

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
4. Práctica 04	35
5. Práctica 05	35

1. Introducción

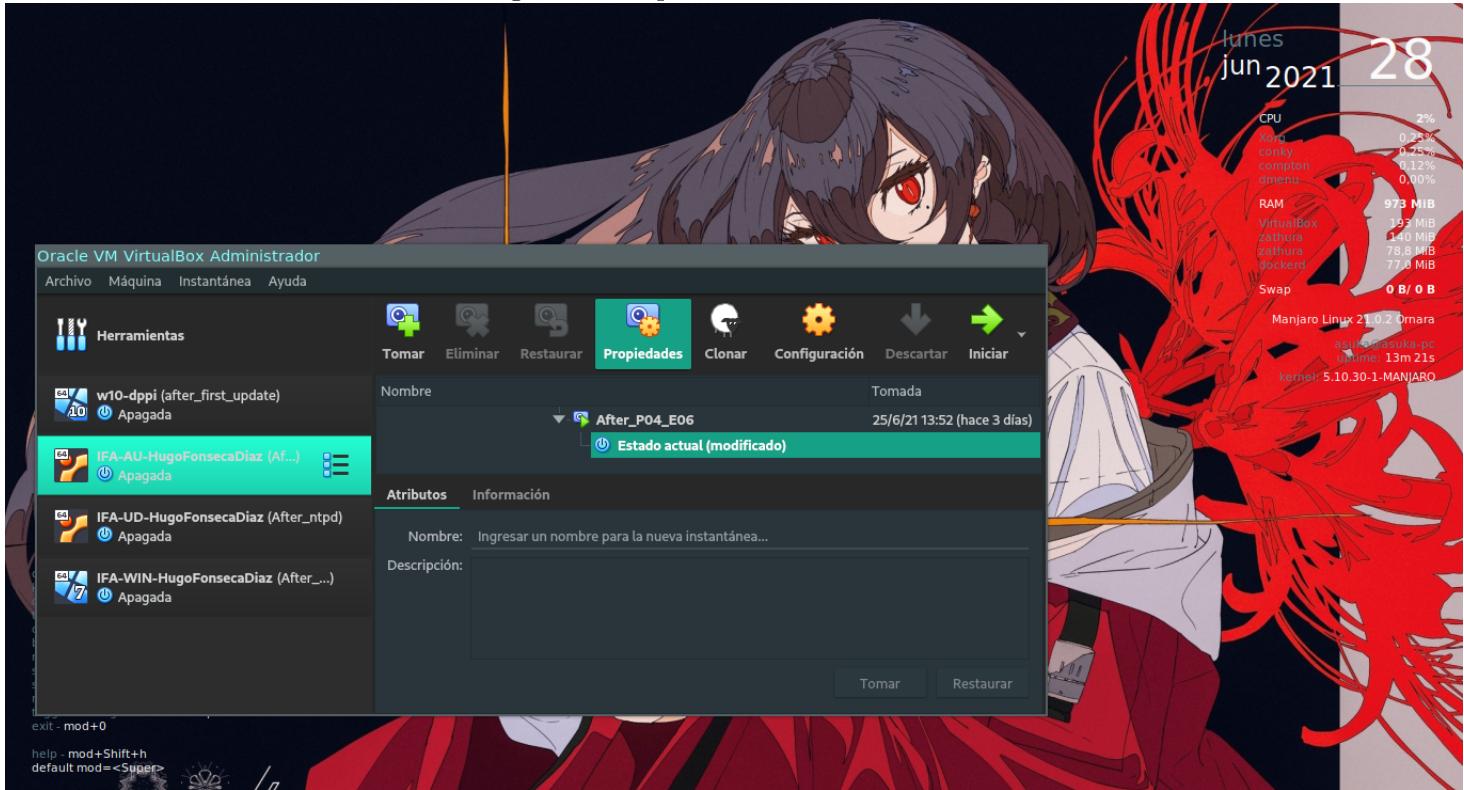
Los ejercicios de este documento se han realizado en una máquina cuyas características se muestran en la siguiente captura.

Figura 1: Sistema del alumno Hugo Fonseca Díaz.



Las máquinas virtuales utilizadas pueden verse en la siguiente imagen.

Figura 2: Máquinas virtuales.

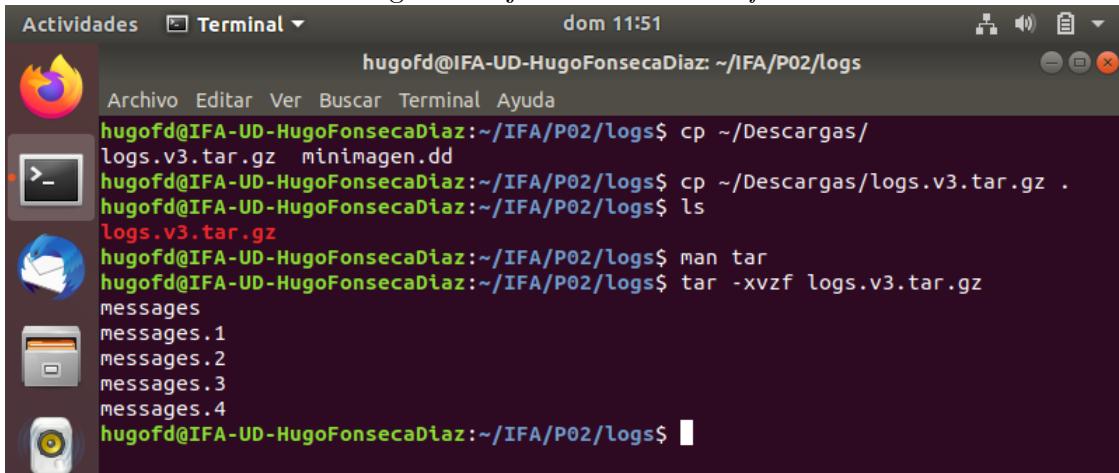


2. Práctica 02

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*.

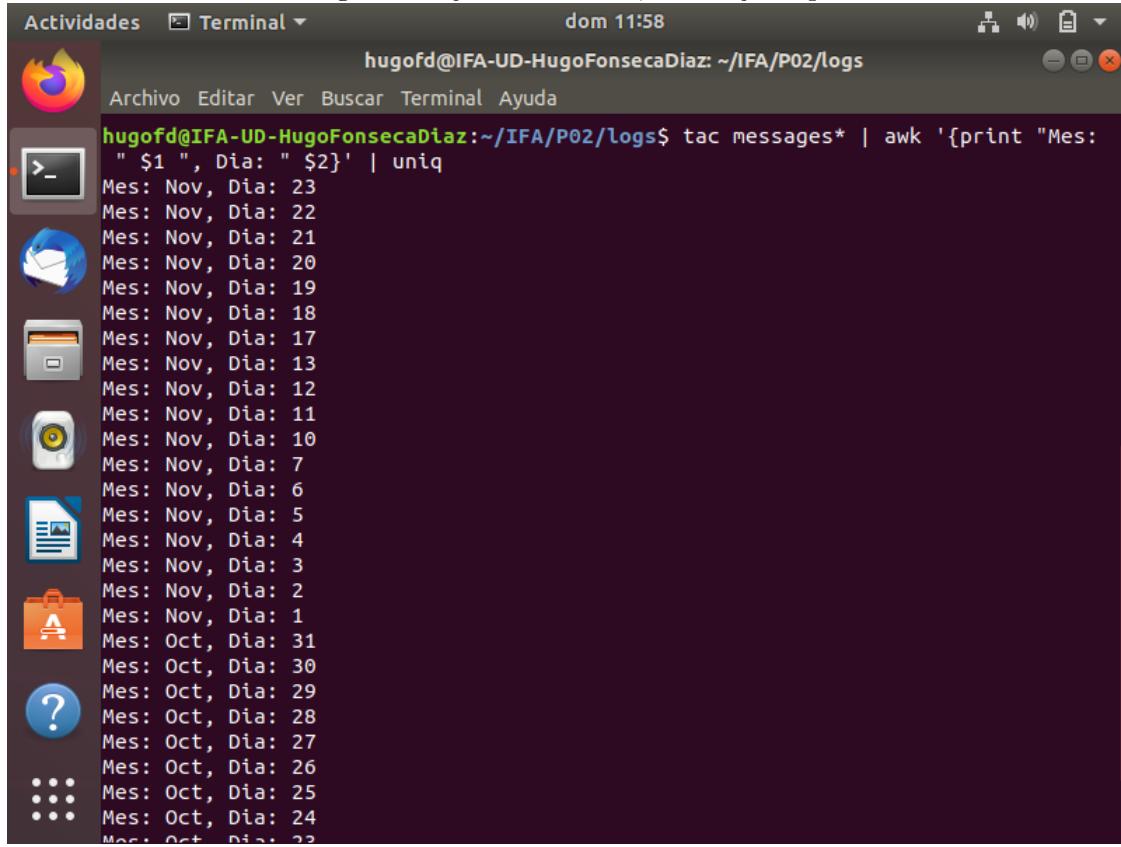


The screenshot shows a terminal window titled "Terminal" running on a Linux desktop. The terminal window has a dark background and contains the following text:

```
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

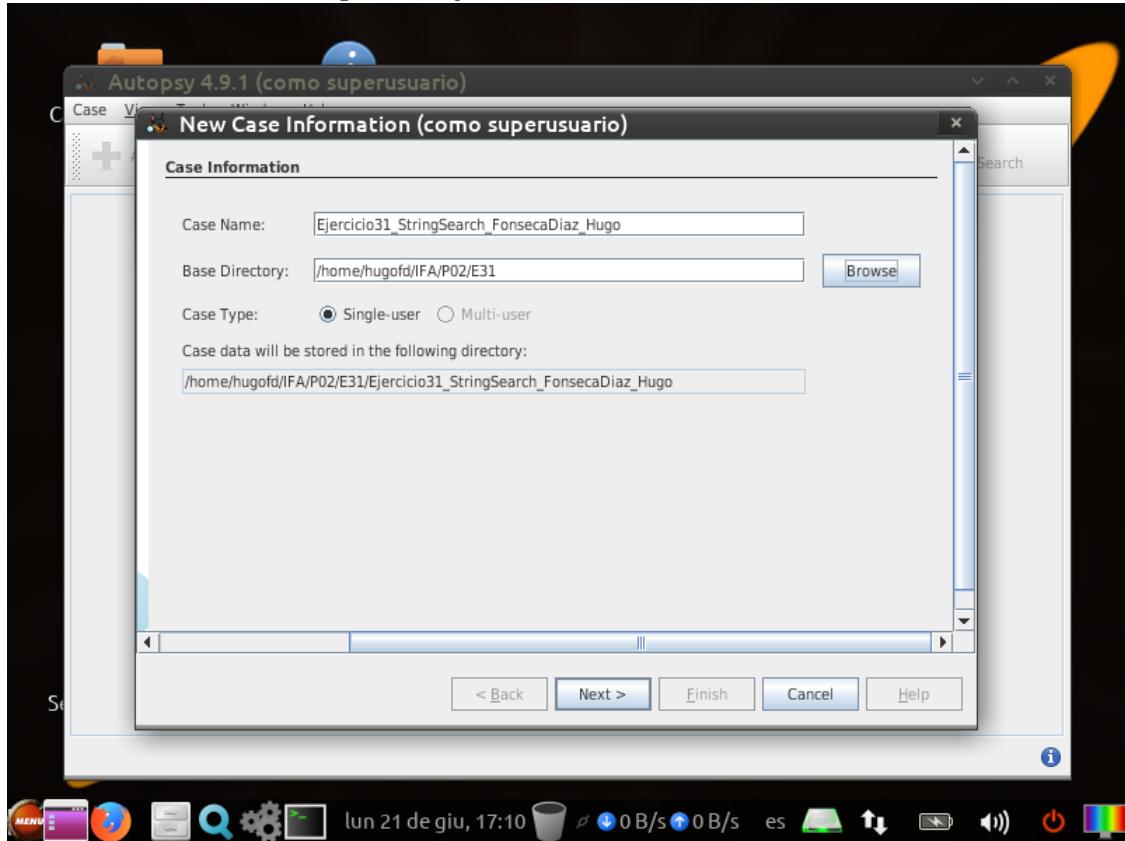
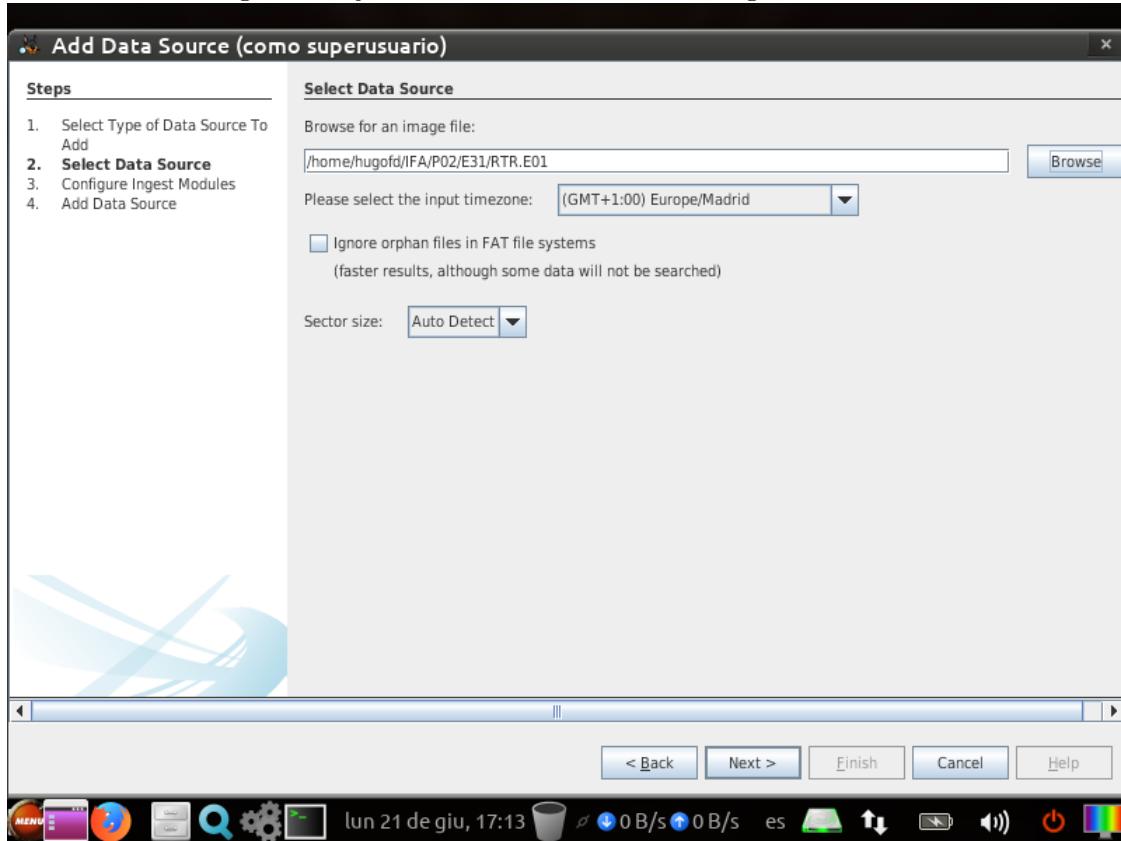


Figura 6: Ejercicio 31: Selección de la imagen a analizar



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

Figura 7: Ejercicio 31: Palabras clave

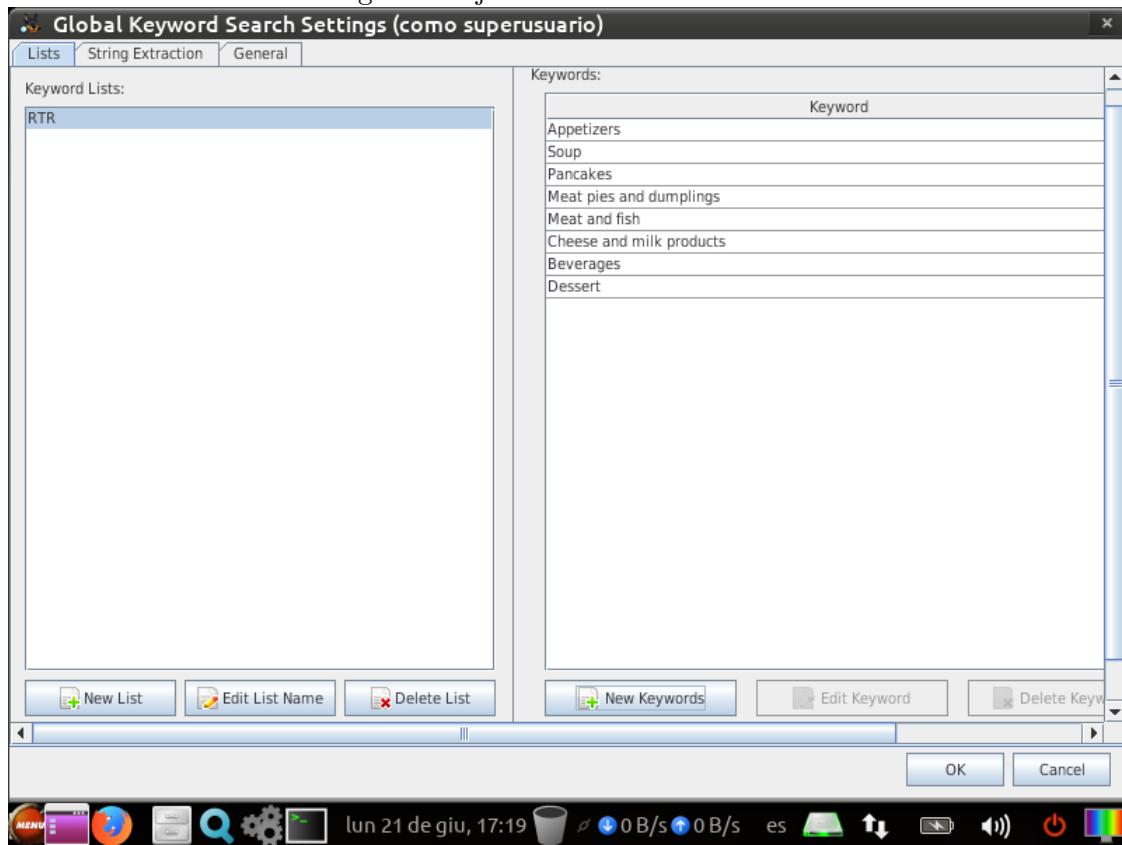


Figura 8: Ejercicio 31: Módulos seleccionados

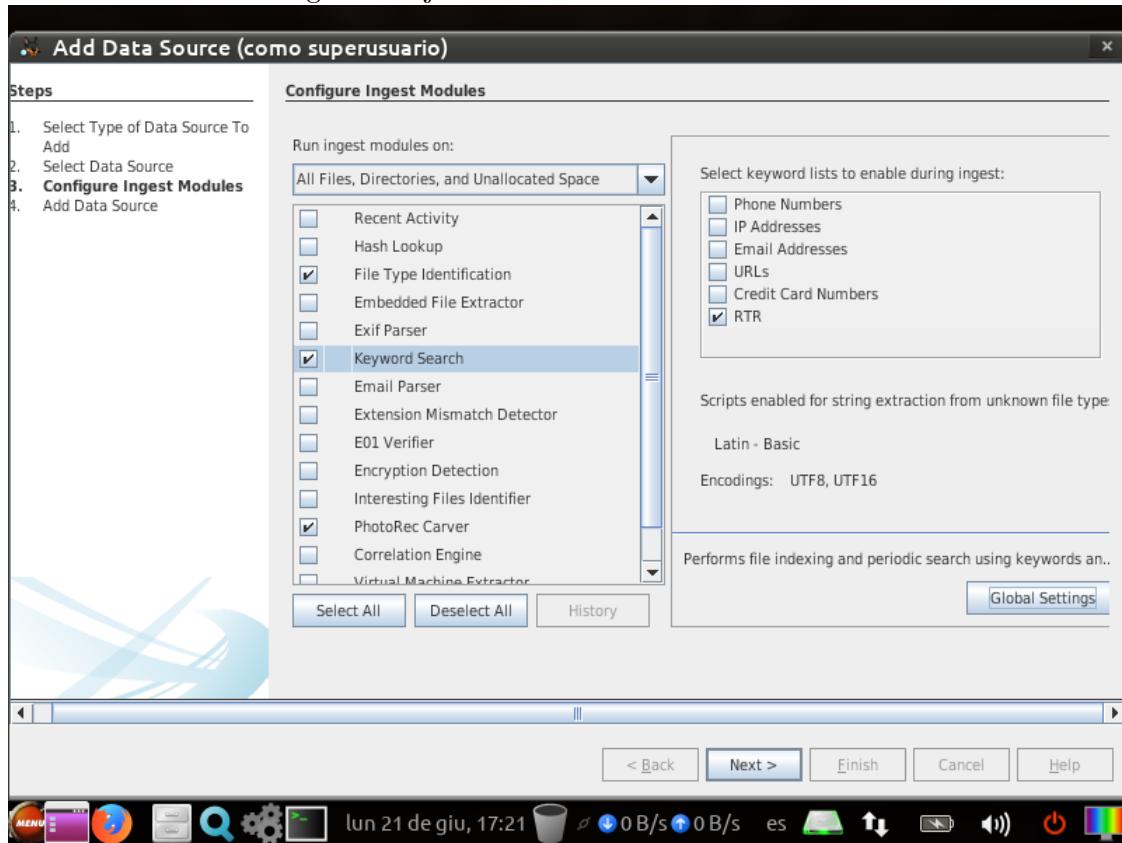
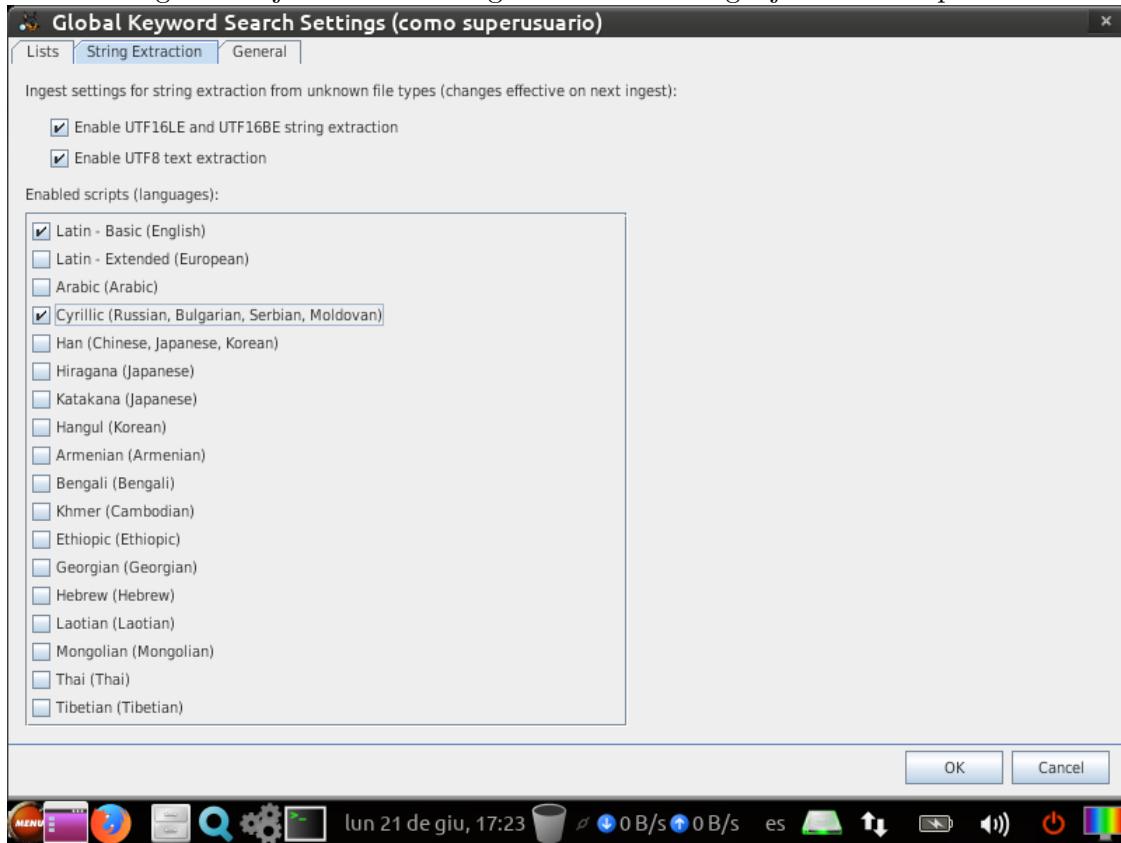
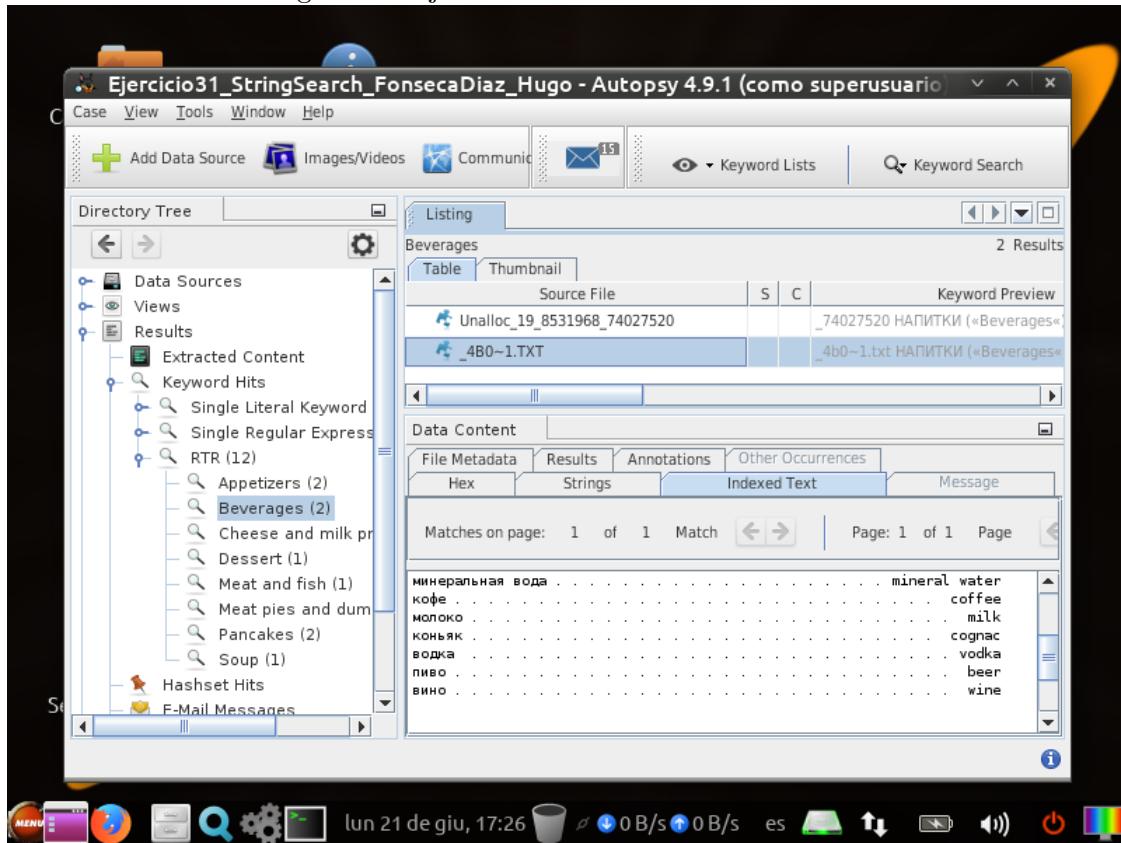


Figura 9: Ejercicio 31: Configuración de los lenguajes de la búsqueda



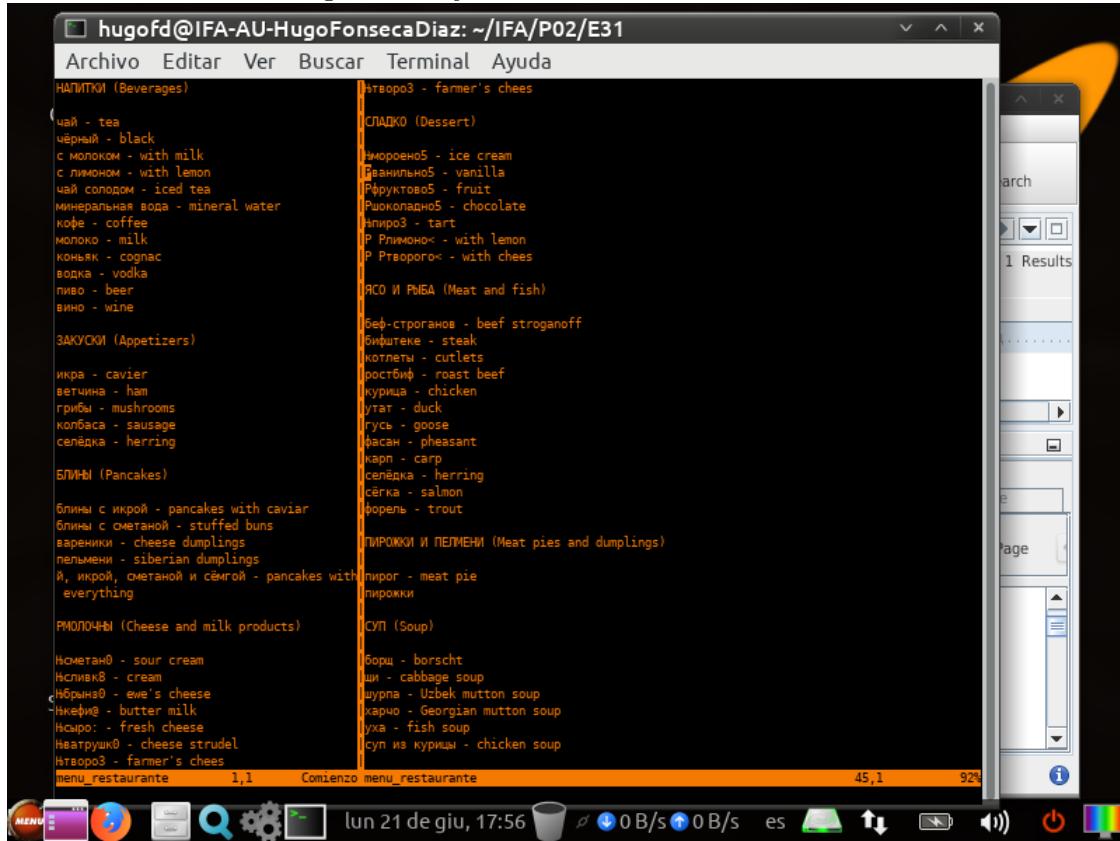
Una vez finalizado el análisis, se pueden observar los ficheros encontrados.

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

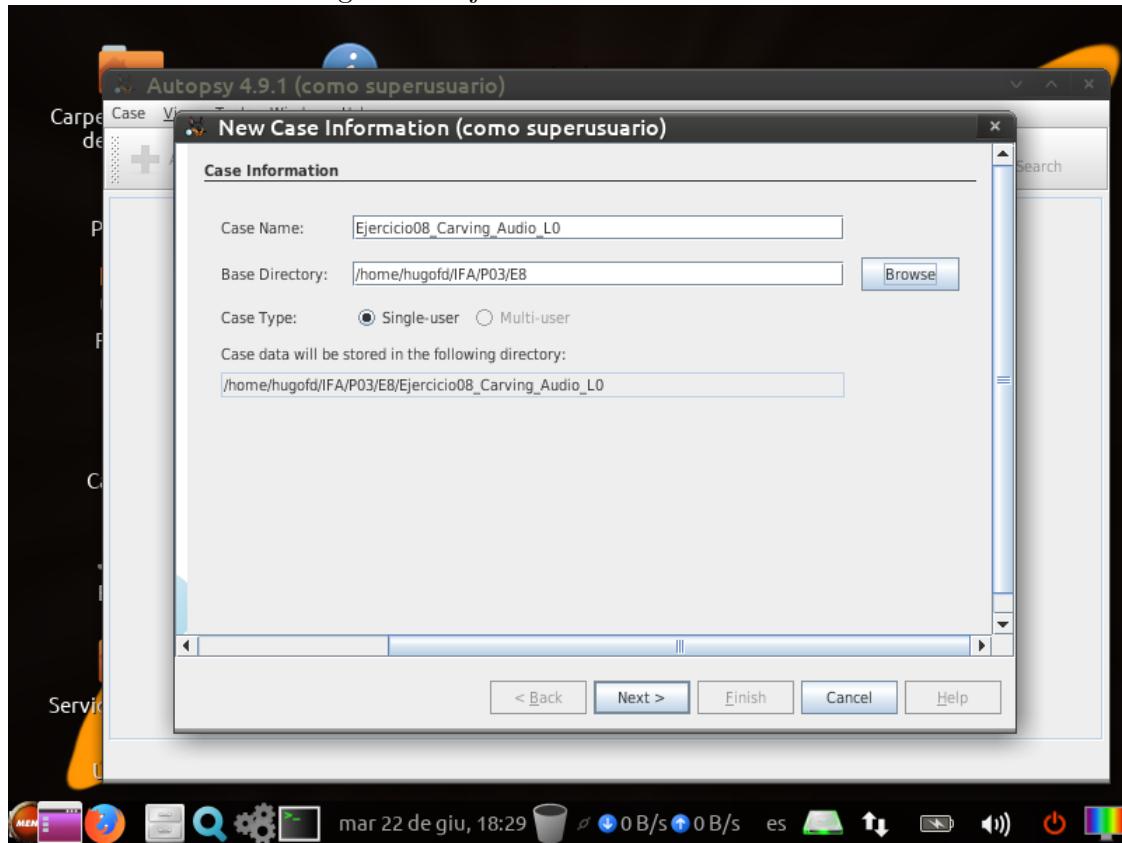
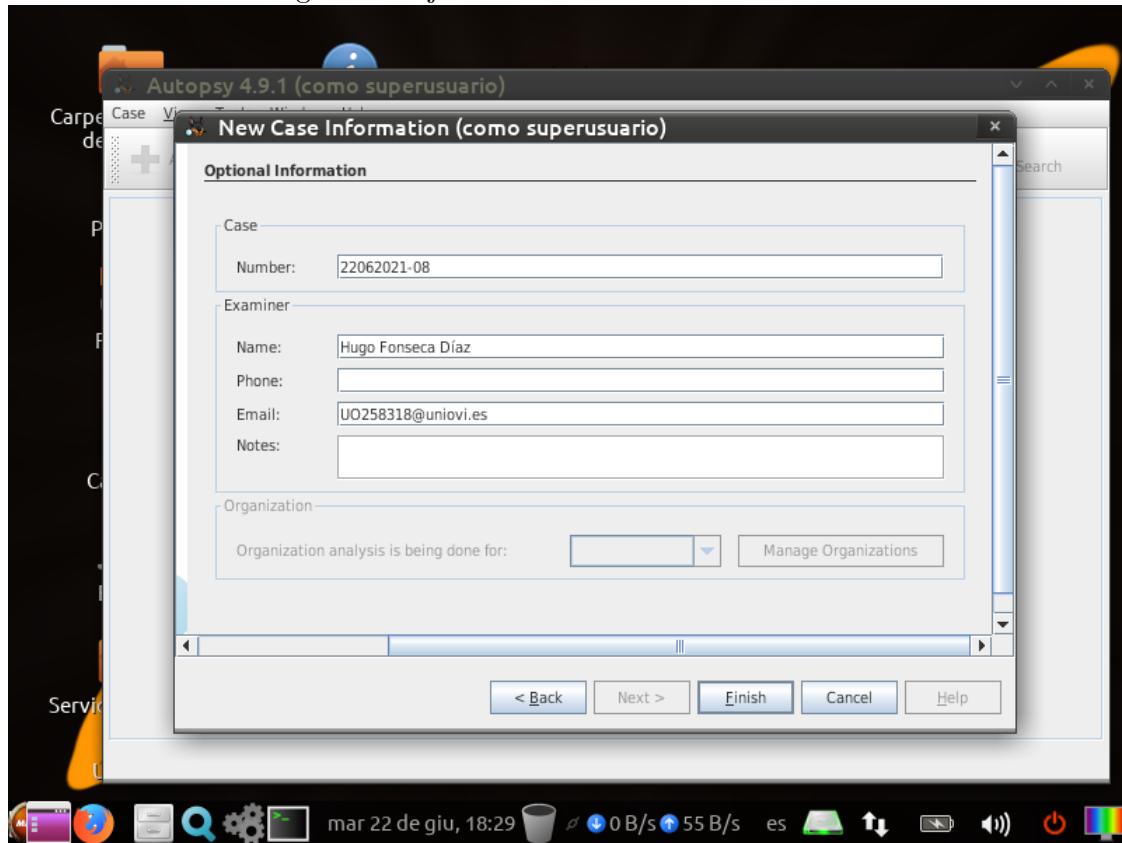
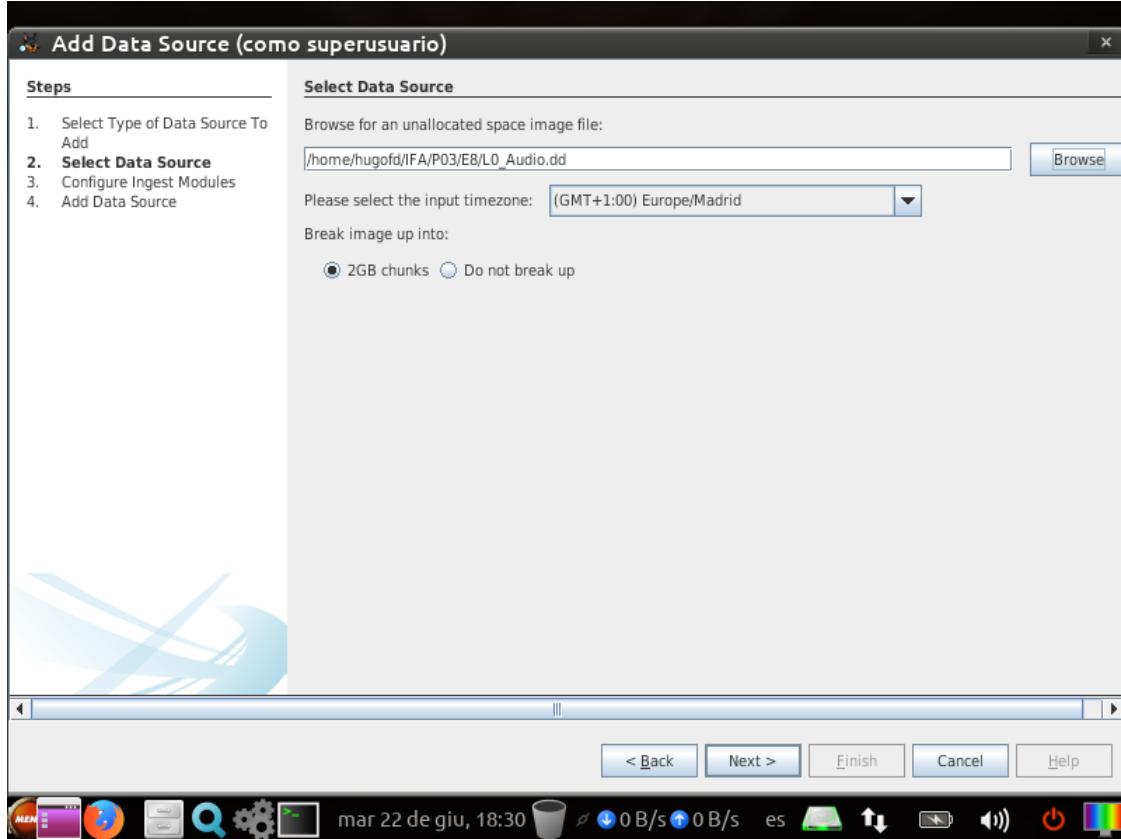


Figura 13: Ejercicio 8: Detalles del examinador



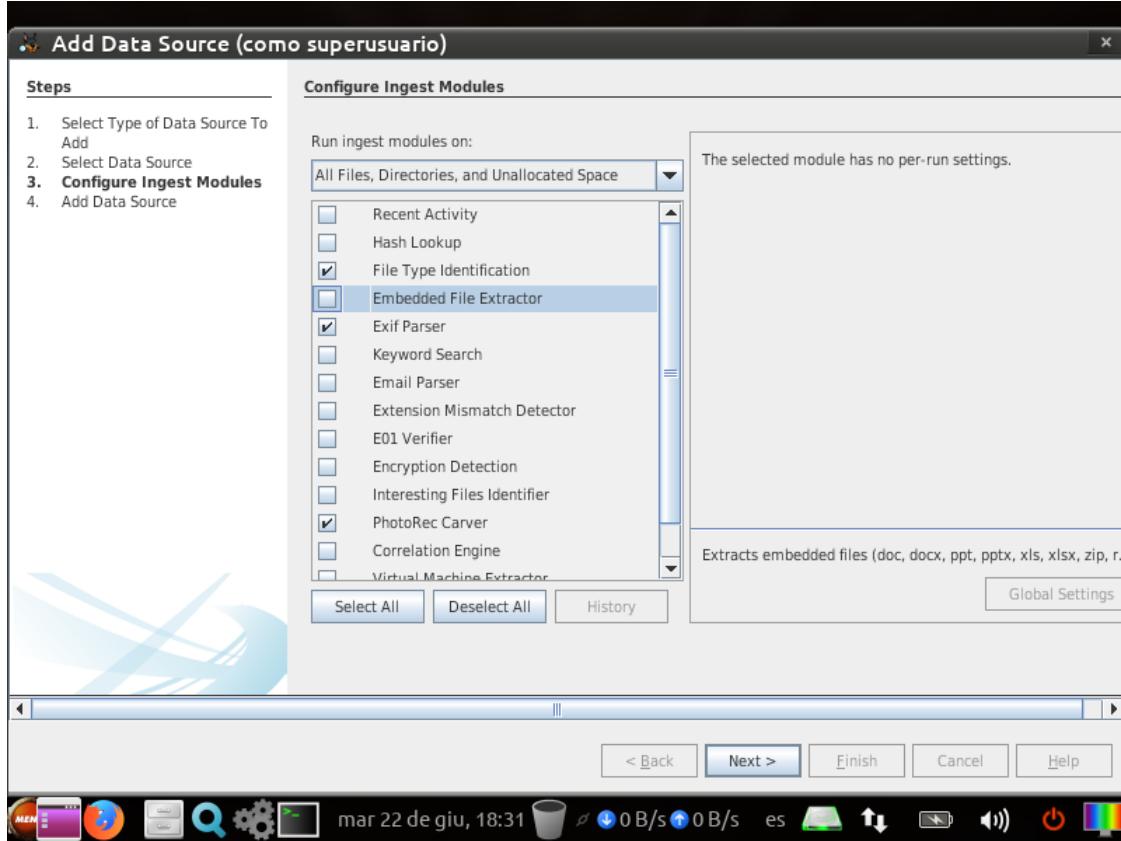
Añadimos la imagen a analizar.

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

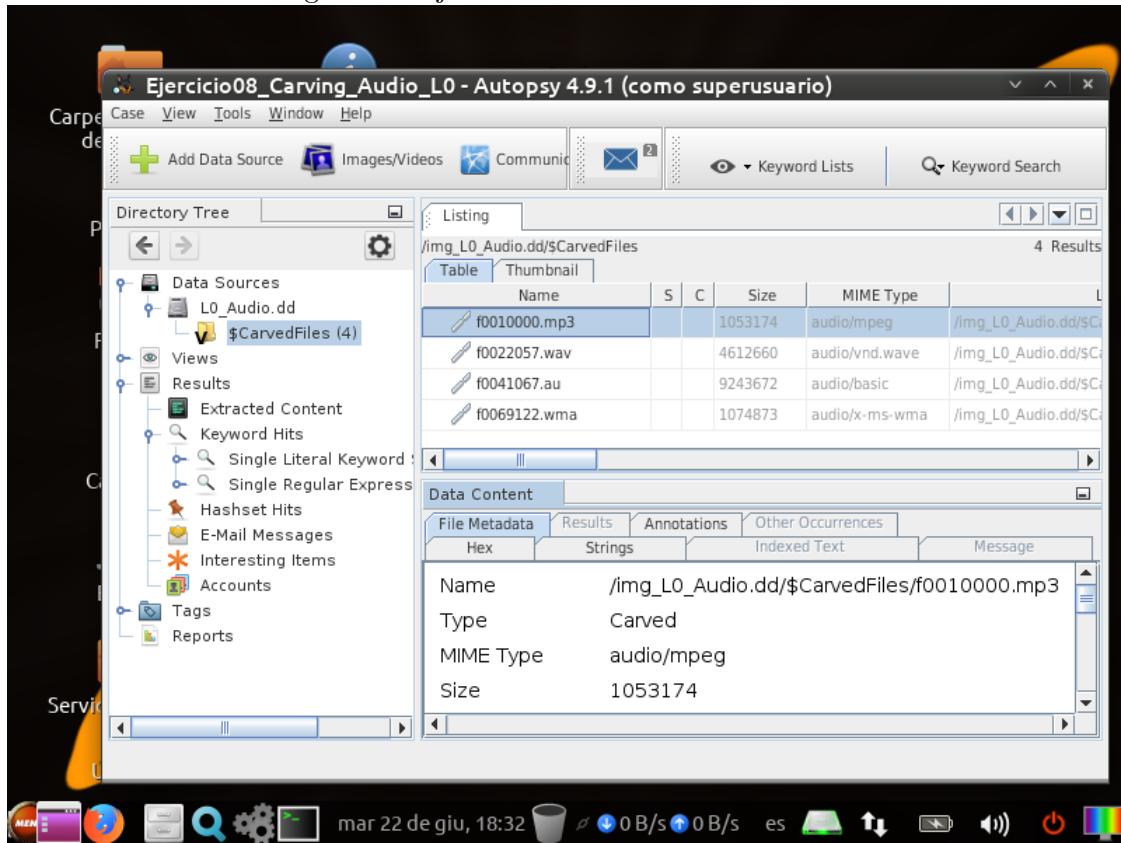
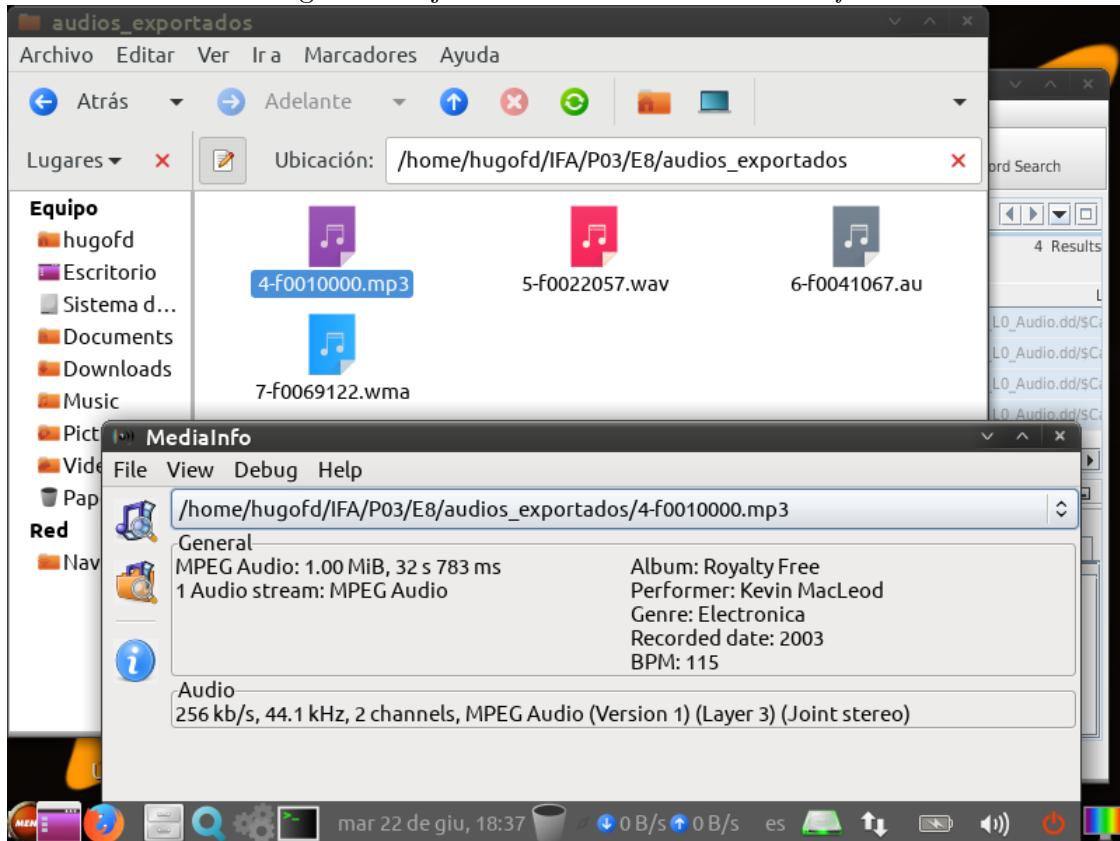


Figura 17: Ejercicio 8: Herramienta *MediaInfo*



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

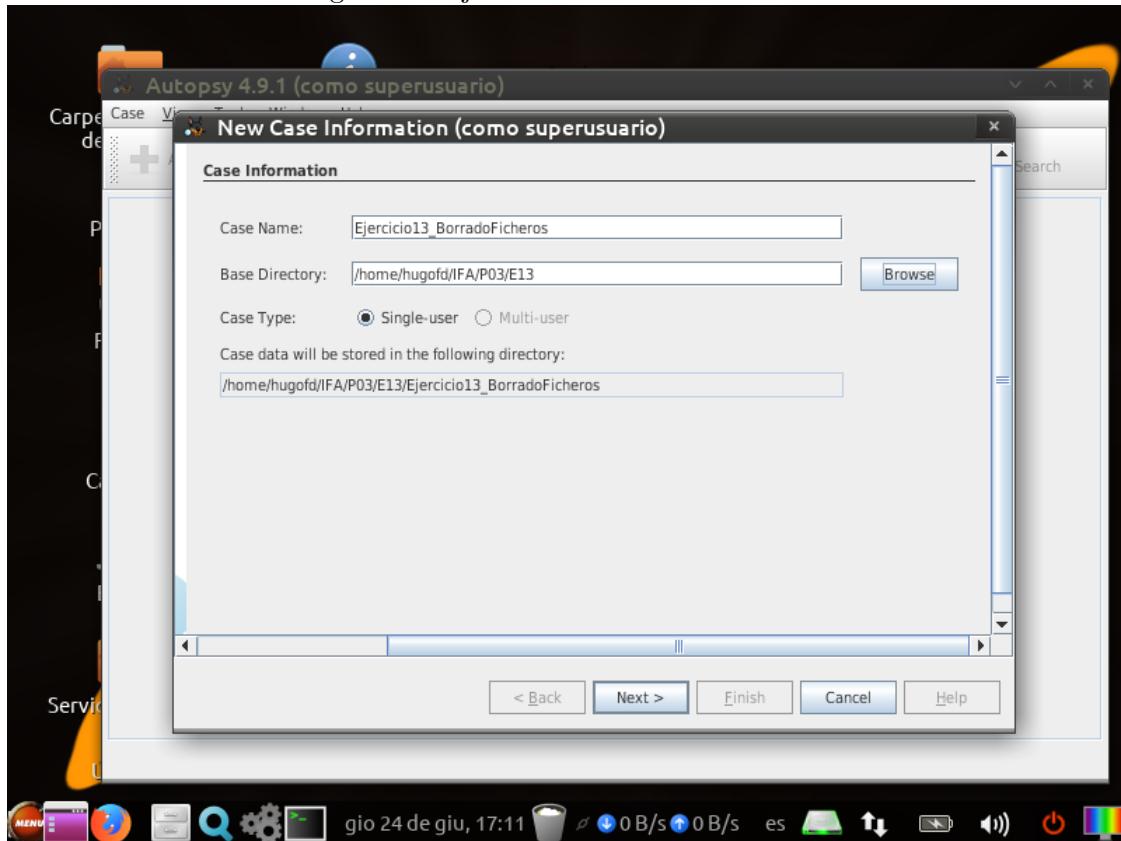
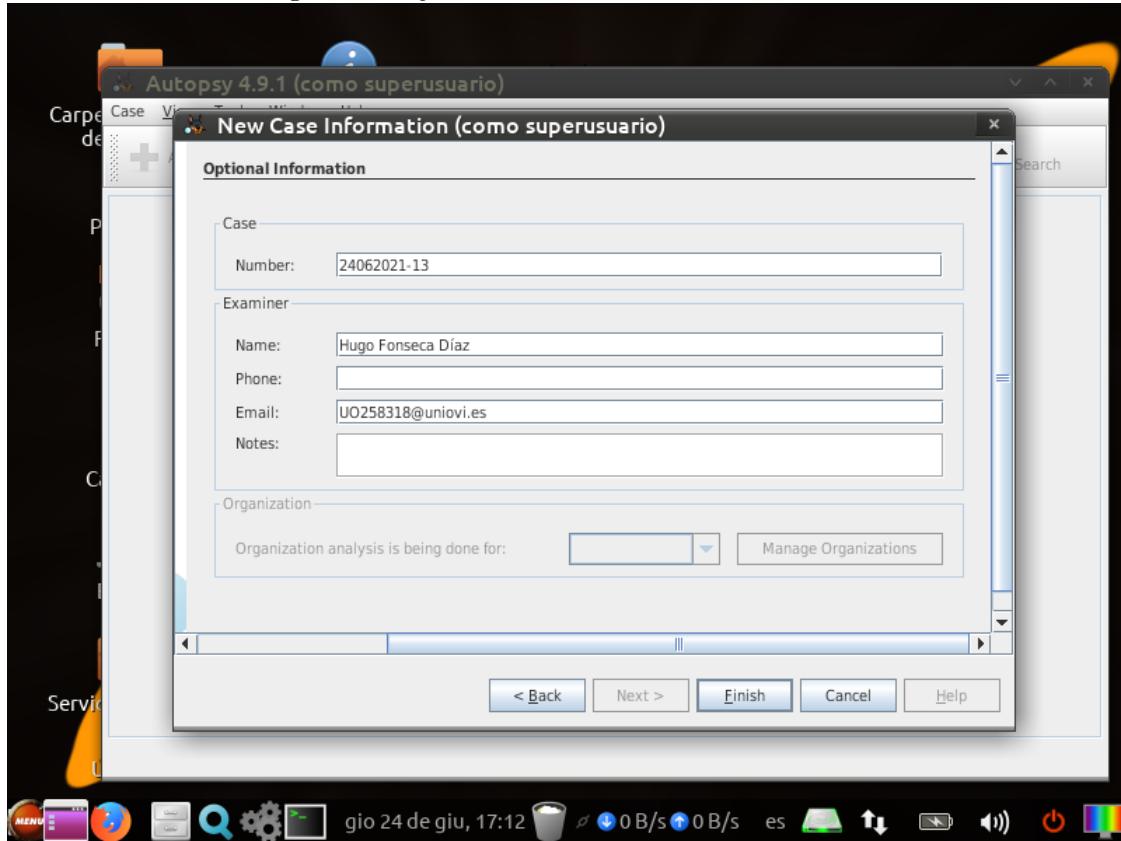
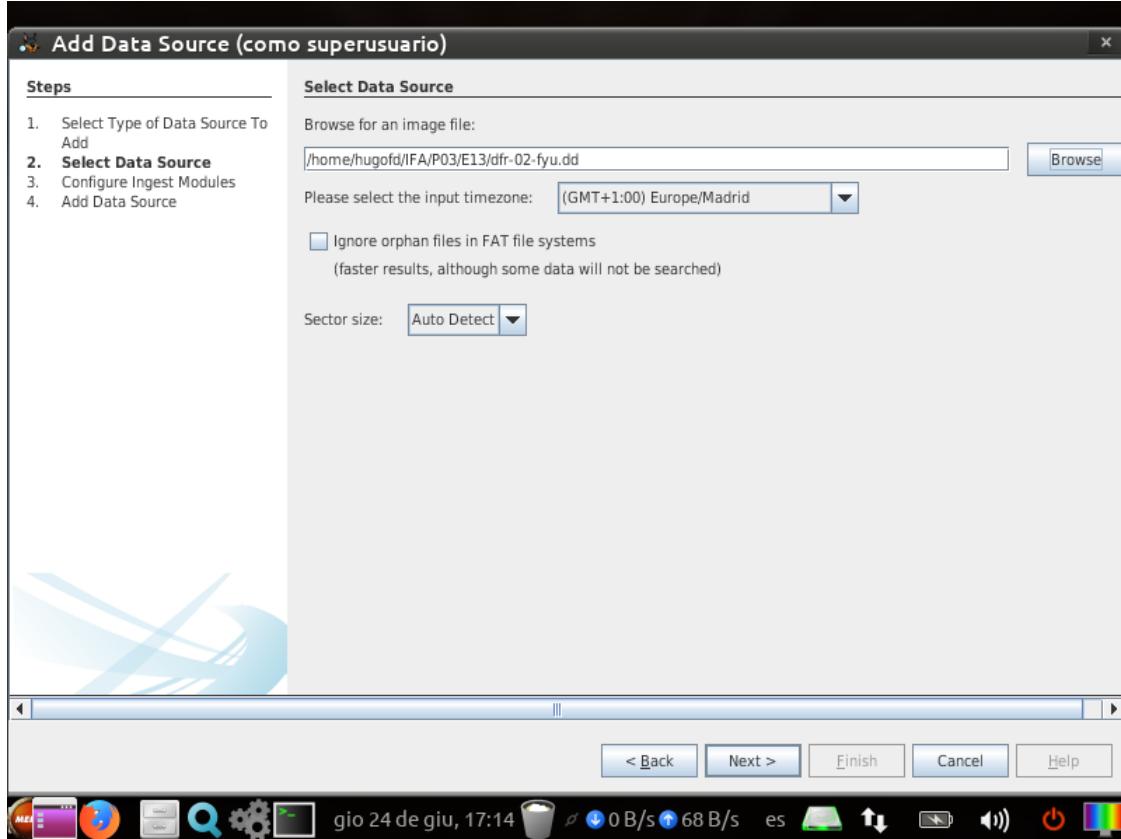


Figura 19: Ejercicio 13: Detalles del examinador



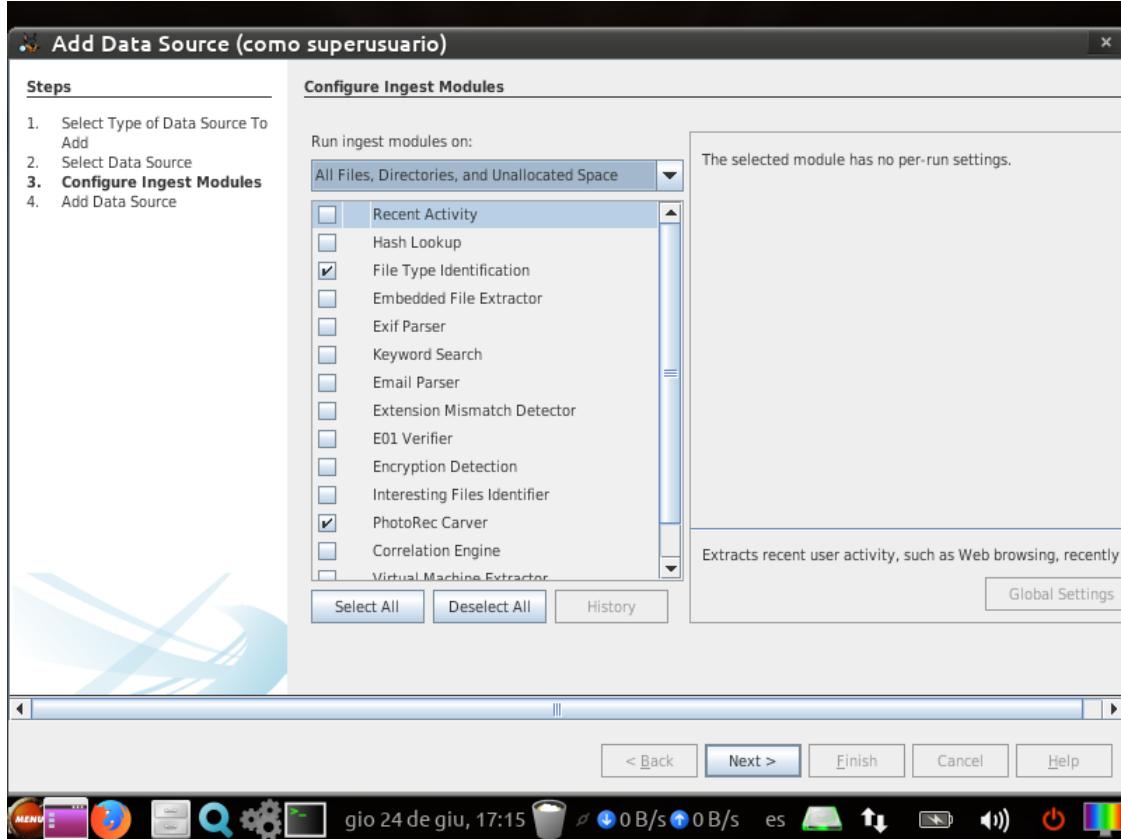
Añadimos la imagen a analizar.

Figura 20: Ejercicio 13: Selección de la imagen



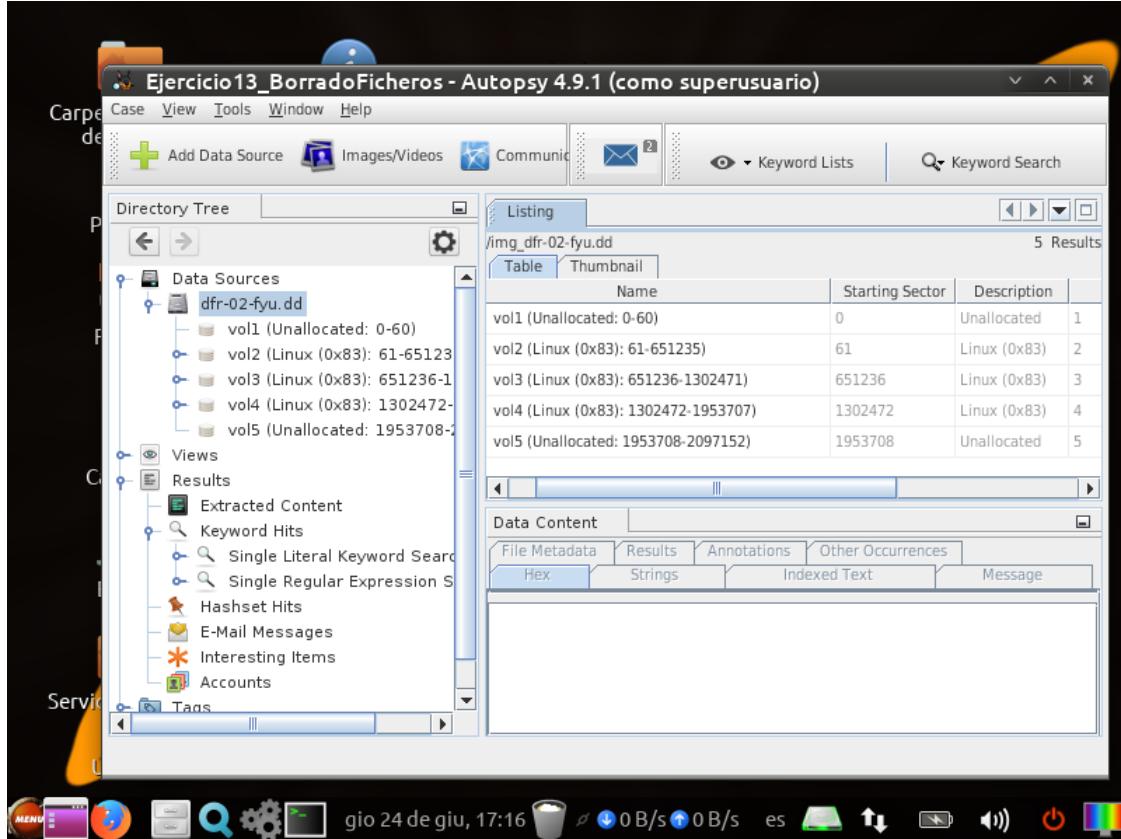
Se seleccionan los módulos de identificación de tipos de fichero y *PhotoRec Carver*.

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

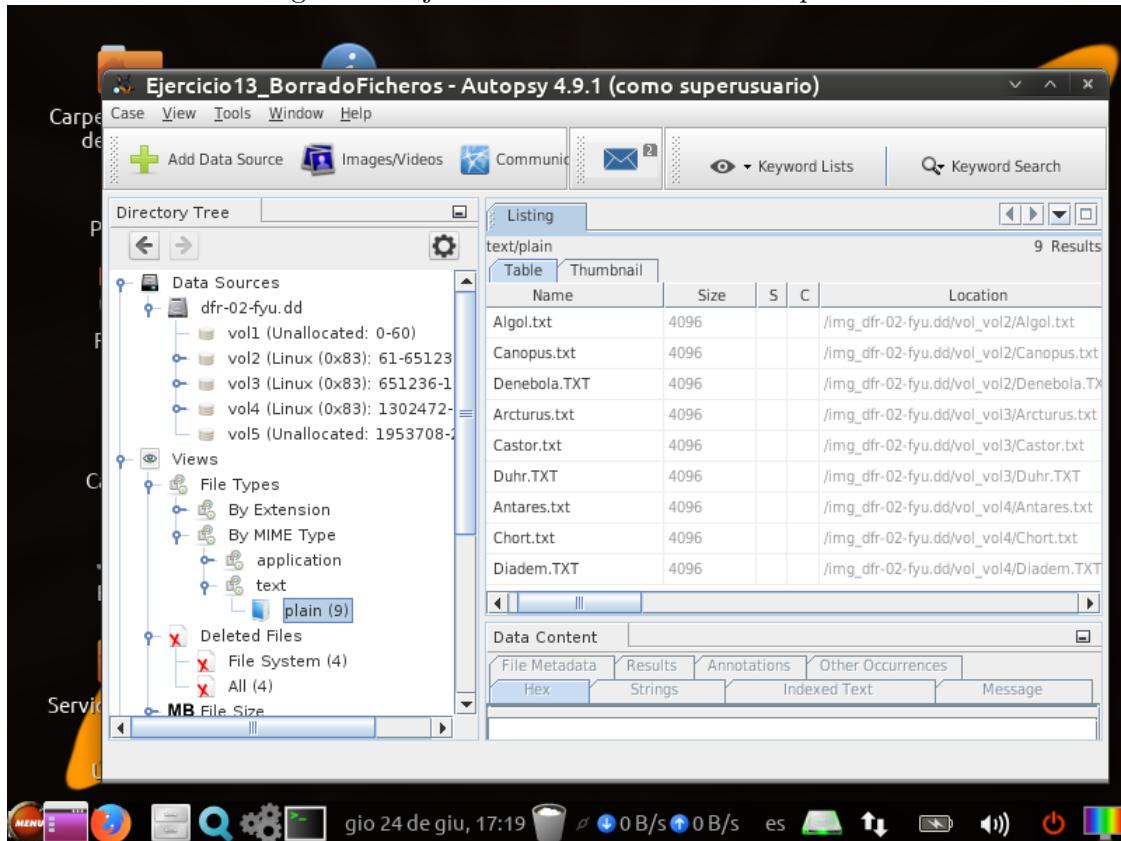


a)

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'.

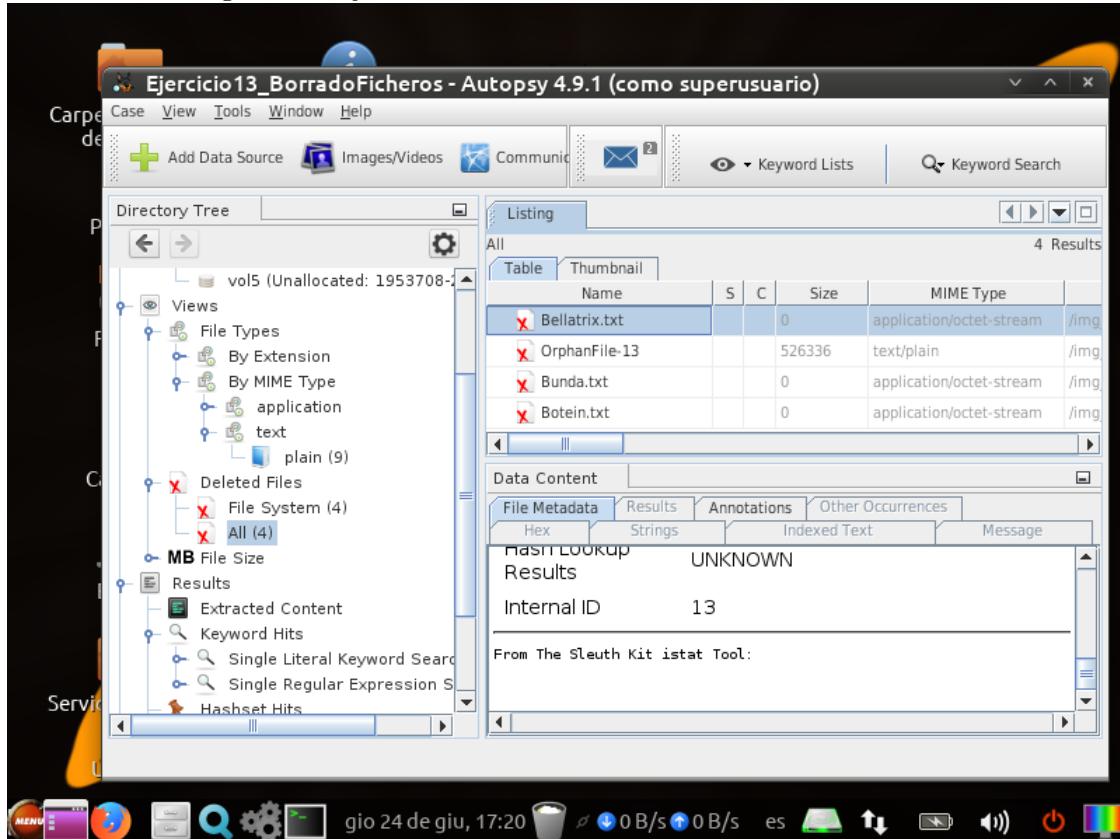
Figura 23: Ejercicio 13: Ficheros de texto plano



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

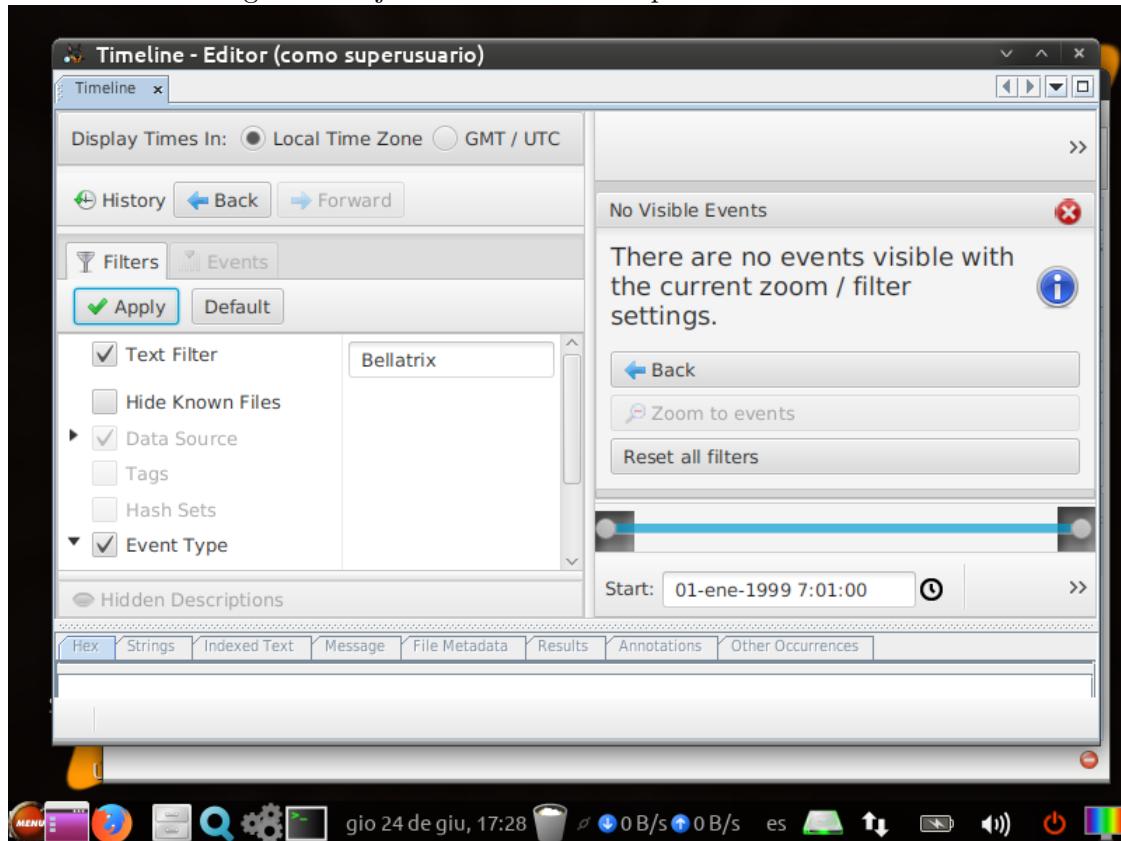


Como se puede observar hay menos metadatos sobre los ficheros borrados que en el ejercicio anterior, por lo que habrá secciones de la tabla sin rellenar.

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*

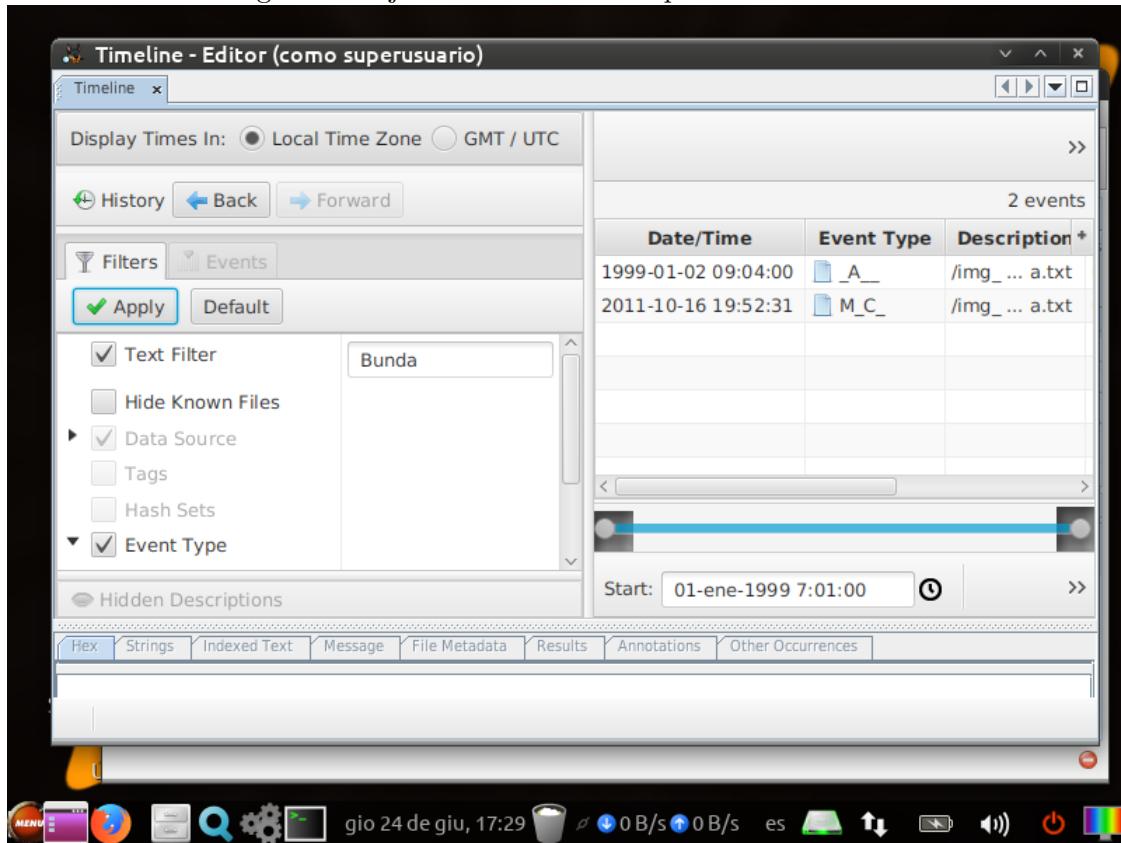
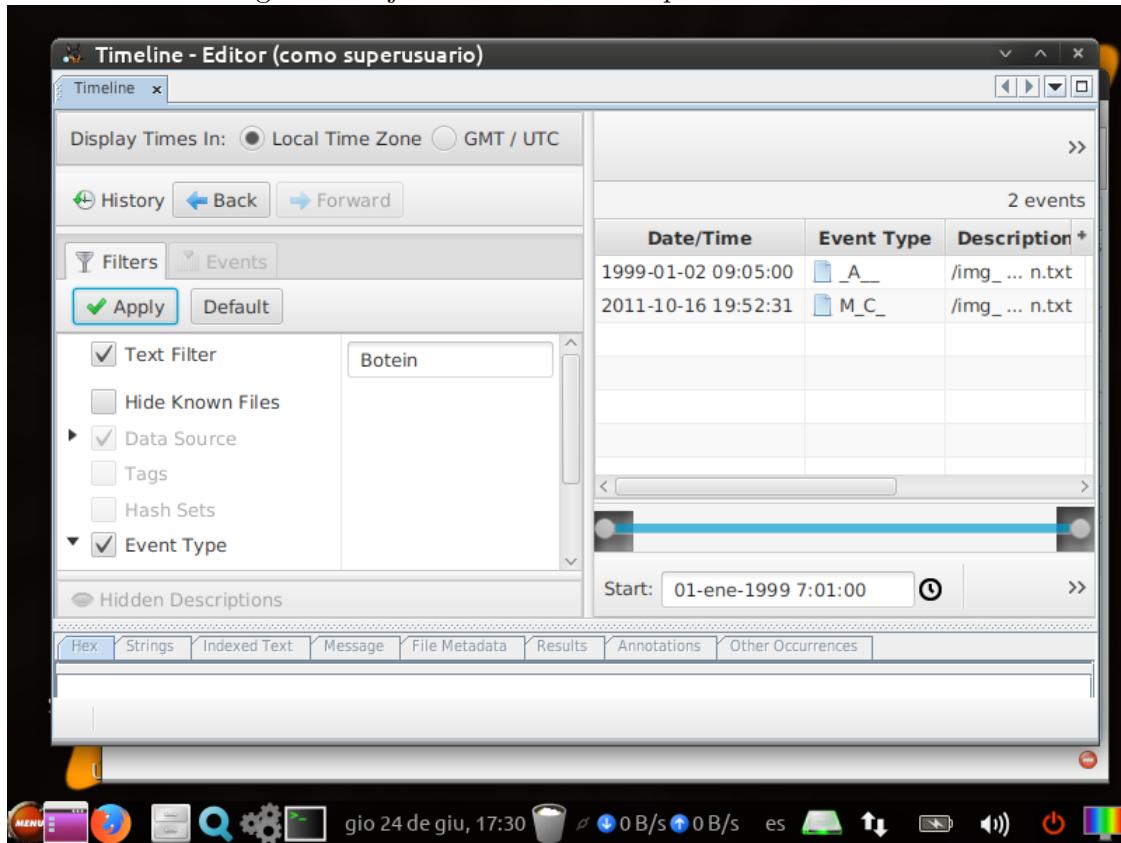


Figura 27: Ejercicio 13: Línea temporal de *Botein.txt*



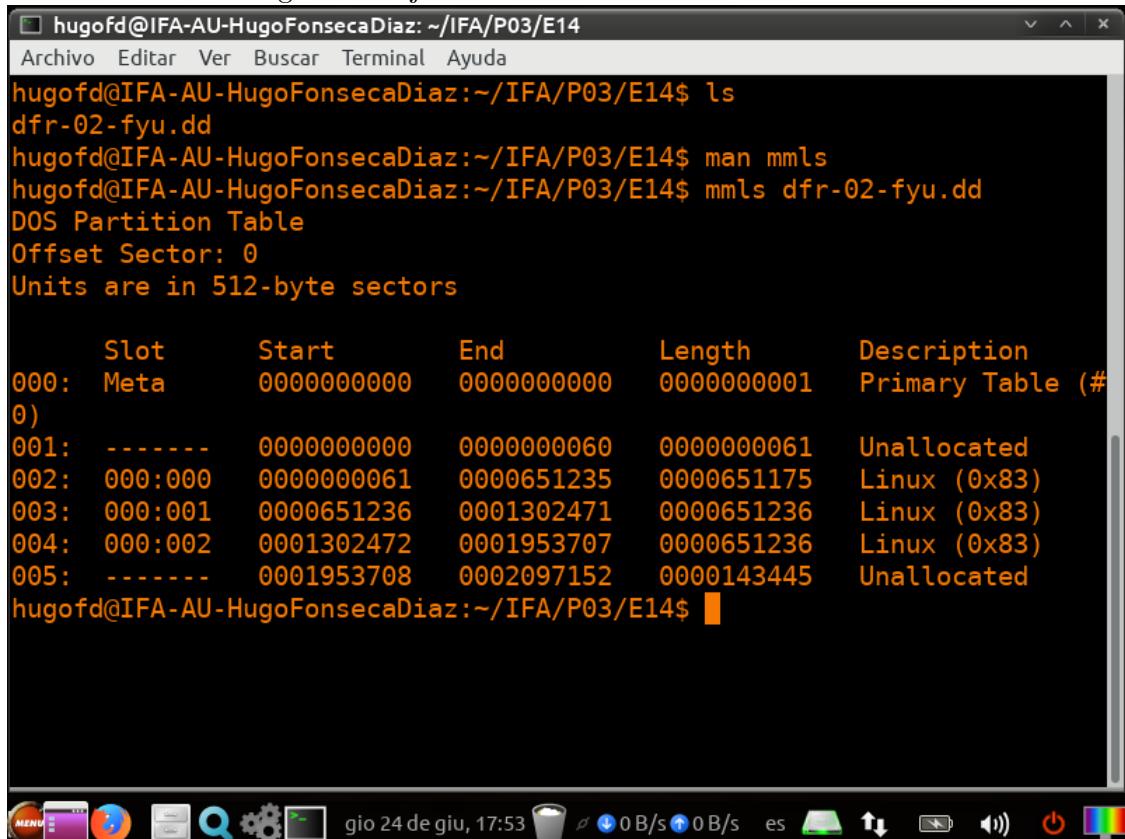
Para *Bunda.txt* y *Botein.txt* sí que se recuperan datos.

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:

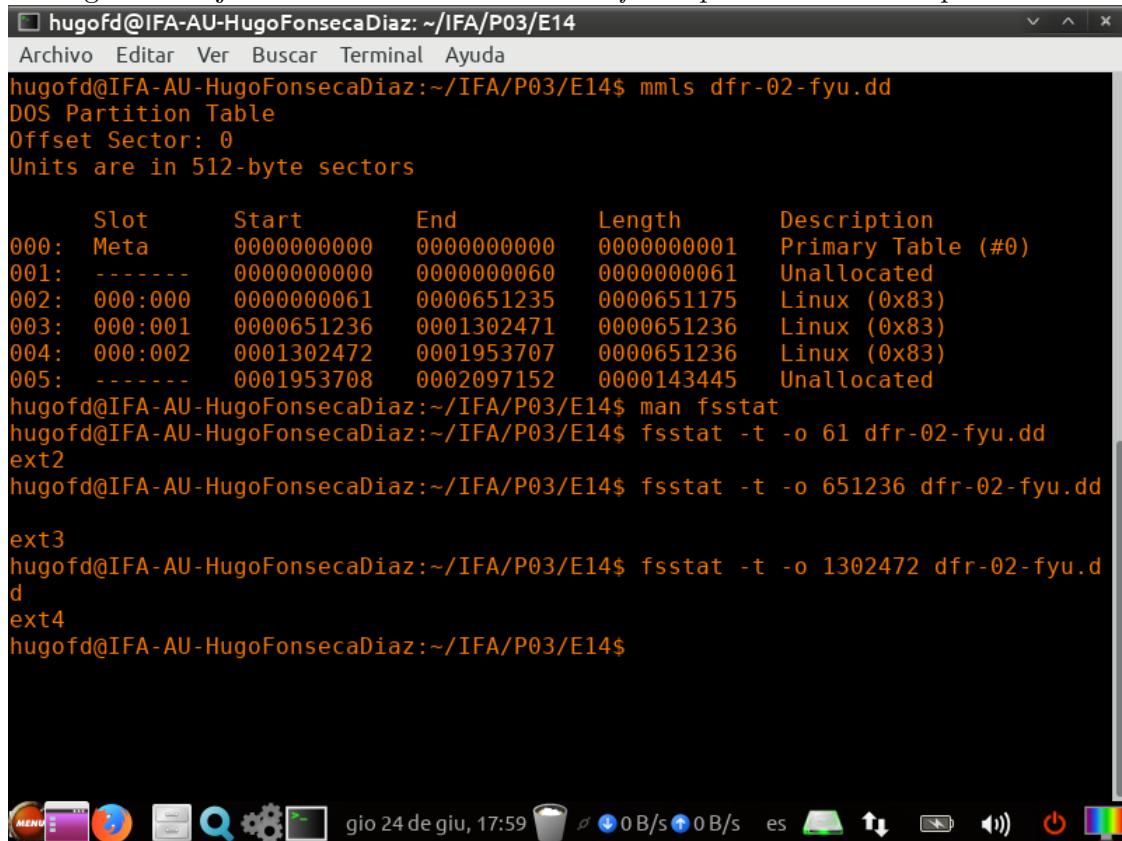
```
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ ls
dfr-02-fyu.dd
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ man mmls
hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14$ mmls dfr-02-fyu.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      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 circle with a white play button, a blue square, a magnifying glass, a gear, and a file 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, terminal, system settings, and power.

- 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*

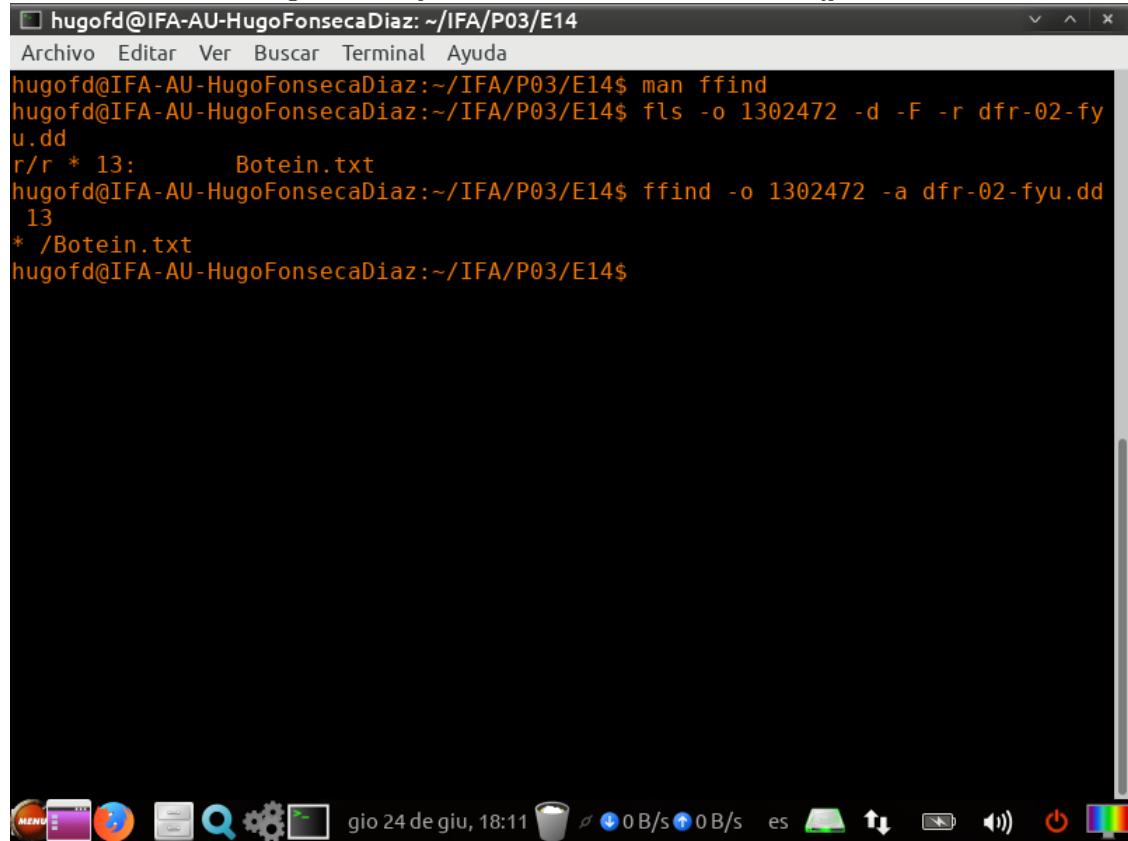
The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz:~/IFA/P03/E14". The window contains the following text:

```
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*

The screenshot shows a terminal window with the following content:

```
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$
```

The terminal window has a dark background and light-colored text. The bottom of the window shows various system icons and status information, including the date and time (gio 24 de giu, 18:14), disk usage (0 B/s down, 0 B/s up), and battery level.

3.4. Ejercicio 19

4. Práctica 04

5. Práctica 05