

IFA. Práctica de laboratorio 03

Hugo Fonseca Díaz
email uo258318@uniovi.es

Escuela de Ingeniería Informática. Universidad de Oviedo.

22 de junio de 2021

1. Ejercicio 1

Se crea el caso en Autopsy con los datos solicitados.

Figura 1: Ejercicio 1: Creación del caso

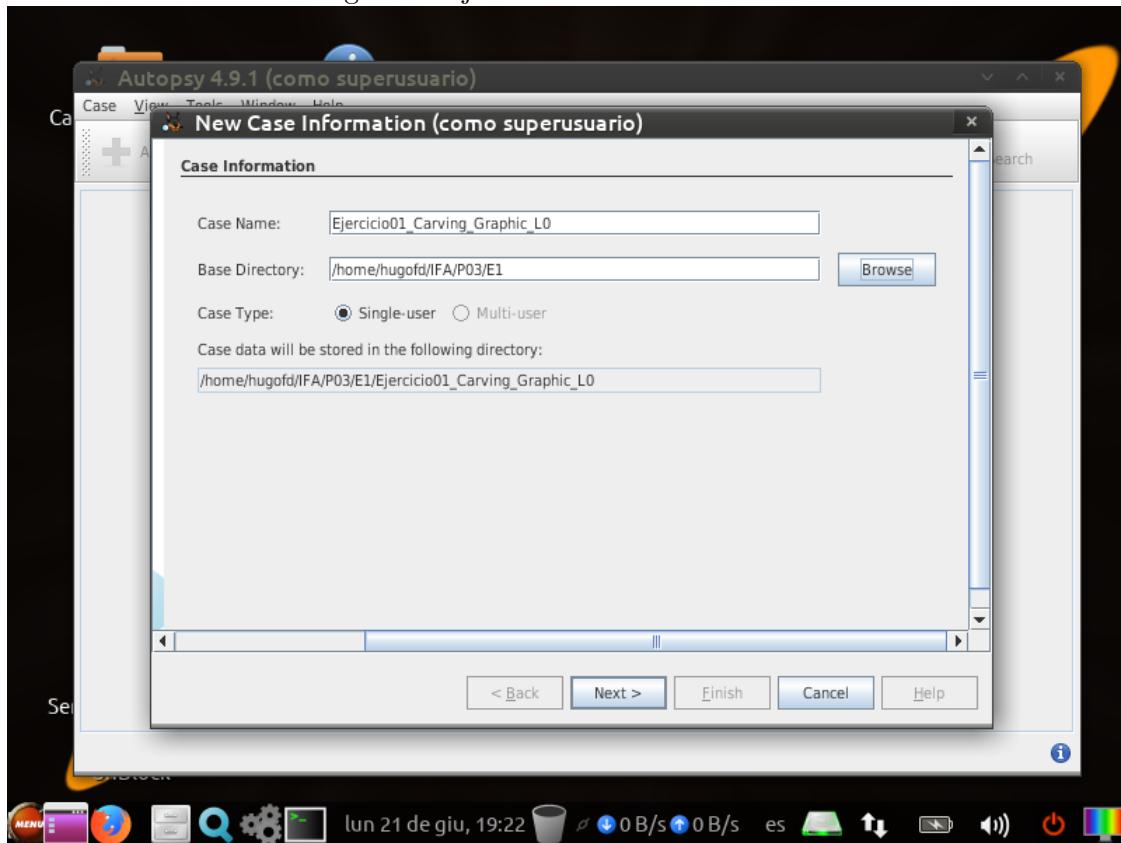
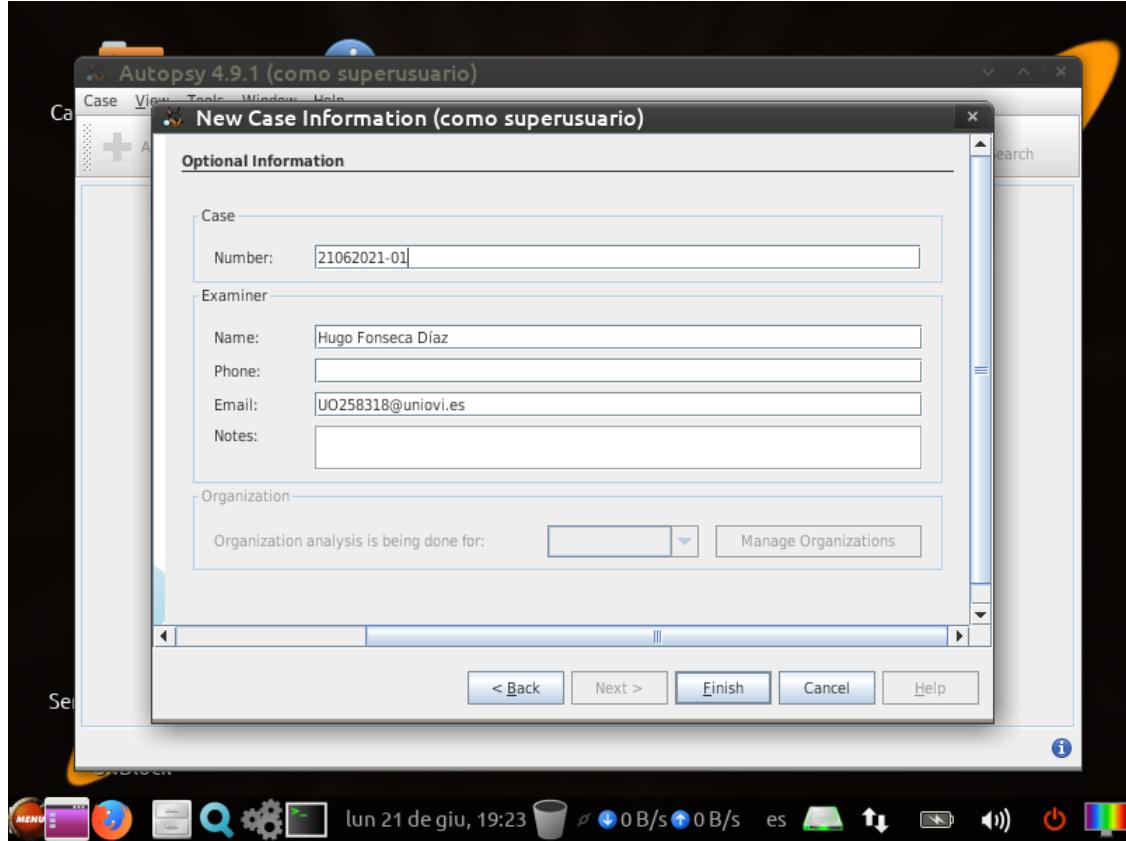
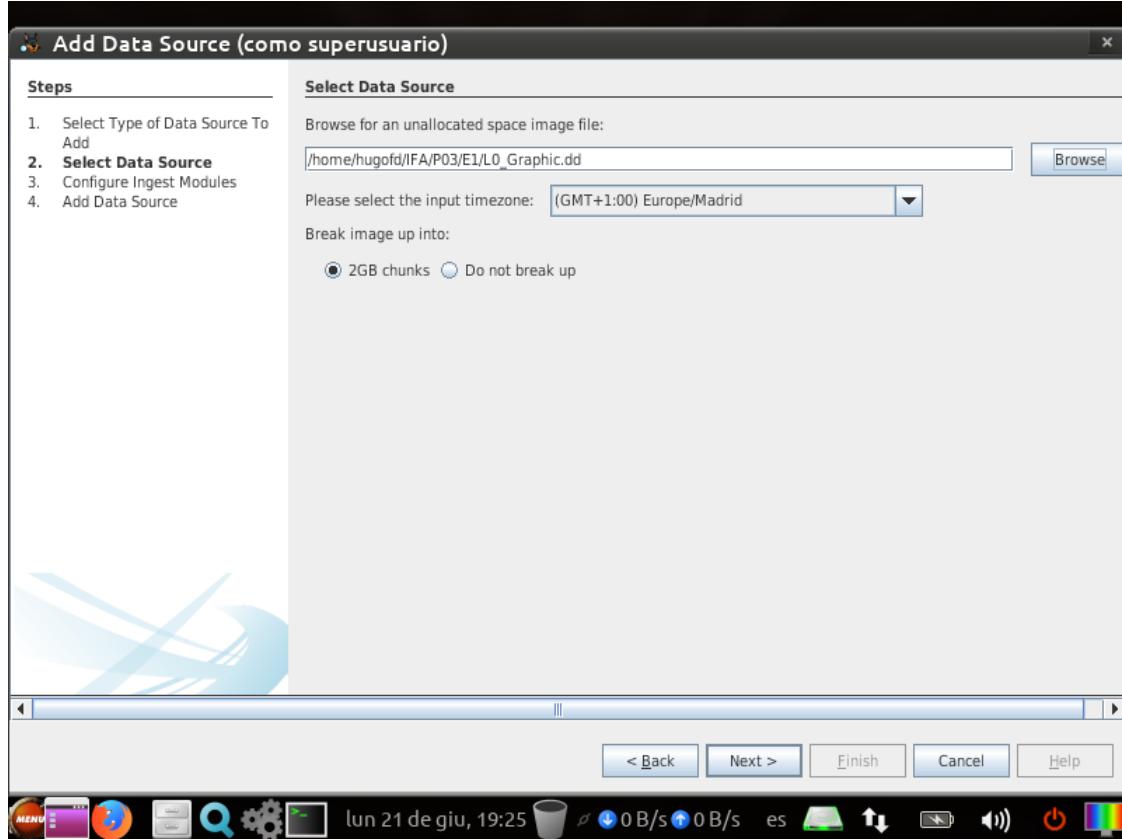


Figura 2: Ejercicio 1: Detalles del examinador



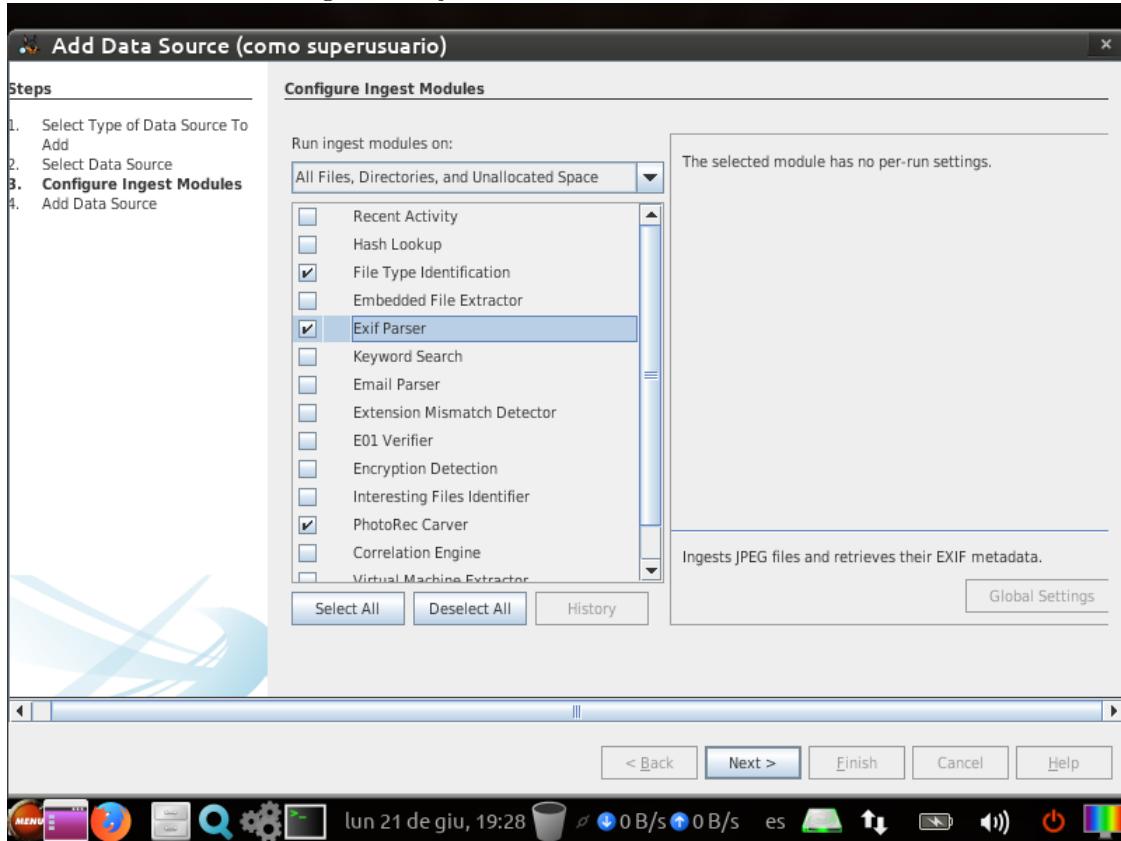
Añadimos la imagen a analizar.

Figura 3: Ejercicio 1: Selección de la imagen



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

Figura 4: Ejercicio 1: Selección de módulos



Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

Figura 5: Ejercicio 1: Resultados del análisis

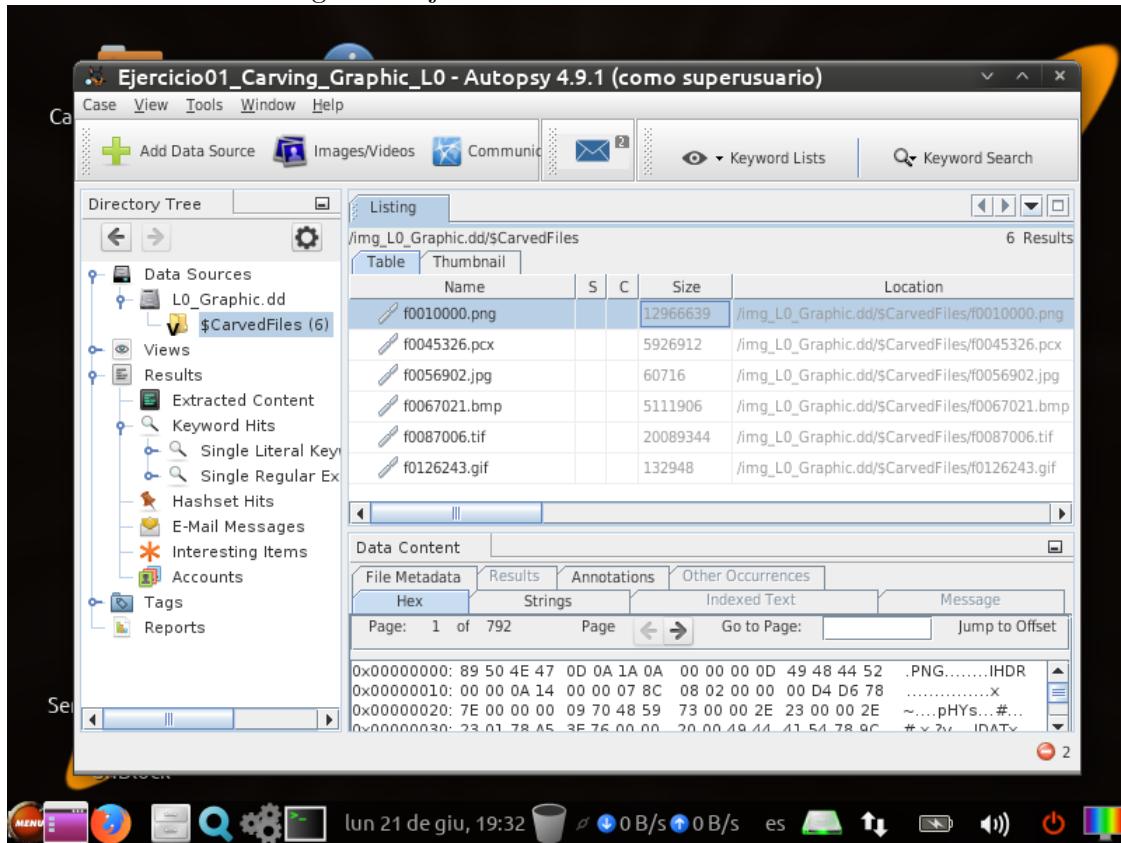
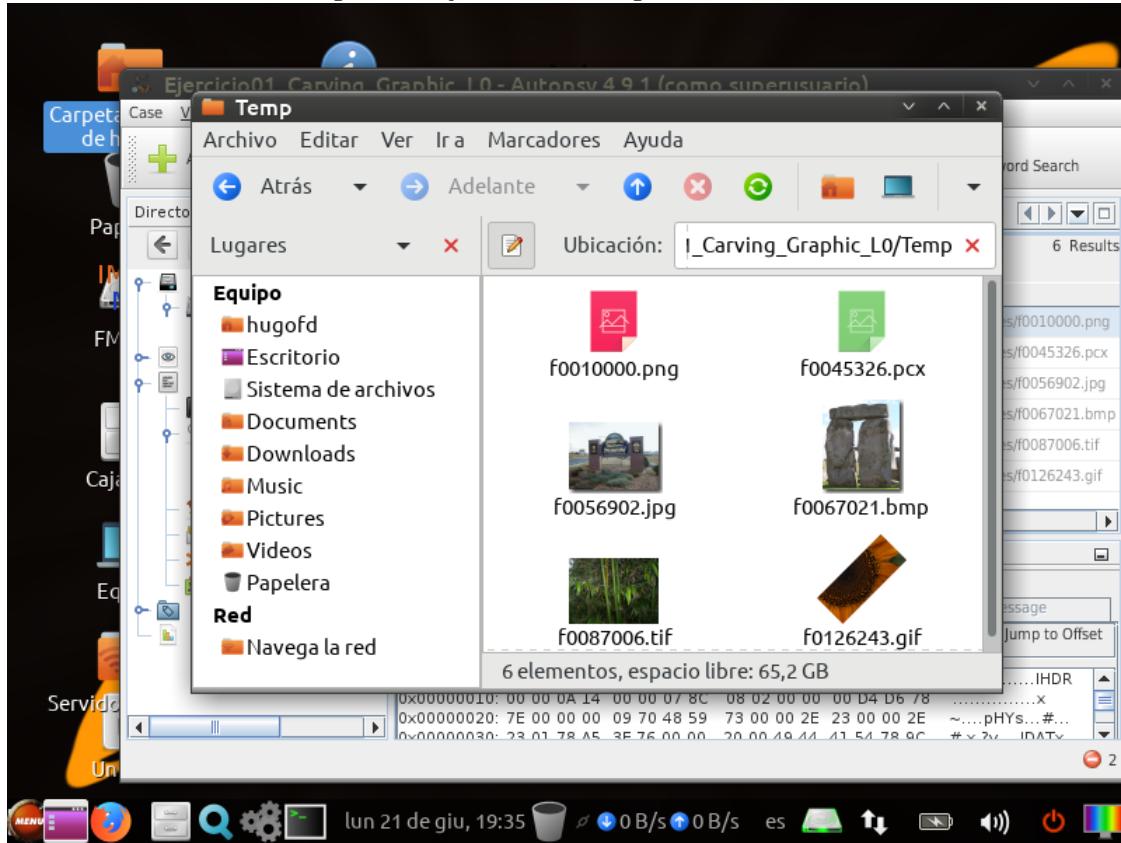


Figura 6: Ejercicio 1: Imágenes obtenidas



Para abrir el archivo con extensión *pcx* se ha utilizado un visor de imágenes online, al no disponer de uno adecuado en el equipo.

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Breve descripción imagen visible
f0010000.png	12966639	Flor morada
f0045326.pcx	5926912	Iglesia y fuente
f0056902.jpg	60716	Cartel 'Welcome to Moscow'
f0067021.bmp	5111906	Piedras en forma de Pi
f0087006.tif	20089344	Cañas de bambú
f0126243.gif	132948	Girasol

2. Ejercicio 2

Se crea el caso en Autopsy con los datos solicitados.

Figura 7: Ejercicio 2: Creación del caso

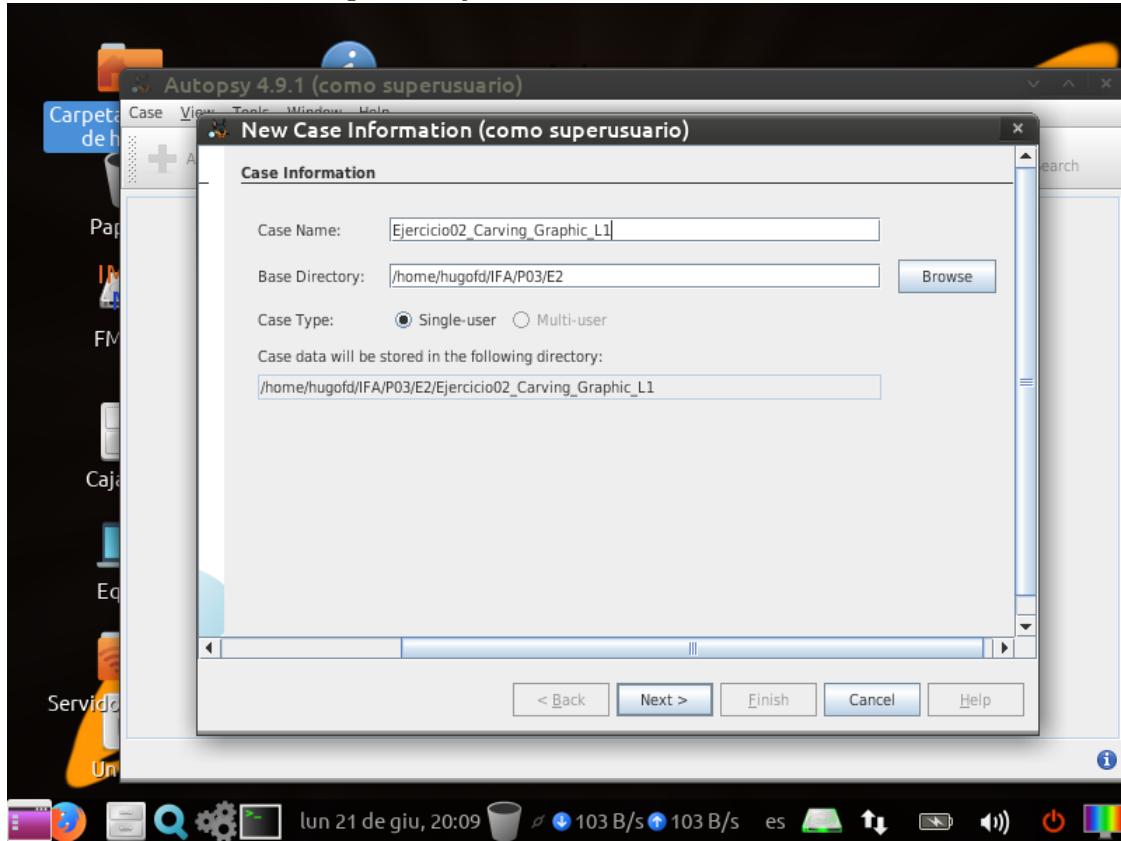
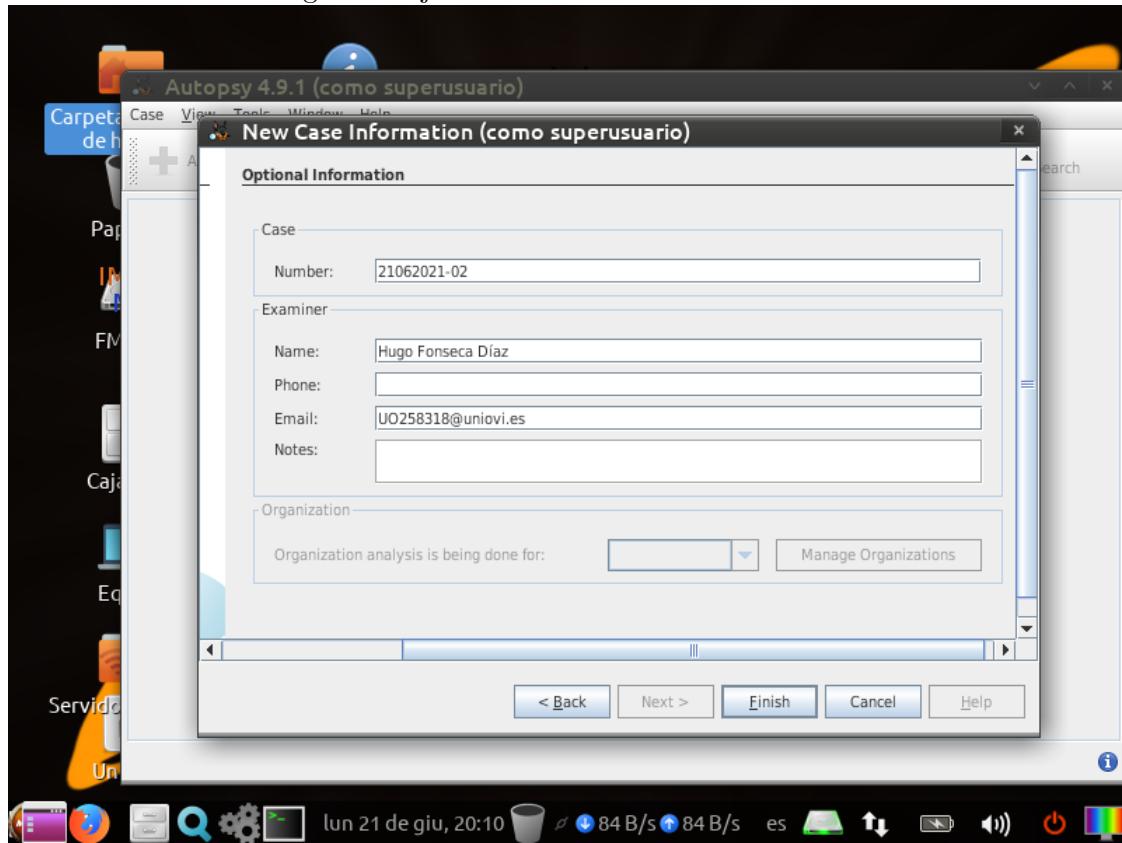
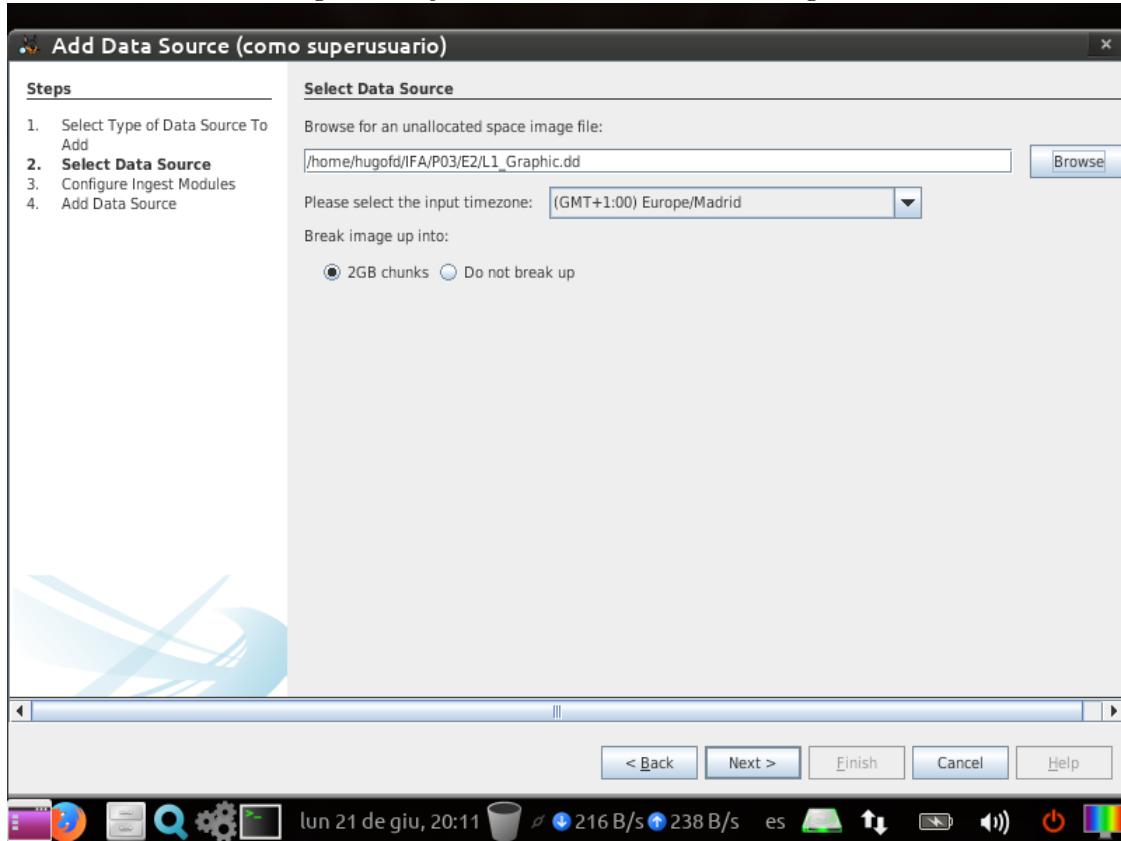


Figura 8: Ejercicio 2: Detalles del examinador



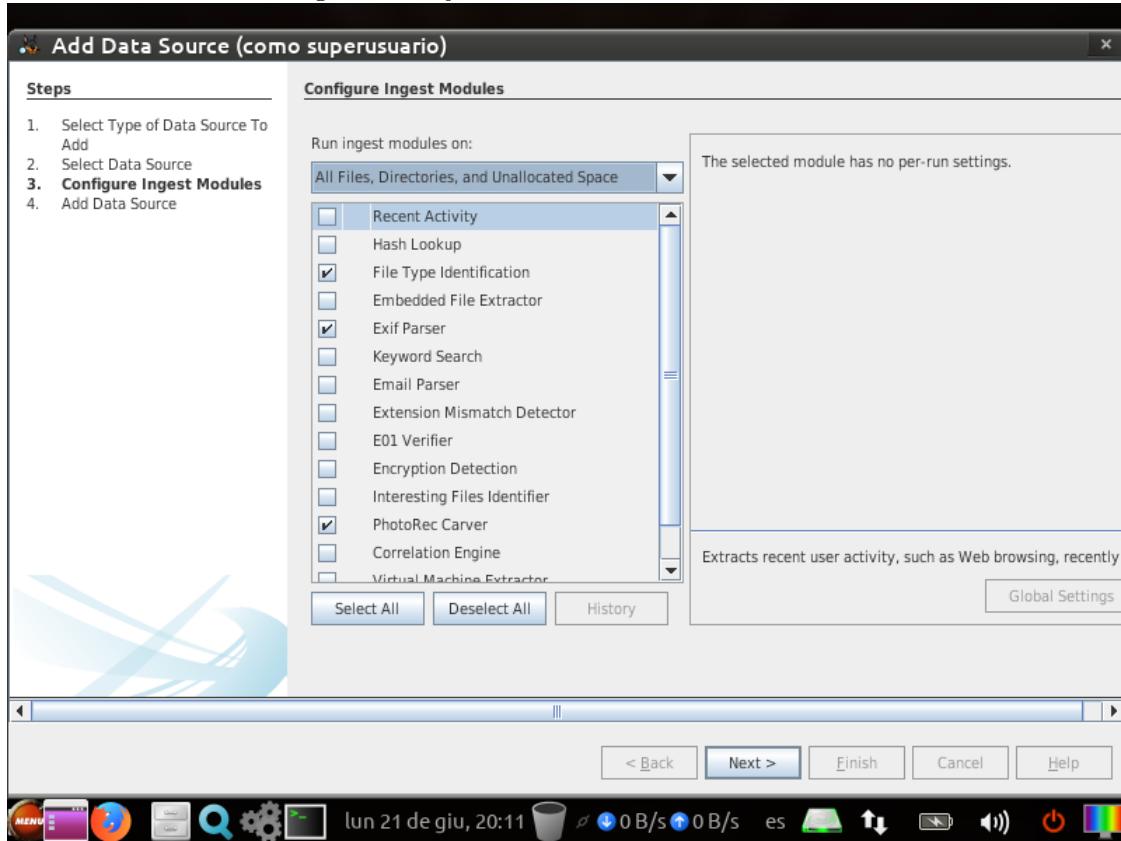
Añadimos la imagen a analizar.

Figura 9: Ejercicio 2: Selección de la imagen



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

Figura 10: Ejercicio 2: Selección de módulos



Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

Figura 11: Ejercicio 2: Resultados del análisis

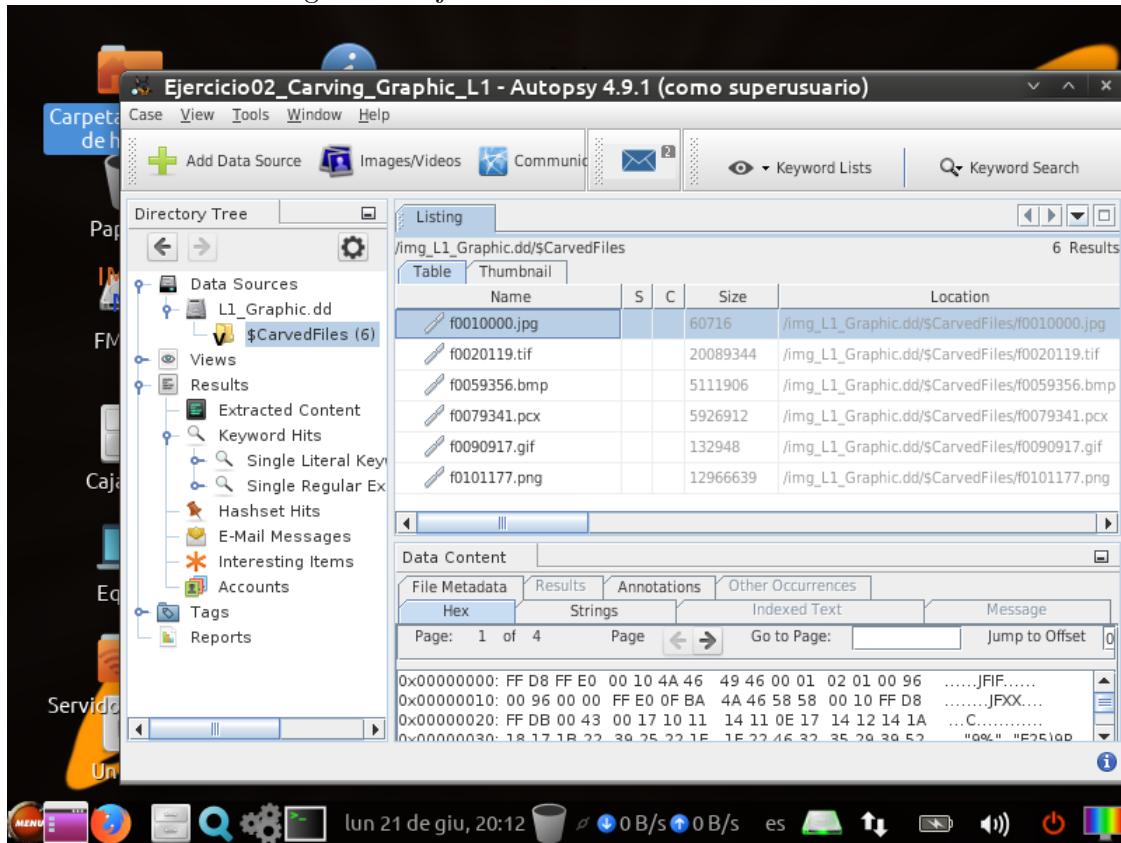
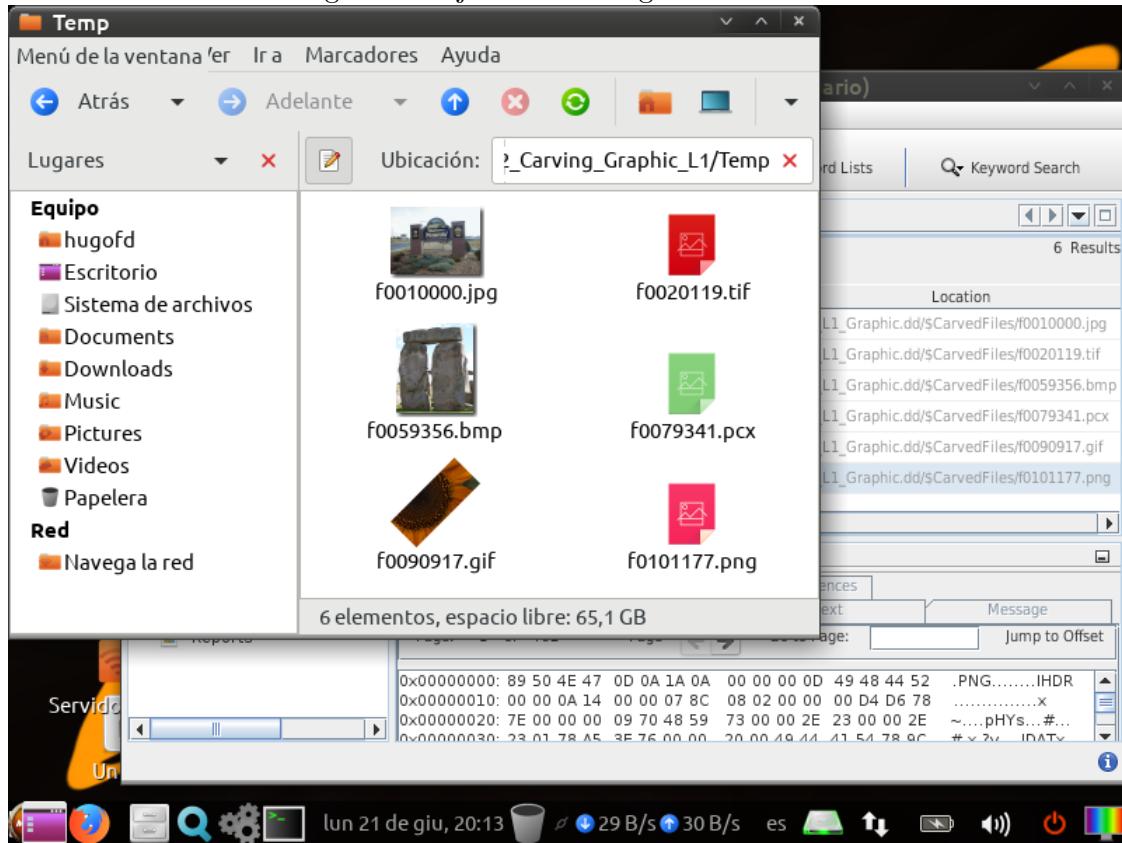


Figura 12: Ejercicio 2: Imágenes obtenidas



Para abrir el archivo con extensión *pcx* se ha utilizado un visor de imágenes online, al no disponer de uno adecuado en el equipo.

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Breve descripción imagen visible
f0010000.jpg	60716	Cartel 'Welcome to Moscow'
f0020119.tif	20089344	Cañas de bambú
f0059356.bmp	5111906	Piedras en forma de Pi
f0079341.pcx	5926912	Iglesia y fuente
f0090917.gif	132948	Girasol
f0101177.png	12966639	Flor morada

3. Ejercicio 3

Se crea el caso en Autopsy con los datos solicitados.

Figura 13: Ejercicio 3: Creación del caso

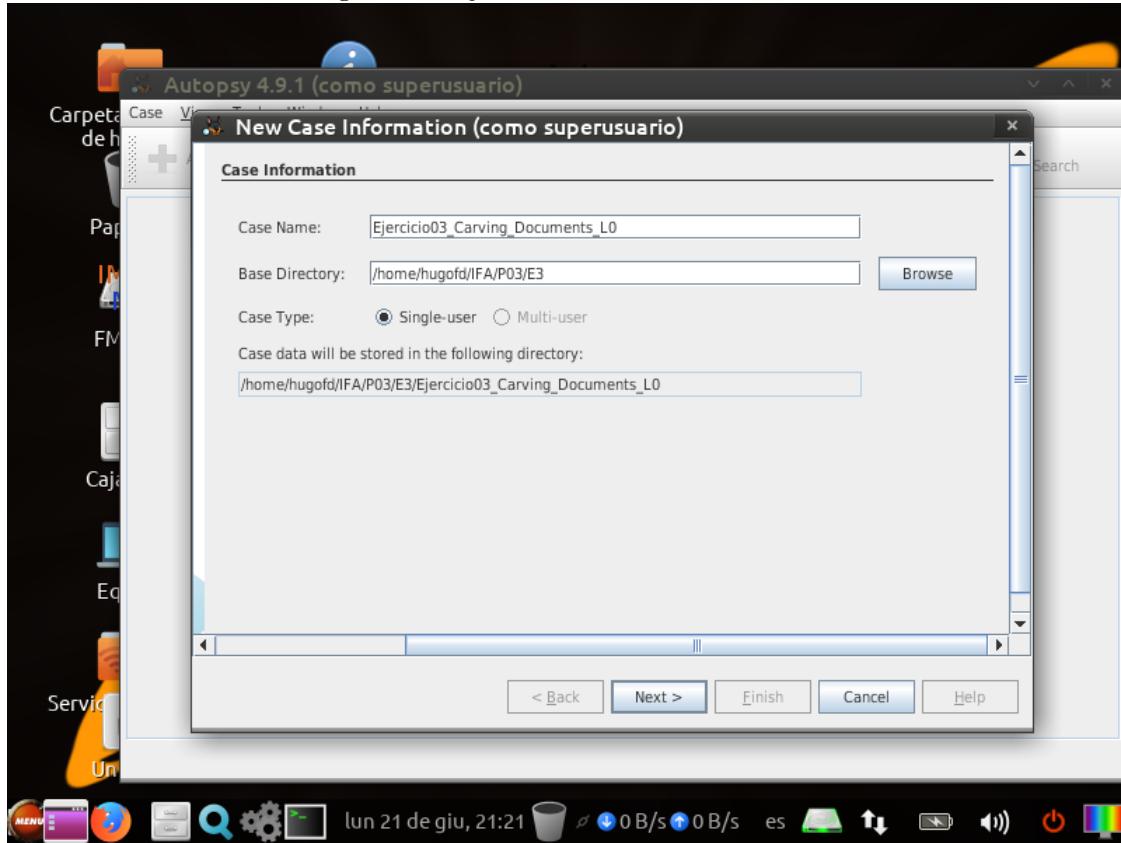
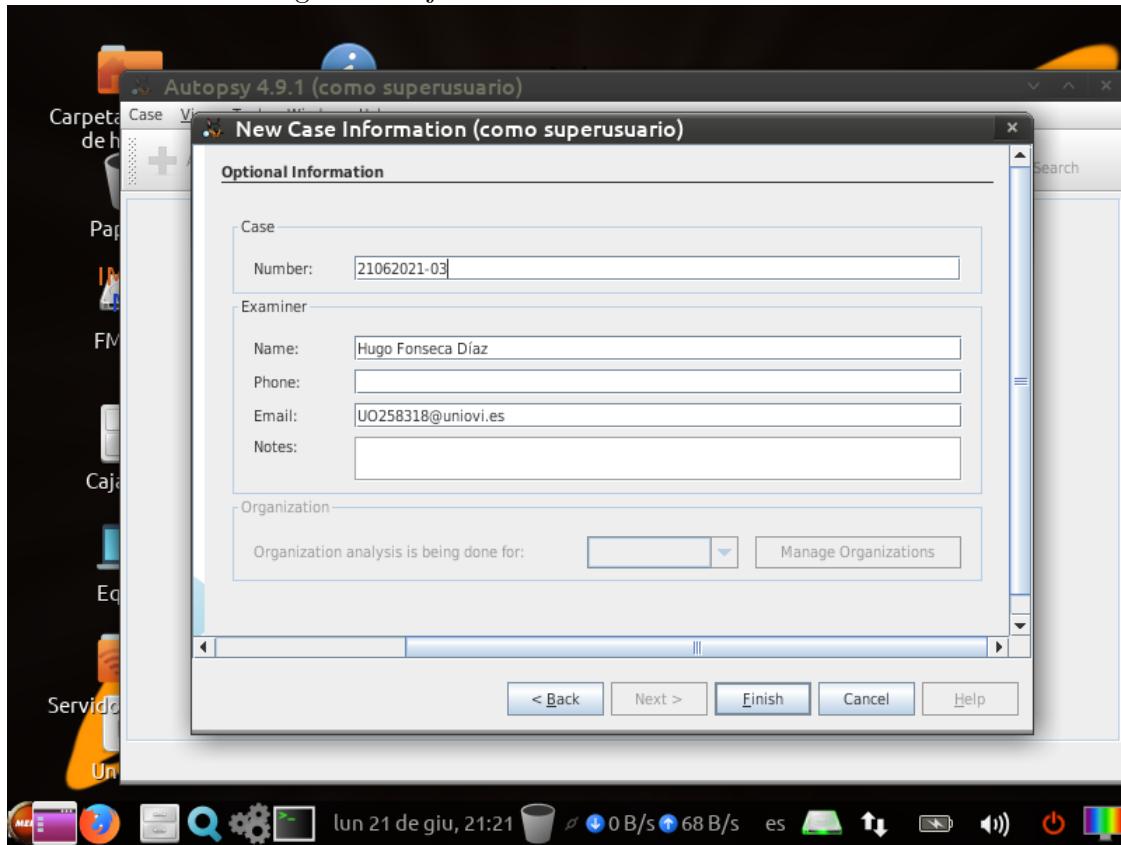
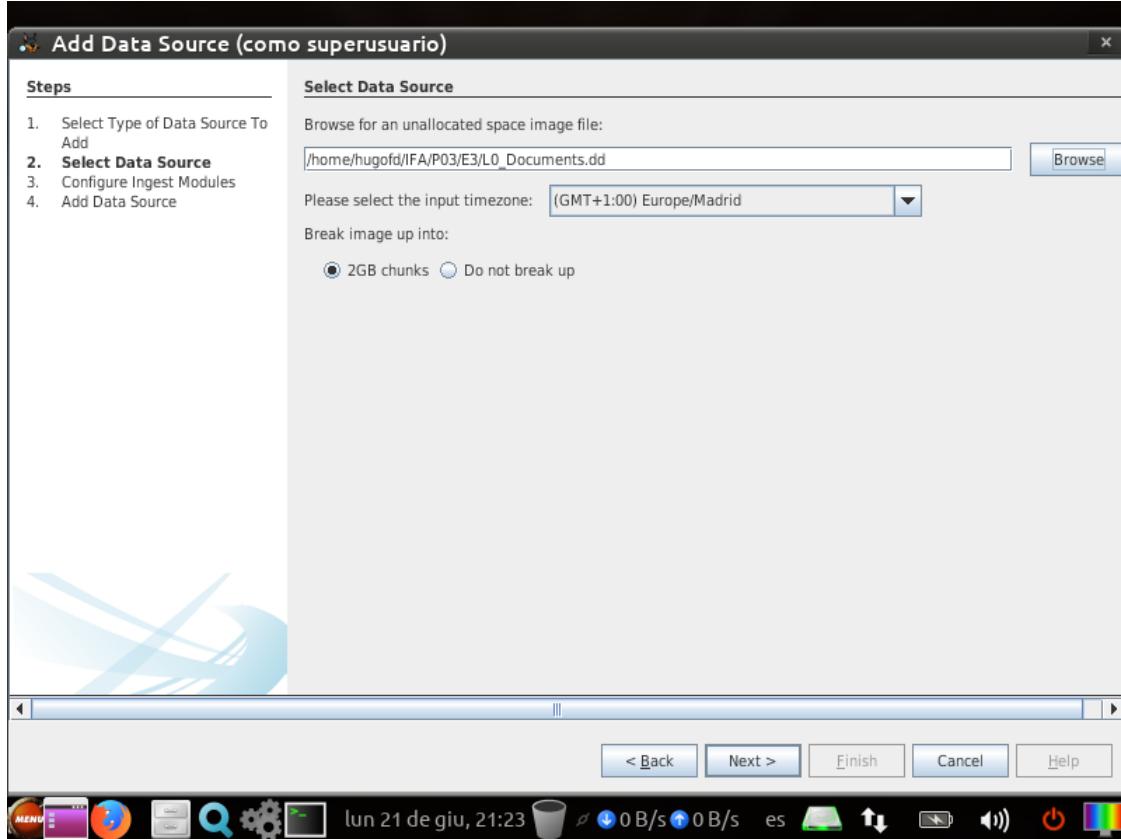


Figura 14: Ejercicio 3: Detalles del examinador



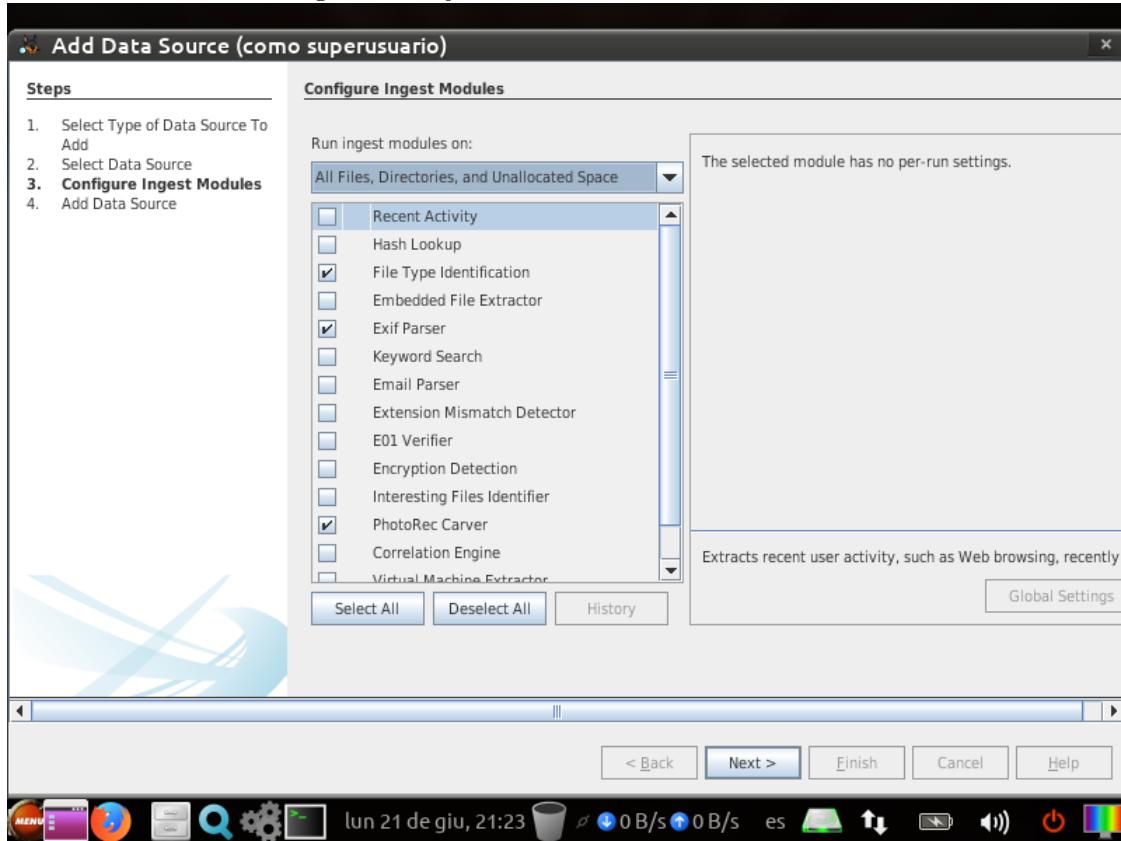
Añadimos la imagen a analizar.

Figura 15: Ejercicio 3: Selección de la imagen



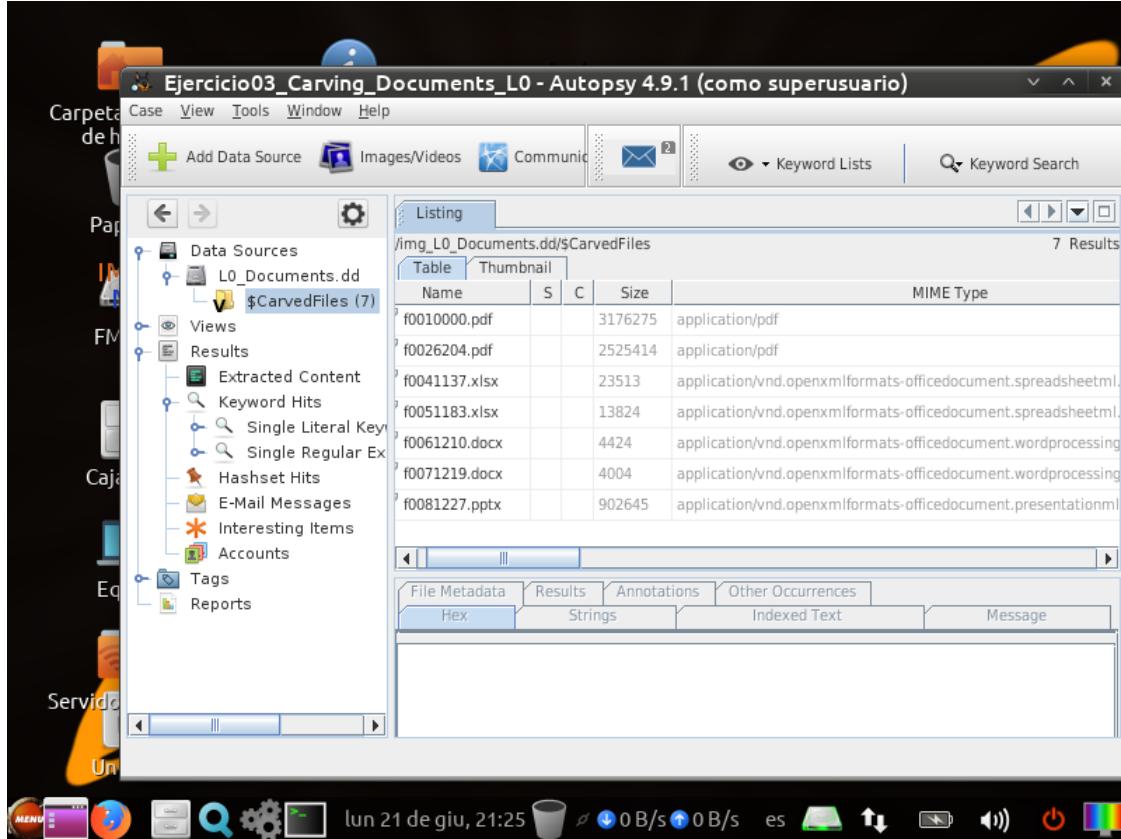
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

Figura 16: Ejercicio 3: Selección de módulos



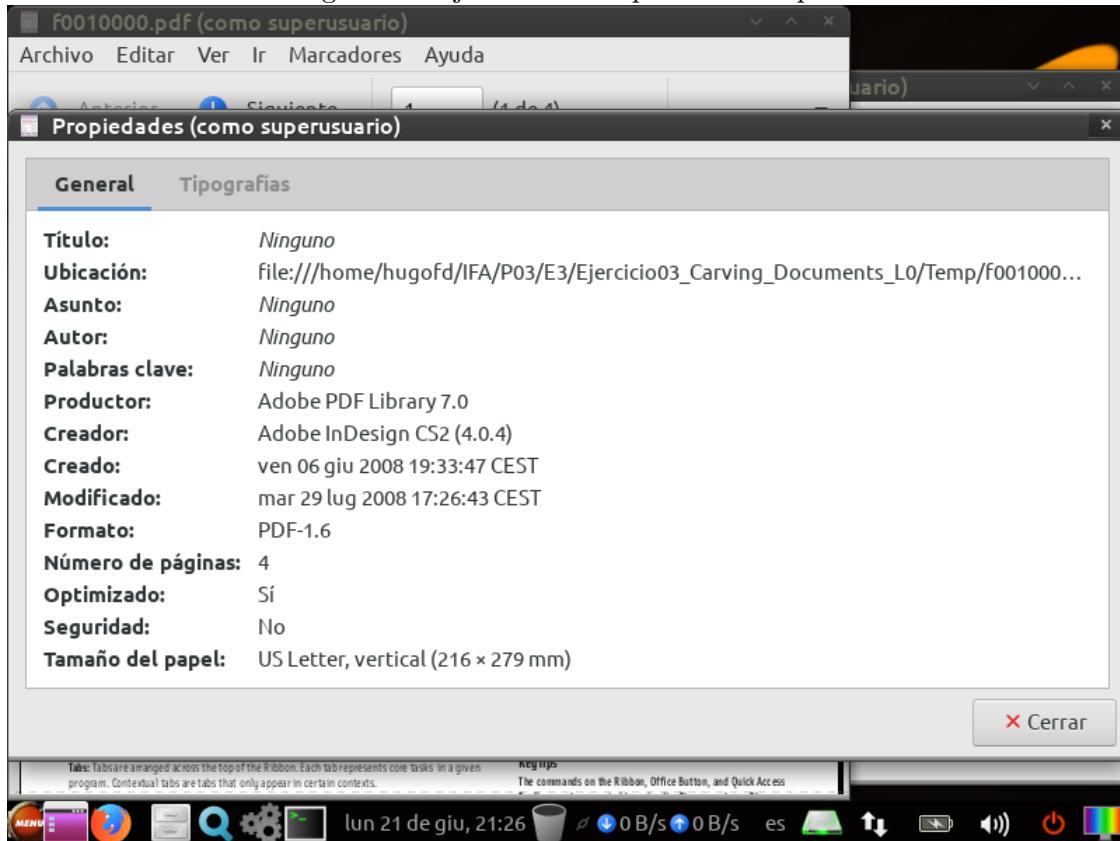
Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

Figura 17: Ejercicio 3: Resultados del análisis



Para obtener las fechas se abren los documentos con las aplicaciones externas correspondientes y se busca en sus propiedades.

Figura 18: Ejercicio 3: Propiedades del pdf



Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME documento	Fecha Creación del documento
f0010000.pdf	3176275	application/pdf	2008/06/06
f0026204.pdf	2525414	application/pdf	2008/06/04
f0041137.xlsx	23513	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	2012/06/13
f0051183.xlsx	13824	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	2012/07/05
f0061210.docx	4424	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Sin especificar
f0071219.docx	4004	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Sin especificar
f0081227.pptx	902645	application/vnd.openxmlformats-officedocument.presentationml.presentation	2010/09/28

4. Ejercicio 4

Se crea el caso en Autopsy con los datos solicitados.

Figura 19: Ejercicio 4: Creación del caso

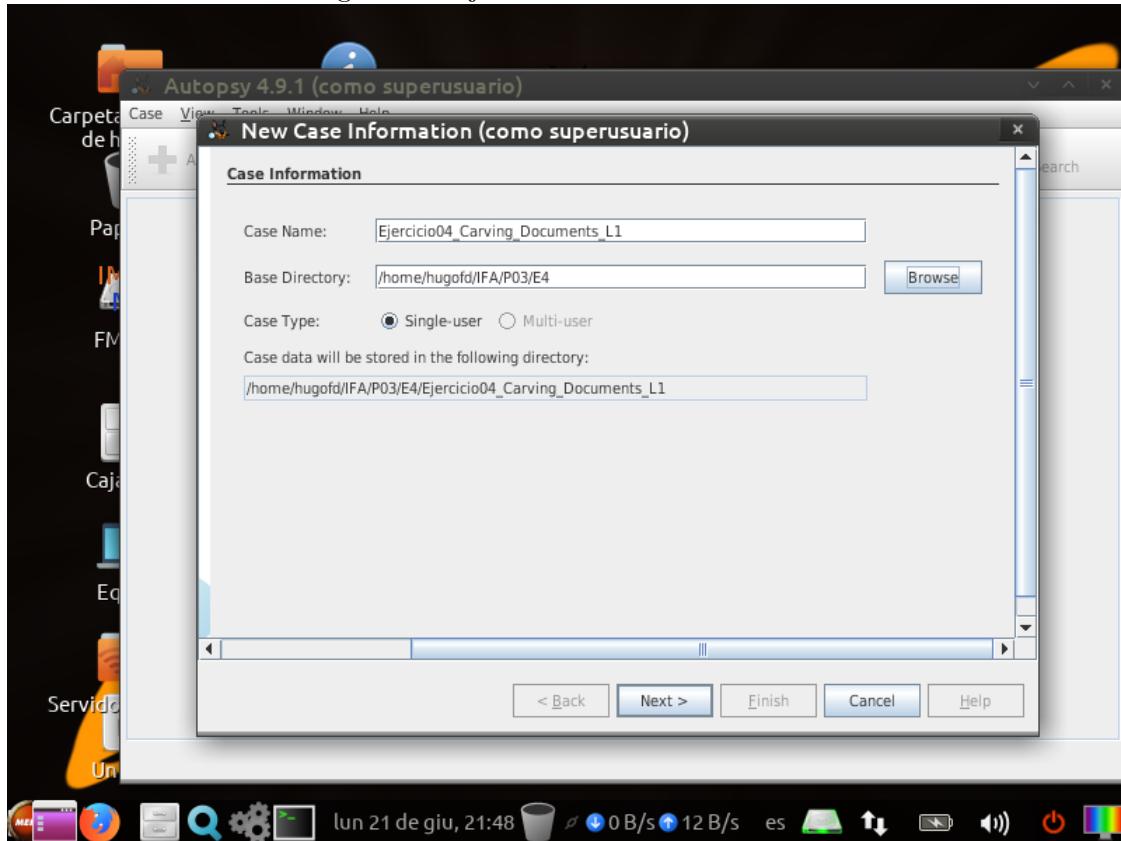
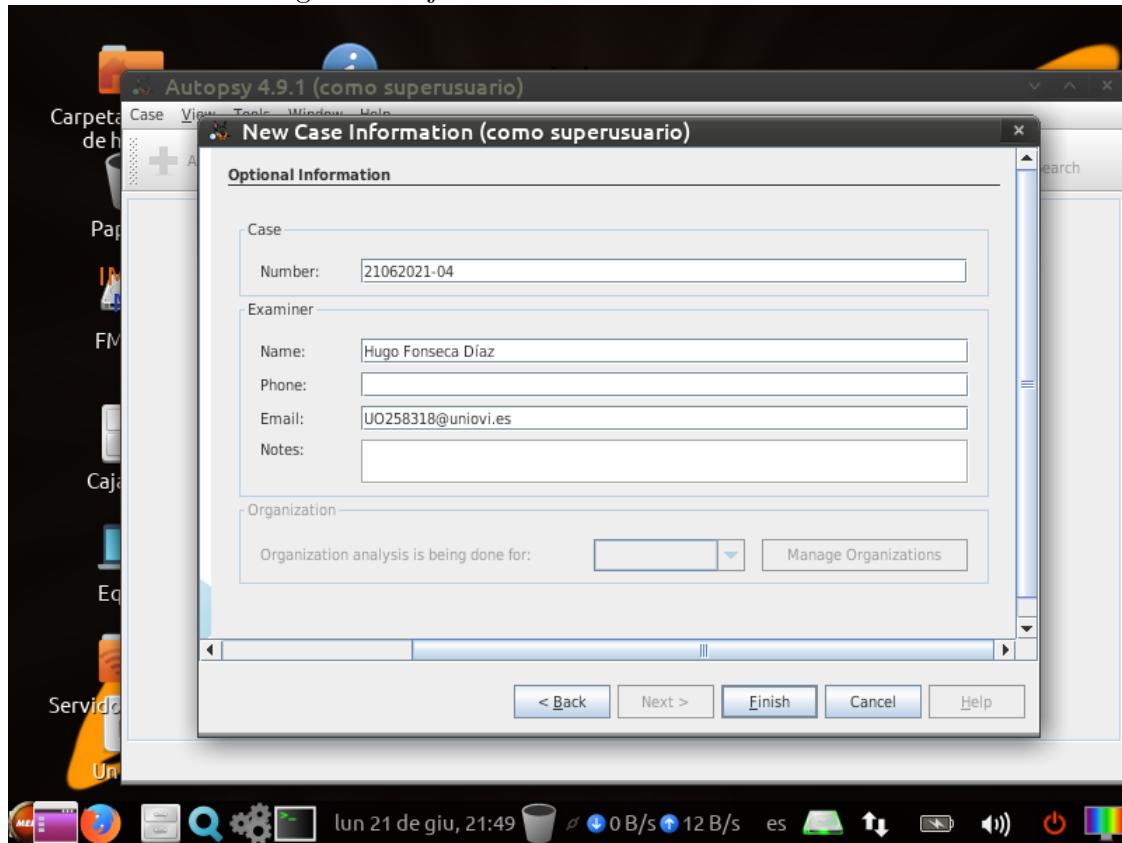
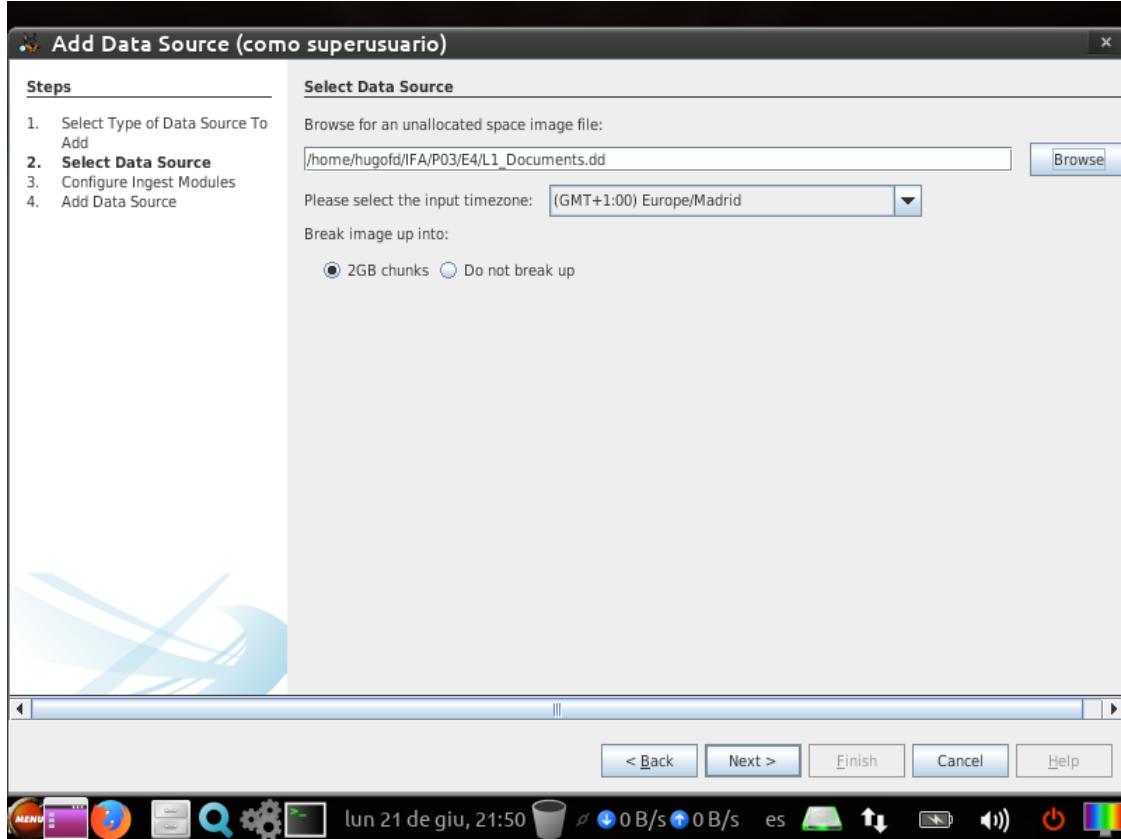


Figura 20: Ejercicio 4: Detalles del examinador



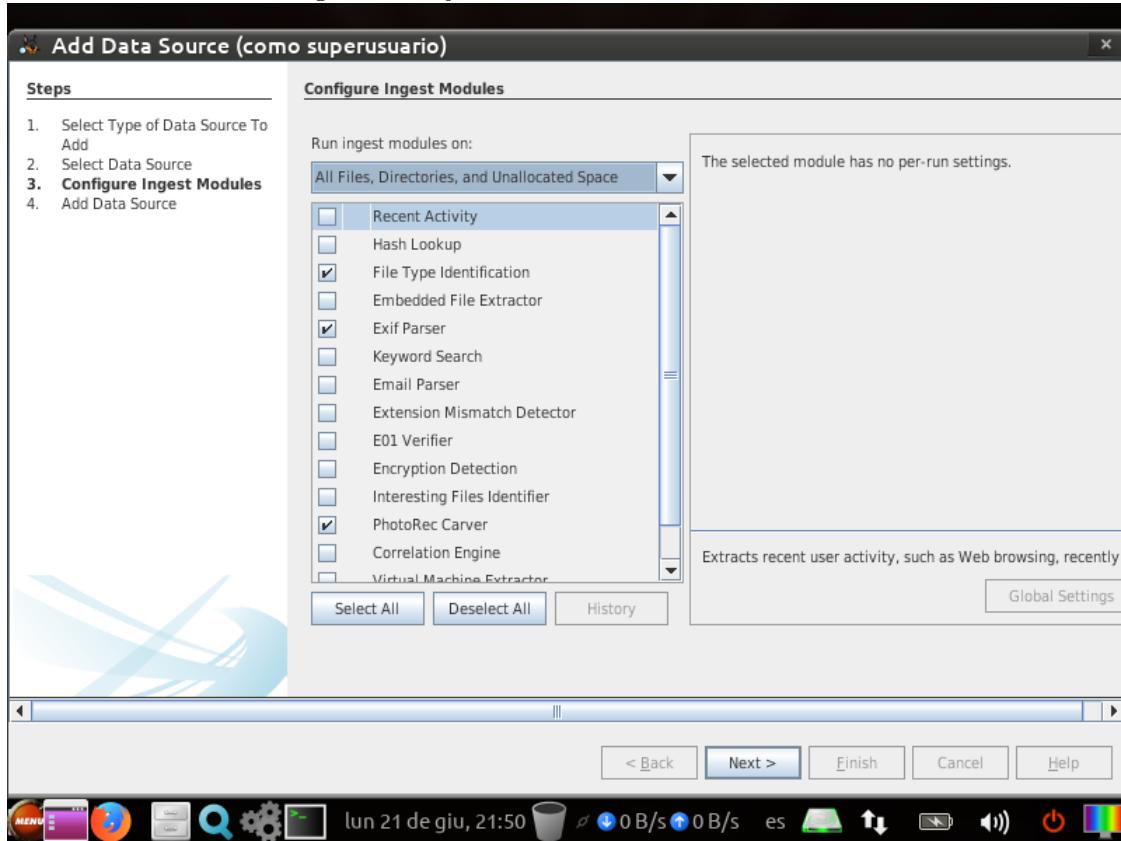
Añadimos la imagen a analizar.

Figura 21: Ejercicio 4: Selección de la imagen



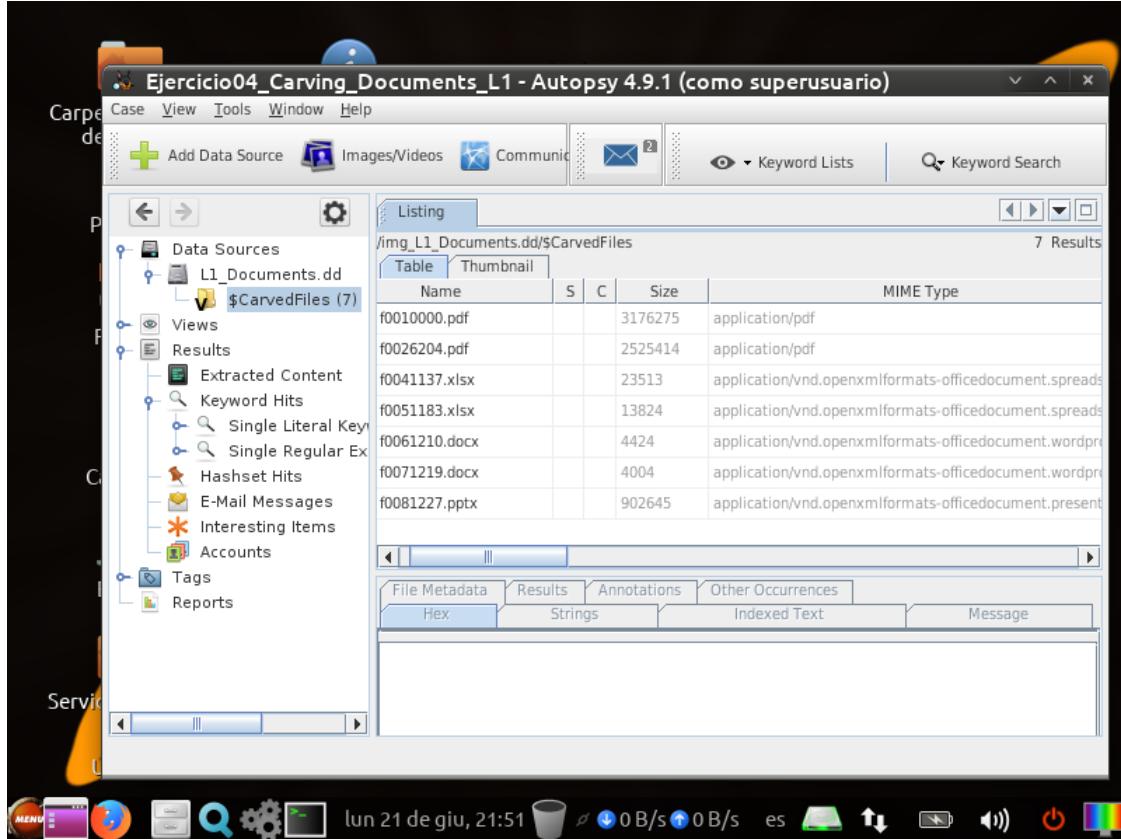
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

Figura 22: Ejercicio 4: Selección de módulos



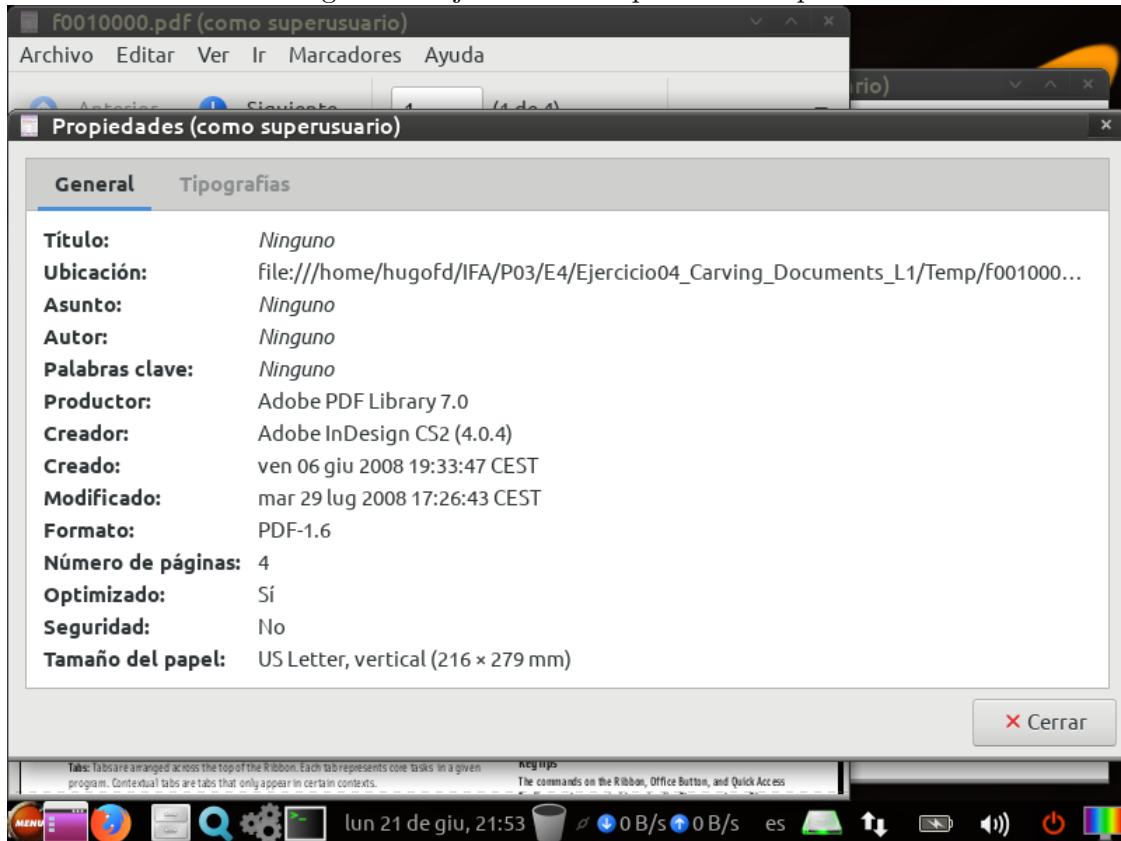
Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

Figura 23: Ejercicio 4: Resultados del análisis



Para obtener las fechas se abren los documentos con las aplicaciones externas correspondientes y se busca en sus propiedades.

Figura 24: Ejercicio 4: Propiedades del pdf



Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME documento	Fecha Creación del documento
f0010000.pdf	3176275	application/pdf	2008/06/06
f0026204.pdf	2525414	application/pdf	2008/06/04
f0041137.xlsx	23513	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	2012/06/13
f0051183.xlsx	13824	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	2012/07/05
f0061210.docx	4424	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Sin especificar
f0071219.docx	4004	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Sin especificar
f0081227.pptx	902645	application/vnd.openxmlformats-officedocument.presentationml.presentation	2010/09/28

5. Ejercicio 5

Se crea el caso en Autopsy con los datos solicitados.

Figura 25: Ejercicio 5: Creación del caso

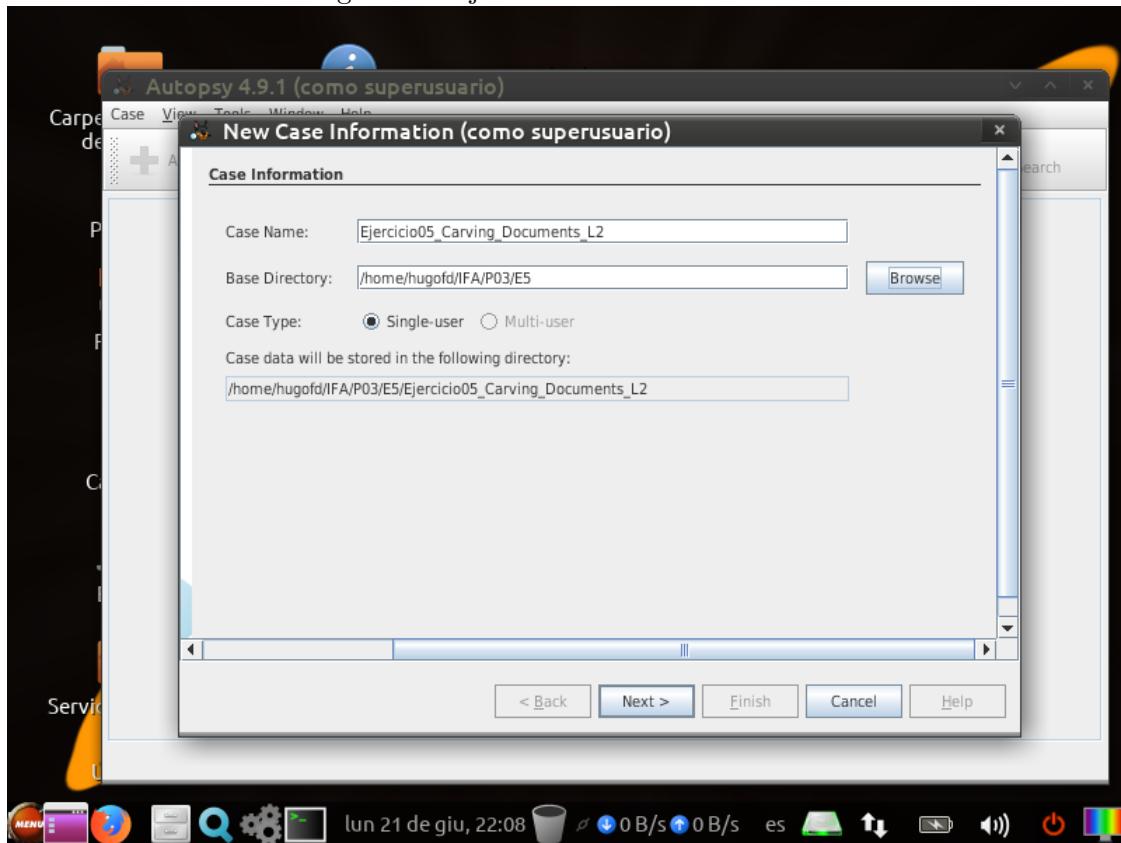
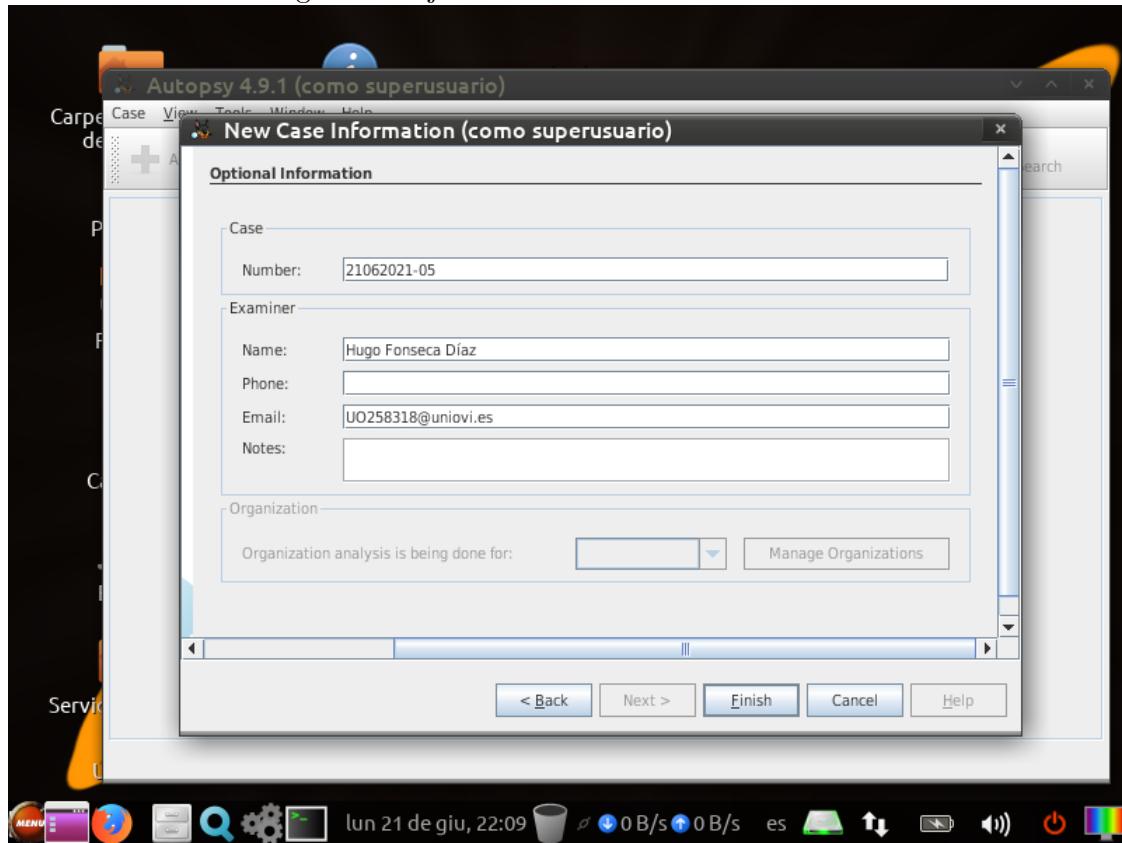
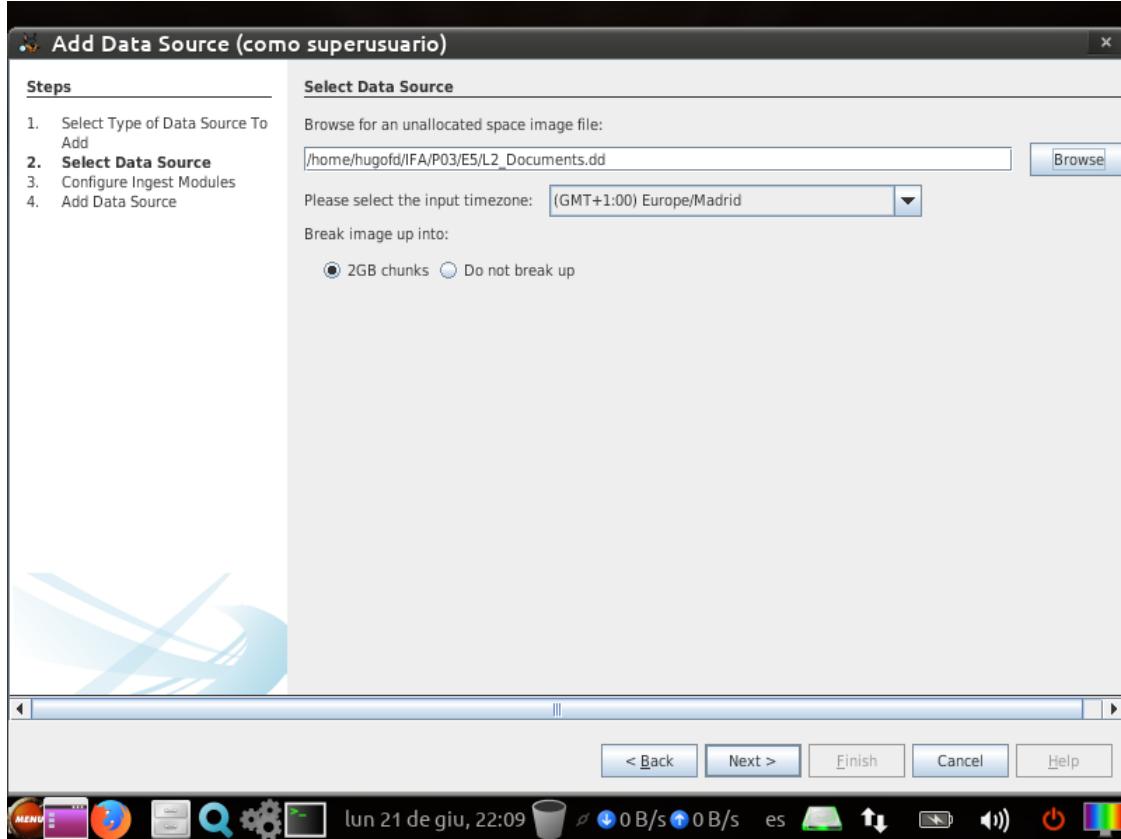


Figura 26: Ejercicio 5: Detalles del examinador



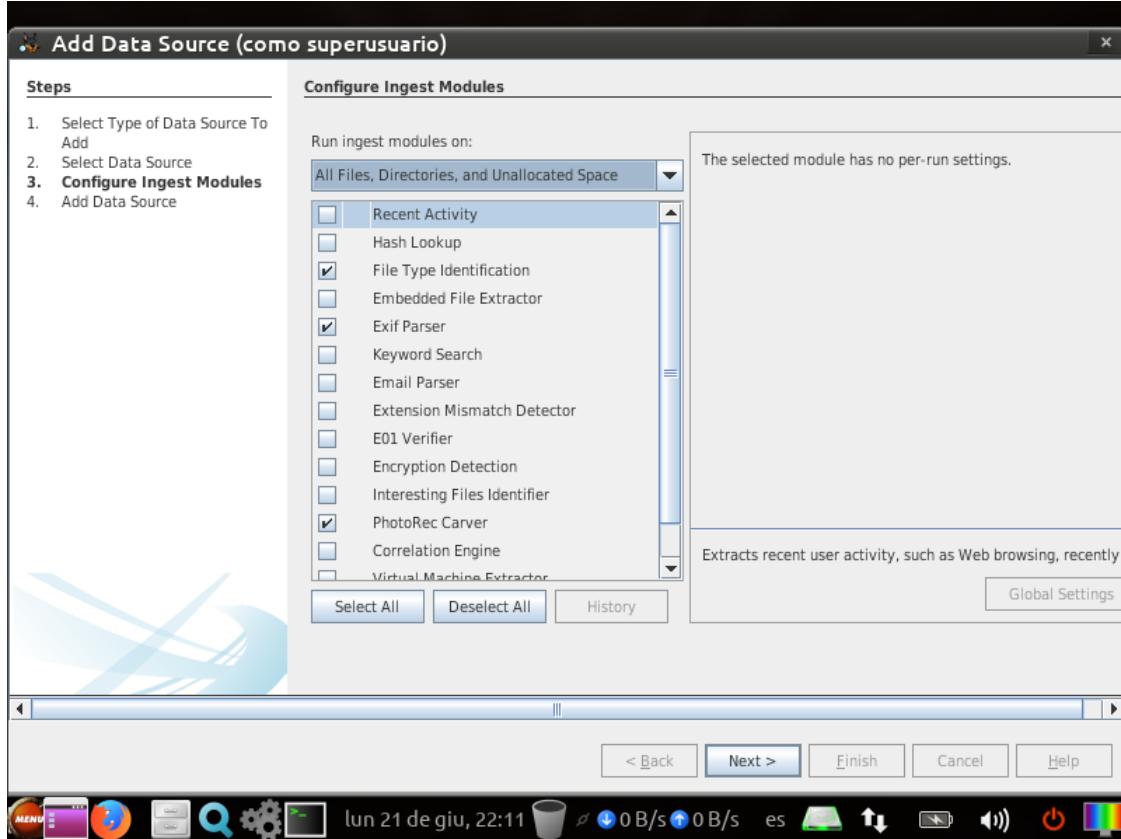
Añadimos la imagen a analizar.

Figura 27: Ejercicio 5: Selección de la imagen



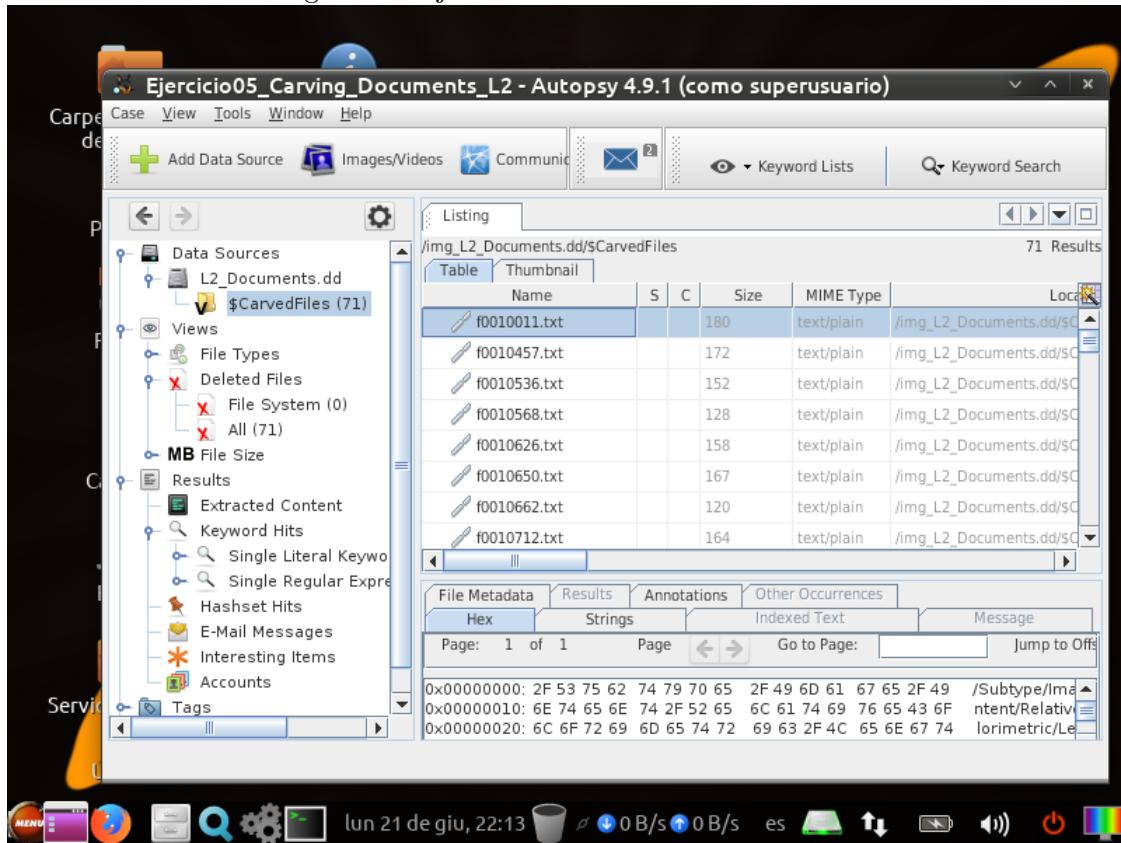
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

Figura 28: Ejercicio 5: Selección de módulos



Se ejecuta el análisis y se obtienen los resultados con los que se responderá a las preguntas.

Figura 29: Ejercicio 5: Resultados del análisis



- a) Hay 71 falsos positivos.
- b) Todos son de tipo texto plano.

Esto puede deberse a que Autopsy no haya sido capaz de recuperar los archivos con sus verdaderos tipos MIME y los fragmentos de esos archivos sean tratados como texto plano.

6. Ejercicio 6

Se crea el caso en Autopsy con los datos solicitados.

Figura 30: Ejercicio 6: Creación del caso

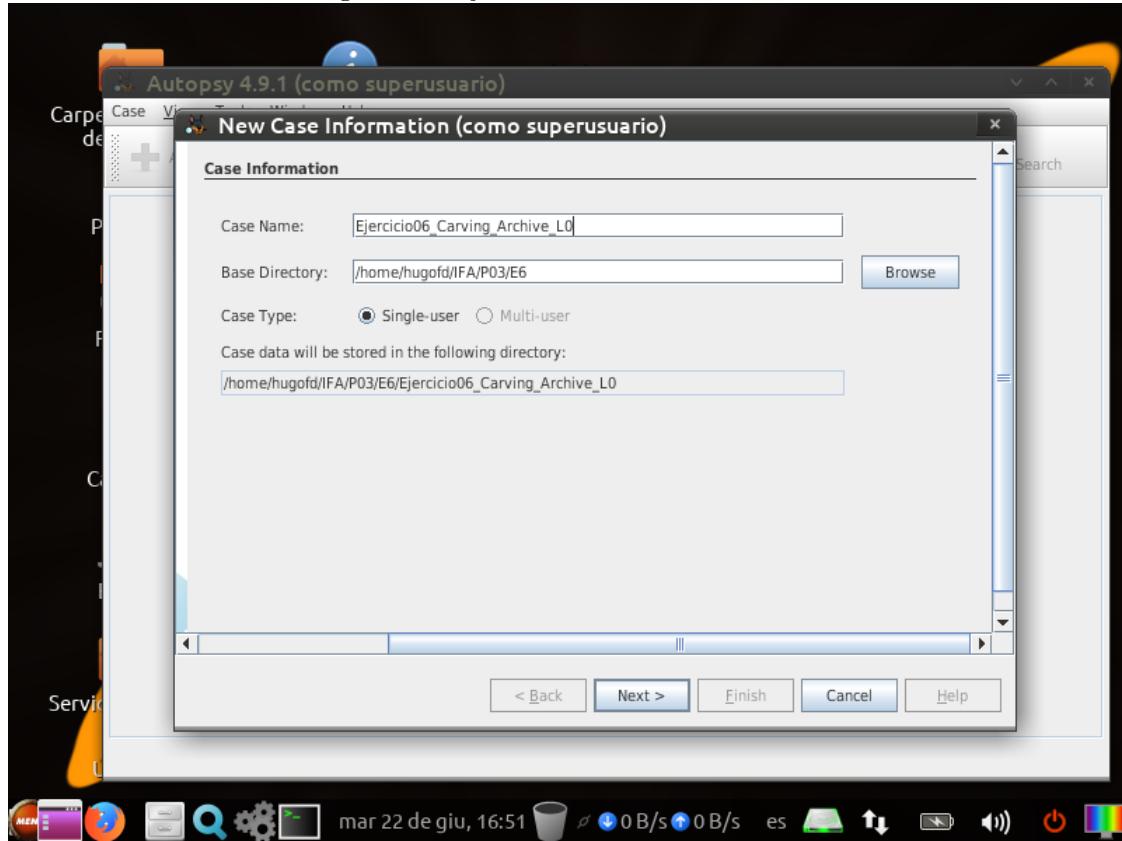
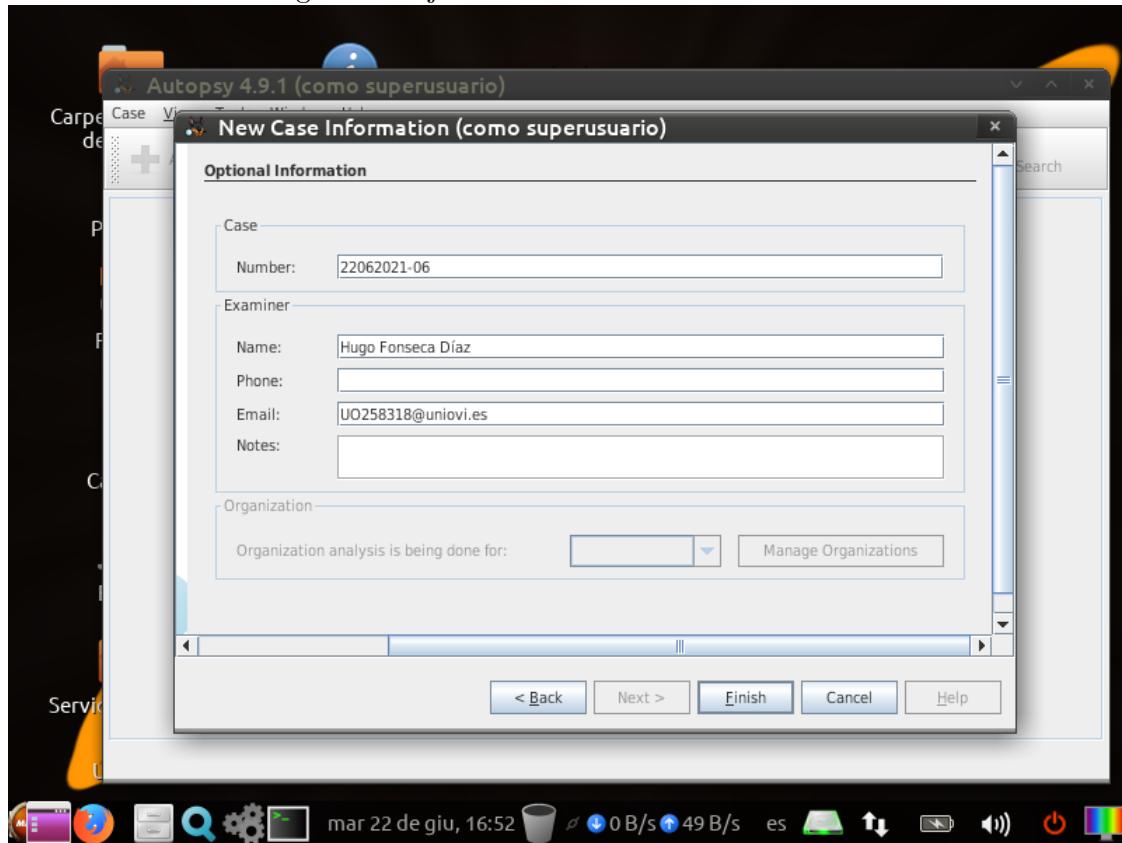
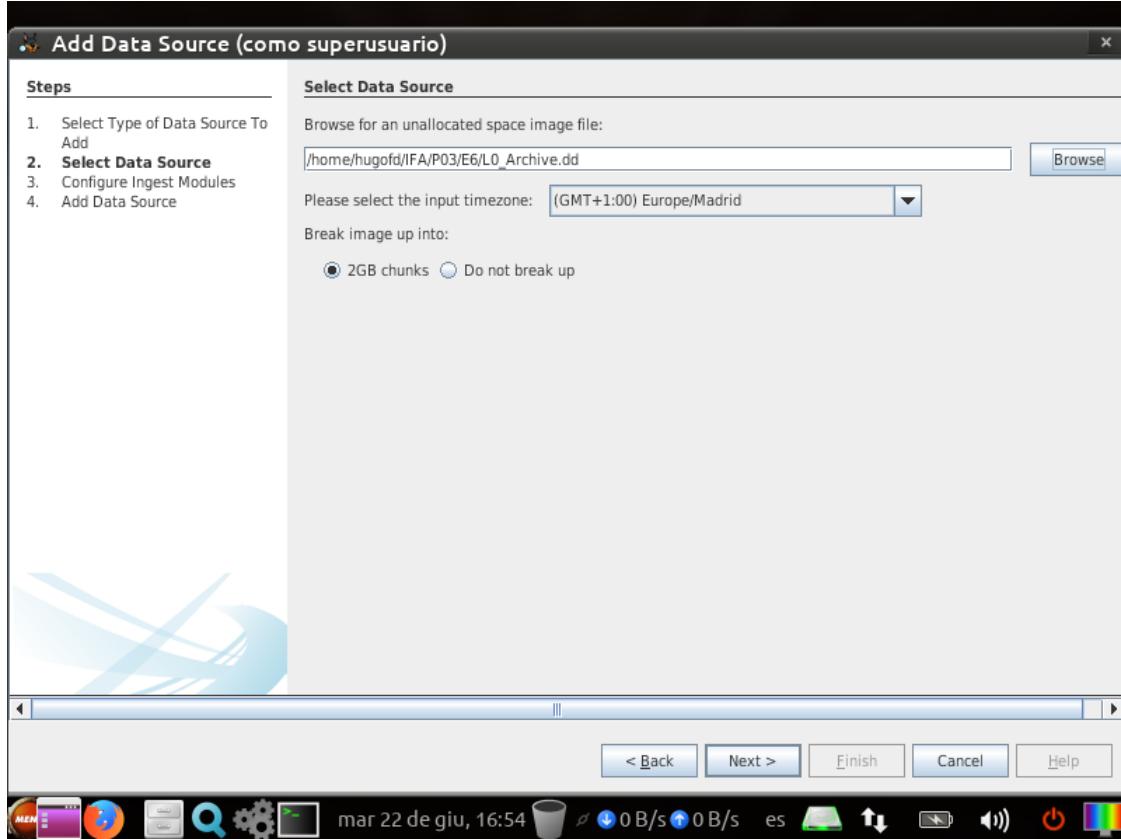


Figura 31: Ejercicio 6: Detalles del examinador



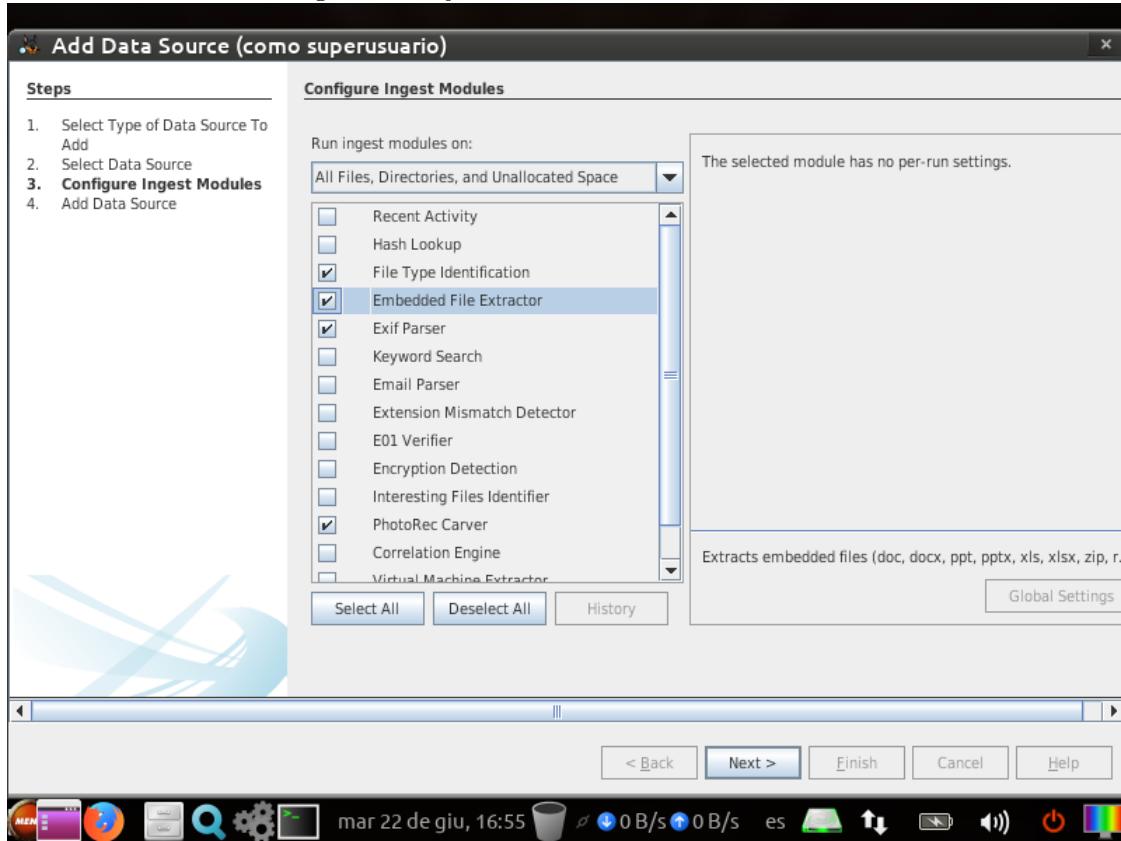
Añadimos la imagen a analizar.

Figura 32: Ejercicio 6: Selección de la imagen



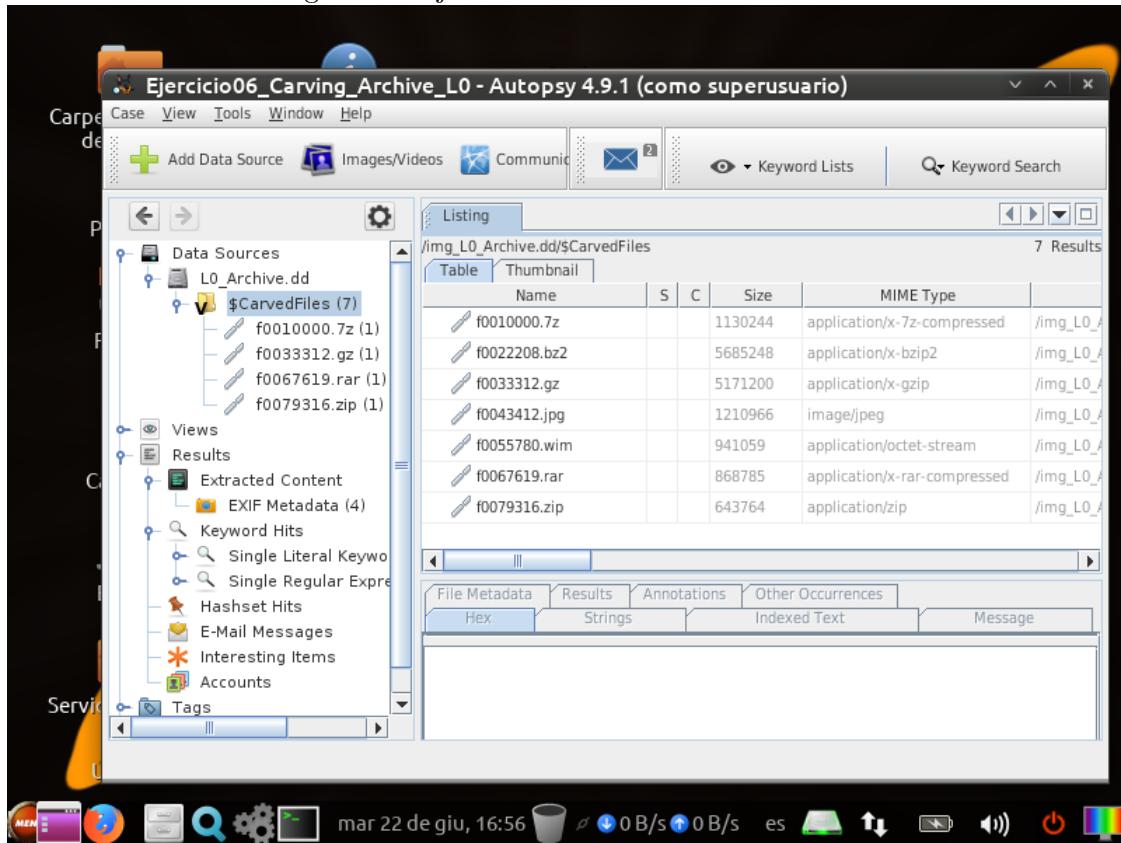
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif, *PhotoRec Carver* y el módulo de extracción de ficheros.

Figura 33: Ejercicio 6: Selección de módulos



Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

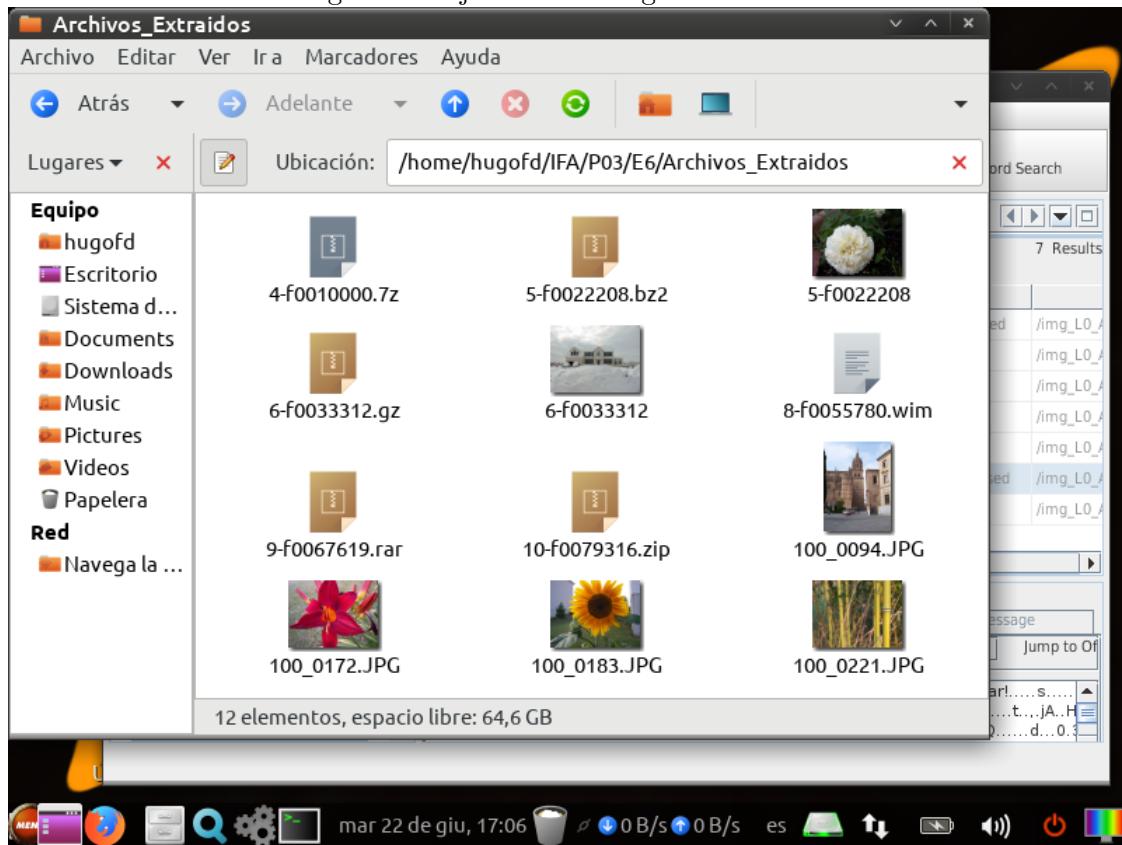
Figura 34: Ejercicio 6: Resultados del análisis



TBD table.

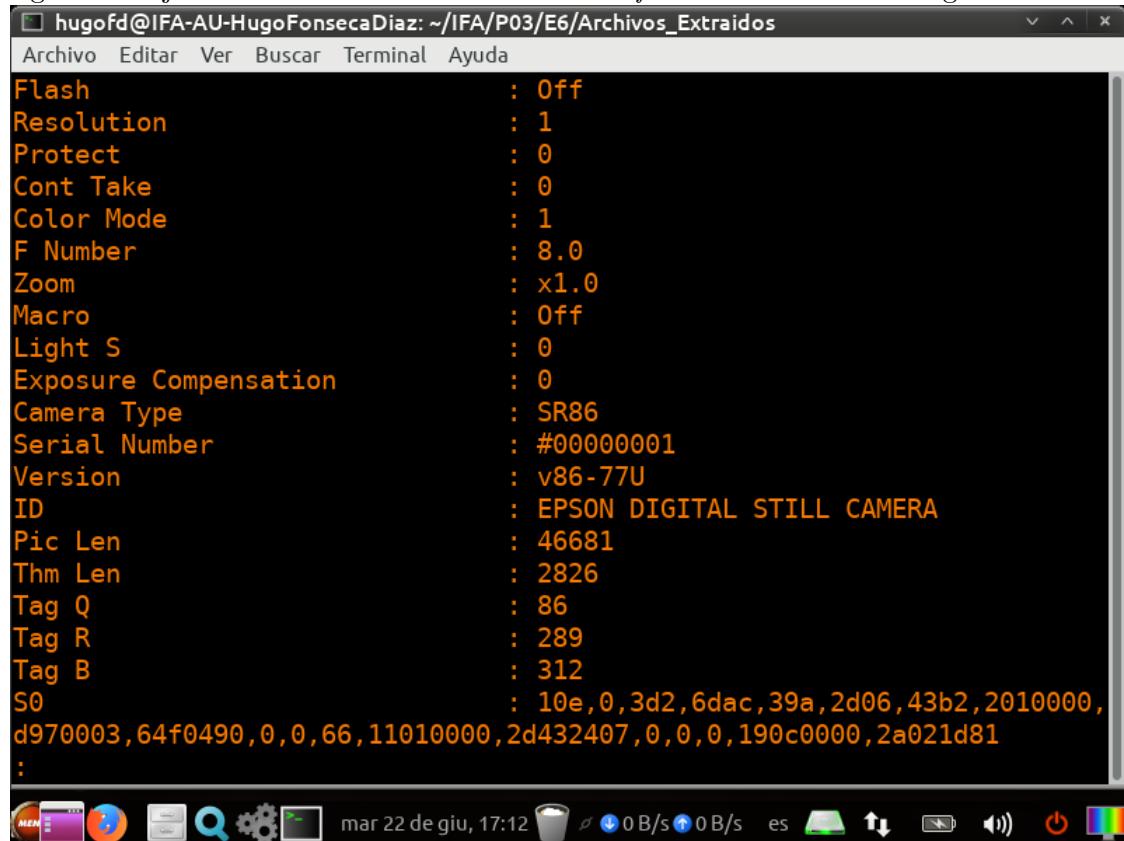
Se extraen las imágenes de los ficheros comprimidos.

Figura 35: Ejercicio 6: Imágenes extraídas



Se ejecuta la herramienta *exiftool* para obtener los datos que se usan a la hora de rellenar la siguiente tabla.

Figura 36: Ejercicio 6: Resultado del comando *exiftool* con una de las imágenes extraídas



The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P03/E6/Archivos_Extraidos". The window contains the output of the "exiftool" command, listing various camera settings and metadata. The output is as follows:

```
Flash : Off
Resolution : 1
Protect : 0
Cont Take : 0
Color Mode : 1
F Number : 8.0
Zoom : x1.0
Macro : Off
Light S : 0
Exposure Compensation : 0
Camera Type : SR86
Serial Number : #00000001
Version : v86-77U
ID : EPSON DIGITAL STILL CAMERA
Pic Len : 46681
Thm Len : 2826
Tag Q : 86
Tag R : 289
Tag B : 312
S0 : 10e,0,3d2,6dac,39a,2d06,43b2,2010000,
d970003,64f0490,0,0,66,11010000,2d432407,0,0,0,190c0000,2a021d81
:
```

The terminal window has a dark background and light-colored text. At the bottom, there is a taskbar with various icons and system status information.

TBD table.

7. Ejercicio 7

Se crea el caso en Autopsy con los datos solicitados.

Figura 37: Ejercicio 7: Creación del caso

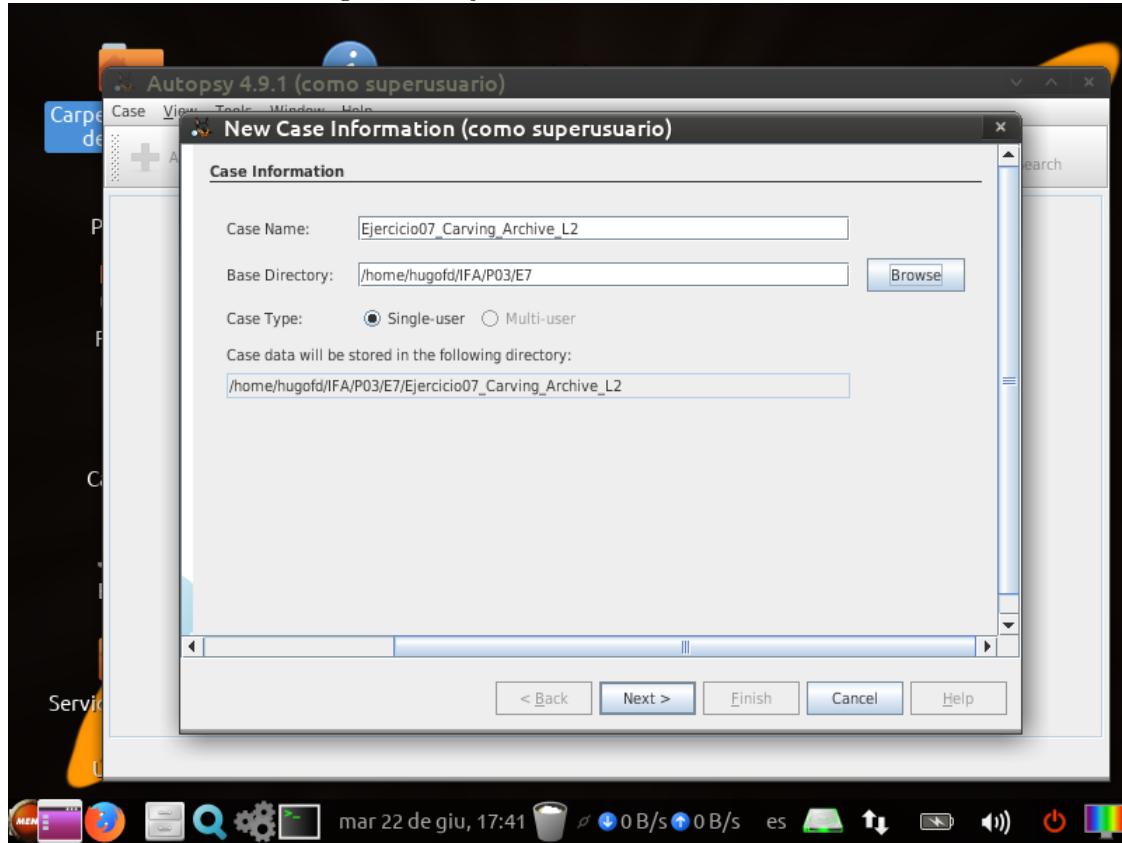
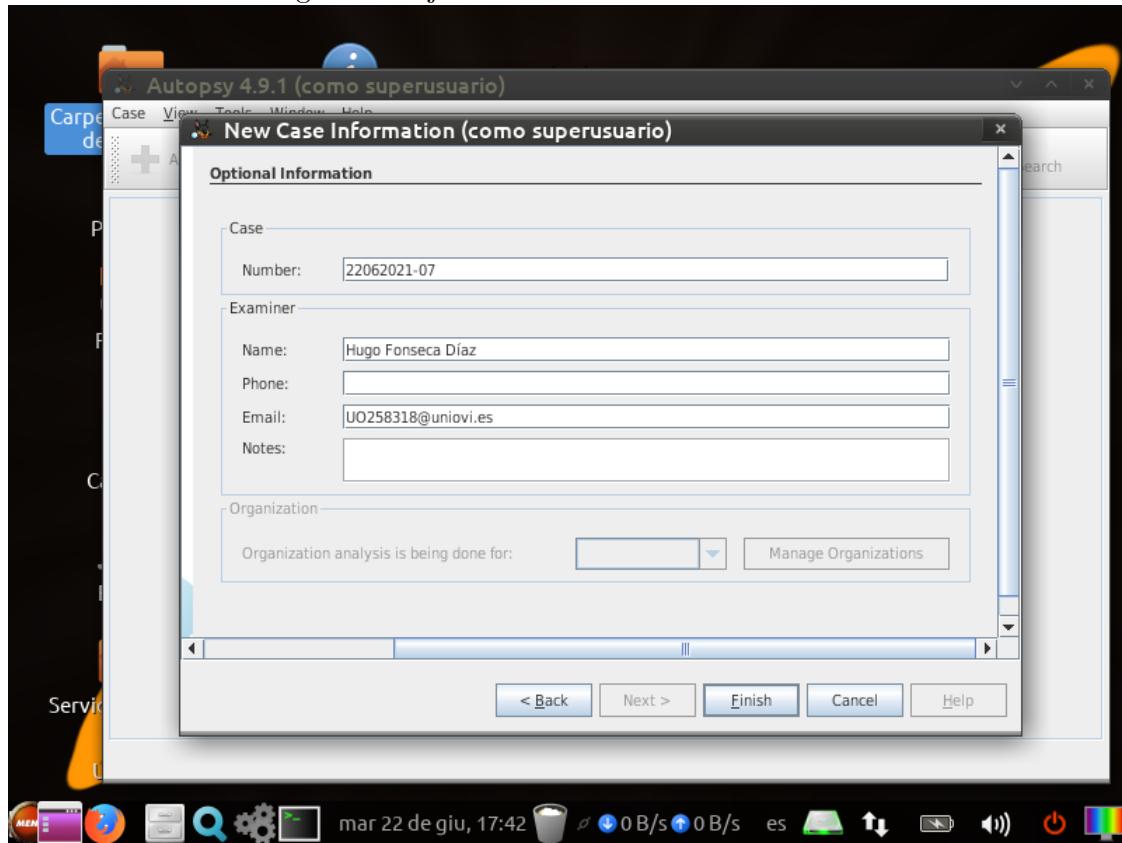
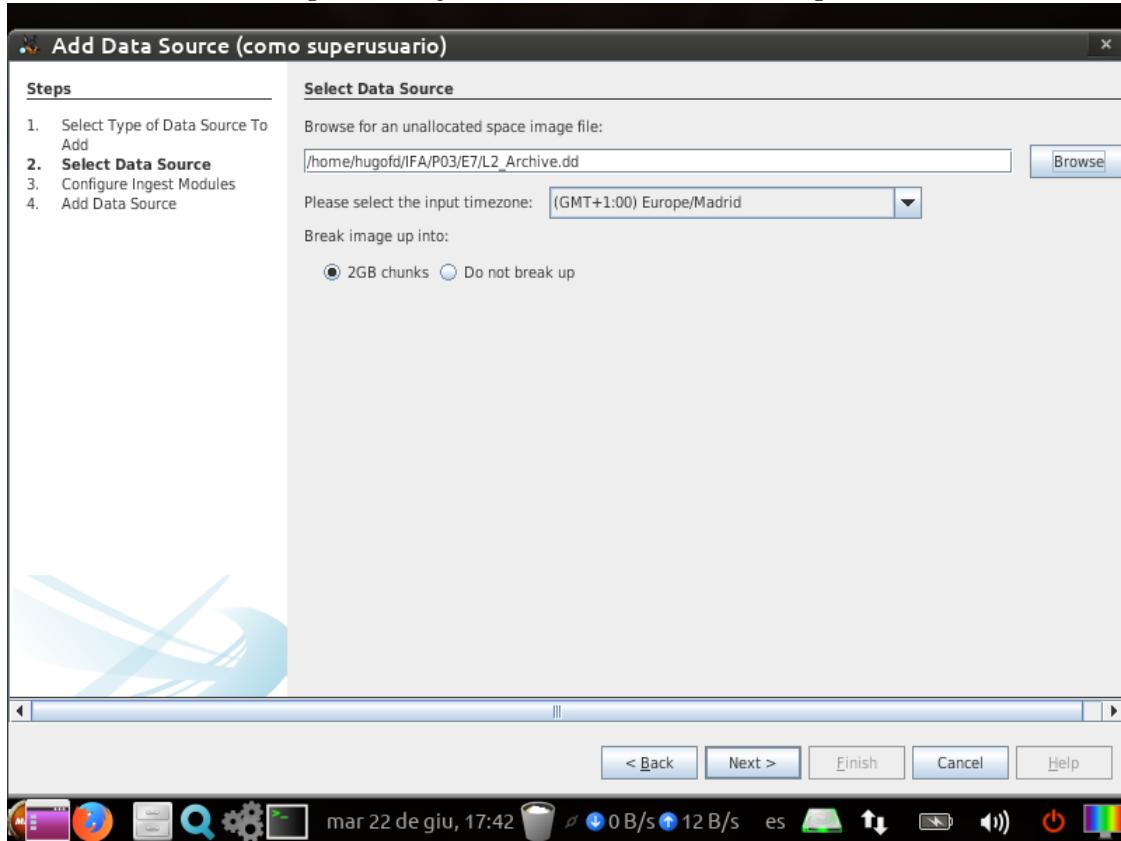


Figura 38: Ejercicio 7: Detalles del examinador



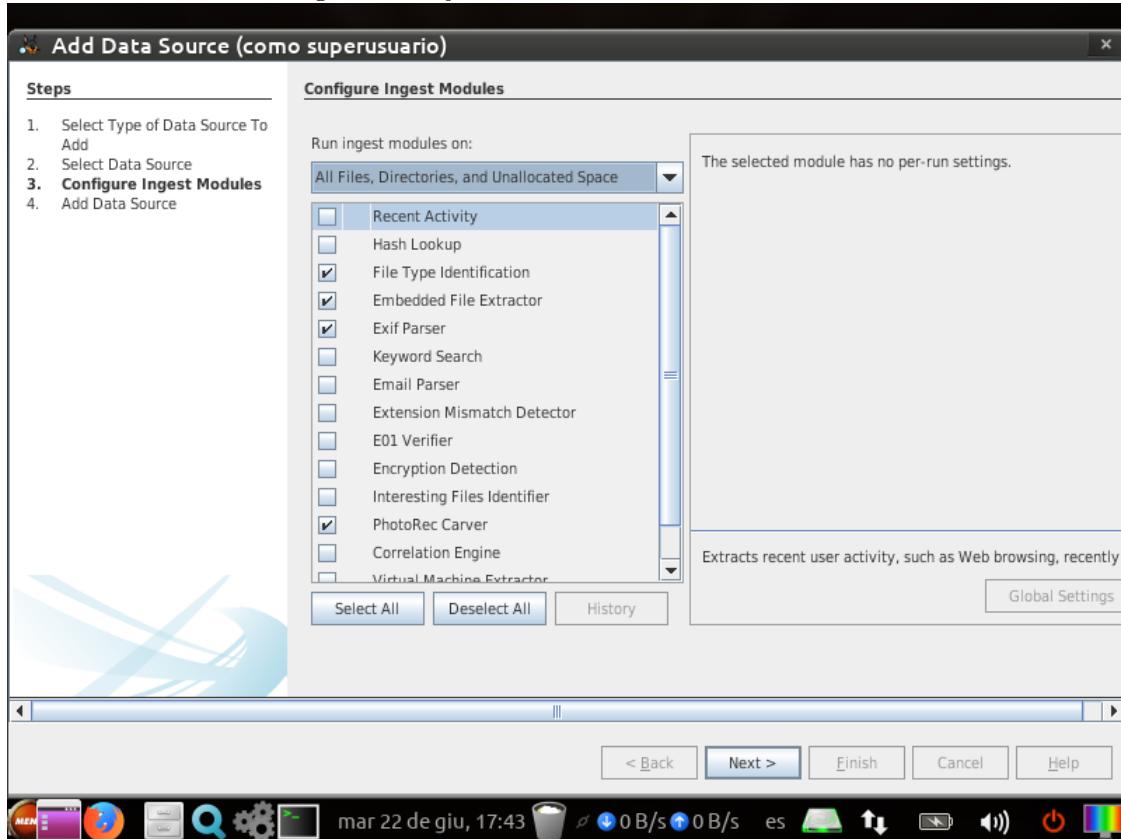
Añadimos la imagen a analizar.

Figura 39: Ejercicio 7: Selección de la imagen



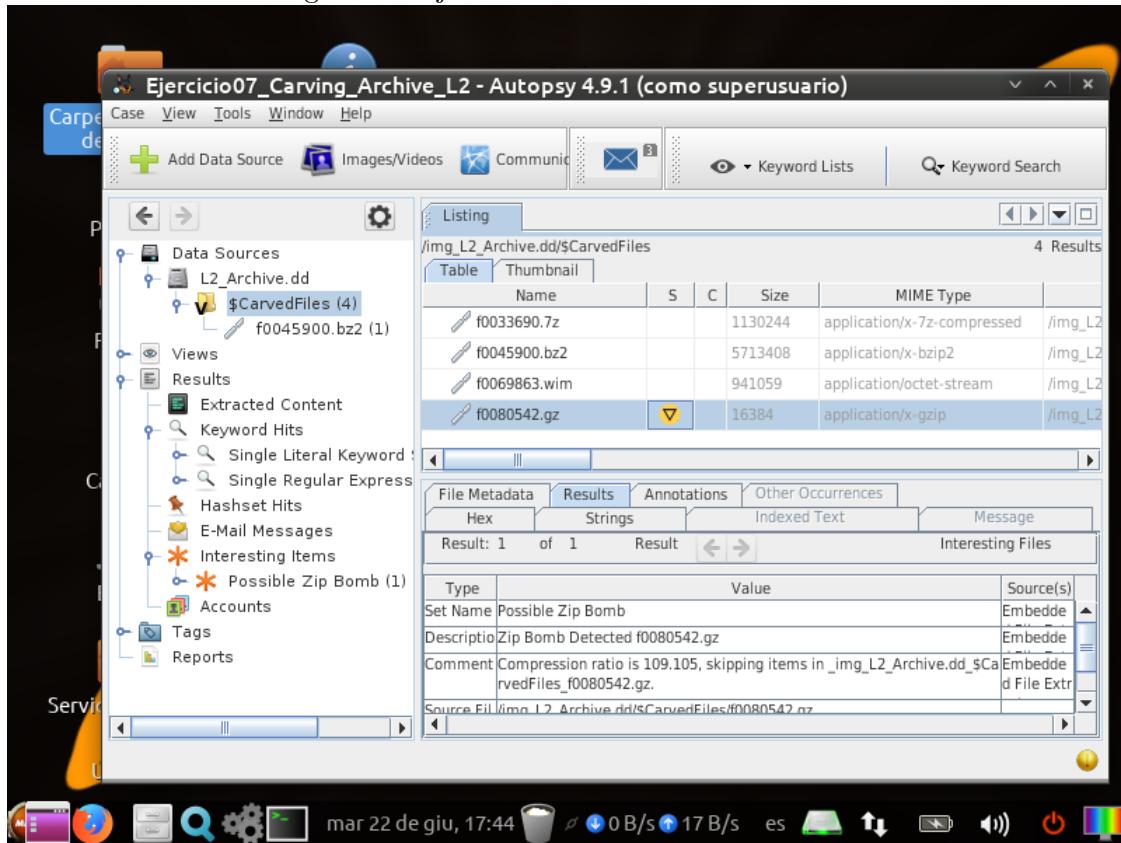
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif, *PhotoRec Carver* y el módulo de extracción de ficheros.

Figura 40: Ejercicio 7: Selección de módulos



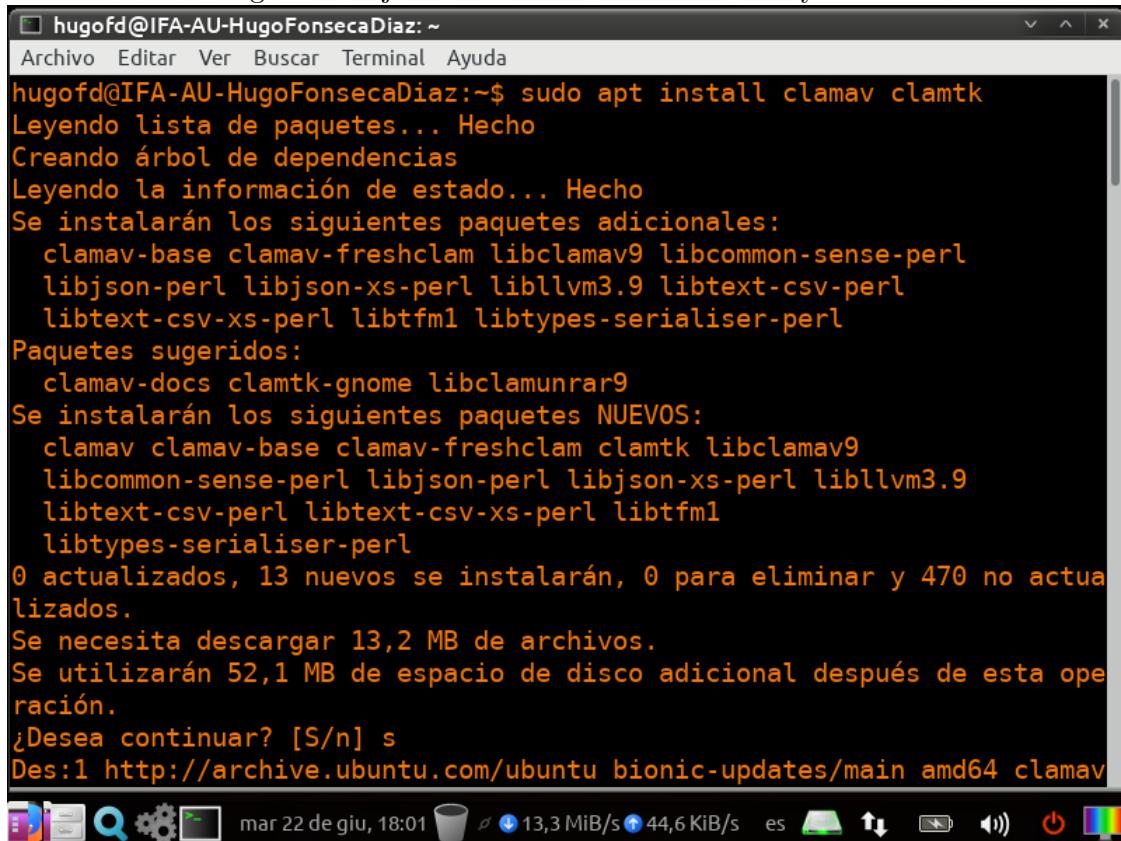
Se ejecuta el análisis y se observa que Autopsy ha detectado una posible bomba zip entre uno de los ficheros comprimidos.

Figura 41: Ejercicio 7: Resultados del análisis



Se instalan los paquetes *clamav* y *clamtk* y se analiza la carpeta donde se extrajeron los ficheros comprimidos.

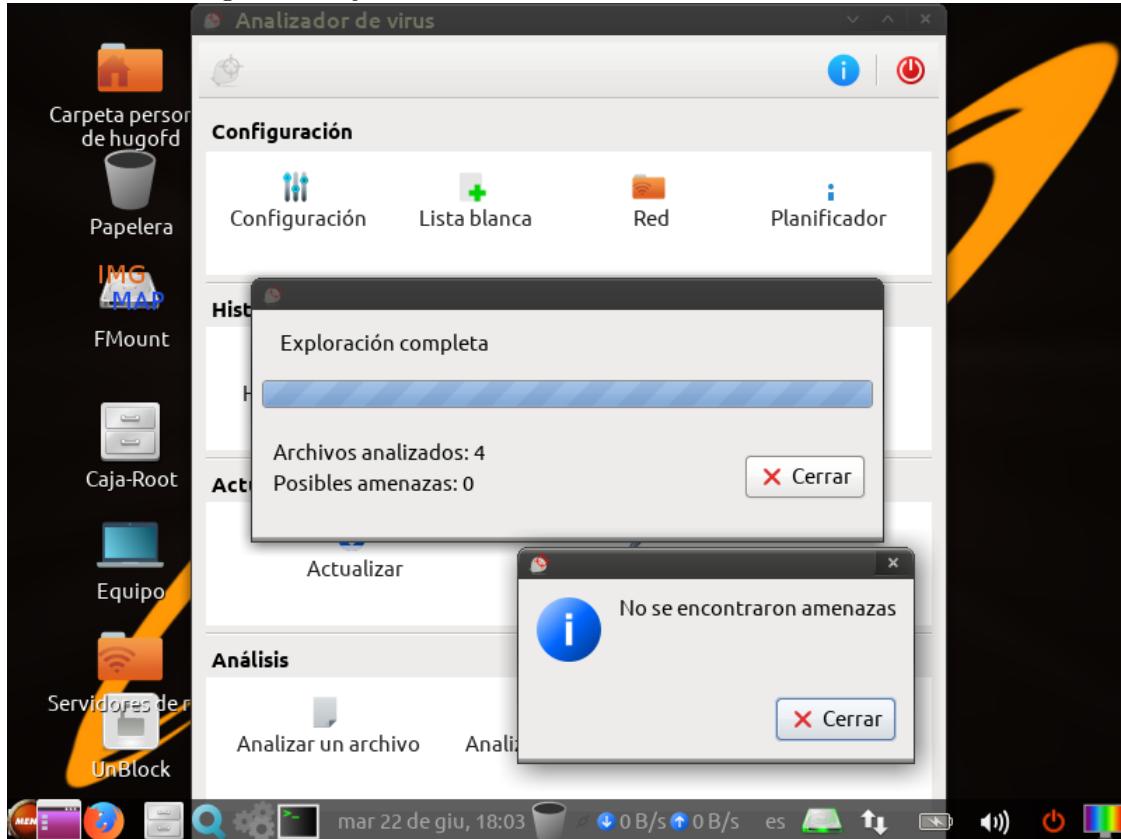
Figura 42: Ejercicio 7: Instalación de *clamav* y *clamtk*



```
hugofd@IFA-AU-HugoFonsecaDiaz: ~
Archivo Editar Ver Buscar Terminal Ayuda
hugofd@IFA-AU-HugoFonsecaDiaz:~$ sudo apt install clamav clamtk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  clamav-base clamav-freshclam libclamav9 libcommon-sense-perl
    libjson-perl libjson-xs-perl libllvm3.9 libtext-csv-perl
    libtext-csv-xs-perl libtfm1 libtypes-serialiser-perl
Paquetes sugeridos:
  clamav-docs clamtk-gnome libclamunrar9
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-freshclam clamtk libclamav9
    libcommon-sense-perl libjson-perl libjson-xs-perl libllvm3.9
    libtext-csv-perl libtext-csv-xs-perl libtfm1
    libtypes-serialiser-perl
0 actualizados, 13 nuevos se instalarán, 0 para eliminar y 470 no actualizados.
Se necesita descargar 13,2 MB de archivos.
Se utilizarán 52,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 clamav

```

Figura 43: Ejercicio 7: Resultados del análisis del antivirus



- a) El antivirus no detecta nada, pero Autopsy si que notificó que uno de los ficheros podía ser una bomba zip. Este es un ataque que comprime con una alta proporción una gran cantidad de datos en un archivo comprimido de pocos datos. Sirve para inutilizar los programas que descomprimen dicho fichero, normalmente se busca inutilizar un antivirus, para luego ejecutar otro tipo de malware.
- b) Bomba zip.

8. Ejercicio 8

Se crea el caso en Autopsy con los datos solicitados.

Figura 44: Ejercicio 8: Creación del caso

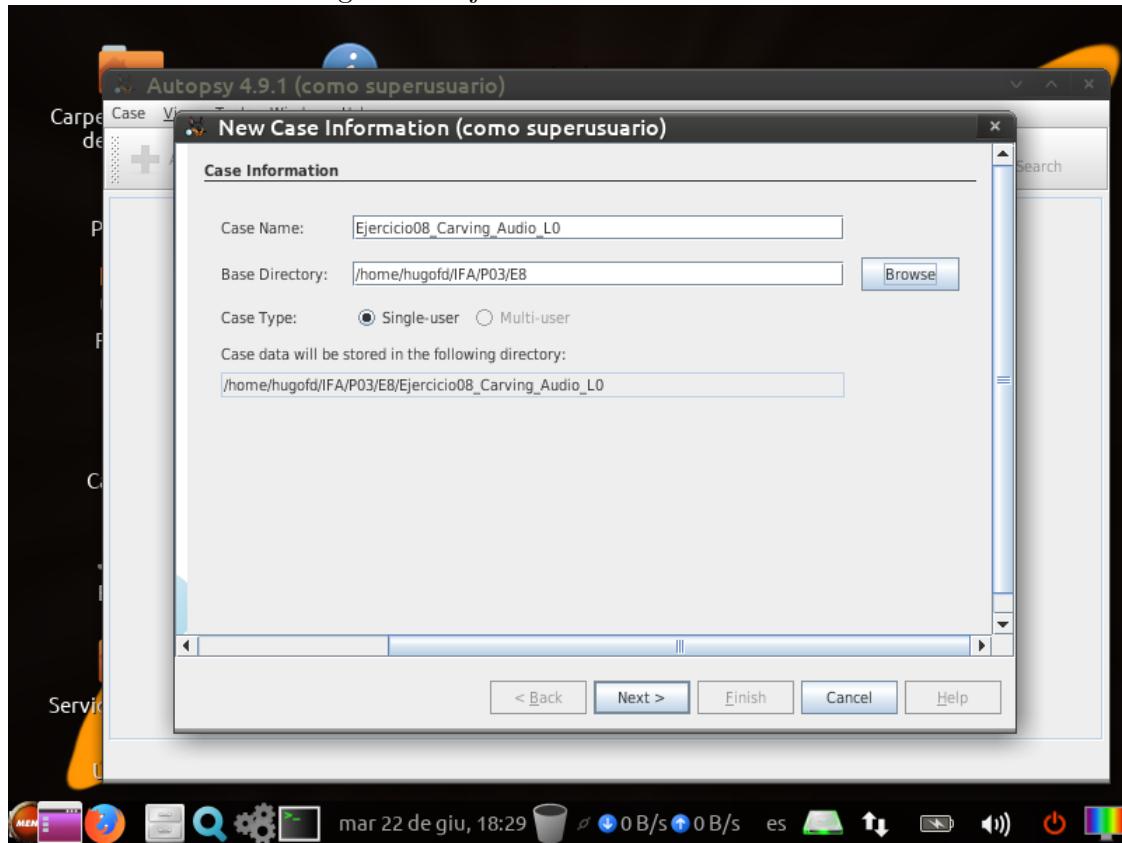
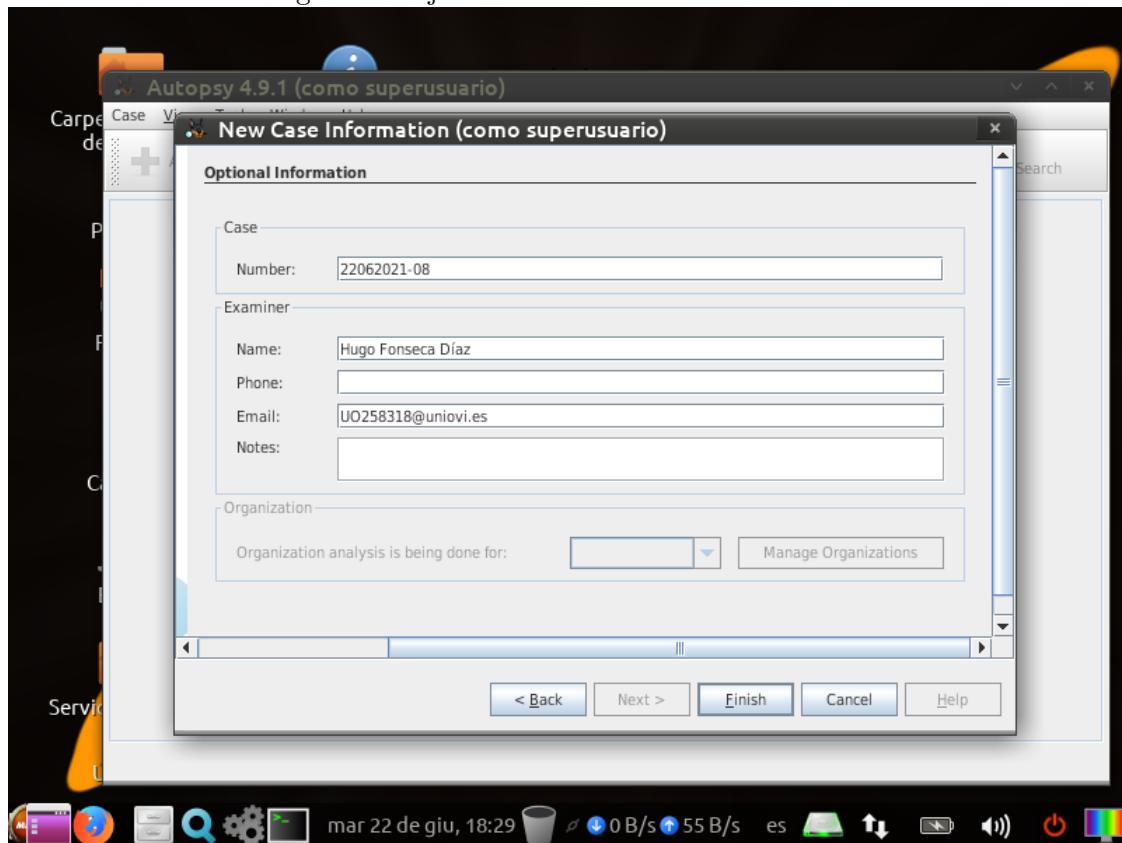
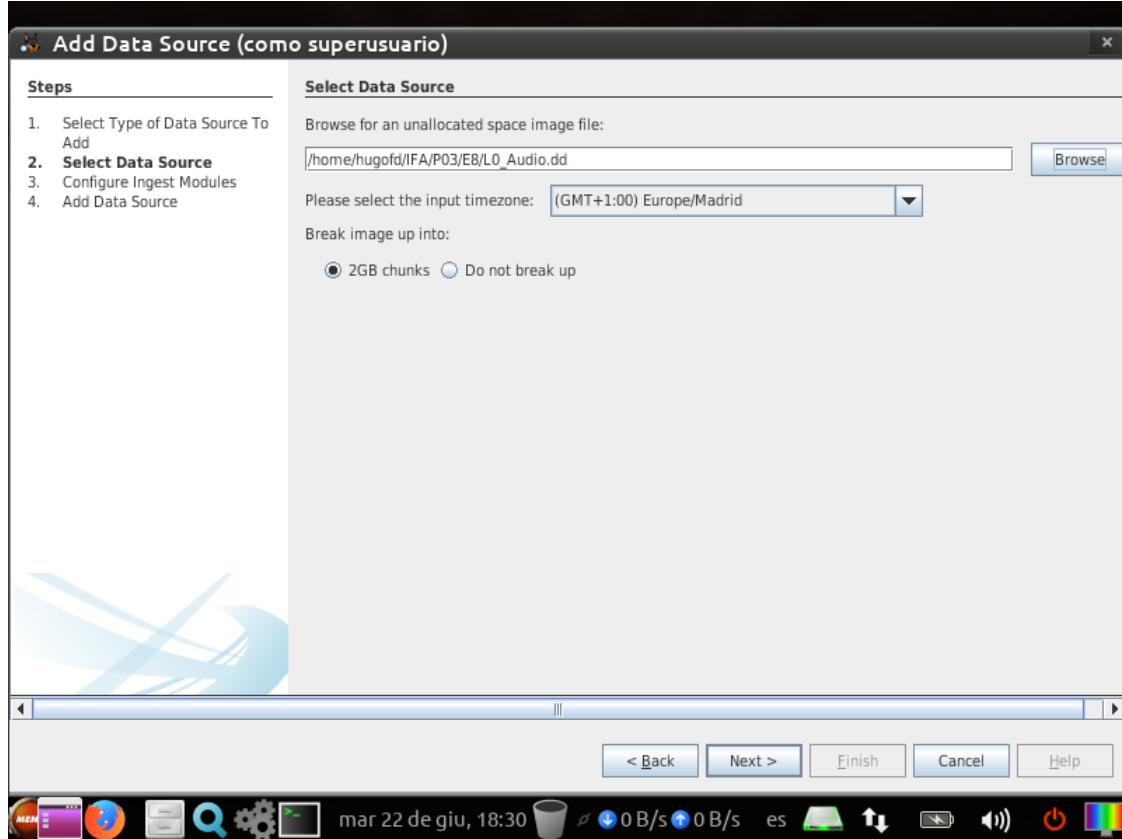


Figura 45: Ejercicio 8: Detalles del examinador



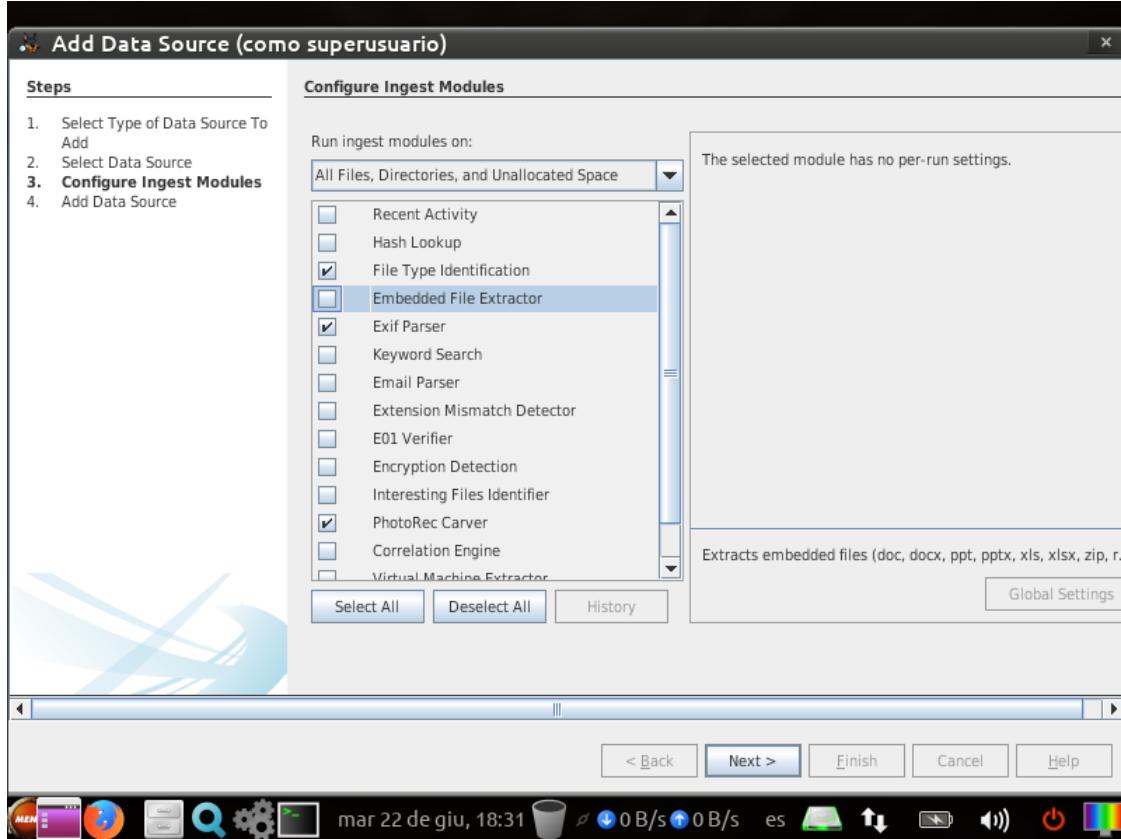
Añadimos la imagen a analizar.

Figura 46: Ejercicio 8: Selección de la imagen



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

Figura 47: 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 48: Ejercicio 8: Resultados del análisis

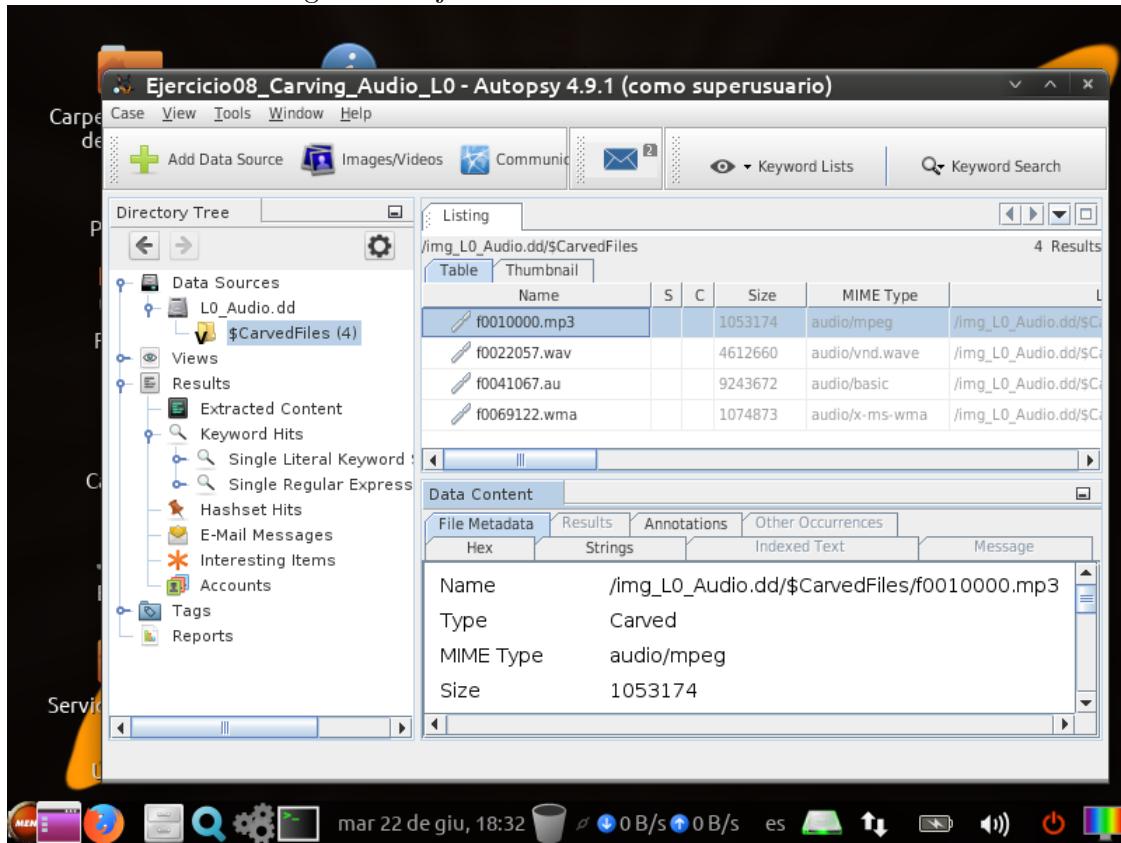
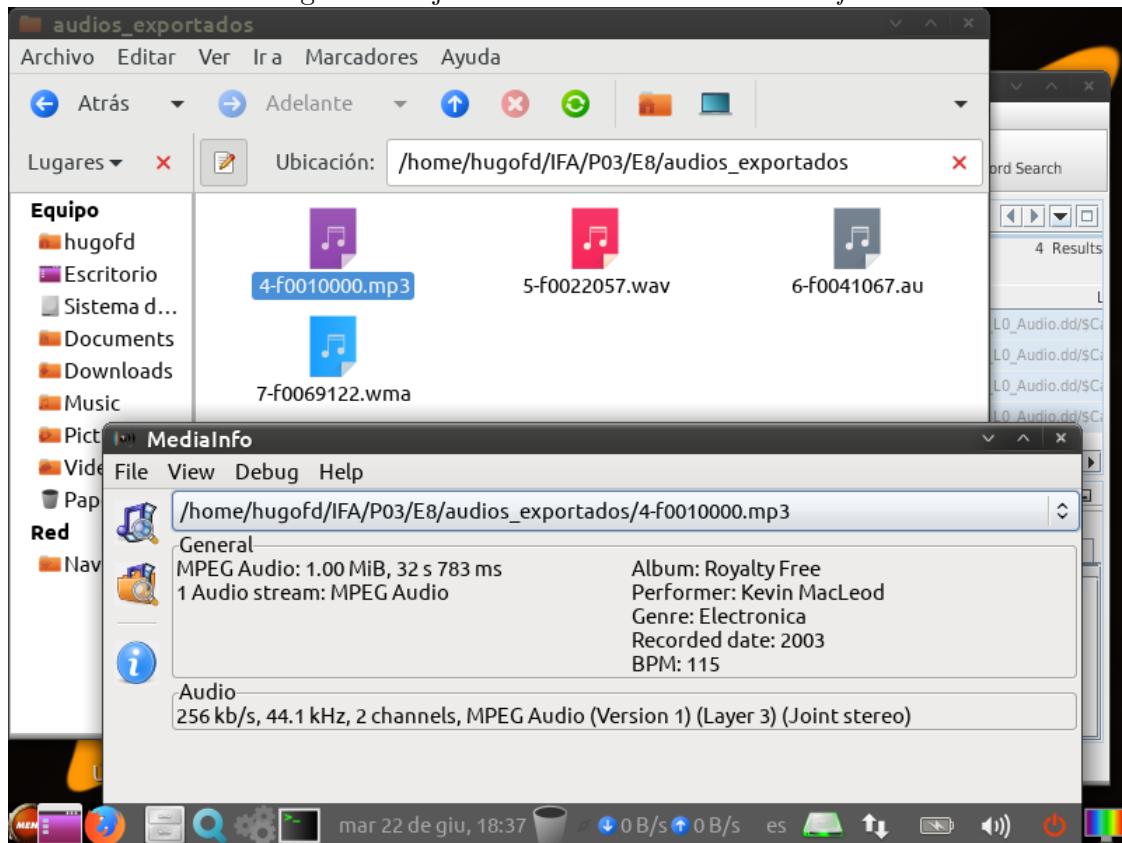


Figura 49: Ejercicio 8: Herramienta *MediaInfo*



TBD table.

9. Ejercicio 9

Se crea el caso en Autopsy con los datos solicitados.

Figura 50: Ejercicio 9: Creación del caso

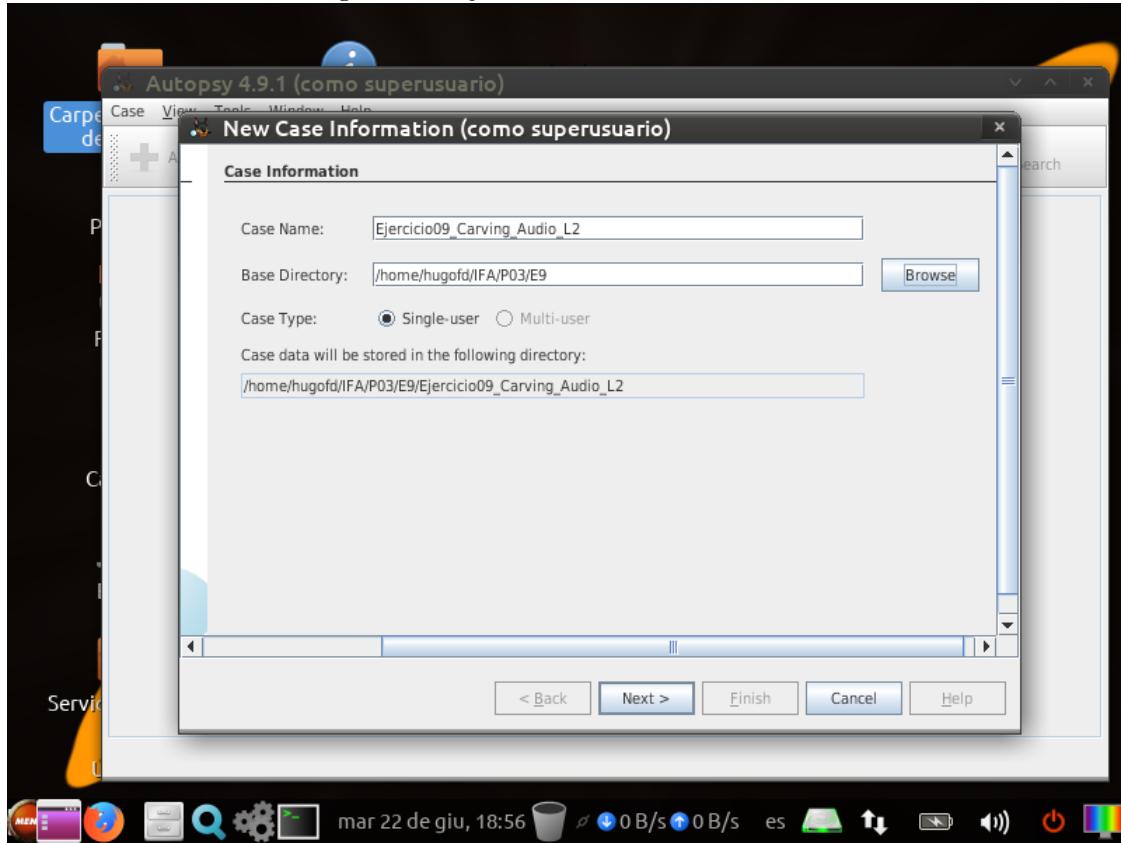
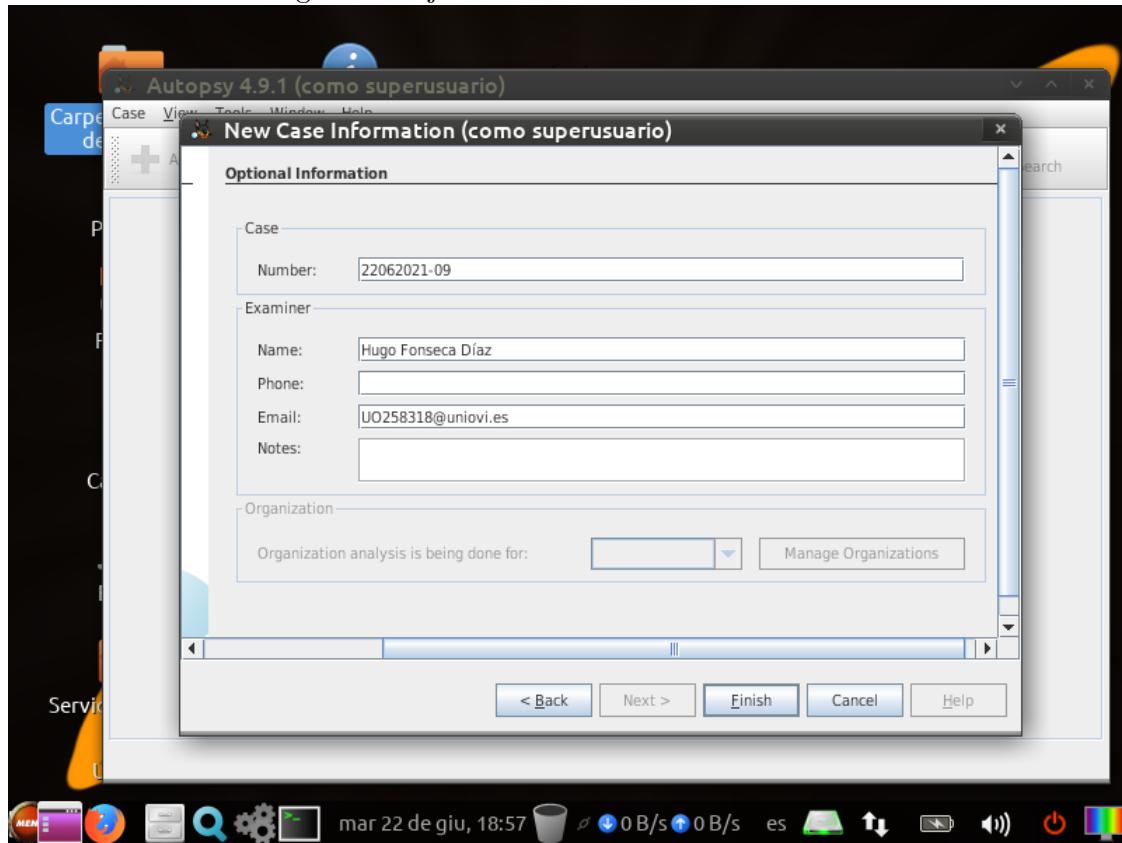
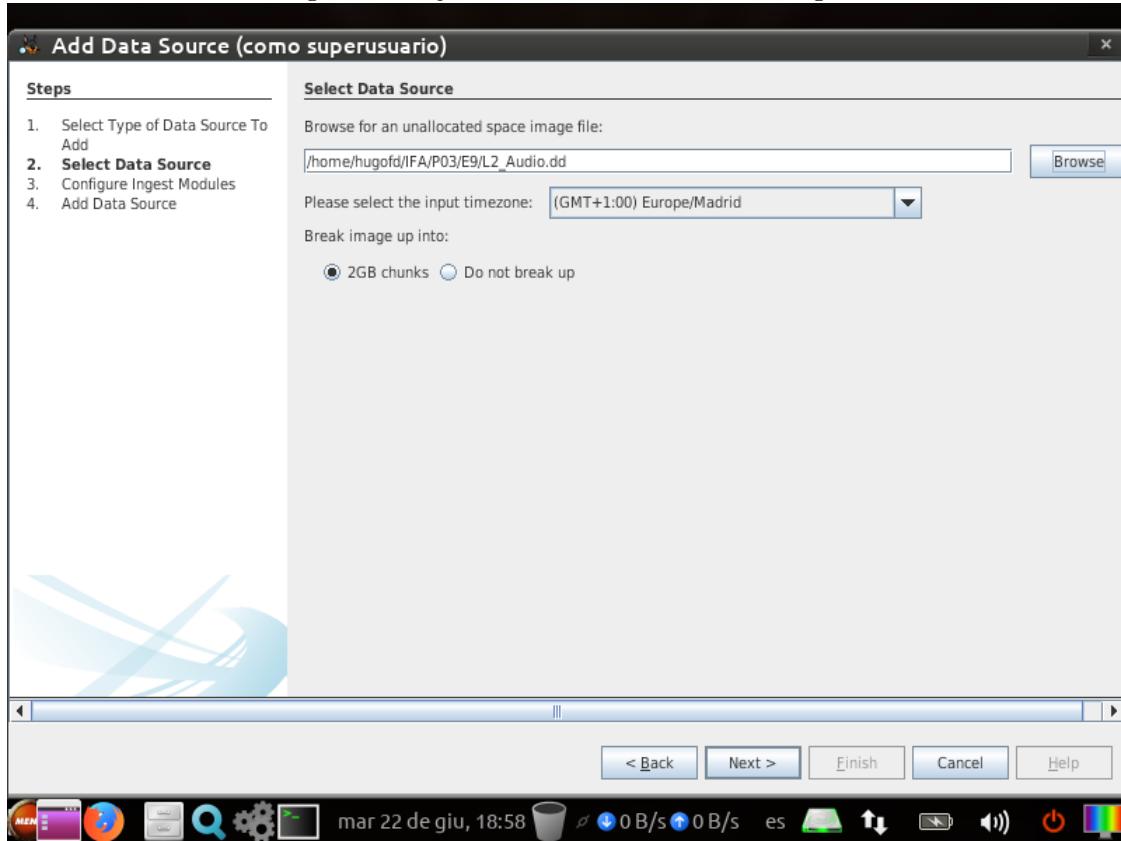


Figura 51: Ejercicio 9: Detalles del examinador



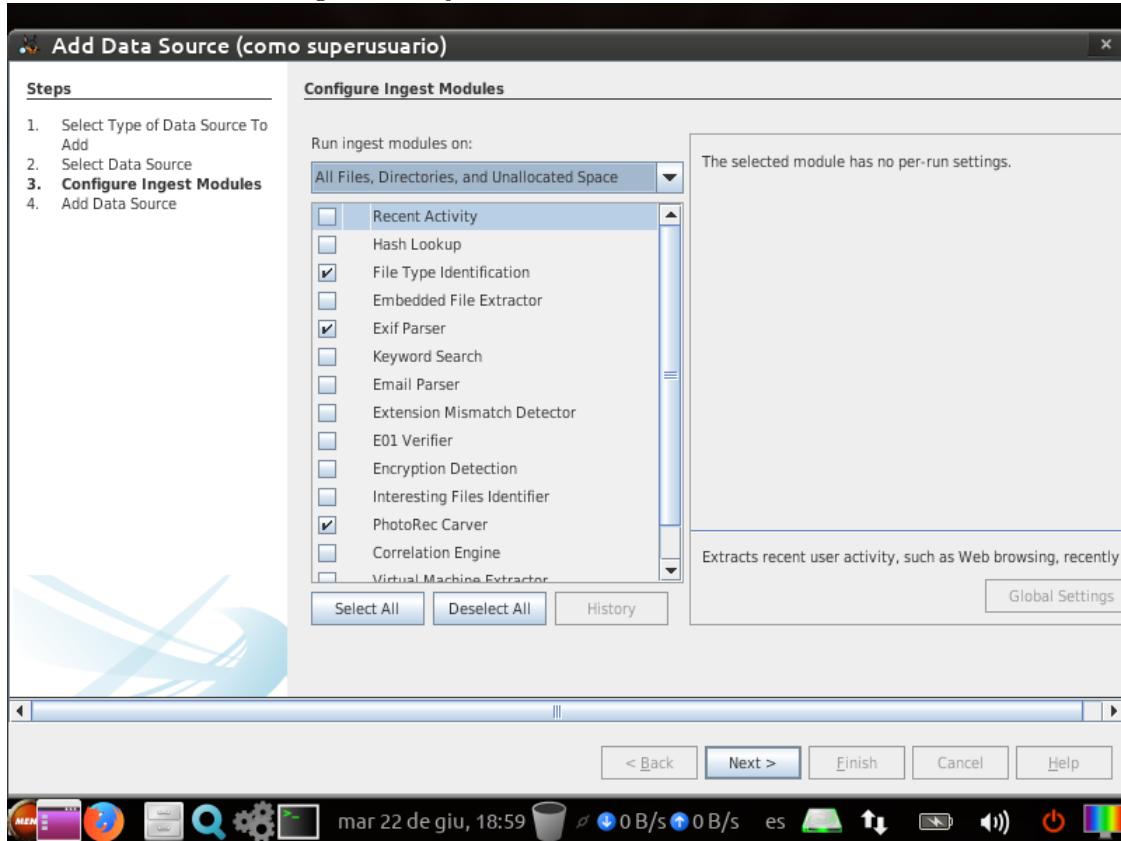
Añadimos la imagen a analizar.

Figura 52: Ejercicio 9: Selección de la imagen



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

Figura 53: Ejercicio 9: 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 54: Ejercicio 9: Resultados del análisis

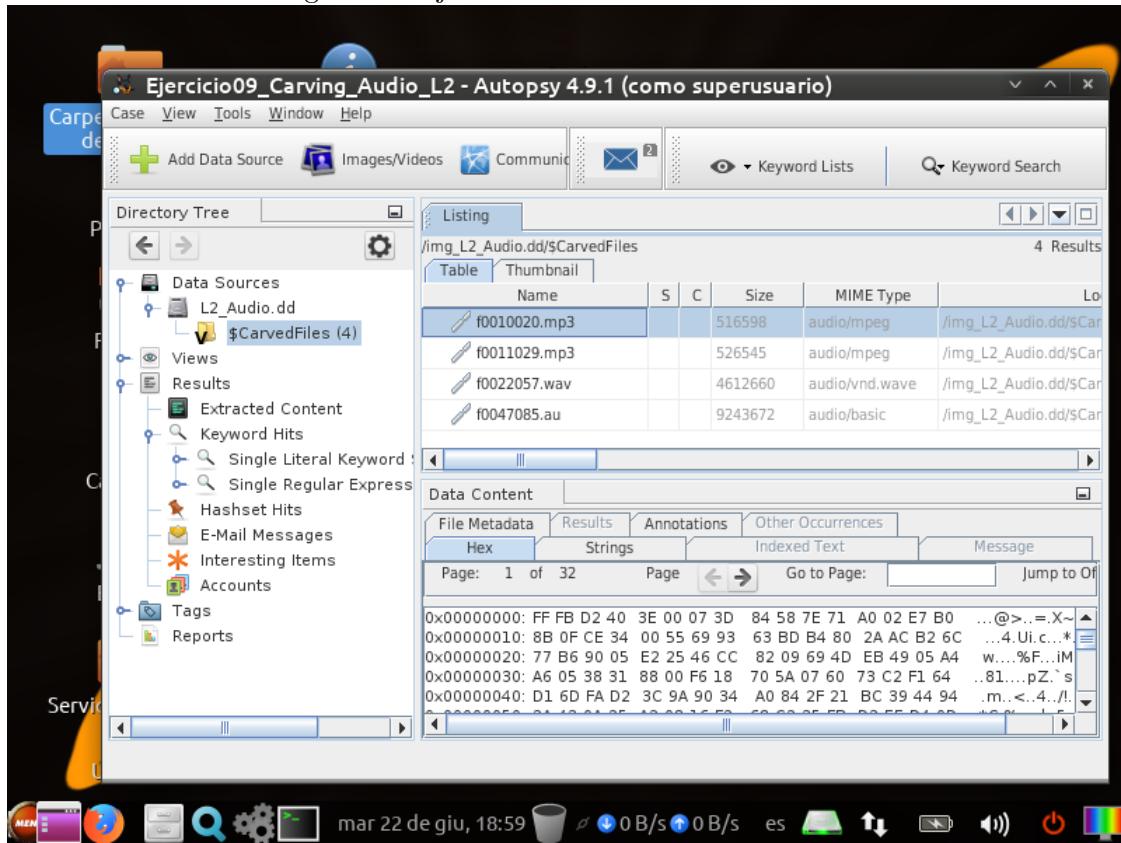
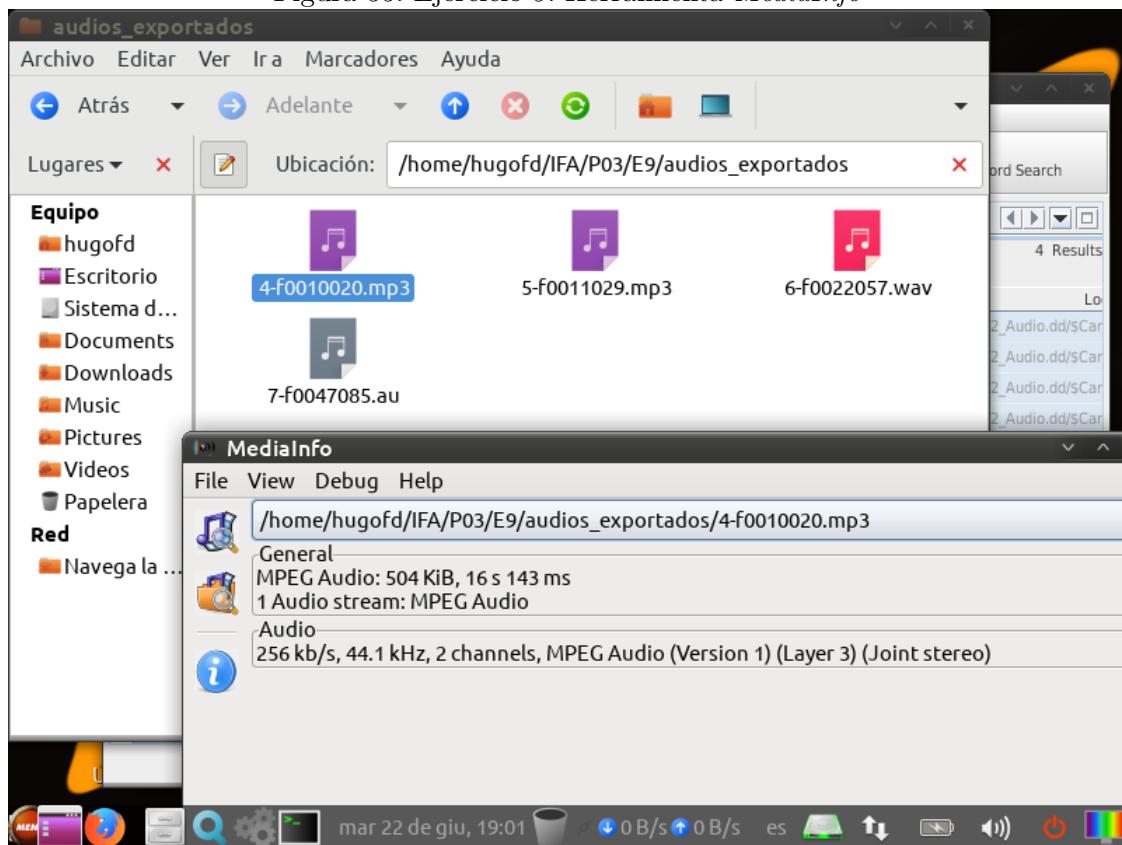


Figura 55: Ejercicio 9: Herramienta *MediaInfo*



TBD table.

Referencias