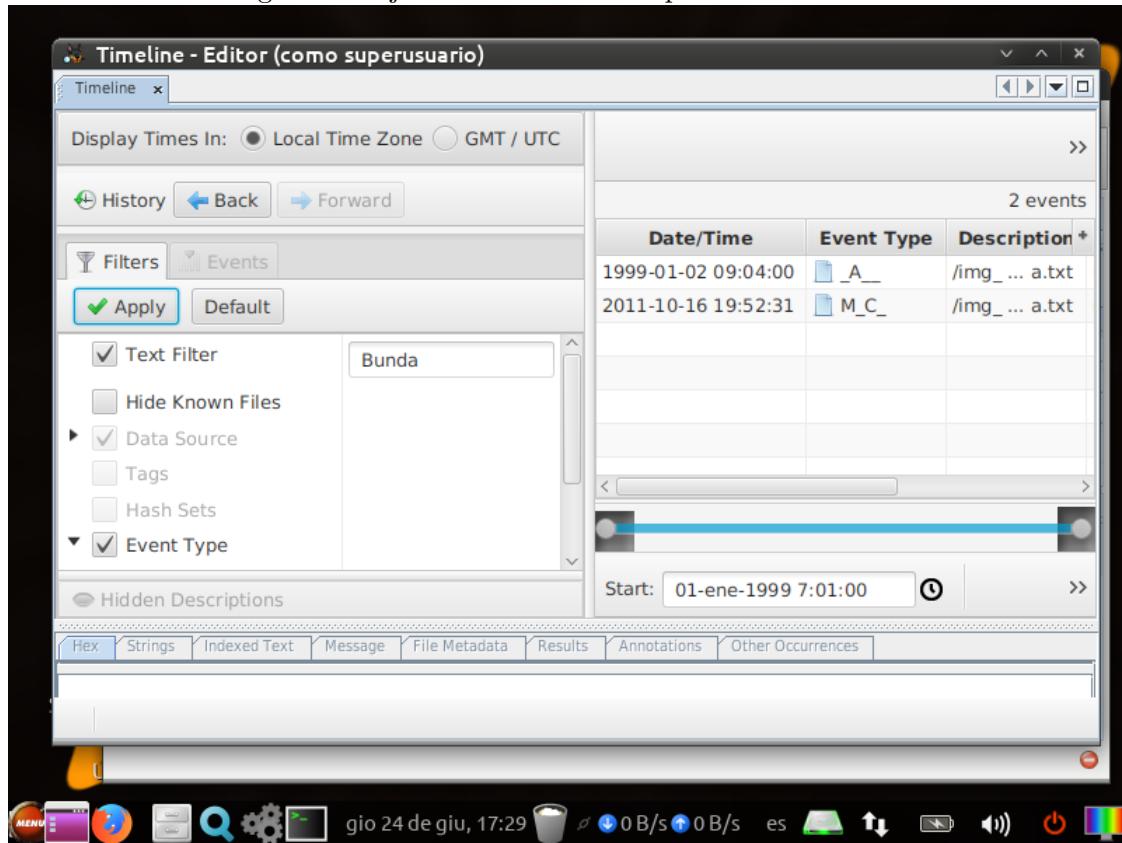
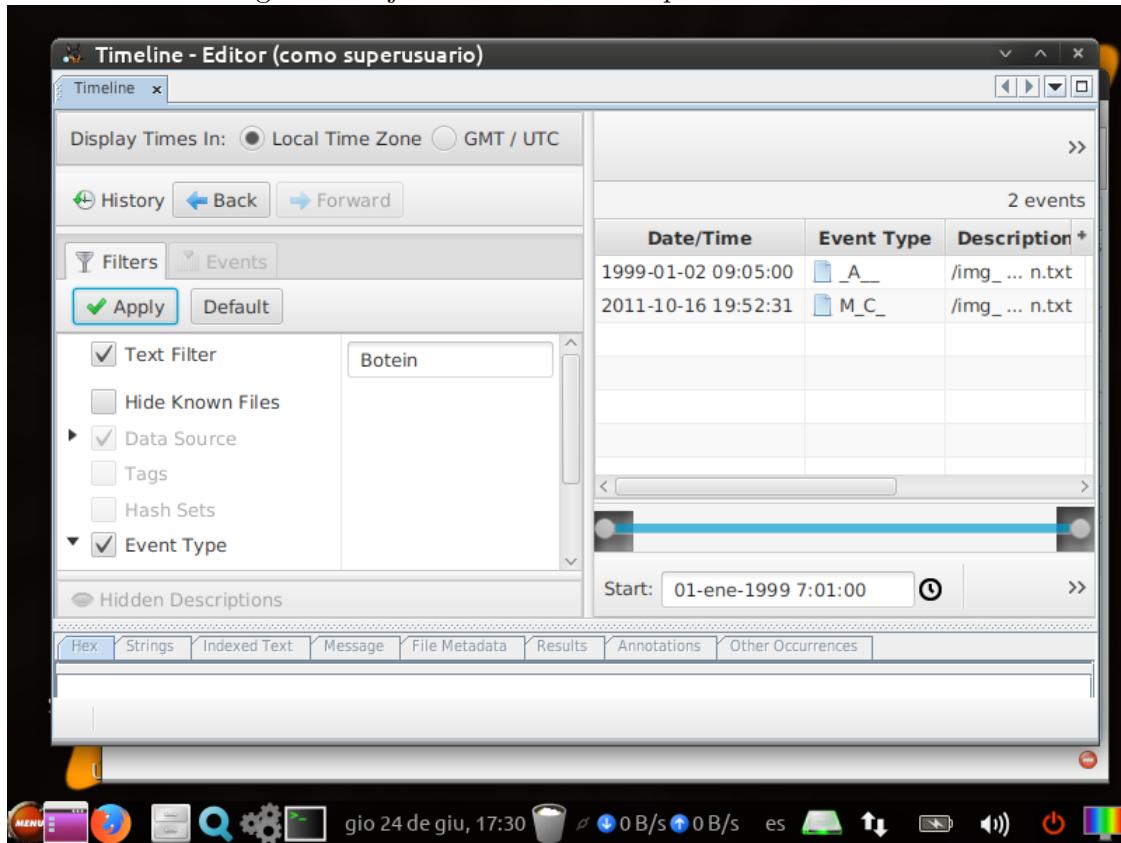


Figura 27: Ejercicio 13: Línea temporal de *Botein.txt*



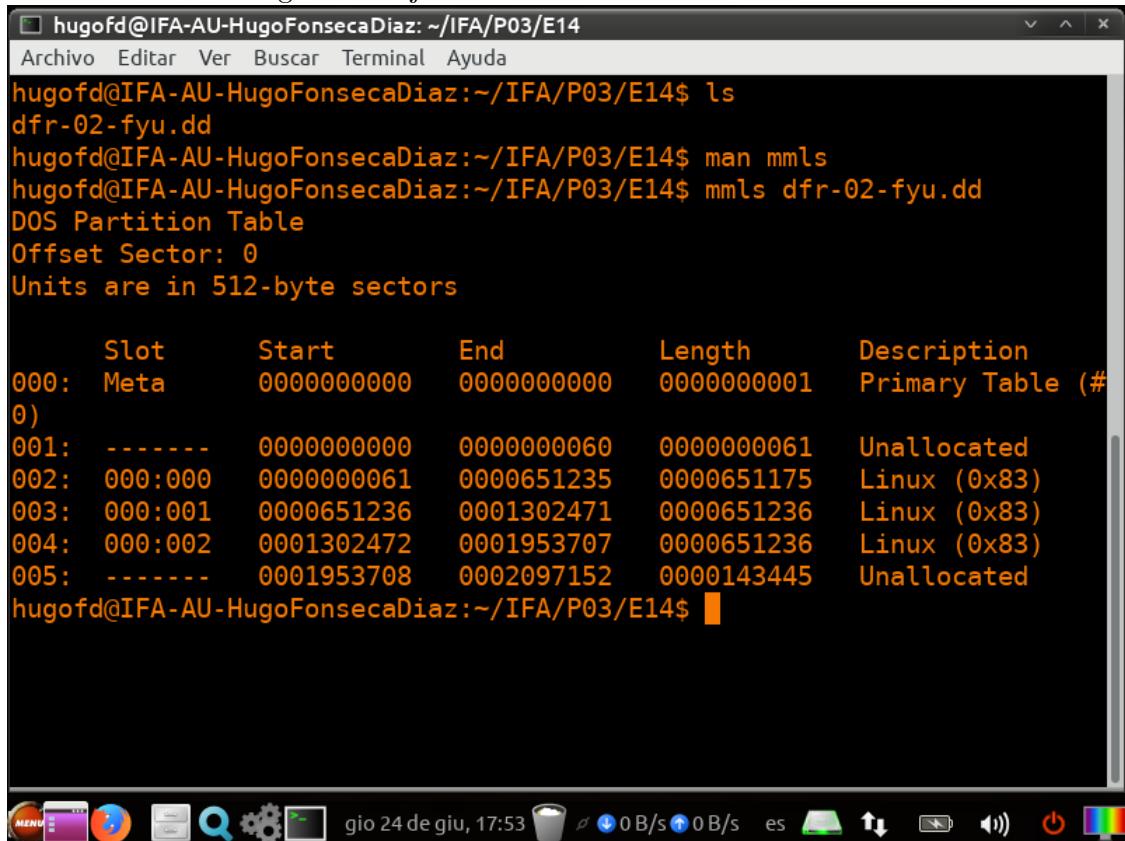
Para *Bunda.txt* y *Botein.txt* sí que se recuperan datos.

3.3. Ejercicio 14

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

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

Figura 28: Ejercicio 14: Salida del comando *mmls*



The screenshot shows a terminal window with the following content:

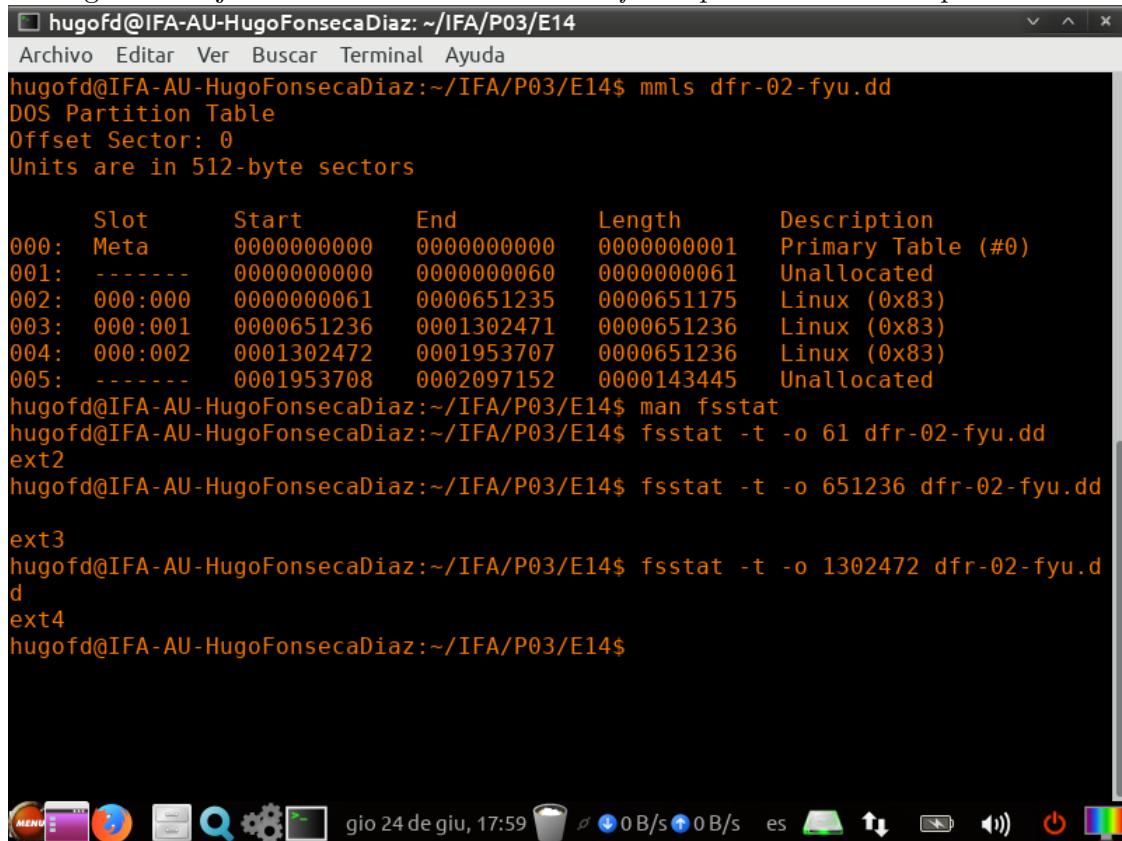
```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ ls
dfr-02-fyu.dd
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man mmls
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ mmls dfr-02-fyu.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      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 29: 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 standard Linux desktop interface at the bottom, including icons for menu, file manager, browser, search, and system settings.

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

Figura 30: 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 terminal 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 31: Ejercicio 14: Salida del comando *fls* con las flags *dFro*

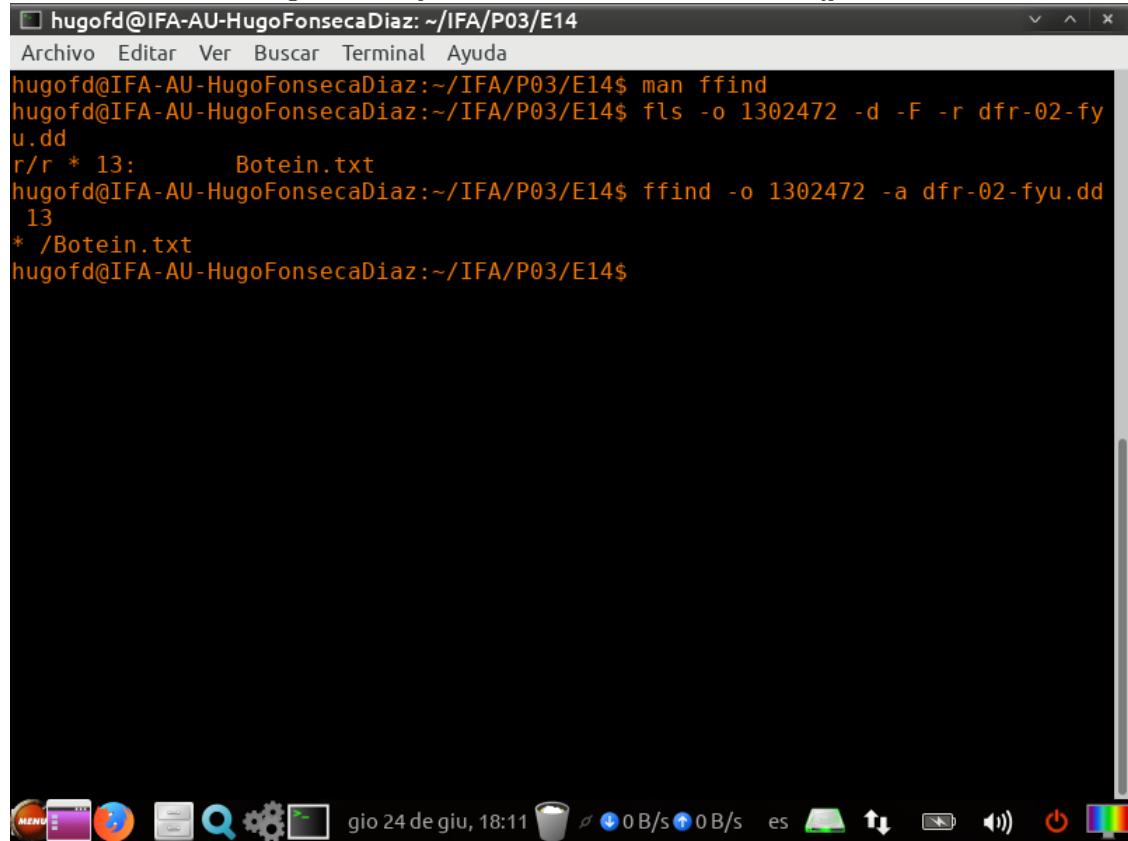
The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14". The window contains the following text:

```
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 taskbar icons at the bottom, which include a menu, a file manager, a browser, a terminal, a search function, system settings, and a power button.

- 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 32: 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 33: 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

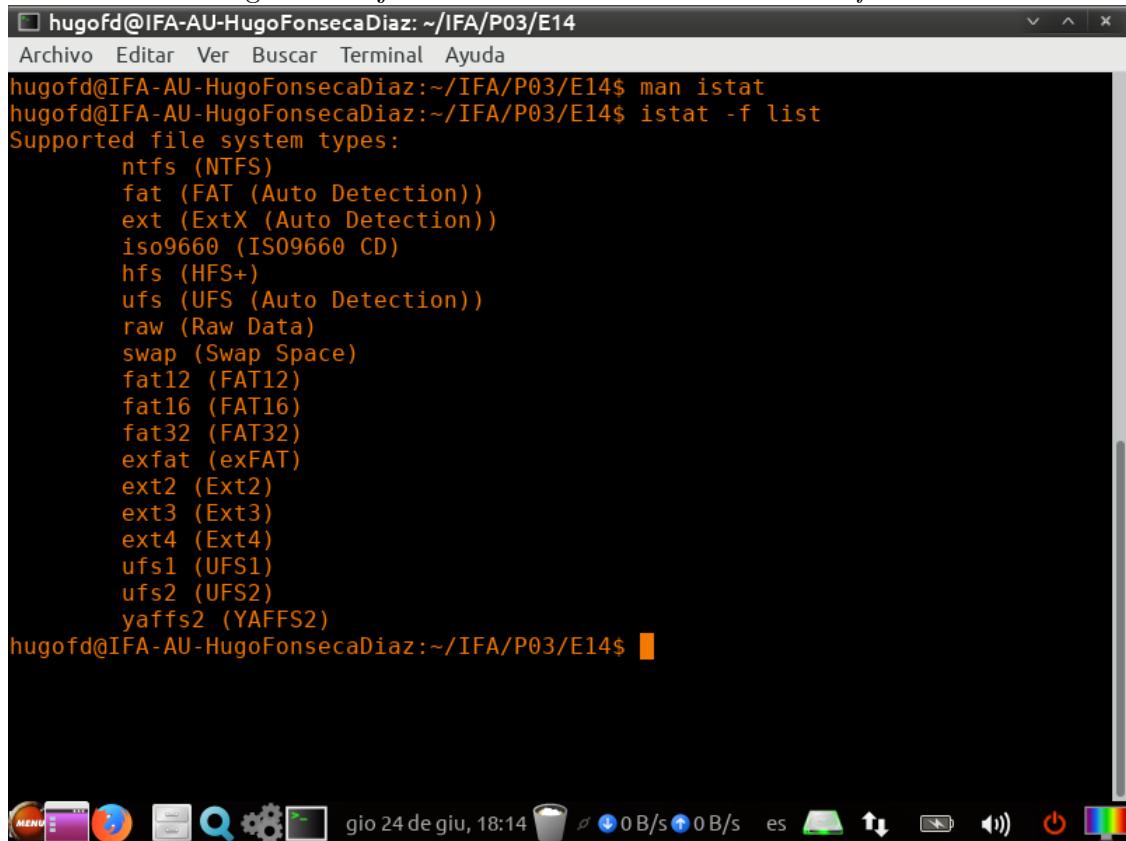
Inode Times:
Accessed: 1999-01-02 09:05:00 (CET)
File Modified: 2011-10-16 19:52:31 (CEST)
Inode Modified: 2011-10-16 19:52:31 (CEST)
Deleted: 2011-10-16 19:52:31 (CEST)

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

The terminal window has a dark background with light-colored 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 34: Ejercicio 14: Salida del comando *istat -f list*



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

3.4. Ejercicio 19

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

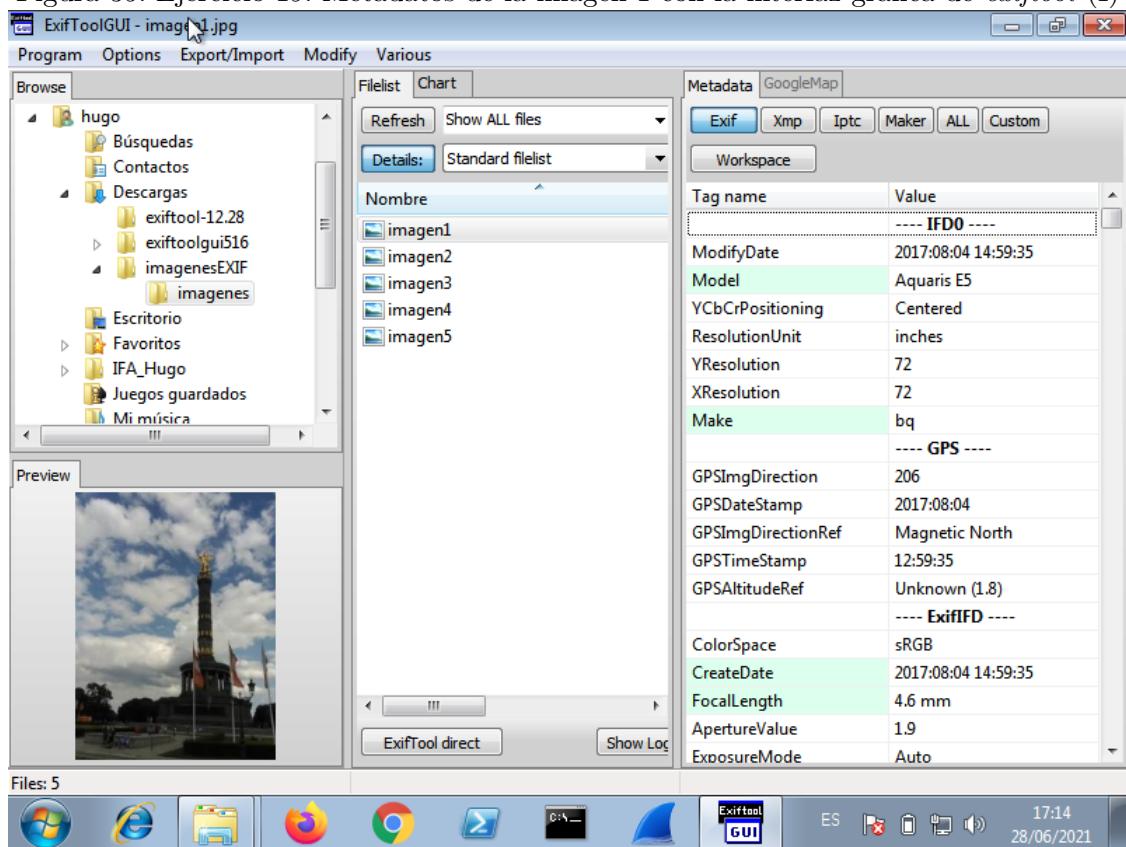


Figura 36: Ejercicio 19: Metadatos de la imagen 1 con la interfaz gráfica de *exiftool* (II)

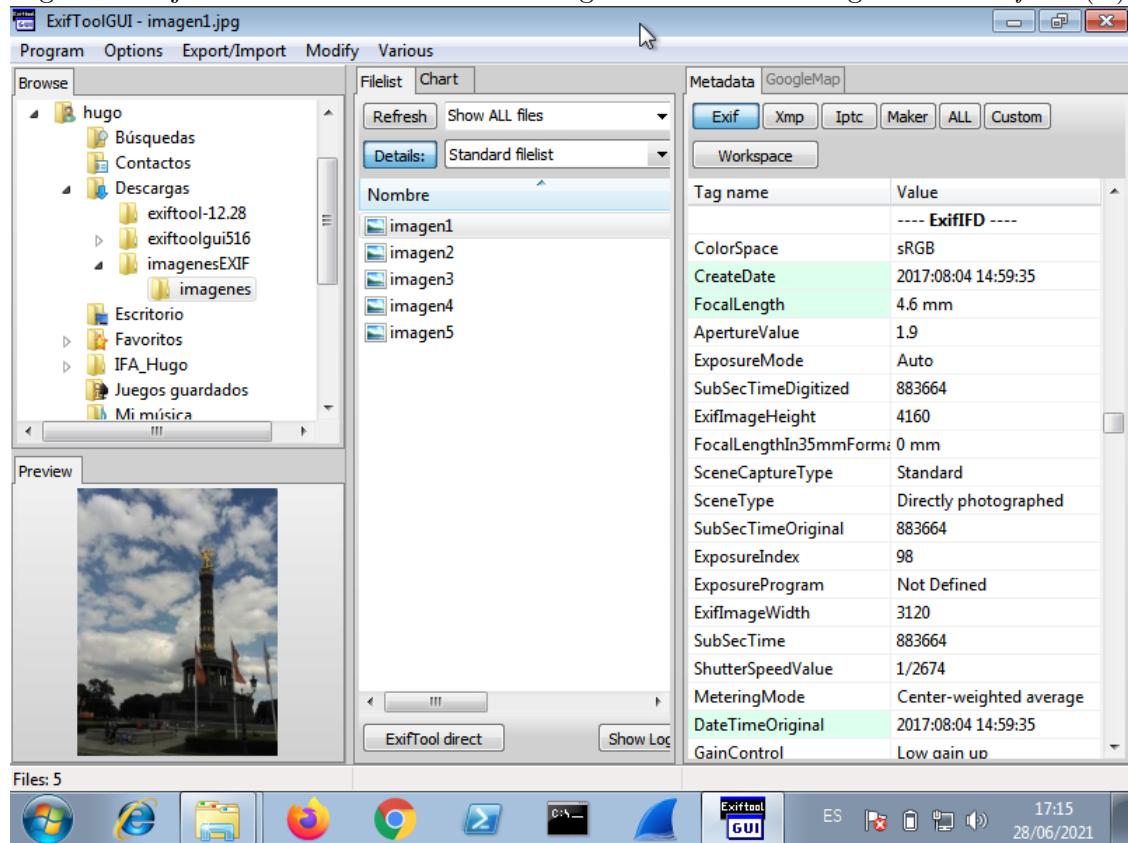
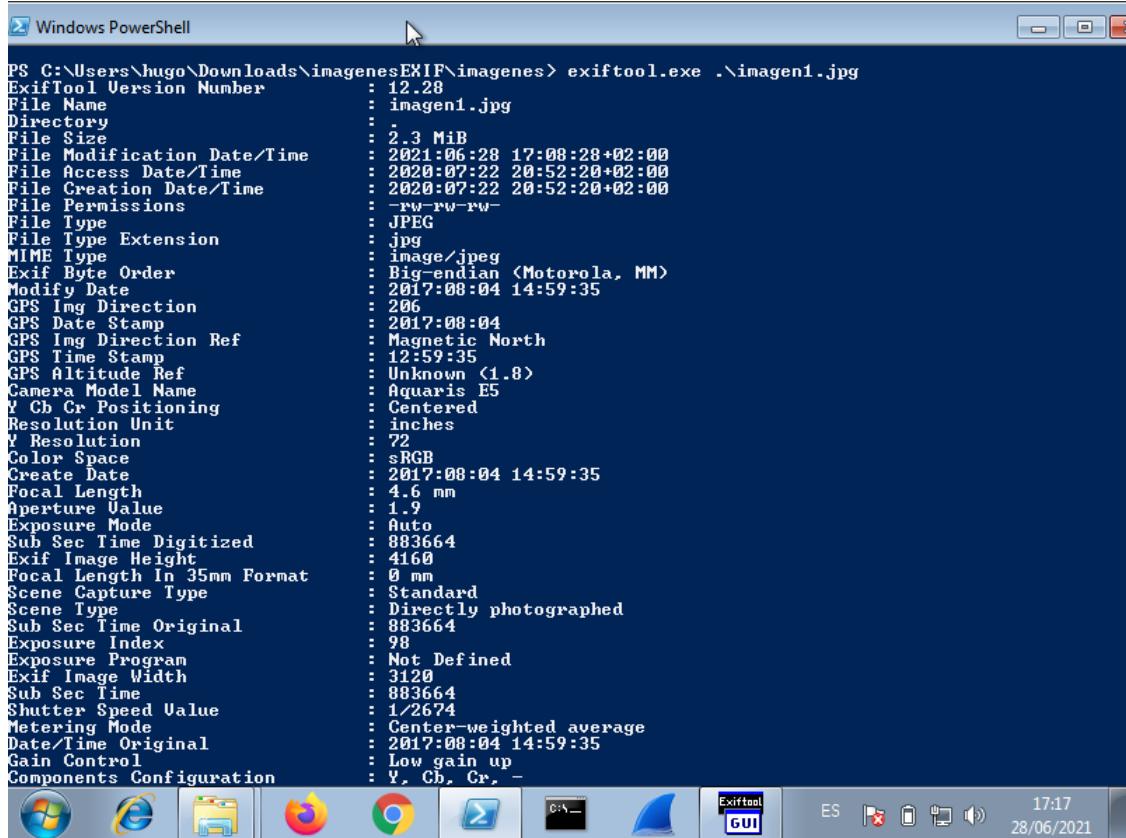


Figura 37: Ejercicio 19: Metadatos de la imagen 1 con el comando *exiftool* (I)



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

```

Windows PowerShell
PS C:\Users\hugo\Downloads\imagenes\EXIF\imagenes1.jpg> exiftool -v
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
YCbCr 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>

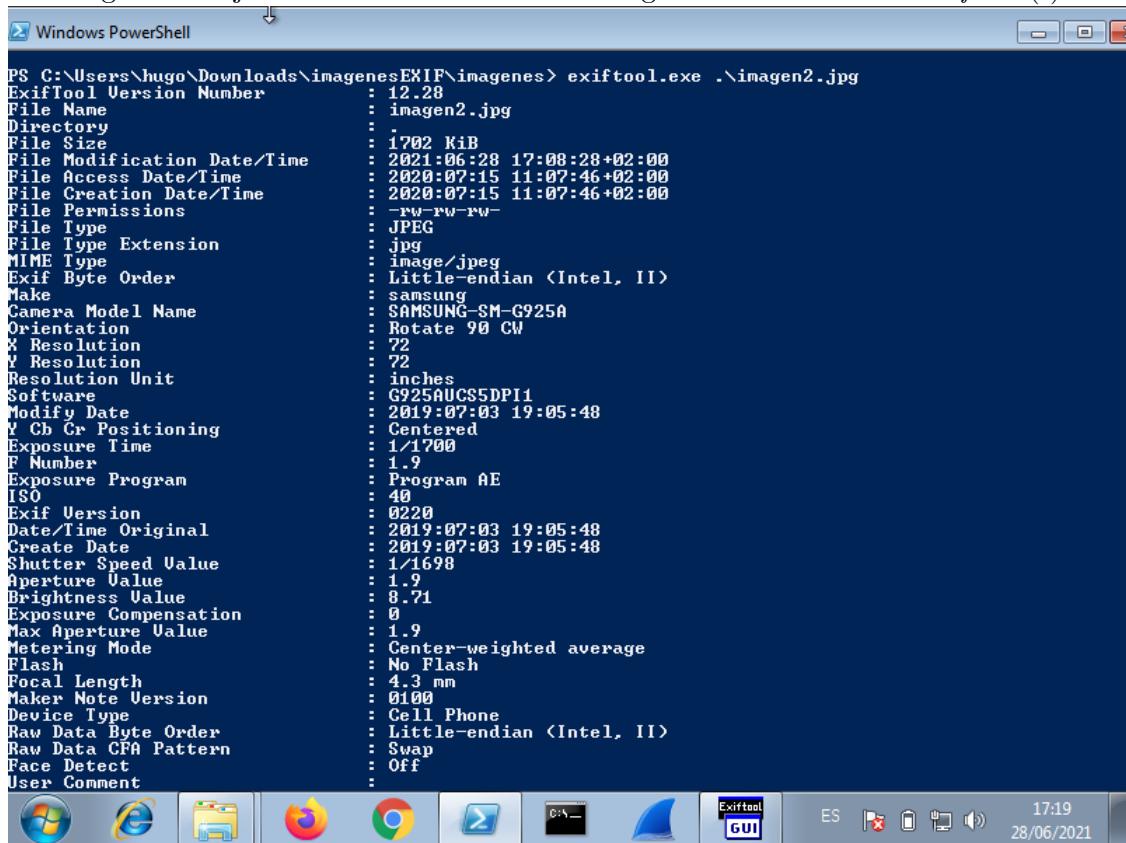
```

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 39: 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                     : G925AUCS5DP11
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 40: 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
Circle Of Confusion : 0.095 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>

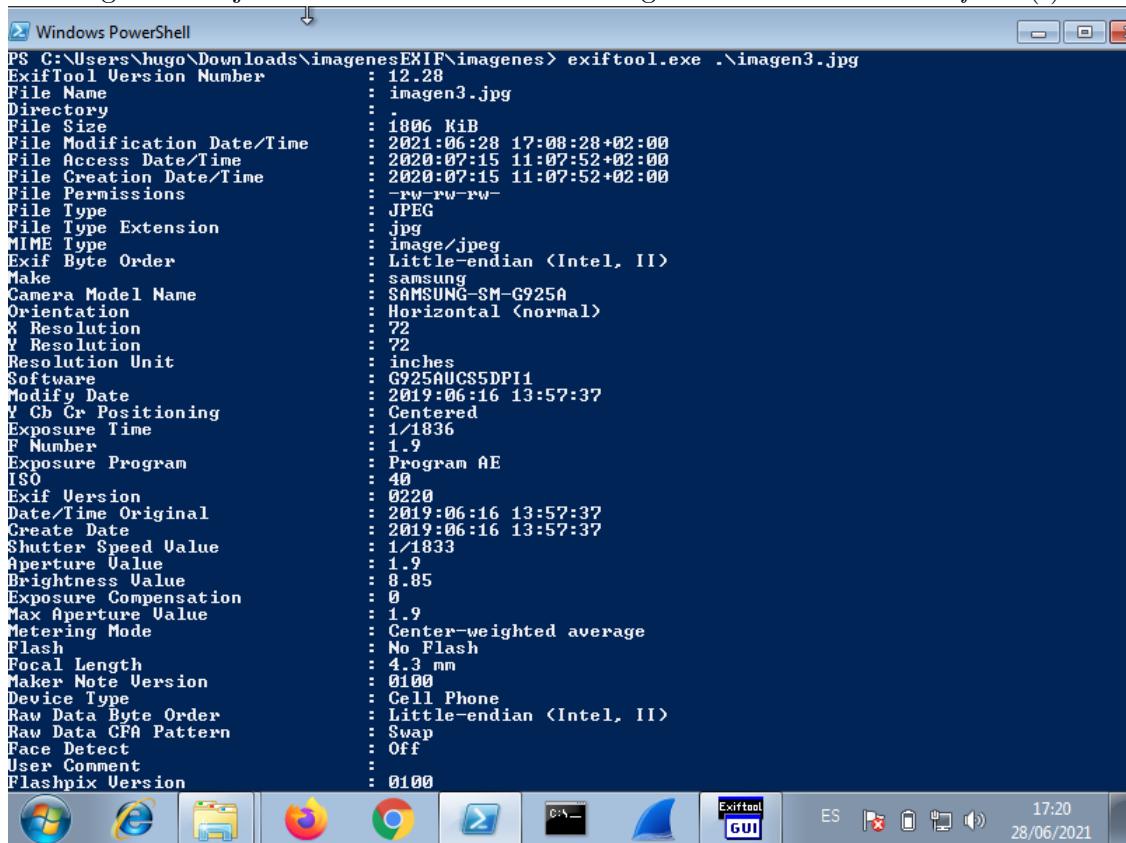
```

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 41: 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 42: Ejercicio 19: Metadatos de la imagen 3 con el comando *exiftool* (II)

```

Windows PowerShell
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes3.jpg

User Comment : 0100
Flashpix Version : sRGB
Color Space : 3264
Exif Image Width : 1836
Exif Image Height : Auto
Exposure Mode : Auto
White Balance : 28 mm
Focal Length In 35mm Format : Standard
Scene Capture Type : A16LSIA00SM A16LSJG01SM.
Image Unique ID : 2.2.0.0
GPS Version ID : North
GPS Latitude 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
GPS Position : 0.005 mm
Circle Of Confusion : 65.5 deg
Field Of View : 4.3 mm <35 mm equivalent: 28.0 mm>
Hyperfocal Distance : 38 deg 42' 51.00" N, 9 deg 8' 23.00" W
Light Value : 2.11 m
Light Value : 14.0
PS C:\Users\hugo\Downloads\imagenesEXIF\imagenes3.jpg>

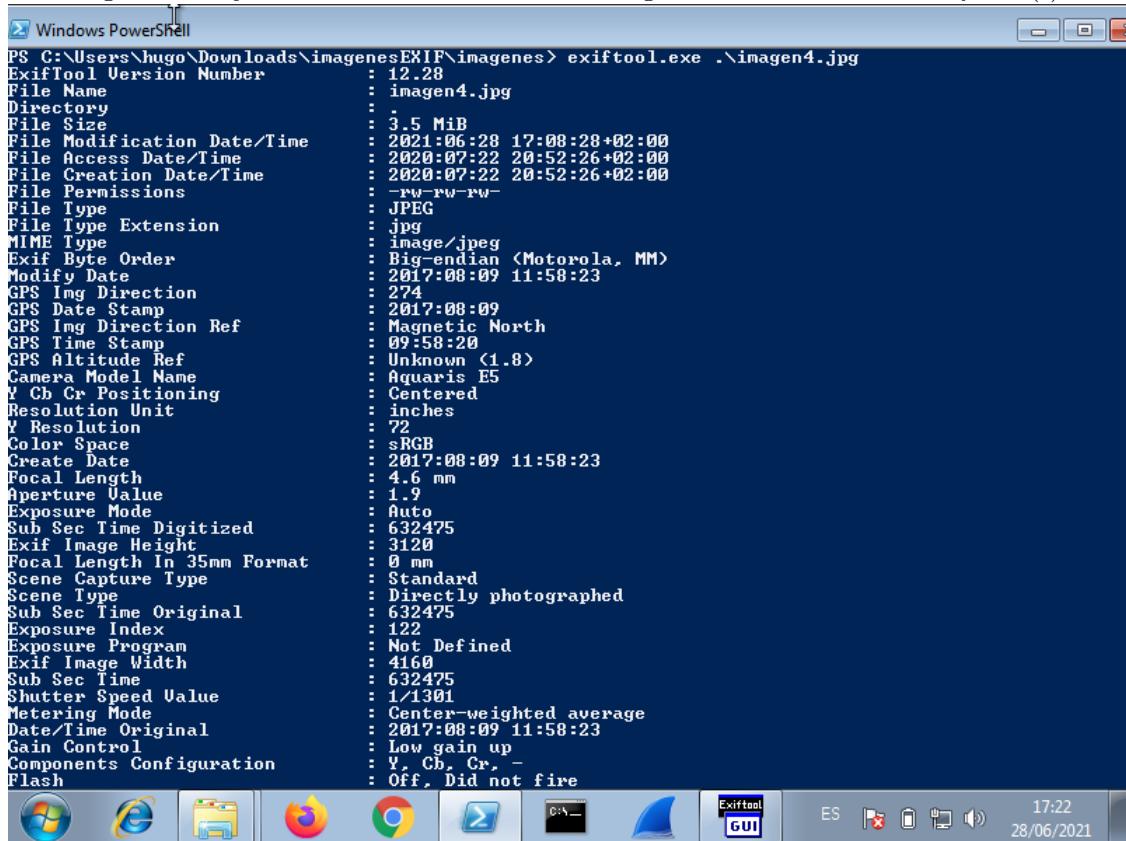

```

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 43: 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
YCbCr 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 44: Ejercicio 19: Metadatos de la imagen 4 con el comando *exiftool* (II)

```

Windows PowerShell
PS C:\Users\hugo\Downloads\imagenes\EXIF\imagenes4.jpg

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
Y Resolution                 : 96
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_Cb_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\imagenes\EXIF\imagenes4.jpg

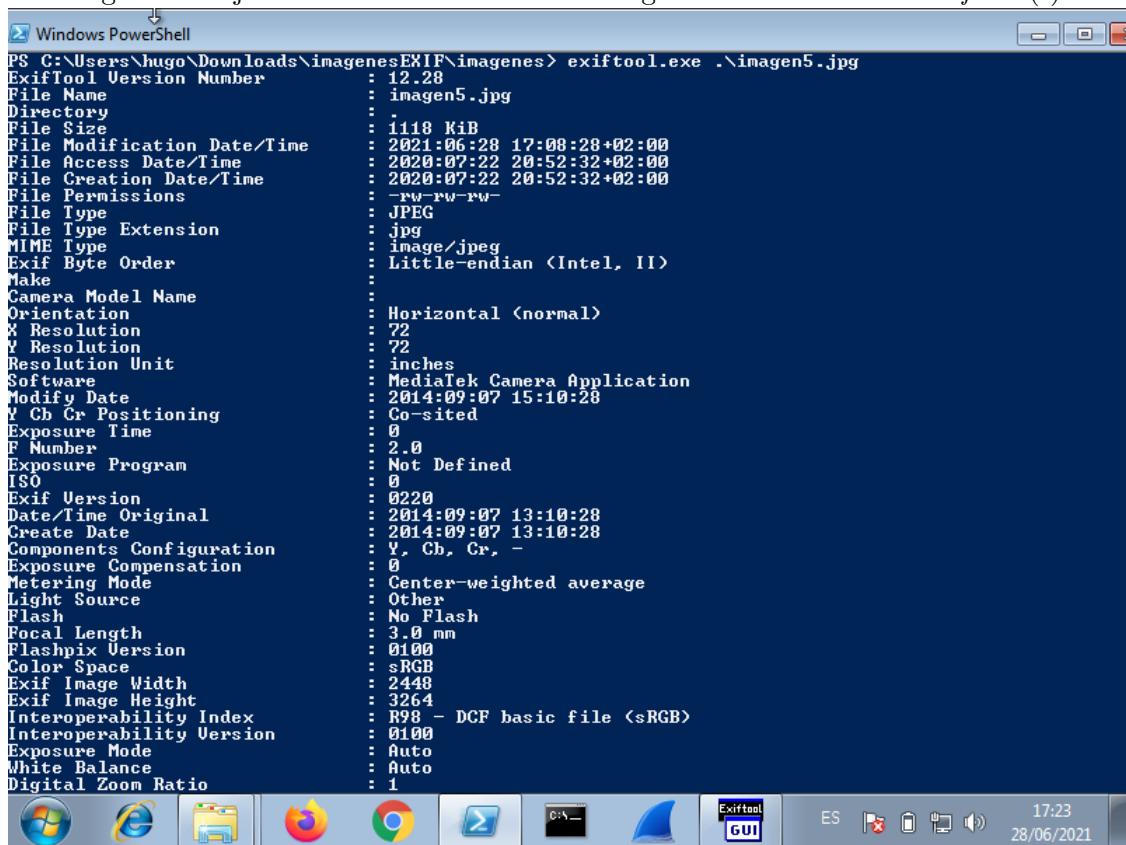
```

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 45: 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 46: Ejercicio 19: Metadatos de la imagen 5 con el comando *exiftool* (II)

```

Windows PowerShell
PS C:\Users\hugo\Downloads\imagenes\EXIF\imagenes> exiftool -v5 5.jpg
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
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

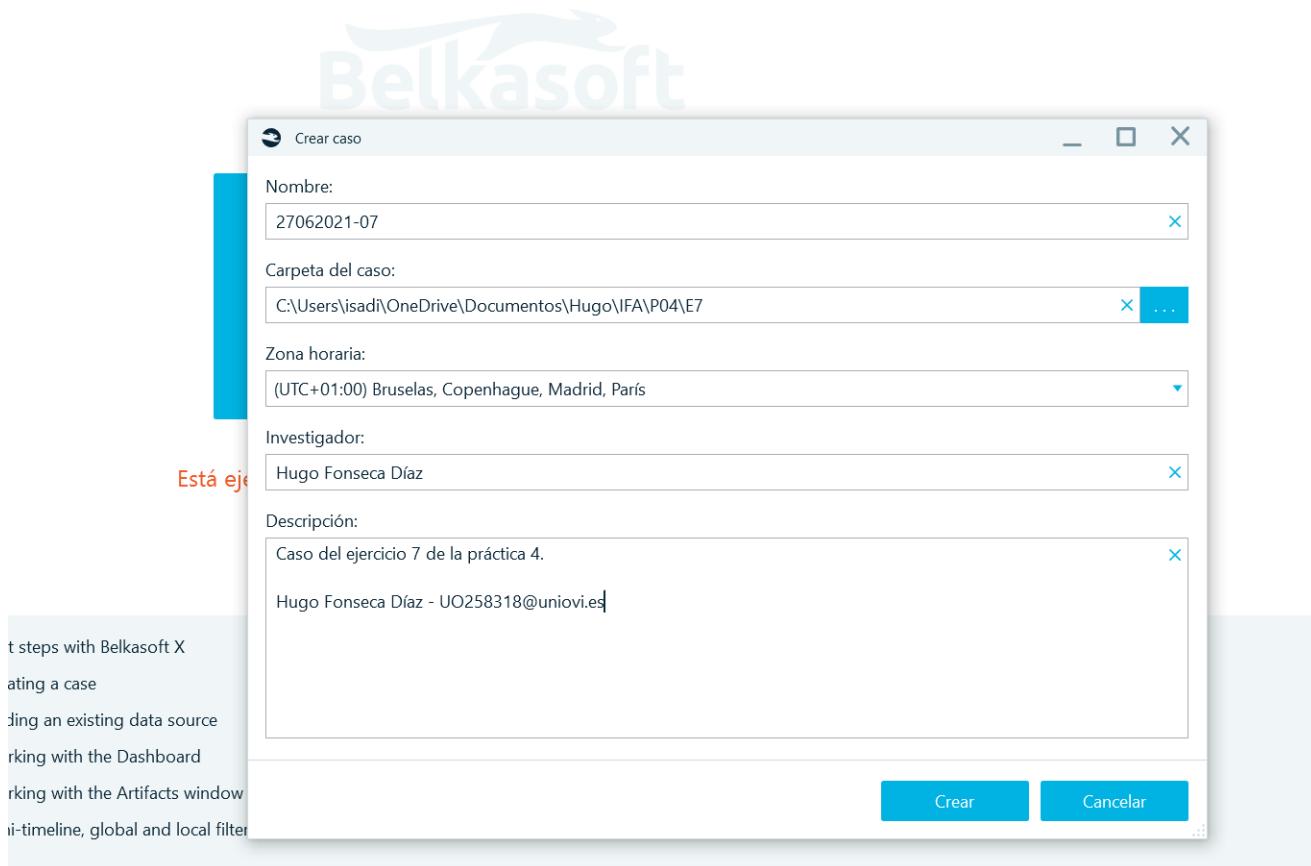
4. Práctica 04

4.1. Ejercicio 7

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 47: Ejercicio 4: Creación del caso

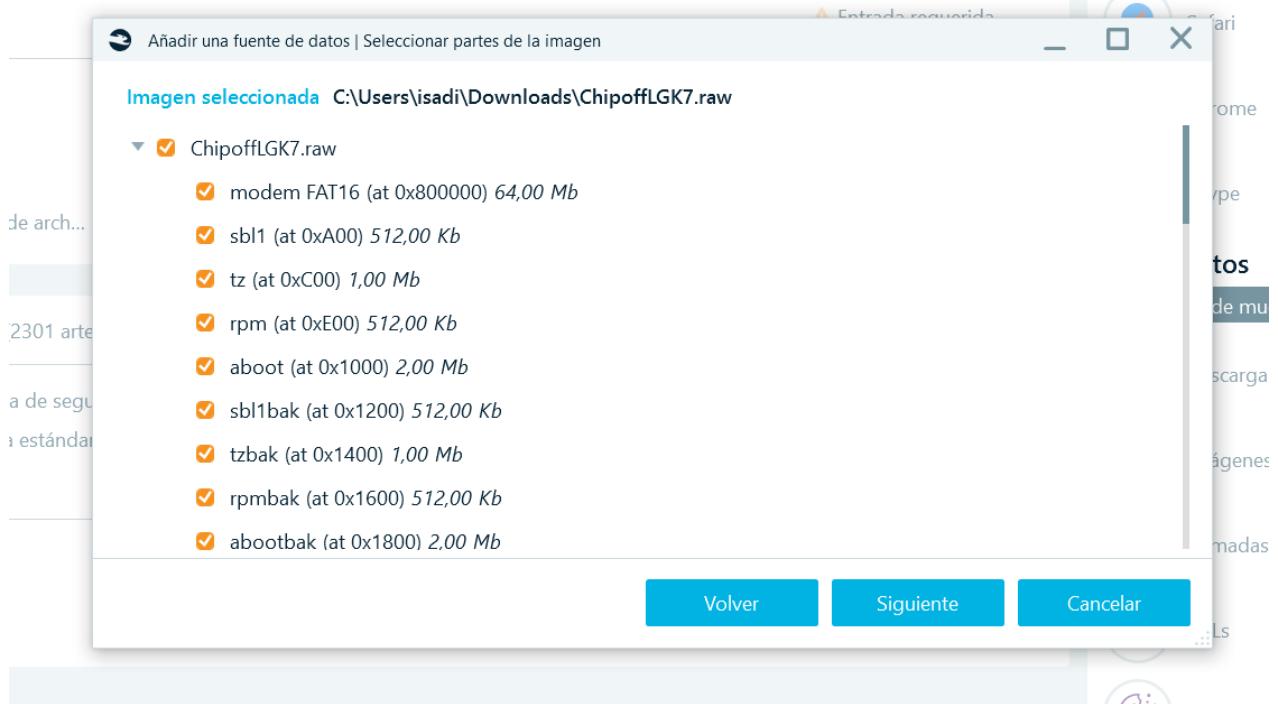


Se selecciona la imagen.

Figura 48: Ejercicio 4: Selección de la imagen

a de seguridad de iTunes

› estándar romance



Se eligen las opciones que pide el enunciado.

Figura 49: 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 sourc...	Carve all space
cache Ext4	Ningún análisis seleccionado	No carving
userdata Ext4	Archivos existentes, Nested data sourc...	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 50: Ejercicio 4: Opciones de análisis avanzadas

Perfil: Custom

Artefactos

- Hashes
- Media
- Encryption

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

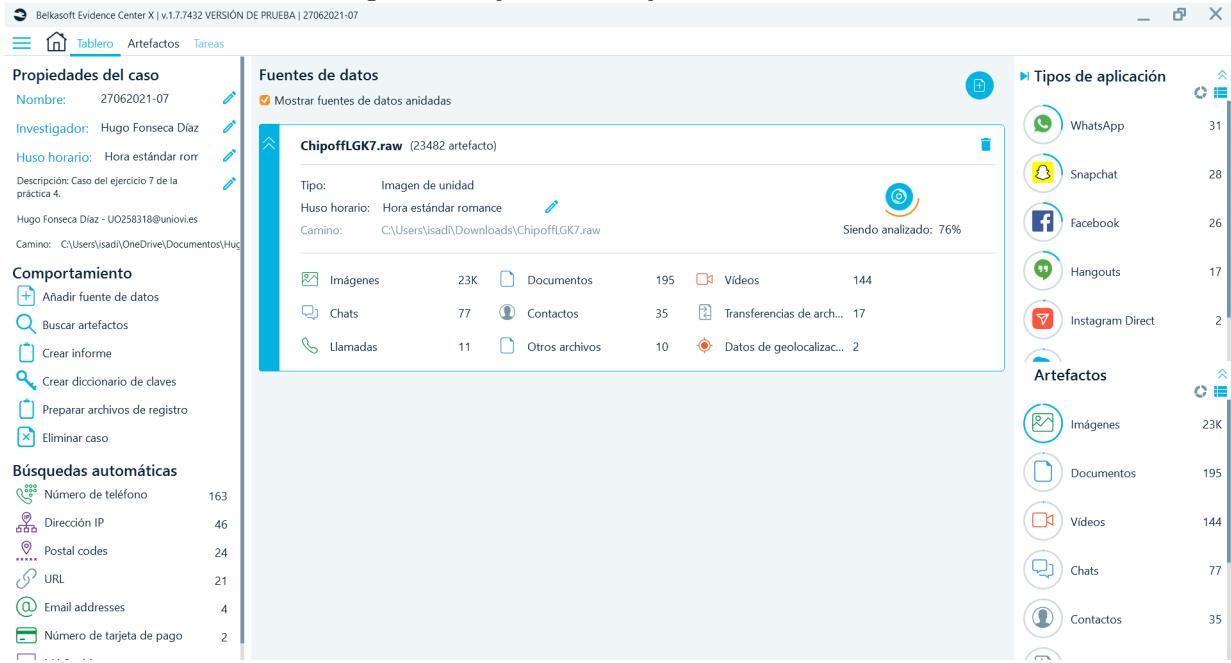
No extraer datos, realice solamente una búsqueda de perfil
(Utilice esta opción para triaje)

Filtro:

Volver Siguiente Cancelar

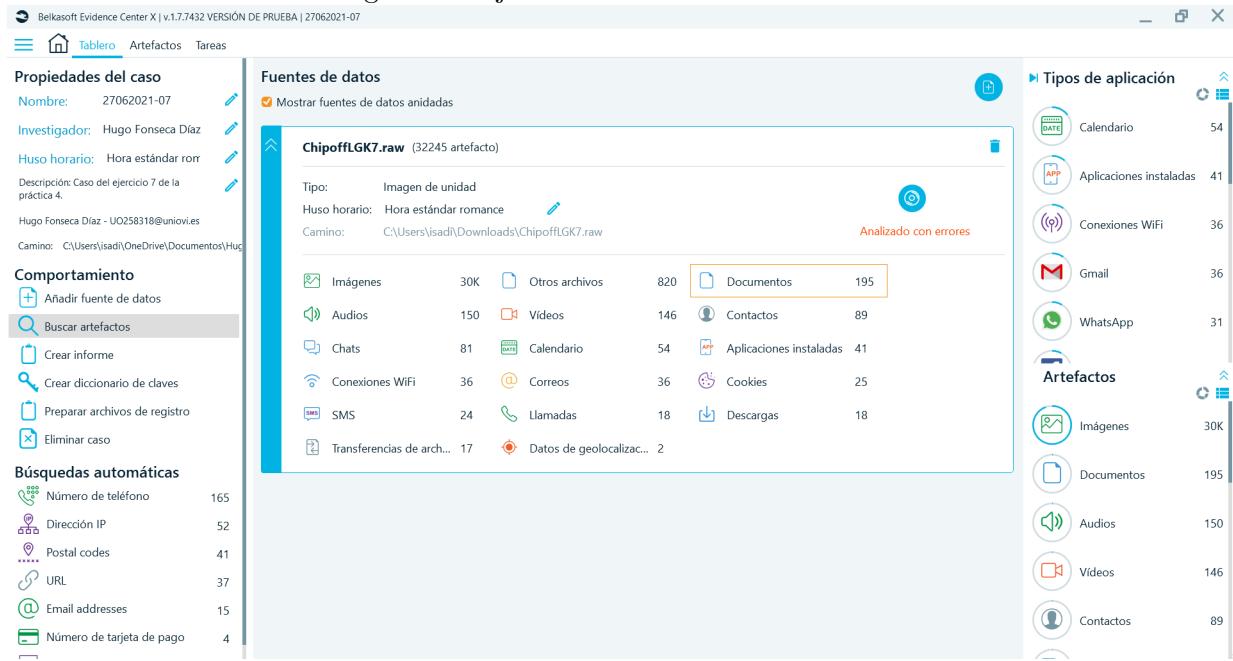
Se ejecuta el análisis, nótese que el tiempo de ejecución es bastante superior al que se obtuvo al analizar la misma imagen con Autopsy, aunque los resultados son más completos.

Figura 51: 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 52: Ejercicio 4: Resultado del análisis



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

ss)

Figura 53: Ejercicio 4: Documentos de tipo *pdf*

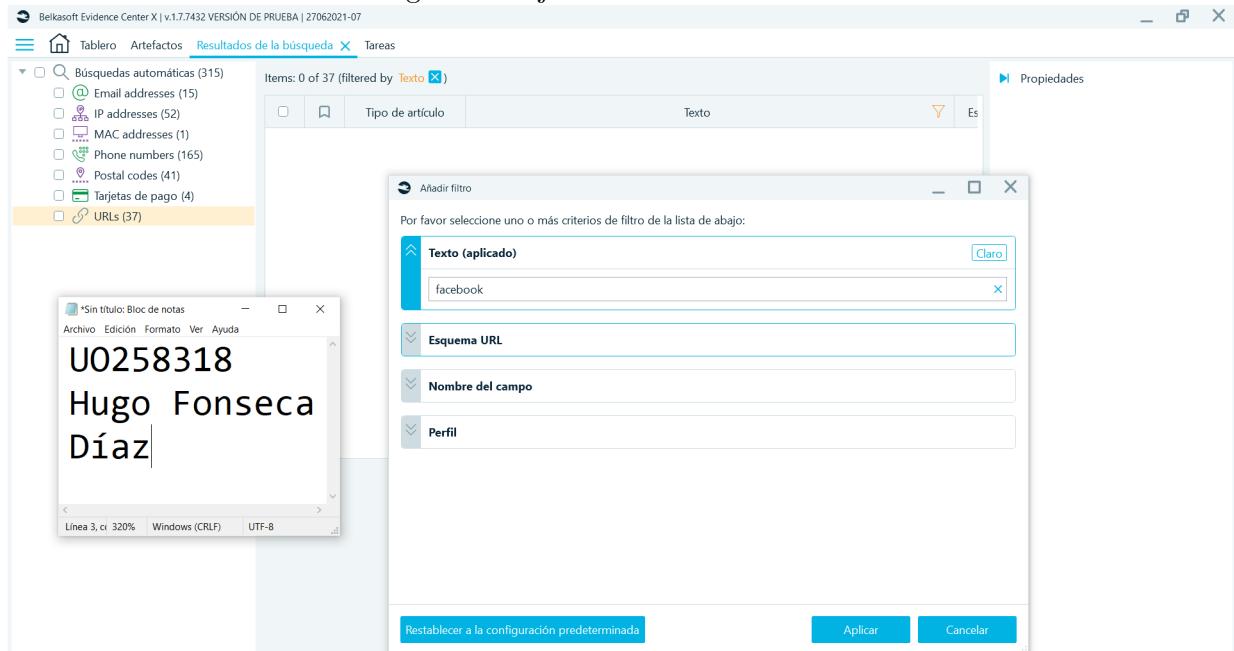
The screenshot shows the Belkasoft Evidence Center X interface. The top navigation bar includes 'Belkasoft Evidence Center X | v.1.7.7432 VERSIÓN DE PRUEBA | 27/06/2021-07'. The main menu has tabs 'Reporte', 'Tablero', 'Artefactos' (selected), and 'Tareas'. Below the menu is a timeline from 2003 to 2020. 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 central area displays a search results 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 bottom of the preview window shows 'Texto del artículo', 'Maleficio', and 'Páginas'. The properties panel on the right is titled 'General' and lists the following information:

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 54: Ejercicio 4: URLs visitadas



No hay ninguna url correspondiente a *Facebook*.

uu)

Figura 55: 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 indicates the analysis period from 2003 to 2020.

The left sidebar shows a tree view of artifacts: 'Estructura' and 'Visión general'. Under 'Visión general', 'Anfitrío' is selected, showing 425 entries. The 'Cookies' node under 'Navegadores' is highlighted.

The main pane displays a table of cookies found on .facebook.com, sorted by 'Fecha de venc...'. One cookie entry is selected, showing its details in a properties panel:

General	
Host	.facebook.com
Clave	fr
Valor	1gRi2BHvBje7w6YjE-AWWXnw4YA-roR8_iwwklpBgRm4Y.bbs5Y6...AAA0.0.Bb5Y6_AWUC5Q6b
Fecha de modificación (UTC)	
Fecha de modificación (Local)	
Fecha de vencimiento (UTC)	09/11/2019 13:42:23
Fecha de vencimiento (Local)	
Hora de creación (UTC)	09/11/2019 13:42:24
Segura	0
Origen	
Tipo de perfil	Android application web-data

A note window titled 'Sin título: Bloc de notas' is open, displaying the following text:

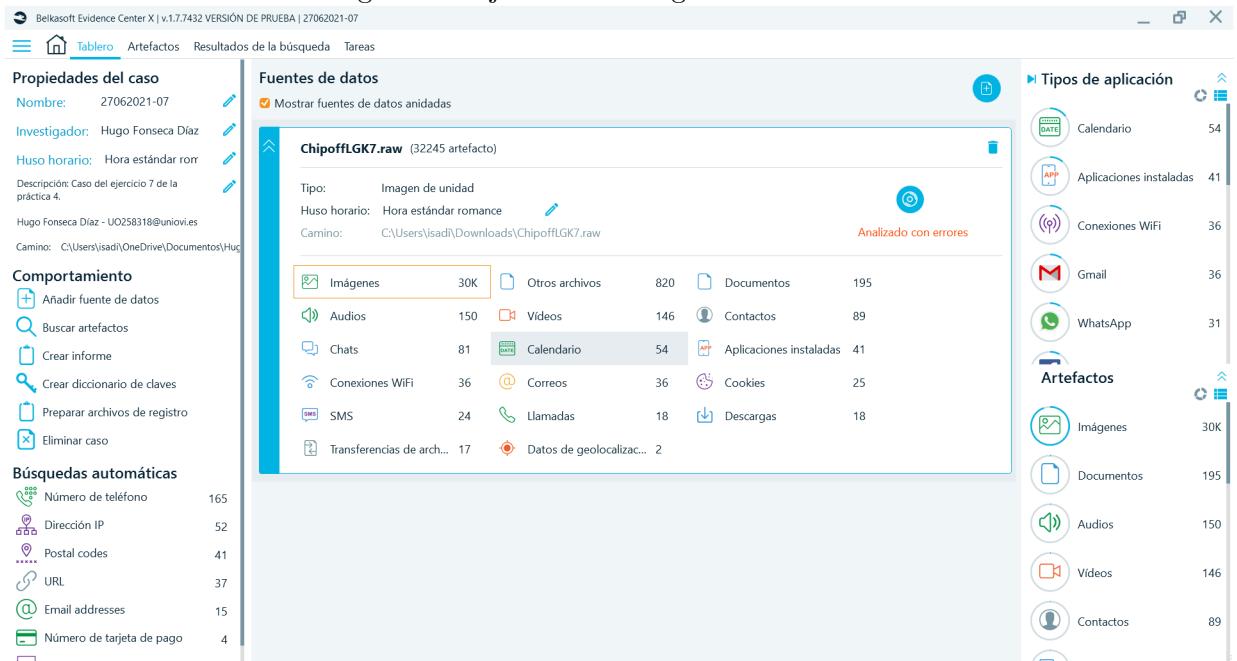
U0258318
Hugo Fonseca
Díaz

The status bar at the bottom of the note window shows: 'Línea 3, cr 320% Windows (CRLF) 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 56: Ejercicio 4: Imágenes identificadas



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

ww)

Figura 57: Ejercicio 4: Imágenes en formato *jpg*

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' and tabs for 'Tablero', 'Artefactos' (selected), 'Resultados de la búsqueda', and 'Tareas'. Below the tabs is a timeline from 2003 to 2020. The main area displays a table of search results:

Estructura	Visión general	Tipo de archivo	Estado	Nombre del archivo	Previsualización
Aplicaciones instaladas (41)			Valid	picture_00003B1D8110.jpg	
Audios (150)			Valid	picture_00003B1D8F13.jpg	
Calendario (54)			Not processed	0.jpg	
Chats (81)			Not processed	1.jpg	
Conexiones WiFi (36)			Not processed	2.jpg	
Contactos (89)			Not processed	3.jpg	
Correos (36)			Not processed	4.jpg	
Datos de geolocalización (2)			Not processed	5.jpg	
Documentos (195)			Not processed	6.jpg	
Imágenes (30493)	Selected		Not processed	7.jpg	
Llamadas (18)			Valid	Message_154177027	
Navegadores (43)			Valid	Message_154177027	
Cookies (25)			Not processed		
Descargas (18)			Not processed		
Otros archivos (820)			Not processed		
SMS (24)			Valid		
Transferencias de archivos (17)			Valid		
Videos (146)			Valid		

A modal window titled 'Previsualización de la imagen' shows a preview of a jpg file named '12402528734.jpg'. The preview contains the text 'UO258318', 'Hugo Fonseca', and 'Díaz'. Below the preview is a hex dump of the file's content.

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000000000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 00 01 y0y...JFIF...
000000000010 00 01 00 00 FF ED 00 B4 50 68 6F 74 6F 73 68 6F ...y1.Photos
000000000020 70 20 33 2E 30 00 38 42 49 4D 04 04 00 00 00 p 3.0.BBIM....
000000000030 00 67 1C 02 28 00 62 46 42 4D 44 30 31 30 30 .g...(.bfBMD01000
000000000040 61 61 34 30 33 30 30 35 39 31 61 30 30 a4030000591a000
000000000050 30 63 33 34 39 30 30 30 33 31 34 62 30 30 c3490000314b000
000000000060 30 37 61 34 63 30 30 30 62 30 37 33 30 30 07a4c00000073000
000000000070 30 39 35 63 62 30 30 30 38 36 64 30 30 095cb000008d0000
000000000080 30 31 39 64 36 30 30 30 34 32 64 62 30 30 0194d6000042ab000

```

Below the hex dump, it says 'Tamaño: 102,4 KB'.

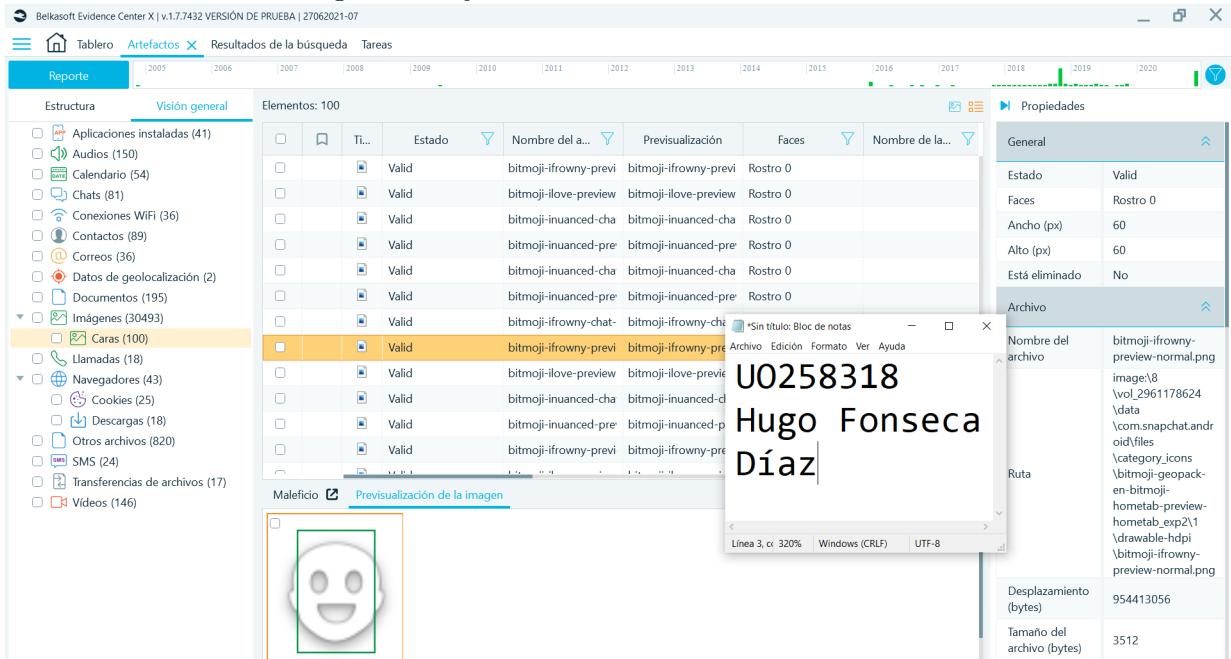
The 'Propiedades' (Properties) panel on the right shows the following details for the selected file:

General	
Estado	Valid
Ancho (px)	640
Alto (px)	640
Está eliminado	No
Archivo	
Nombre del archivo	12402528734.jpg
Ruta	image:\8\vol_2961178624\data\com.whatsapp\cache\Profile\Pictures\12402528734.jpg
Desplazamiento (bytes)	947257344
Tamaño del archivo (bytes)	104886
Creado (UTC)	09/11/2018 13:48:43
Modificado (UTC)	09/11/2018 13:48:43
Hora de acceso (UTC)	09/11/2018 13:48:43

Se han encontrado 1011 imágenes en formato *jpg*. Sin embargo, se han buscado mediante el nombre de usuario, 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)

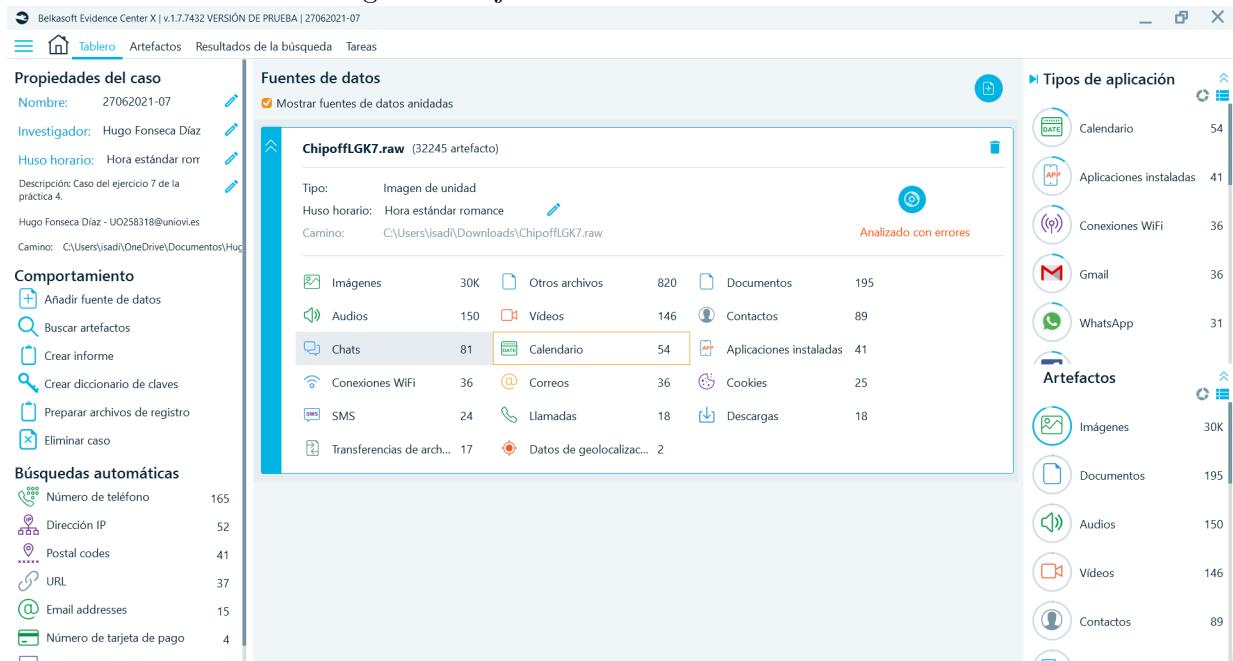
Figura 58: Ejercicio 4: Reconocimiento de rostros



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

yy)

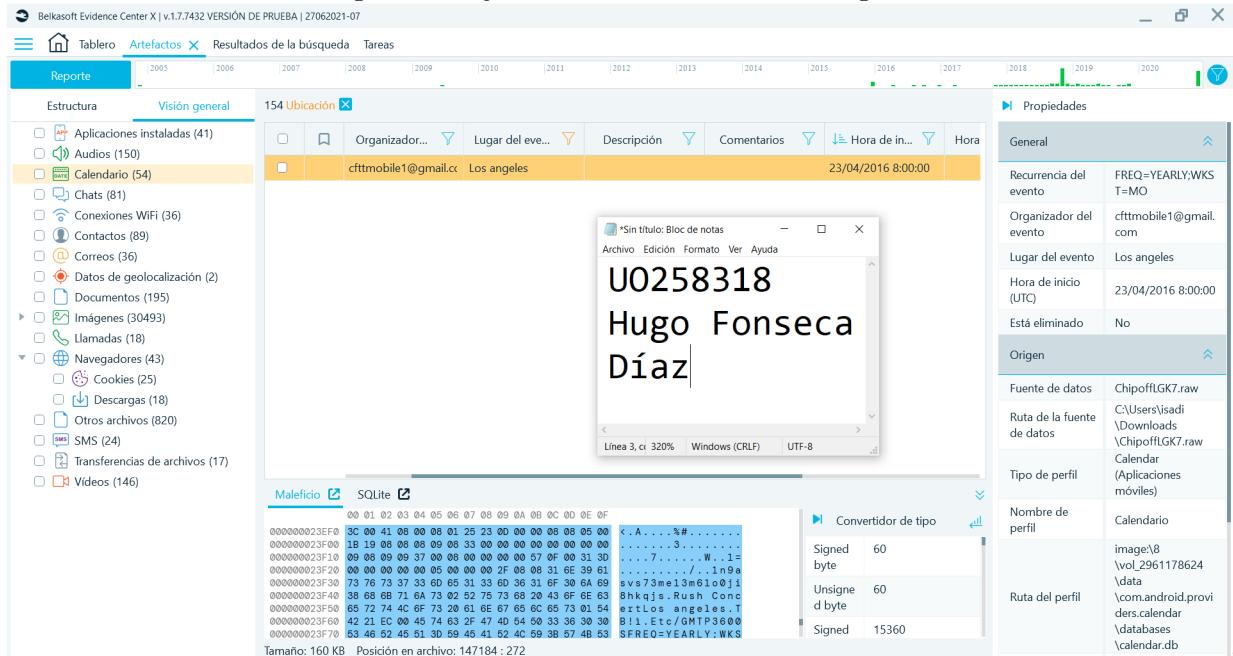
Figura 59: Ejercicio 4: Eventos de calendario



Se han identificado 54 eventos de calendario.

zz)

Figura 60: Ejercicio 4: Eventos en Los Ángeles



Solo uno se desarrolla en Los Ángeles.

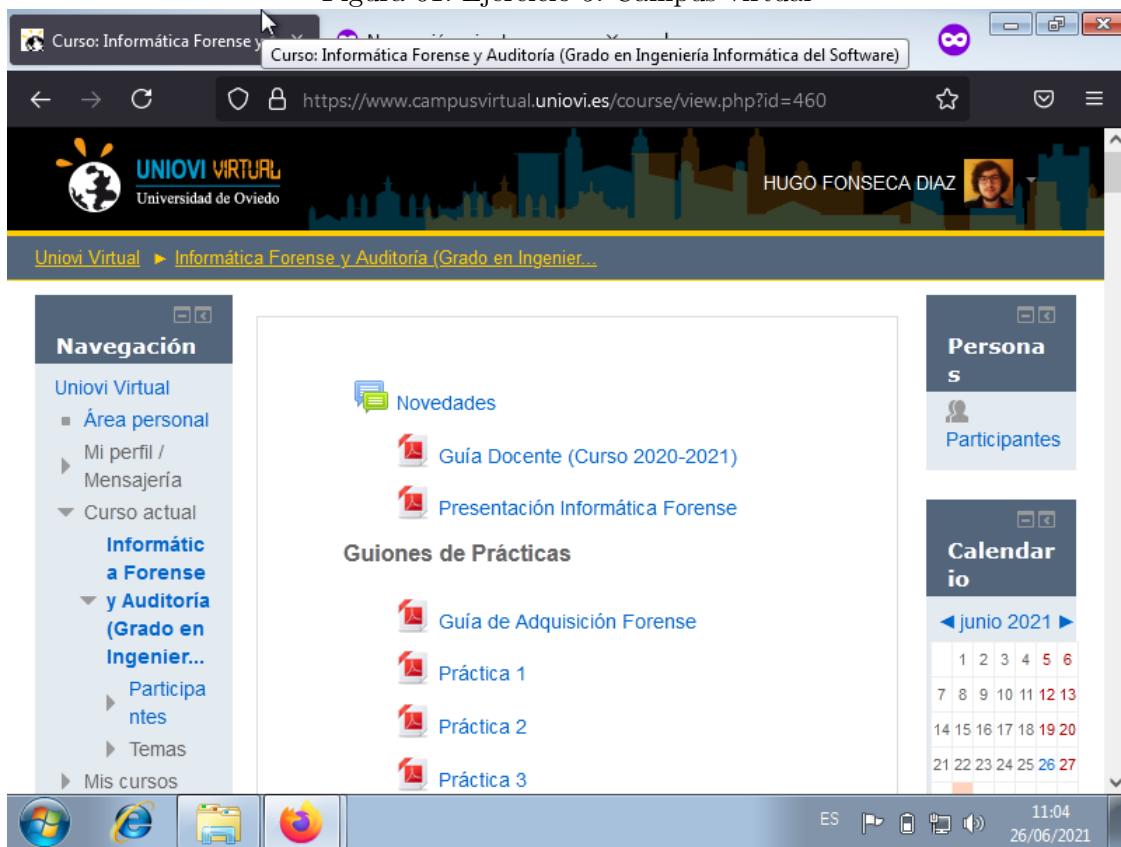
aaa) La fecha de comienzo del evento puede verse en la anterior captura, es el 2016/04/23 a las 8:00:00.

5. Práctica 05

5.1. Ejercicio 5

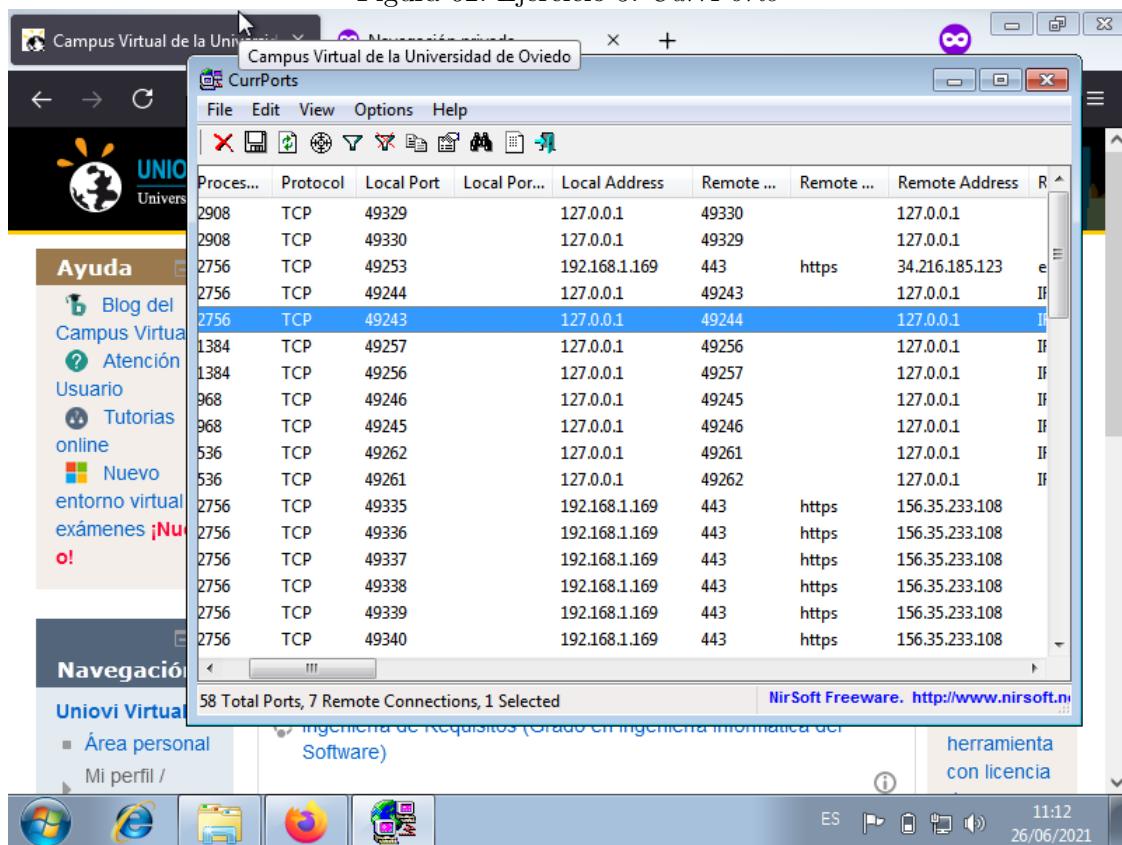
Se realiza una conexión al campus virtual con el navegador Firefox en navegación privada.

Figura 61: Ejercicio 5: Campus virtual



Se utiliza la aplicación de Nirsoft llamada *CurrPorts*.

Figura 62: Ejercicio 5: *CurrPorts*



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

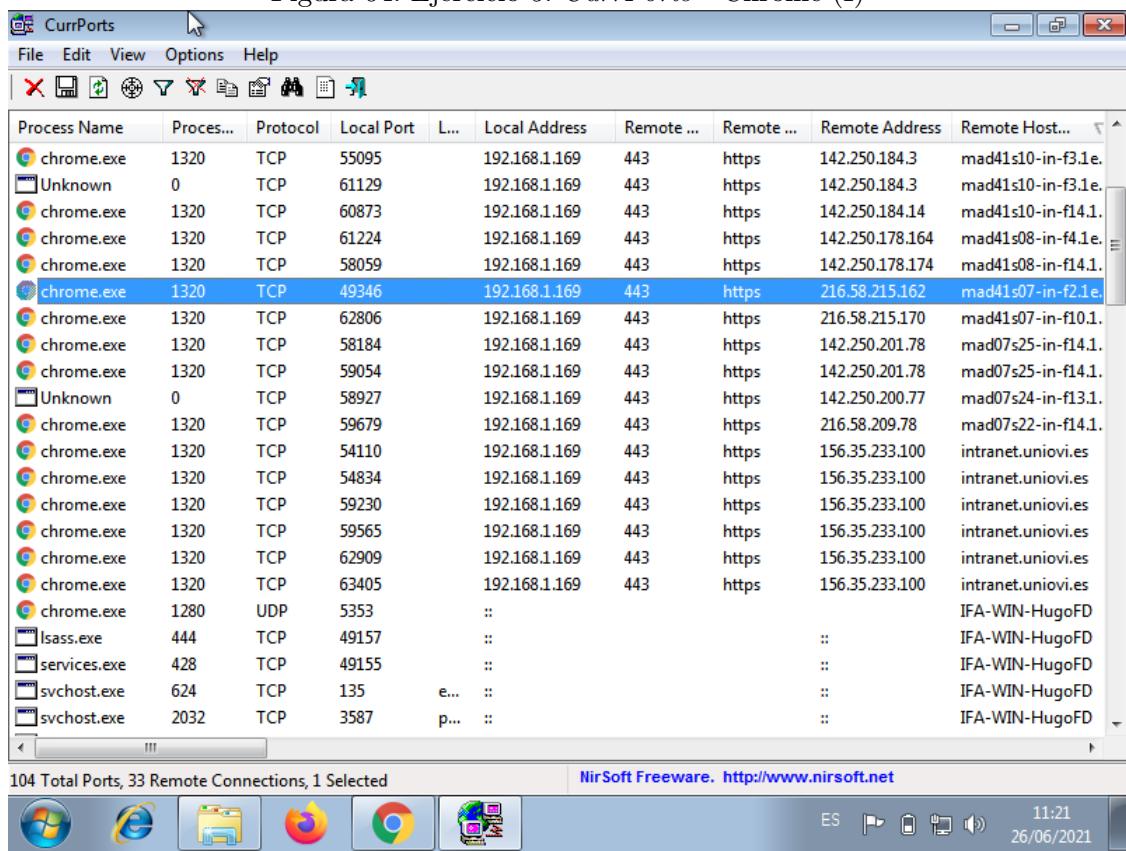
Figura 63: Ejercicio 5: *CurrPorts* - Firefox

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), lsass.exe (process ID 444), and services.exe (process ID 428). Most connections are TCP, with some UDP entries. Local ports range from 49243 down to 1900. Remote ports and addresses are mostly 127.0.0.1 or 0.0.0.0, except for one entry to 34.216.185.123. 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	ec2-34-216-185-123
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 64: Ejercicio 5: *CurrPorts* - Chrome (I)

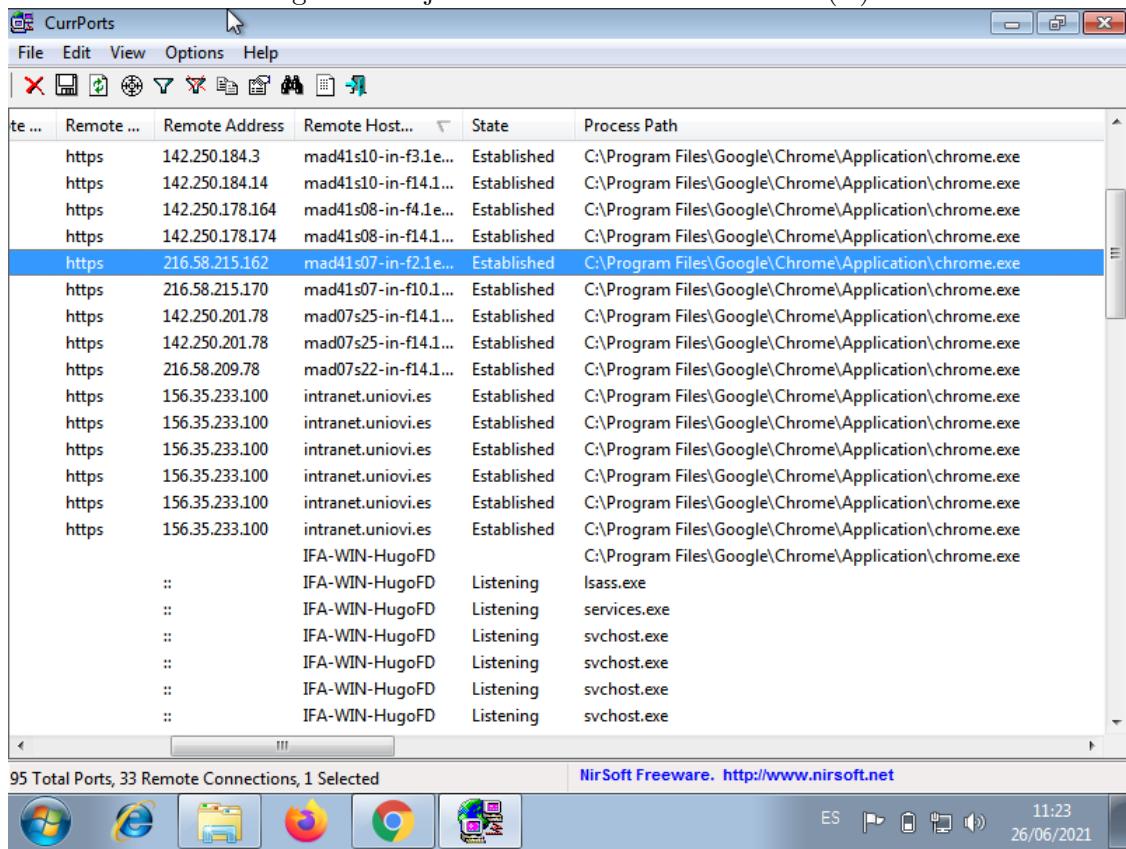


The screenshot shows the CurrPorts application interface. At the top is a menu bar with File, Edit, View, Options, and Help. Below the menu is a toolbar with various icons. The main area is a table with the following columns: Process Name, Proces..., Protocol, Local Port, L..., Local Address, Remote ..., Remote ..., Remote Address, and Remote Host... . The table contains 33 rows of data. One row, corresponding to 'chrome.exe' with a local port of 49346, is highlighted with a blue background. The data in the table is as follows:

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-f3.1e.
Unknown	0	TCP	61129		192.168.1.169	443	https	142.250.184.3	mad41s10-in-f3.1e.
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-f4.1e.
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-f2.1e.
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

At the bottom of the window, there is a status bar with the text "104 Total Ports, 33 Remote Connections, 1 Selected" and a link "NirSoft Freeware. http://www.nirsoft.net". Below the status bar is a taskbar with several icons, including the Windows logo, Internet Explorer, File Explorer, Mozilla Firefox, Google Chrome, and a system tray icon. The system tray also shows the date and time as "11:21 26/06/2021".

Figura 65: Ejercicio 5: *CurrPorts* - Chrome (II)



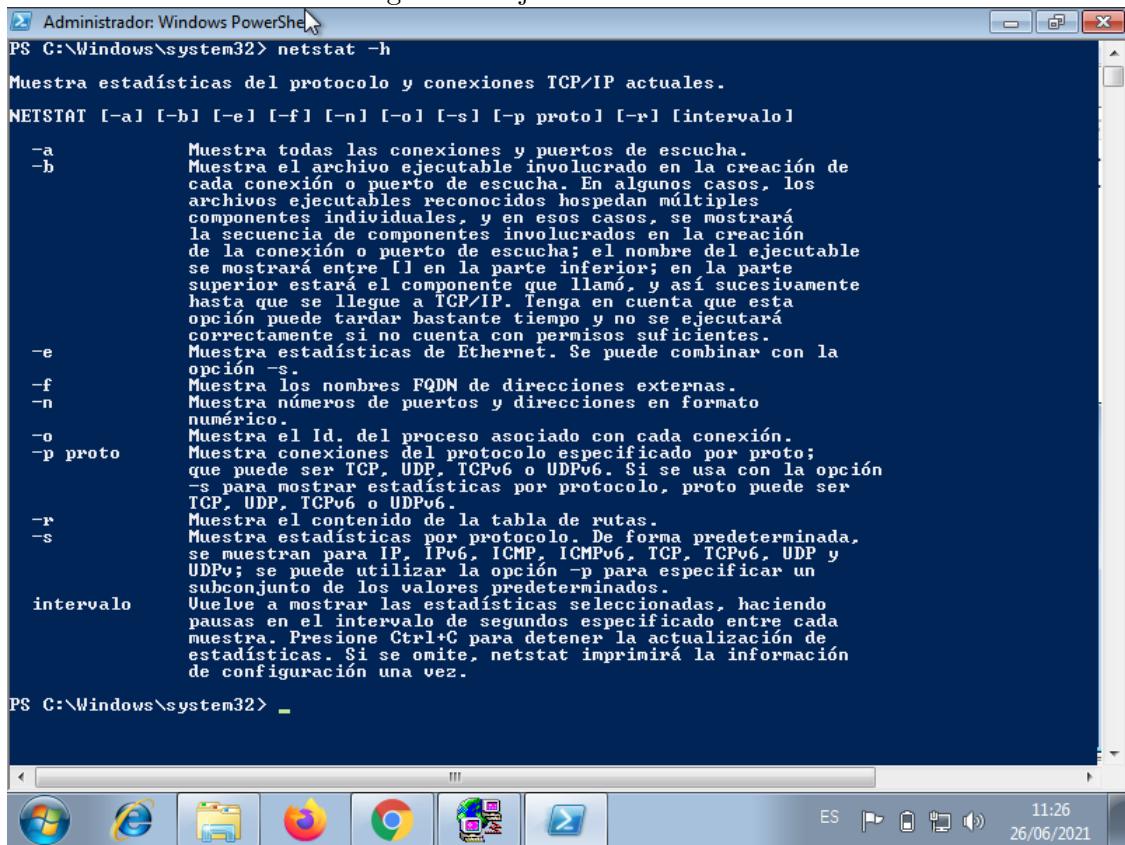
The screenshot shows the CurrPorts application interface. The main window displays a table of network connections. The columns are labeled: Local Port, Remote Port, Remote Address, Remote Host..., State, and Process Path. The table lists numerous https connections from various IP addresses (e.g., 142.250.184.3, 216.58.215.162) to ports 4100-4107, all established and associated with chrome.exe. Below this, several listening ports are listed for services.exe and svchost.exe. At the bottom of the application window, status information shows 95 Total Ports, 33 Remote Connections, and 1 Selected. The application is identified as NirSoft Freeware with a link to http://www.nirsoft.net.

Local Port	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-f1.1e...	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
	:	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 66: 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]

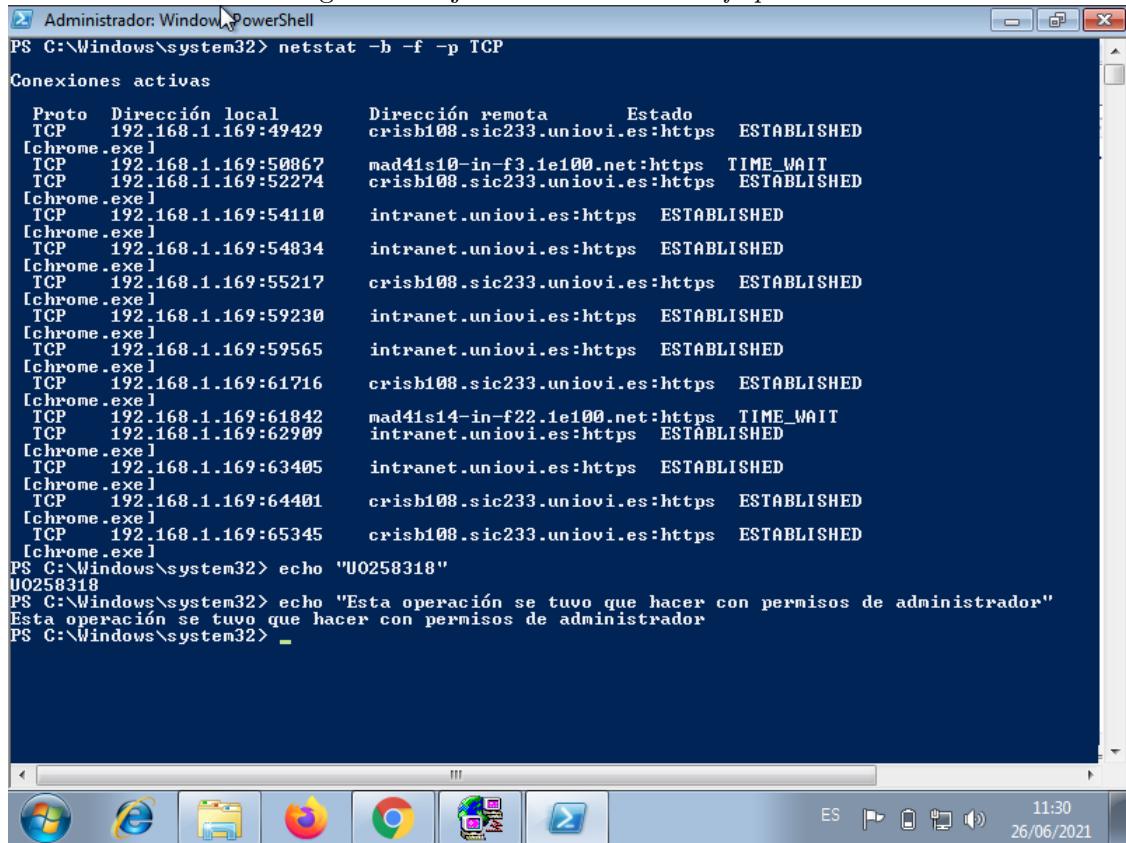
-a      Muestra todas las conexiones y puertos de escucha.
-b      Muestra el archivo ejecutable involucrado en la creación de
       cada conexión o puerto de escucha. En algunos casos, los
       archivos ejecutables reconocidos hospedan múltiples
       componentes individuales, y en esos casos, se 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 (shows all connections and listening ports), -b (shows the executable involved in connection creation), -e (Ethernet statistics), -f (FQDN of external addresses), -n (numerical port and address), -o (process ID associated with each connection), -p (specifies protocol: TCP, UDP, TCPv6, UDPv6), -r (route table content), -s (statistics by protocol: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, UDPv6), and -intervalo (repeated statistics with specified interval). The PowerShell window has a blue title bar and a dark blue background. Below the window is the Windows taskbar with icons for Start, Internet Explorer, File Explorer, Firefox, Google Chrome, and Task View. The system tray shows the date (26/06/2021) and time (11:26).

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 67: Ejercicio 5: `netstat -b -f -p TCP`



```
PS C:\Windows\system32> netstat -b -f -p TCP
Conexiones activas

  Proto  Dirección local          Dirección remota        Estado
  [chrome.exe]  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
  [chrome.exe]  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
  [chrome.exe]  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>
```

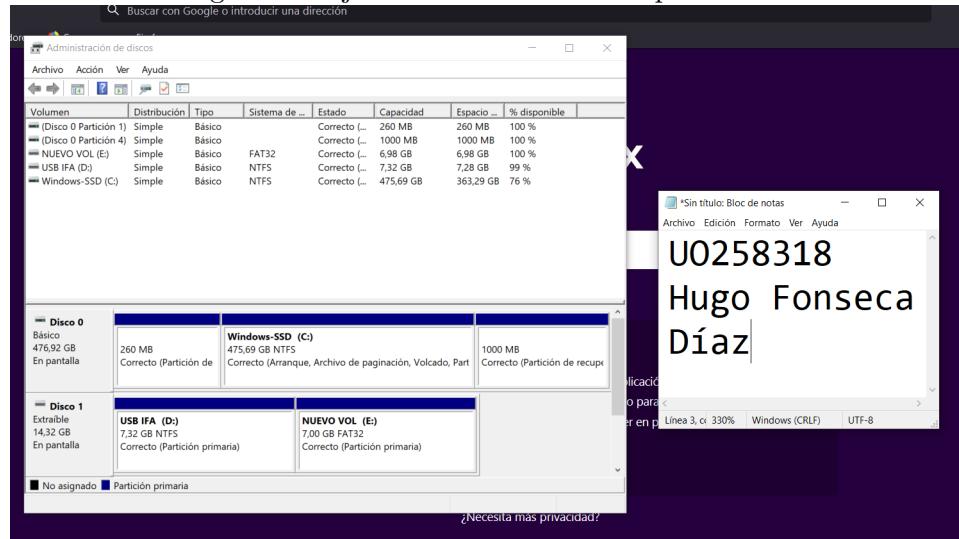
La operación debe realizarse con permisos de administrador.

5.2. Ejercicio 25

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.

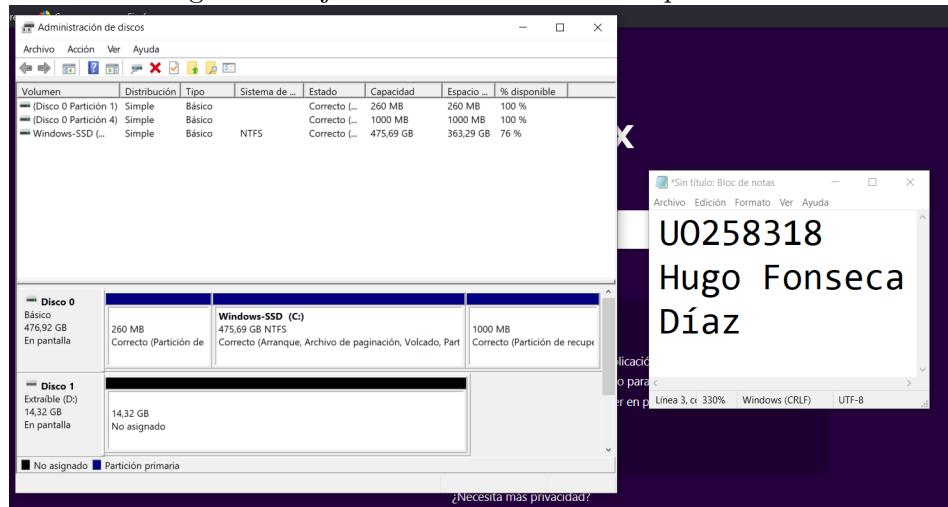
Lo primero que se va a hacer es formatear un USB con el sistema de archivos NTFS y posteriormente se van a crear dos particiones, una en NTFS y otra en FAT32.

Figura 68: Ejercicio 25: USB con las particiones



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

Figura 69: 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 70: Ejercicio 25: Fallo al instalar los drivers de los puertos de USB 3.0

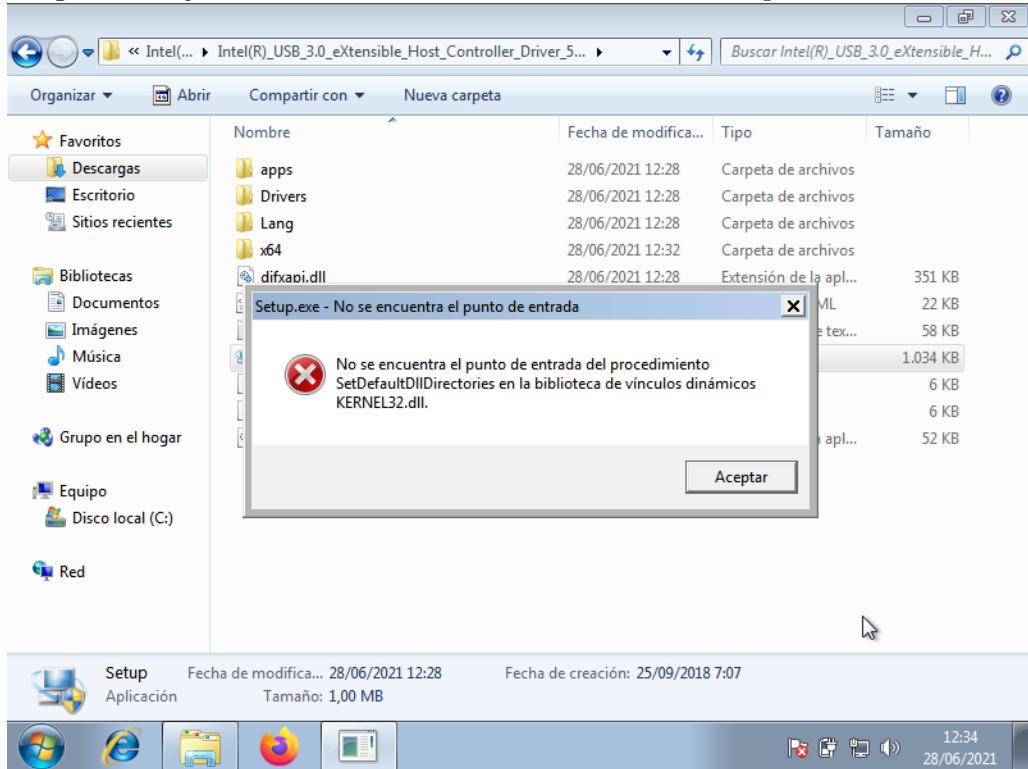
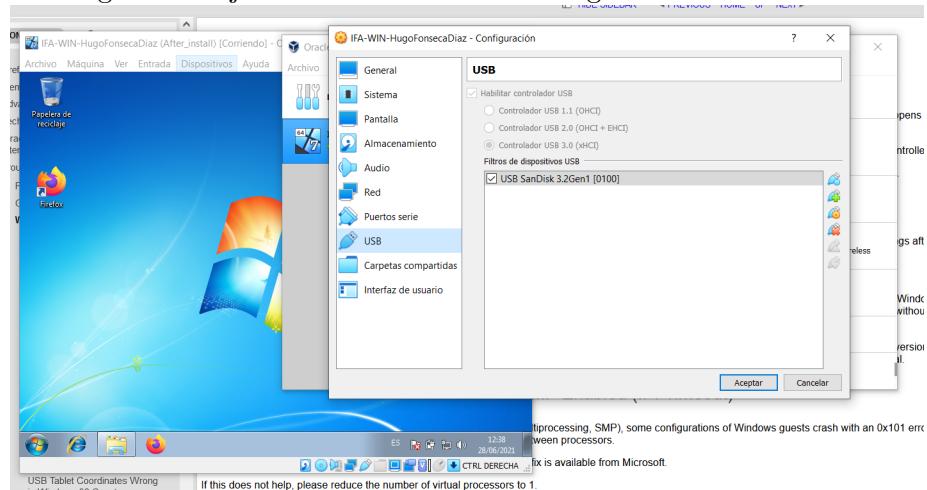
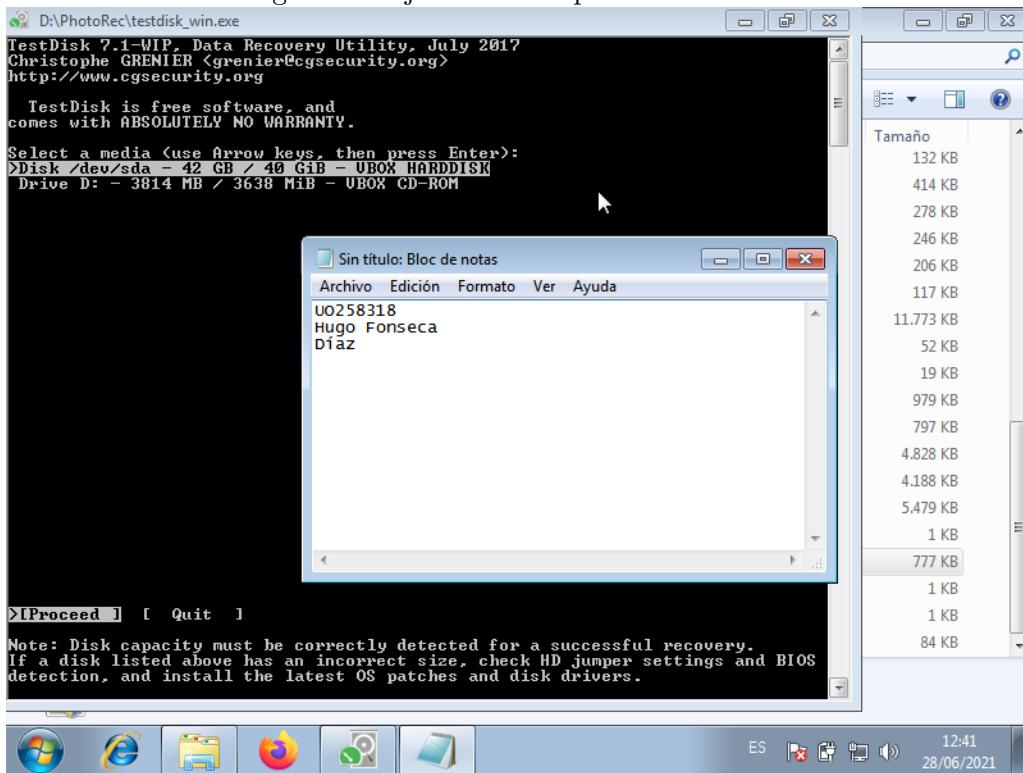


Figura 71: Ejercicio 25: Filtro USB configurado correctamente



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

Figura 72: 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

TBD