IFA. Práctica de laboratorio 03

Hugo Fonseca Díaz
email uo258318@uniovi.es

Escuela de Ingeniería Informática. Universidad de Oviedo.

21 de junio de 2021

1. Ejercicio 1

Se crea el caso en Autopsy con los datos solicitados.

Figura 1: Ejercicio 1: Creación del caso

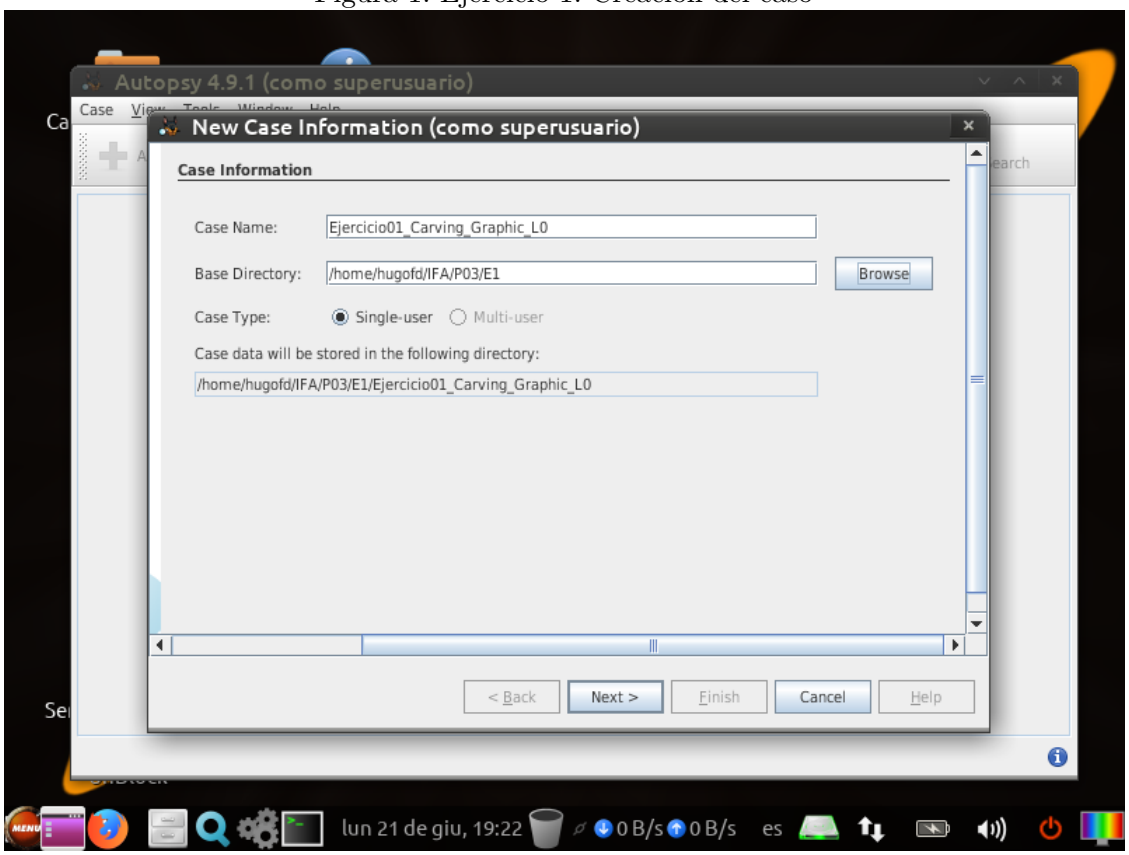
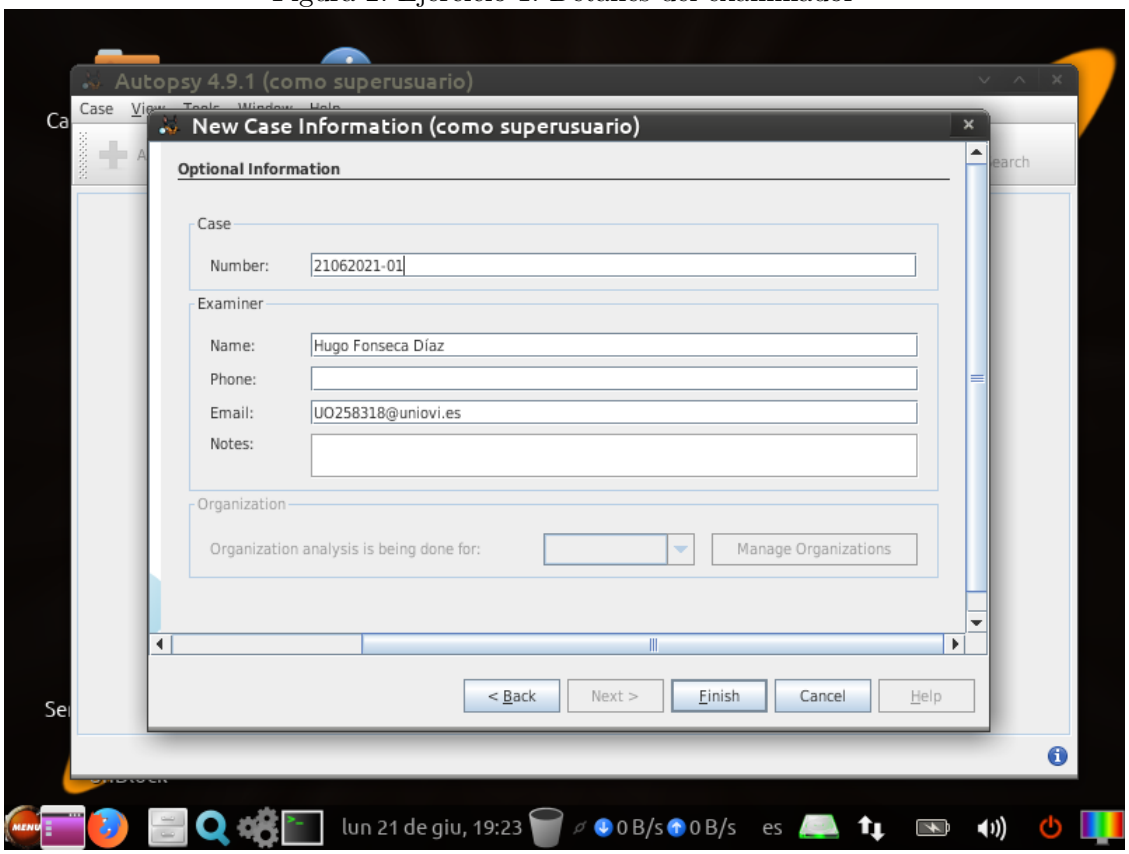
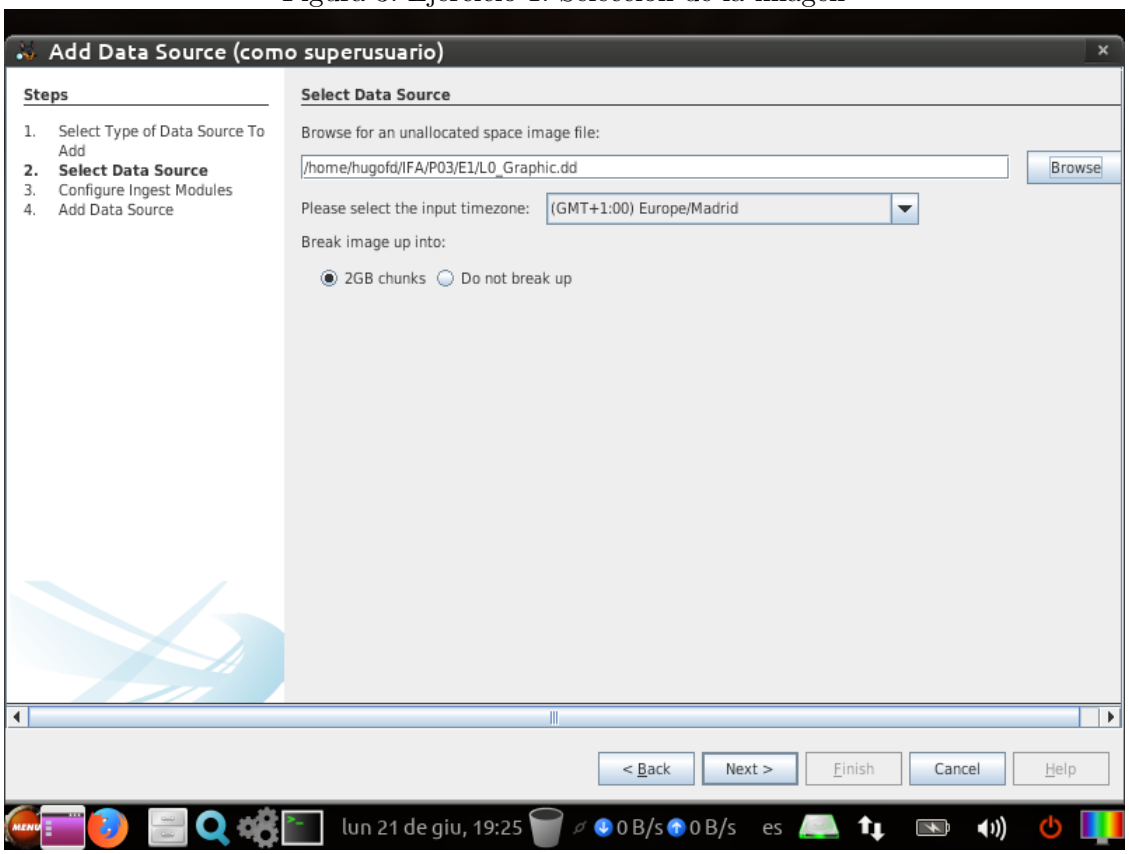


Figura 2: Ejercicio 1: Detalles del examinador



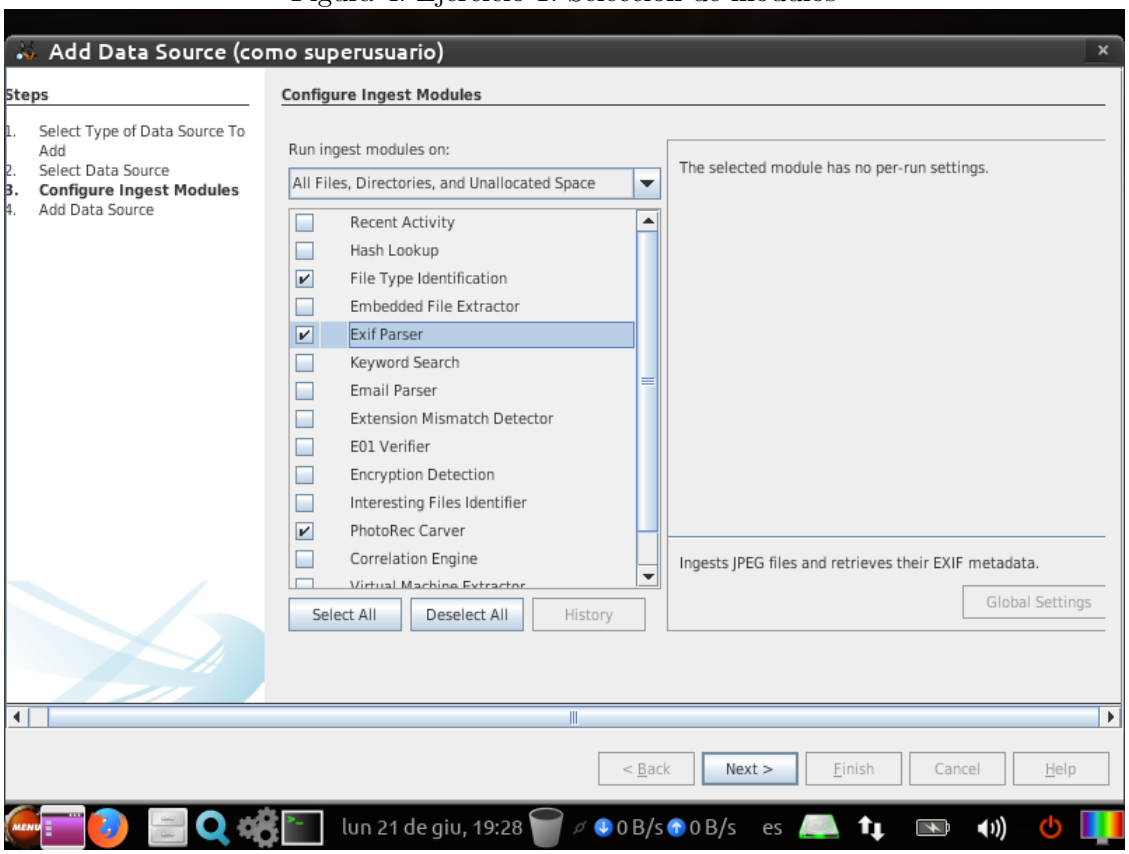
Añadimos la imagen a analizar.

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

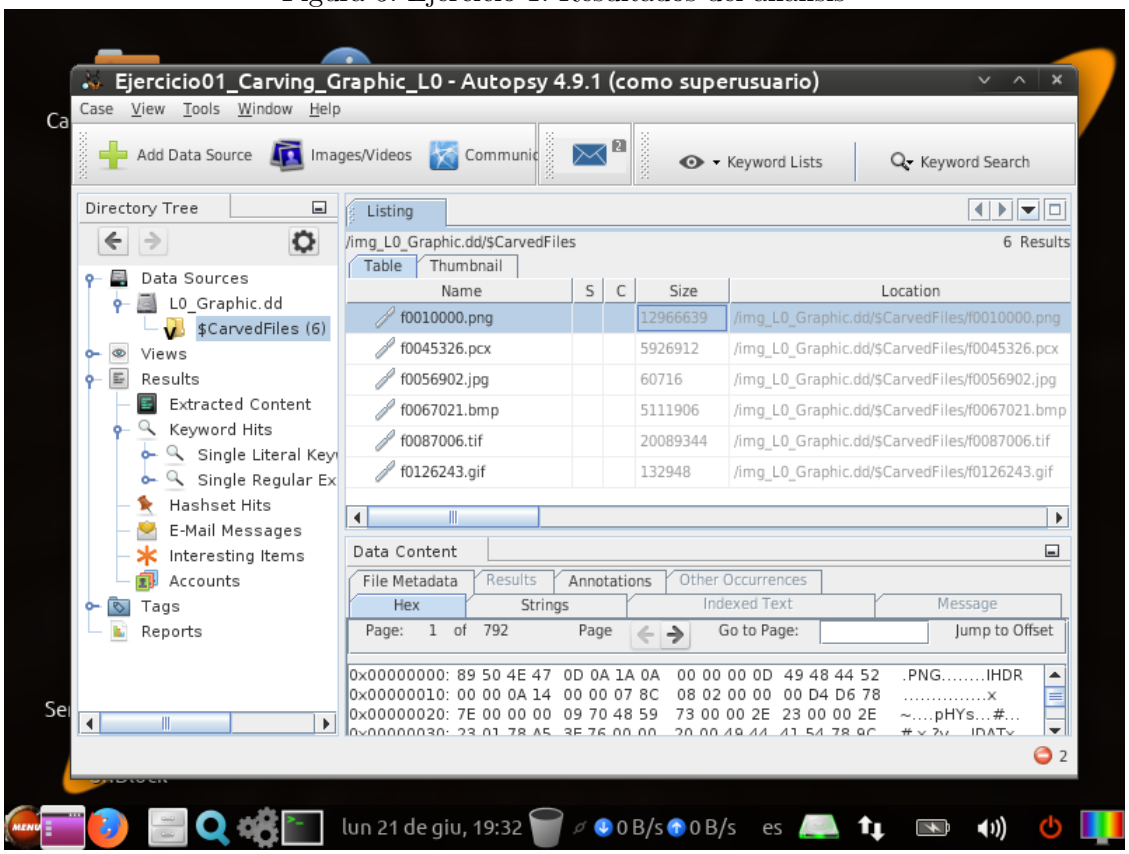
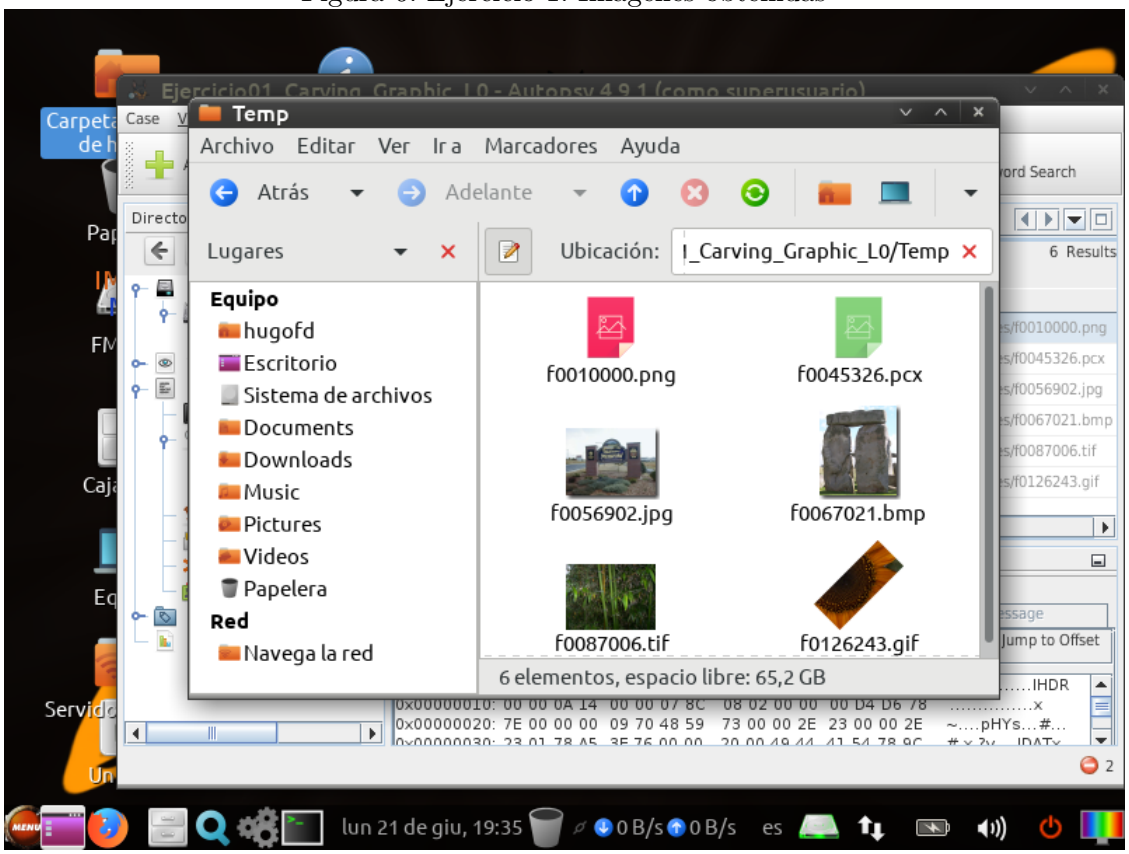


Figura 6: Ejercicio 1: Imágenes obtenidas



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

TBD: tabla

2. Ejercicio 2

Se crea el caso en Autopsy con los datos solicitados.

Figura 7: Ejercicio 2: Creación del caso

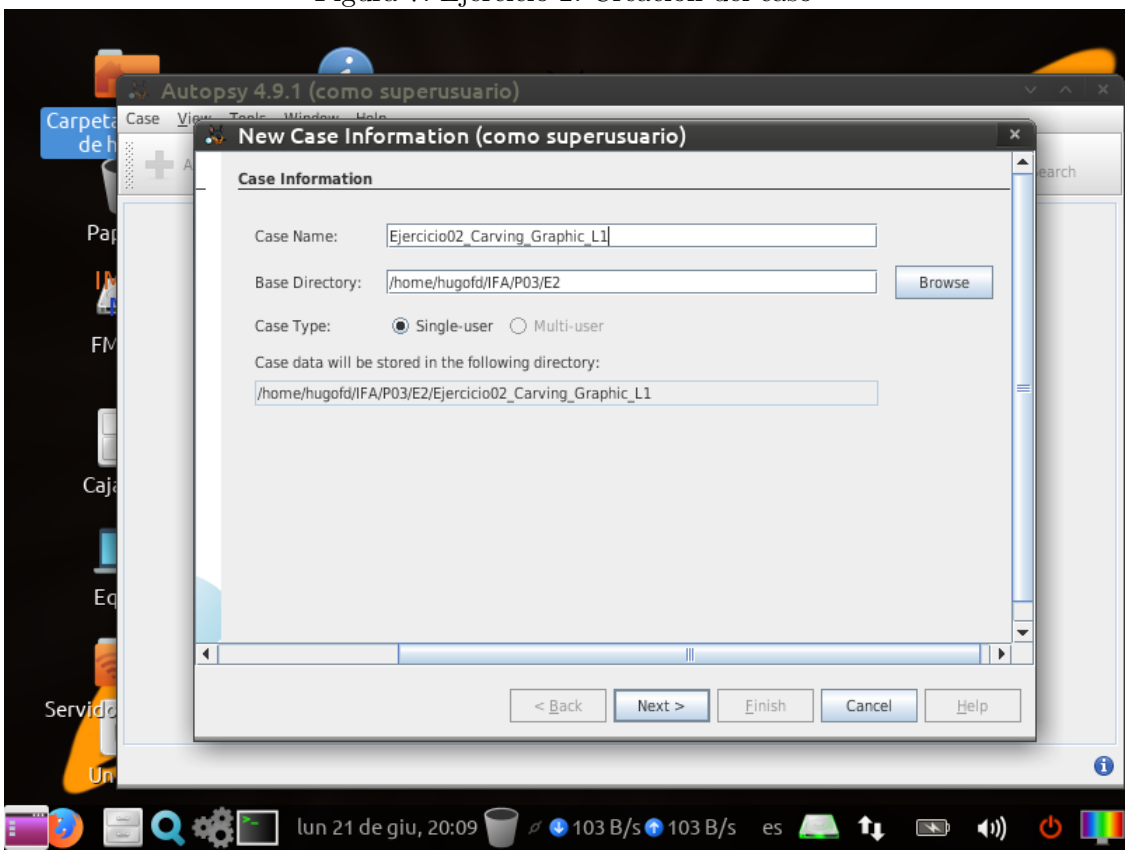
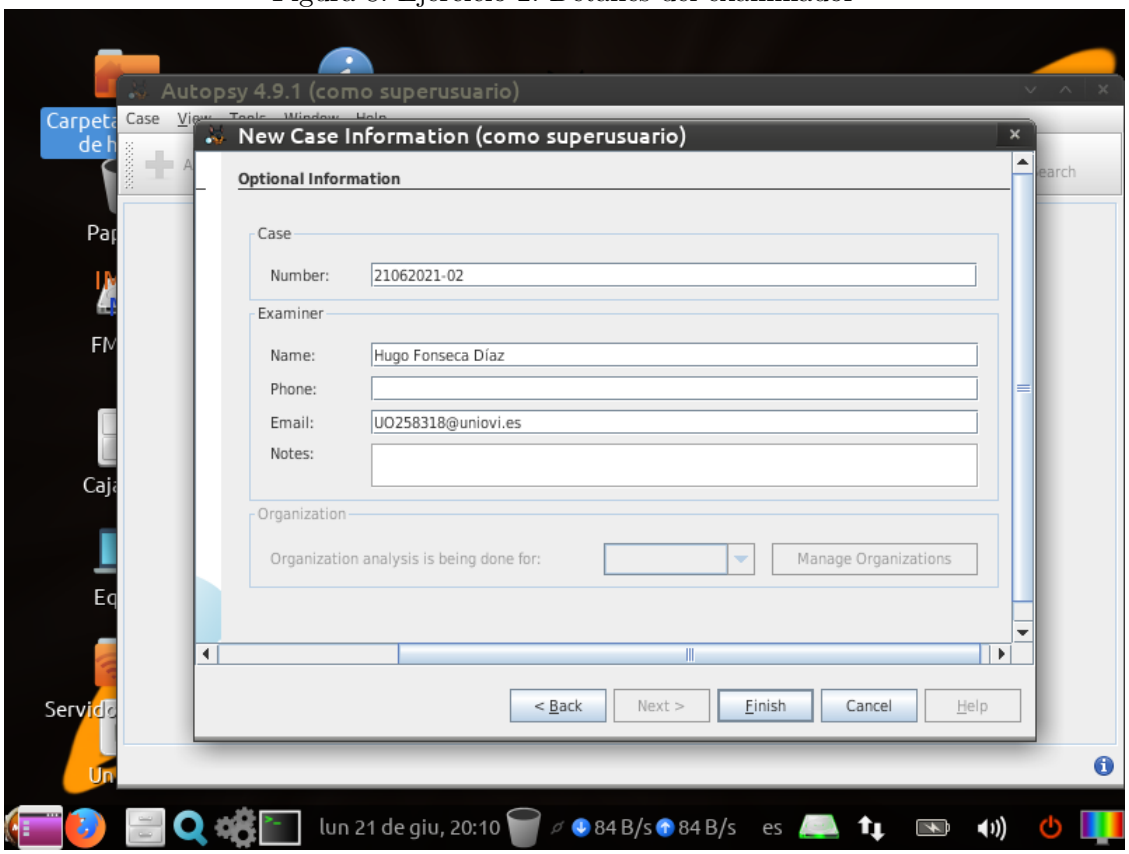
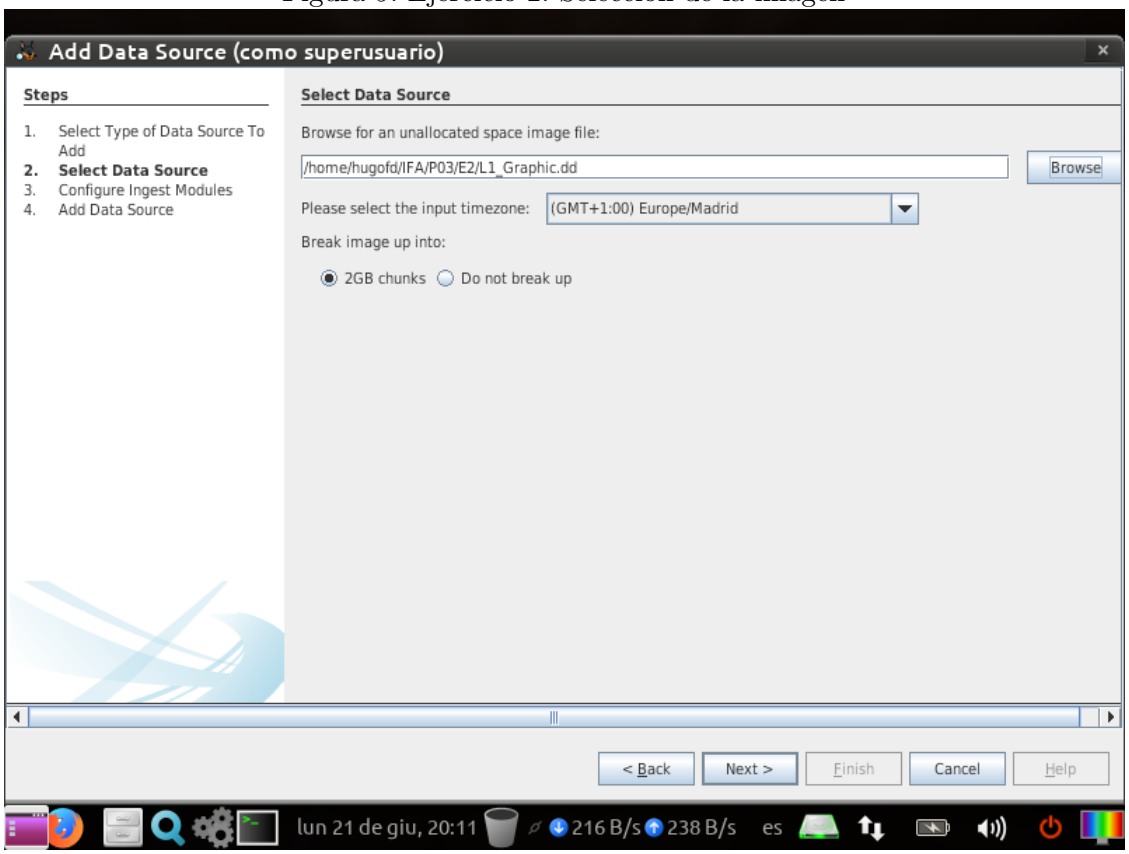


Figura 8: Ejercicio 2: Detalles del examinador



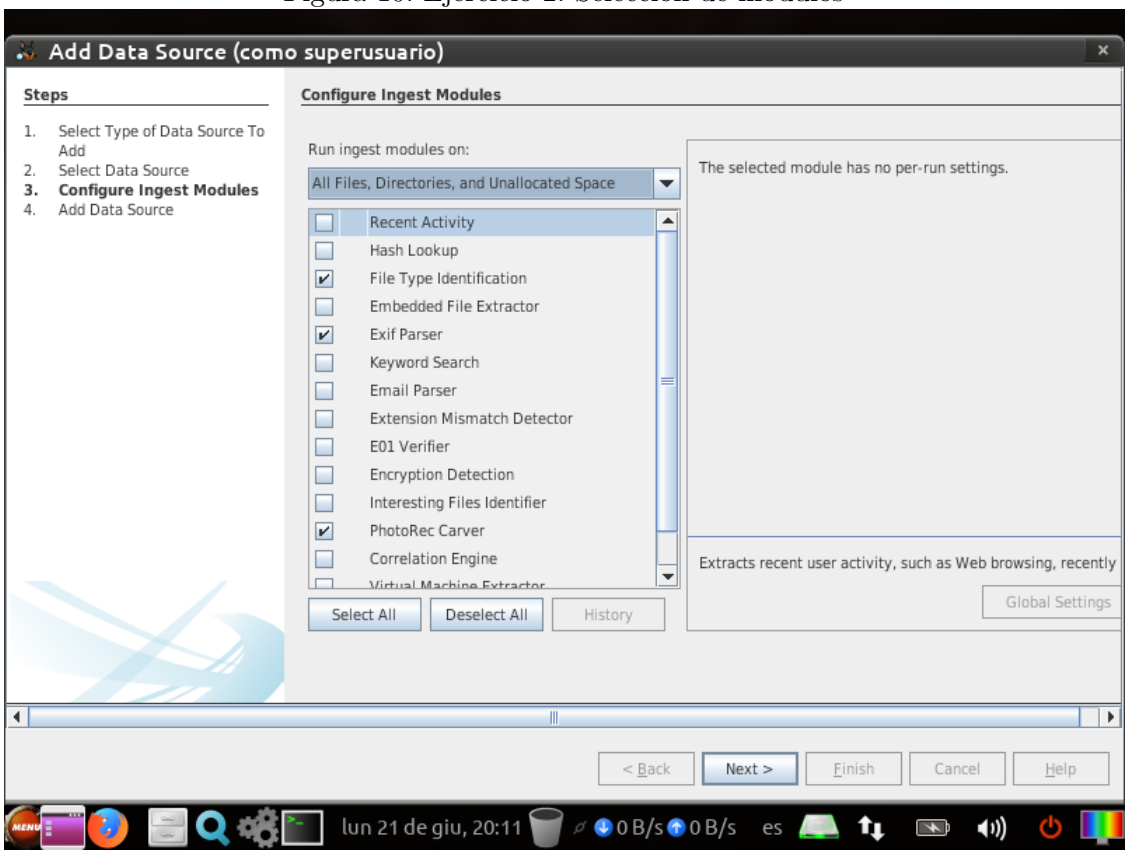
Añadimos la imagen a analizar.

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

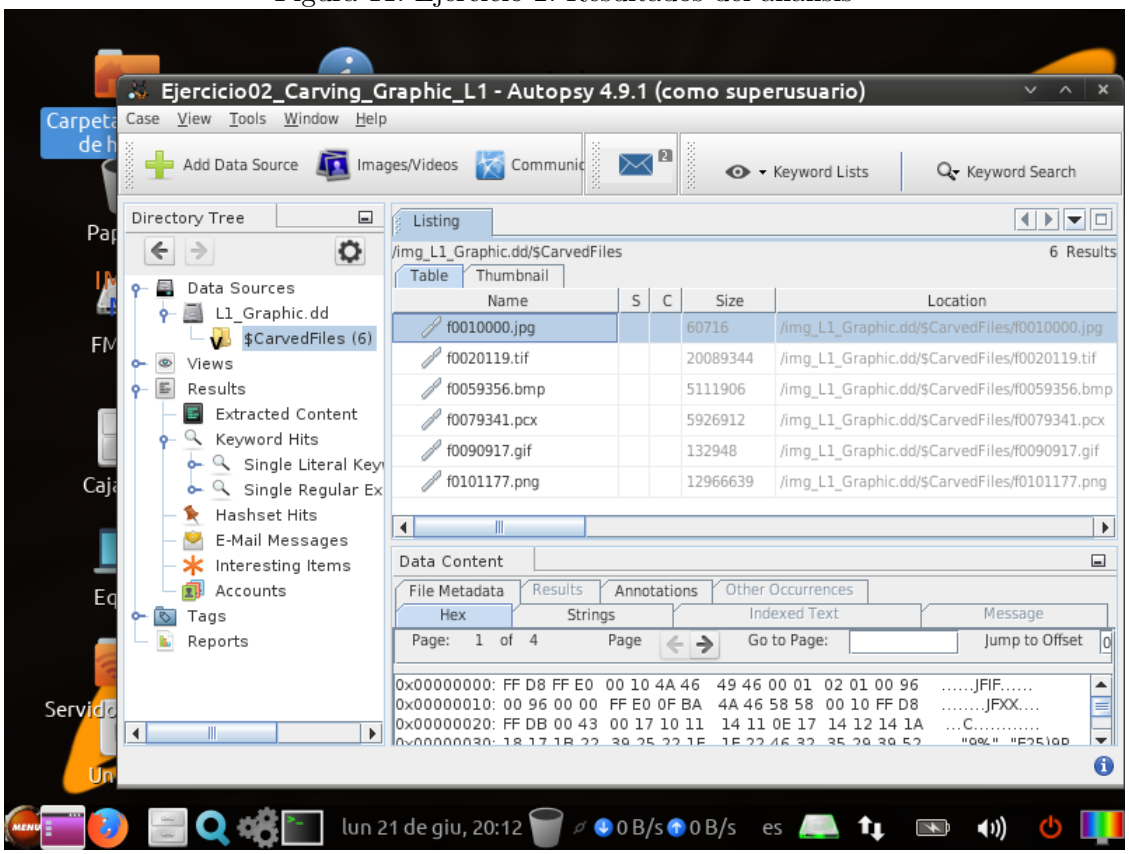
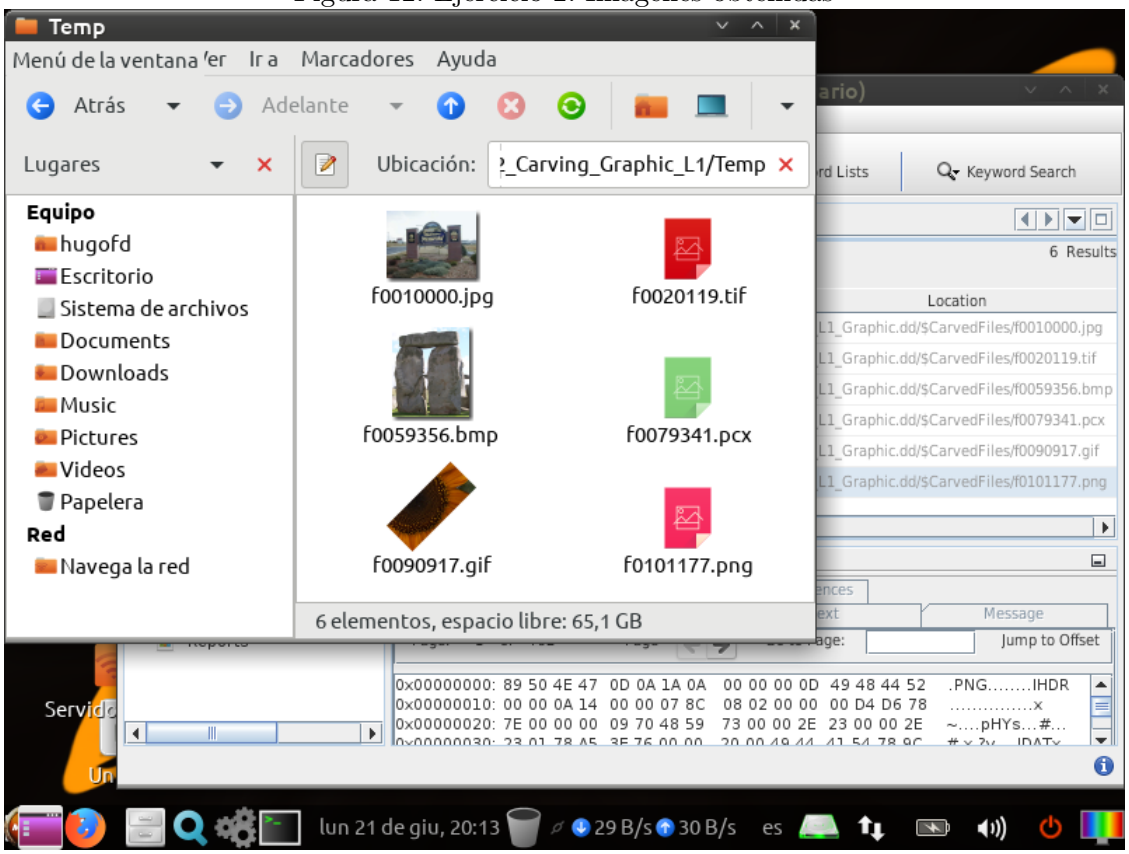


Figura 12: Ejercicio 2: Imágenes obtenidas



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

TBD: tabla

3. Ejercicio 3

Se crea el caso en Autopsy con los datos solicitados.

Figura 13: Ejercicio 3: Creación del caso

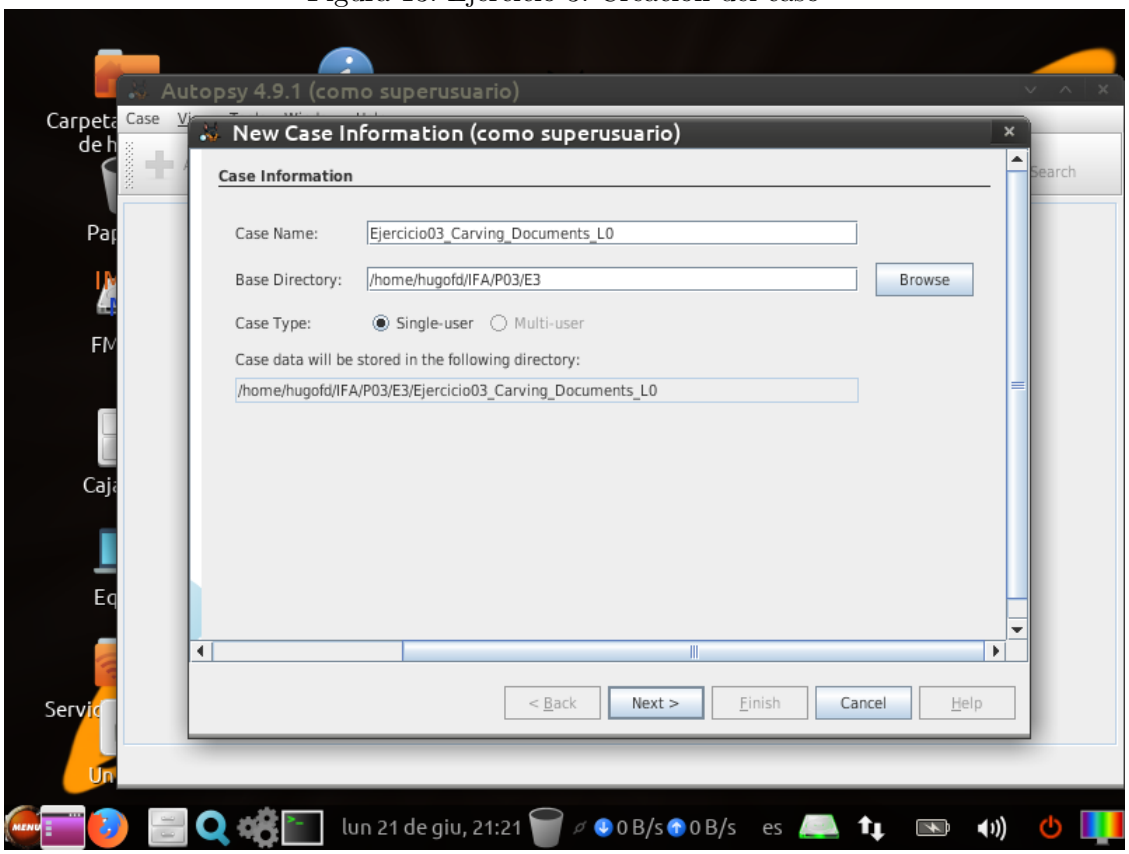
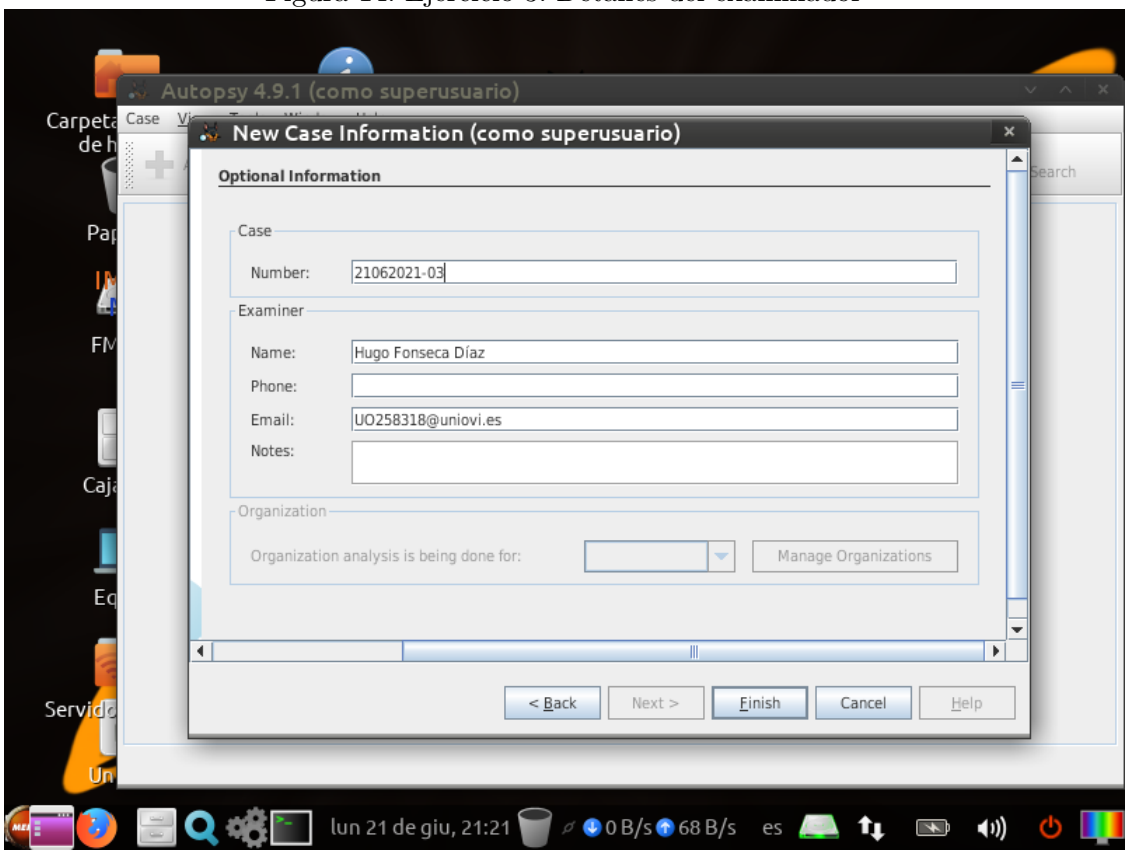
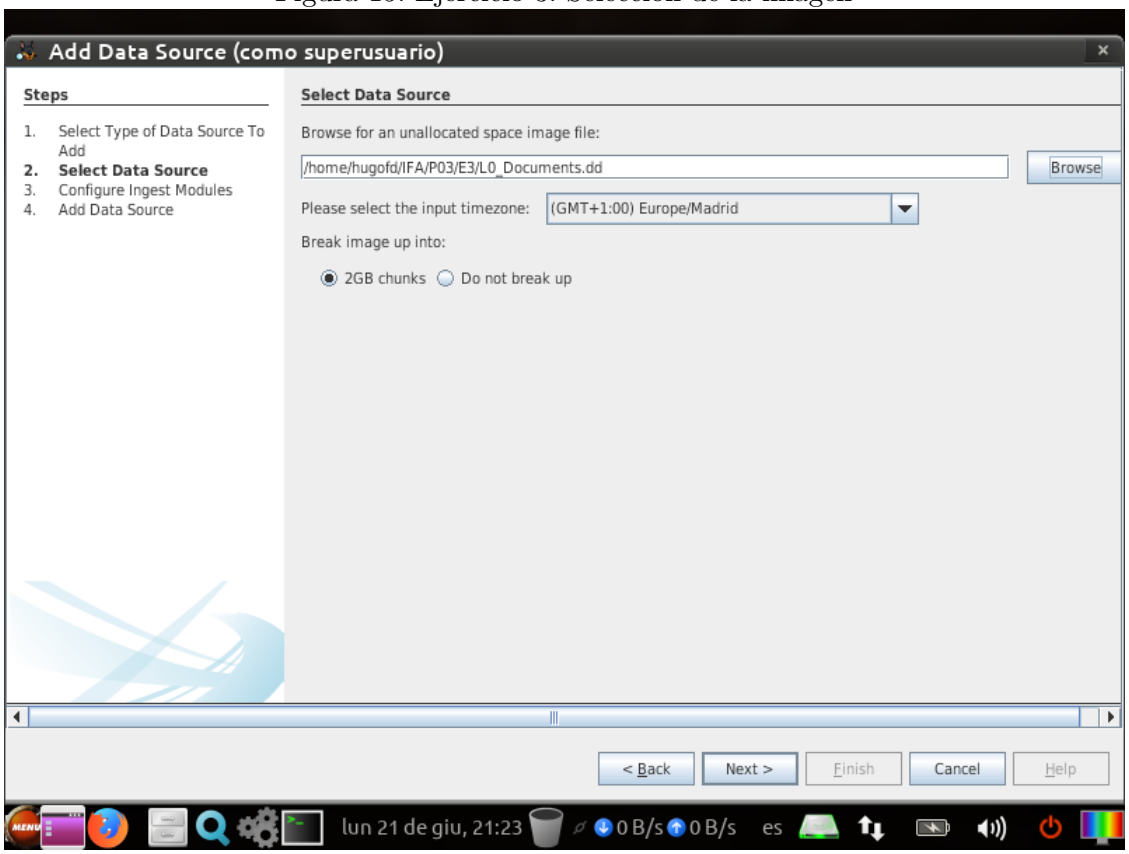


Figura 14: Ejercicio 3: Detalles del examinador



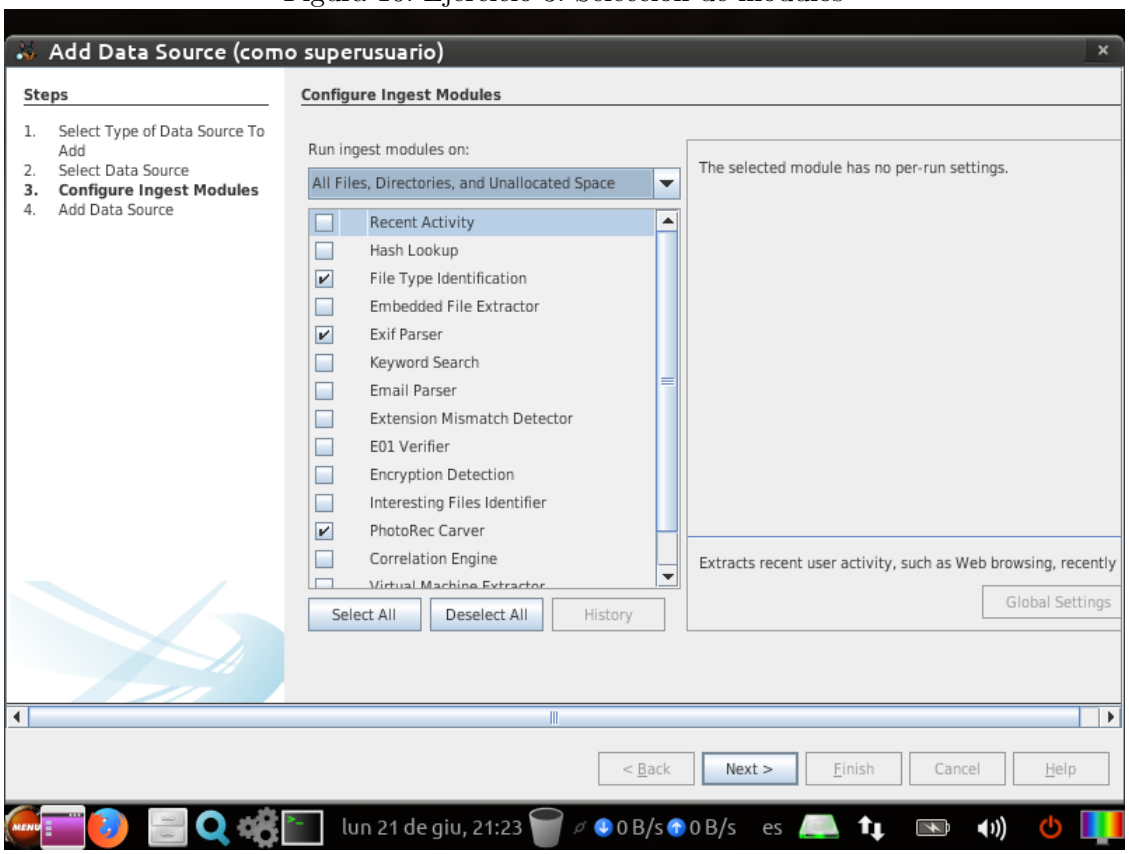
Añadimos la imagen a analizar.

Figura 15: Ejercicio 3: Selección de la imagen



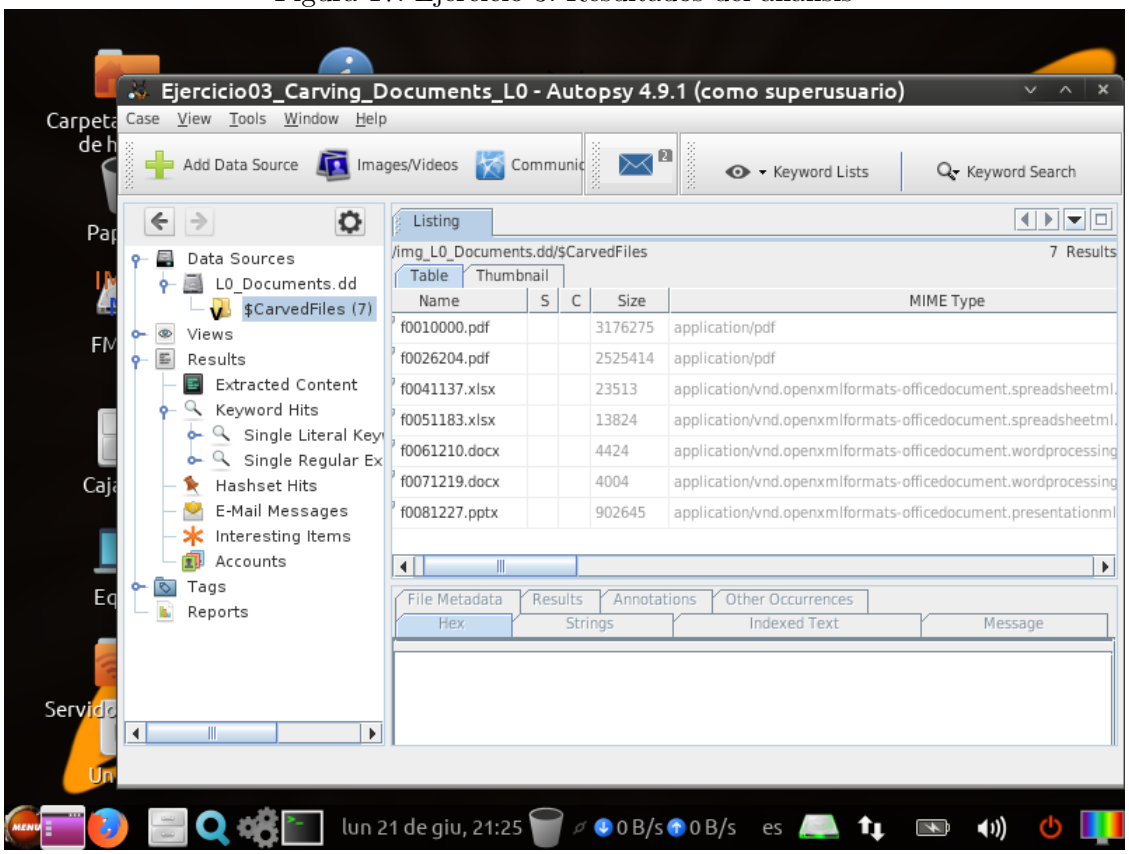
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

Figura 16: Ejercicio 3: Selección de módulos



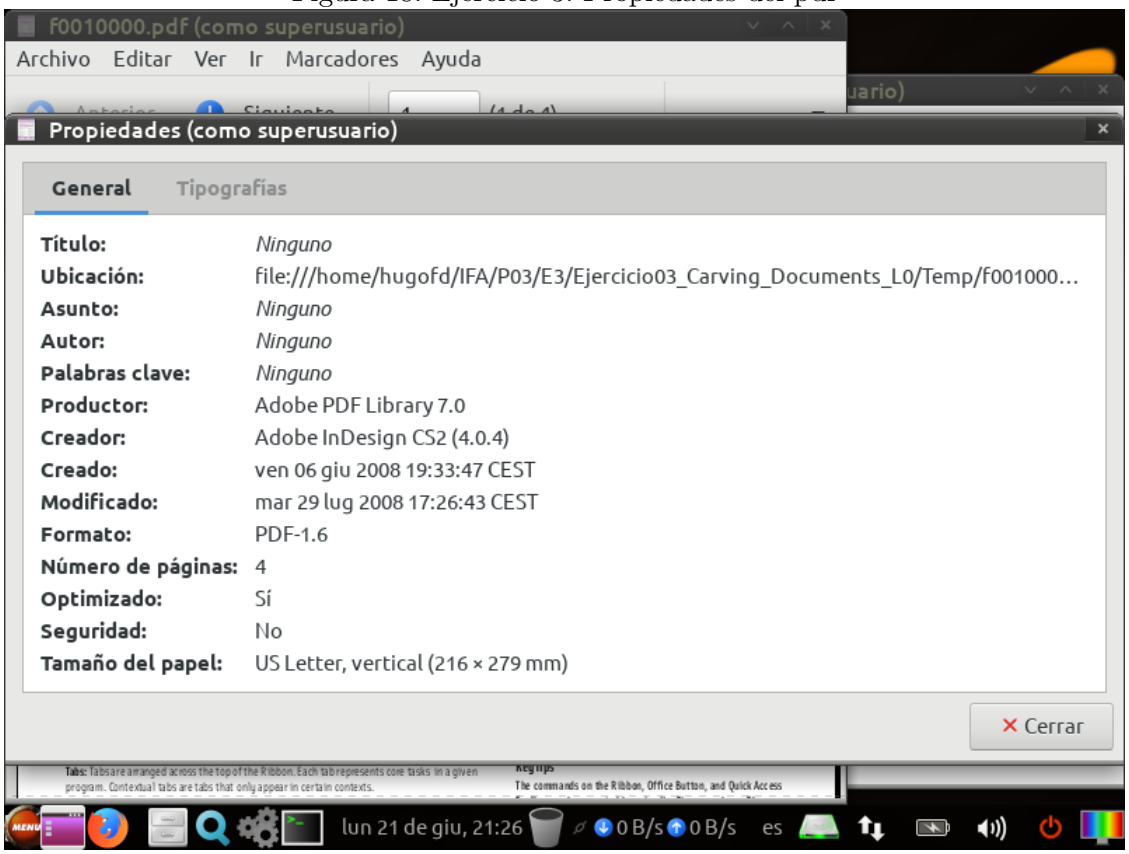
Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

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



TBD: tabla

4. Ejercicio 4

Se crea el caso en Autopsy con los datos solicitados.

Figura 19: Ejercicio 4: Creación del caso

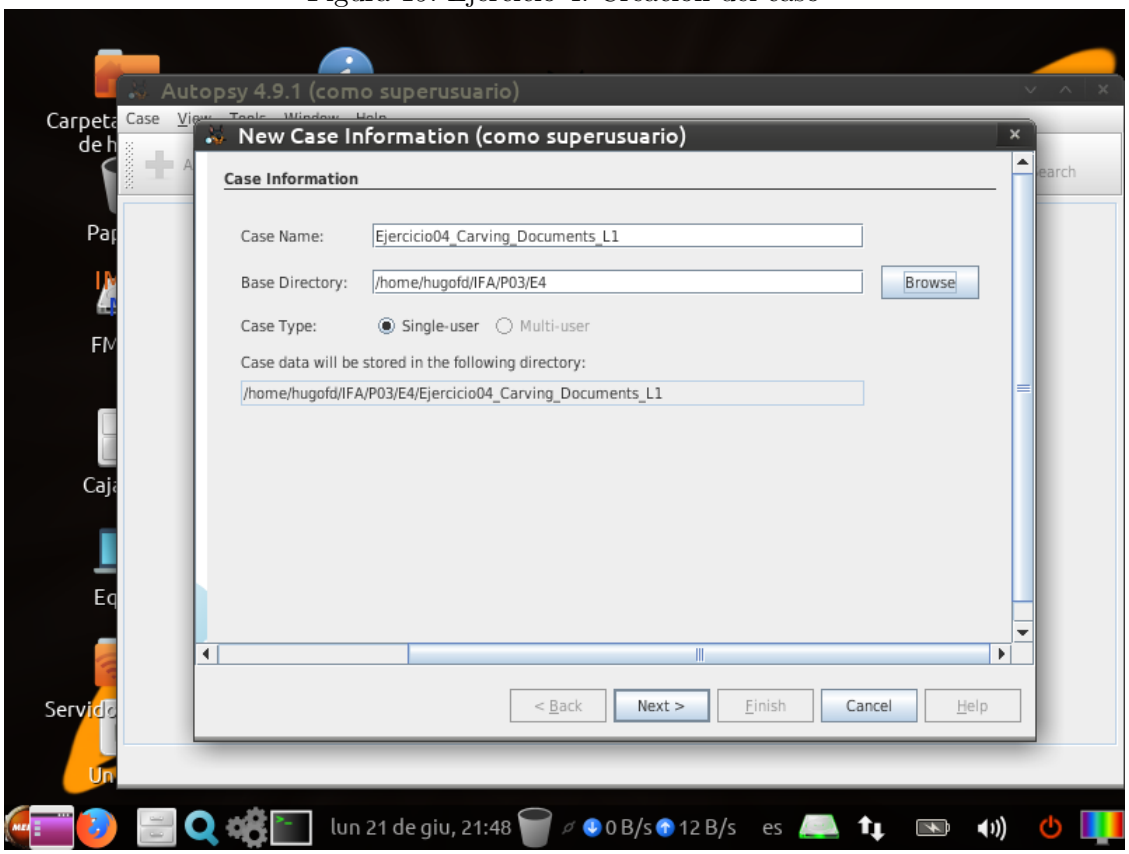
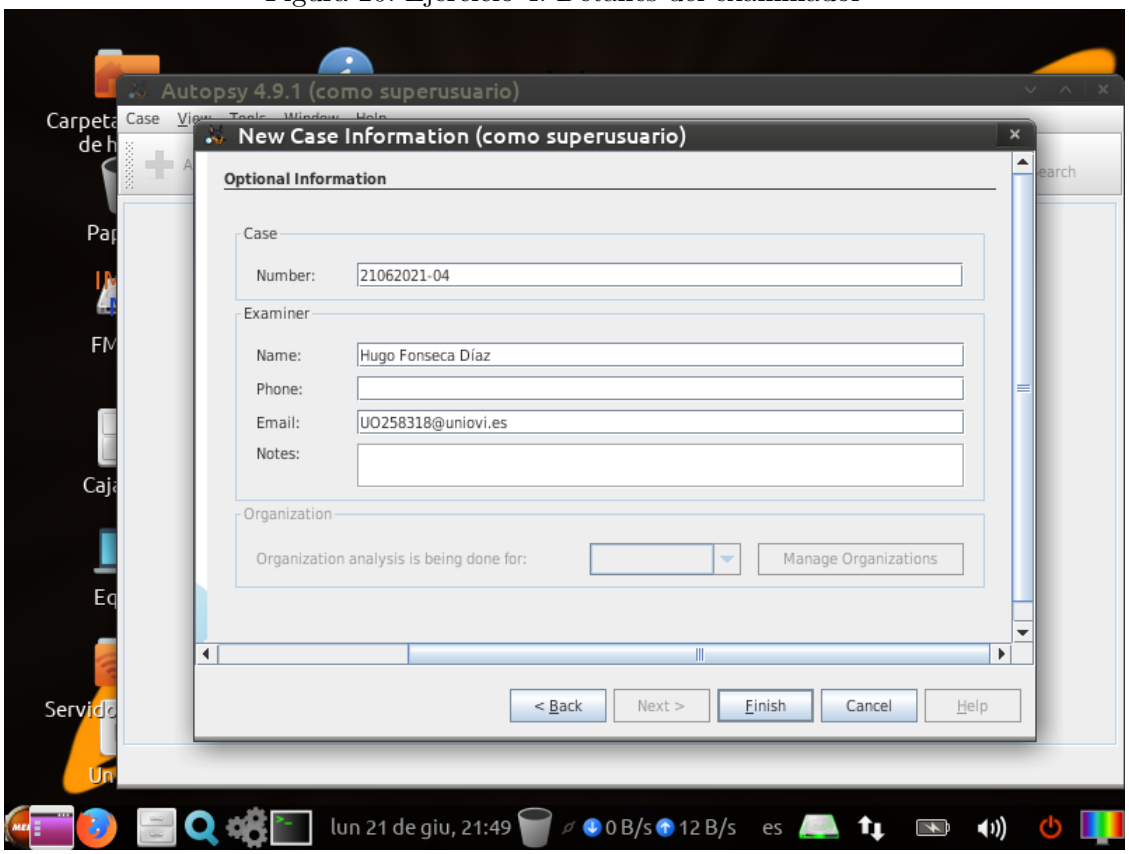
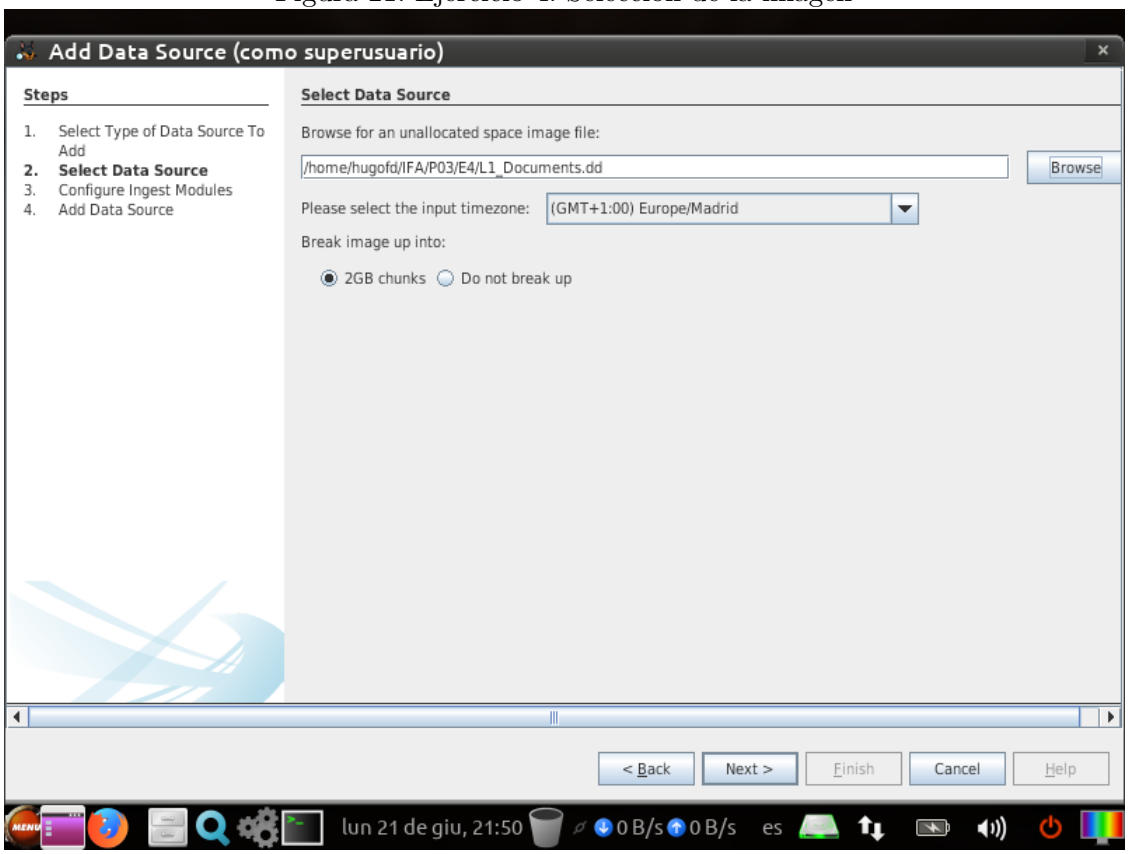


Figura 20: Ejercicio 4: Detalles del examinador



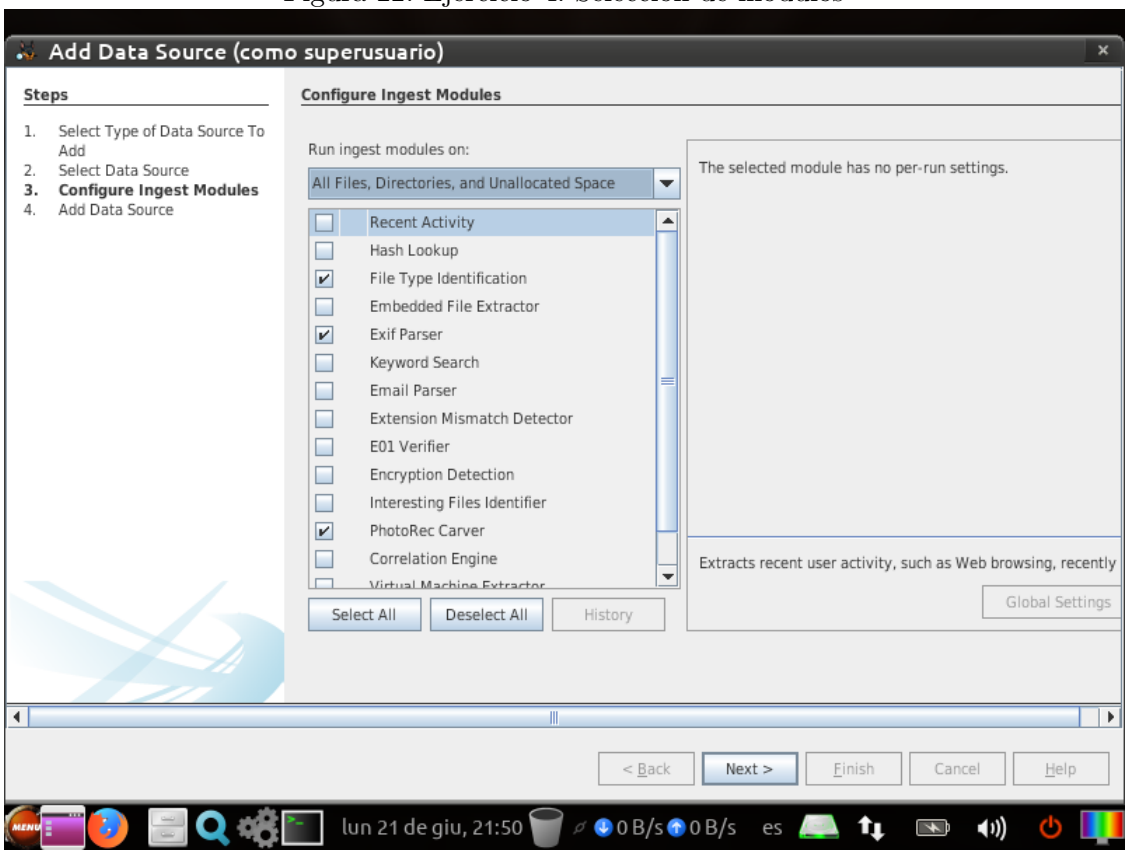
Añadimos la imagen a analizar.

Figura 21: Ejercicio 4: Selección de la imagen



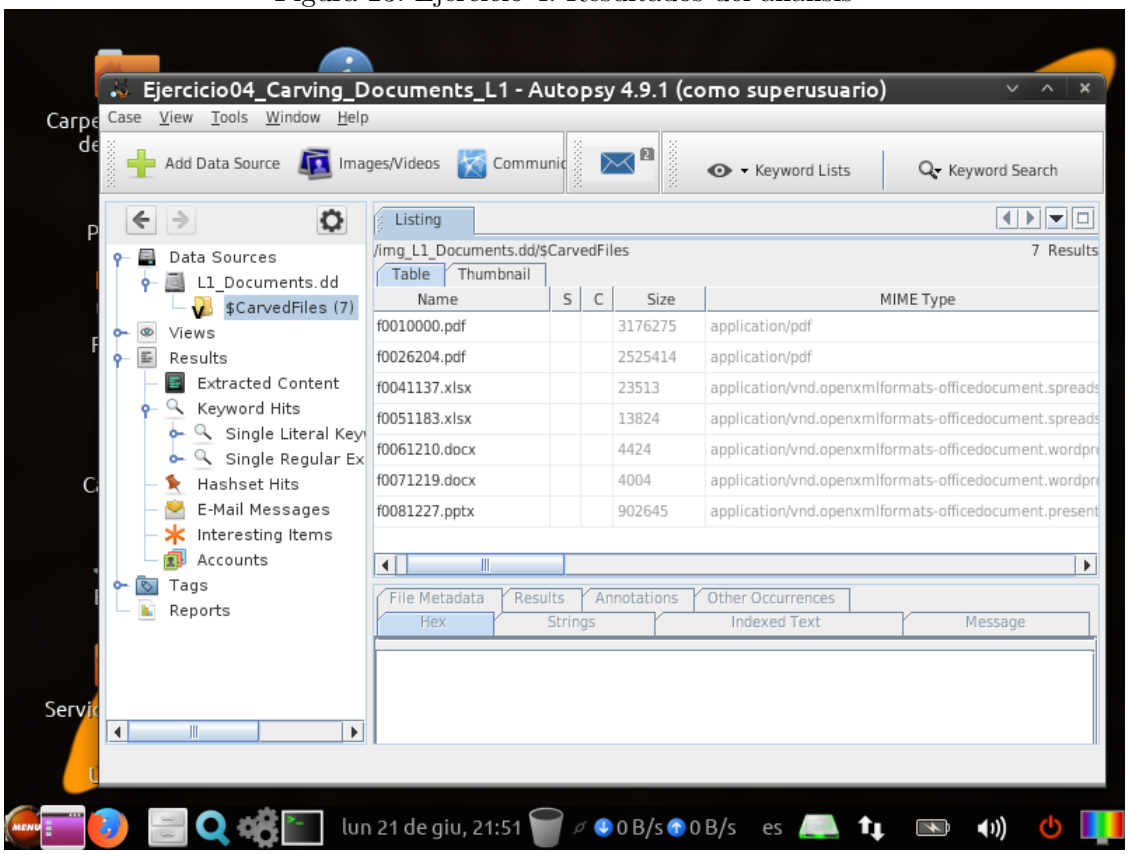
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

Figura 22: Ejercicio 4: Selección de módulos



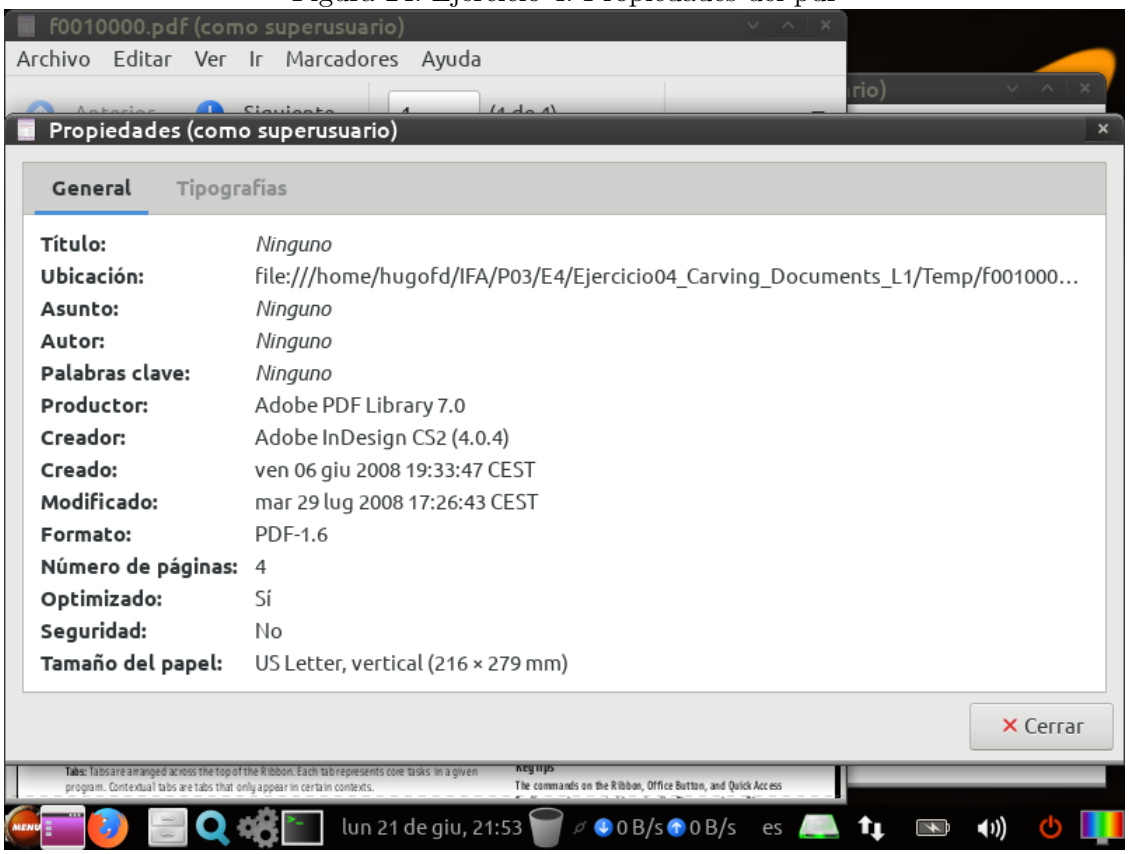
Se ejecuta el análisis y se obtienen los resultados con los que se rellenará la tabla.

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



TBD: tabla

5. Ejercicio 5

Se crea el caso en Autopsy con los datos solicitados.

Figura 25: Ejercicio 5: Creación del caso

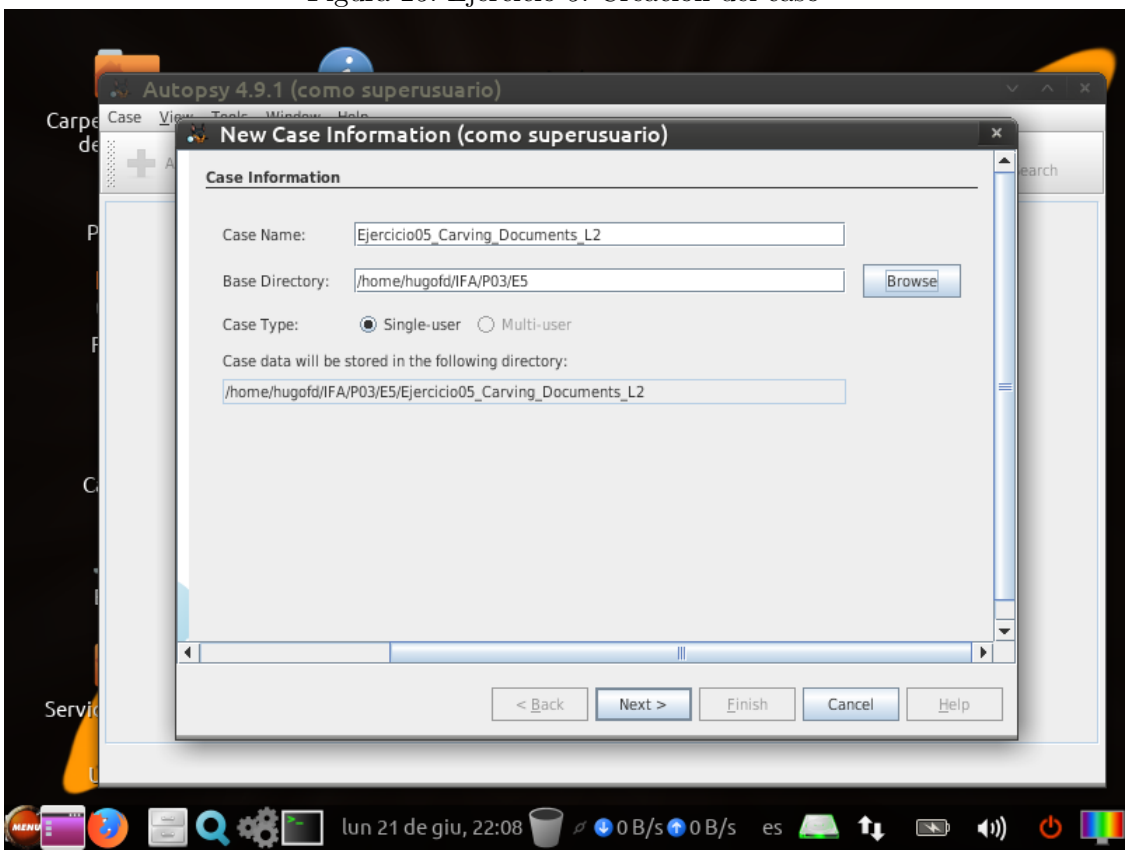
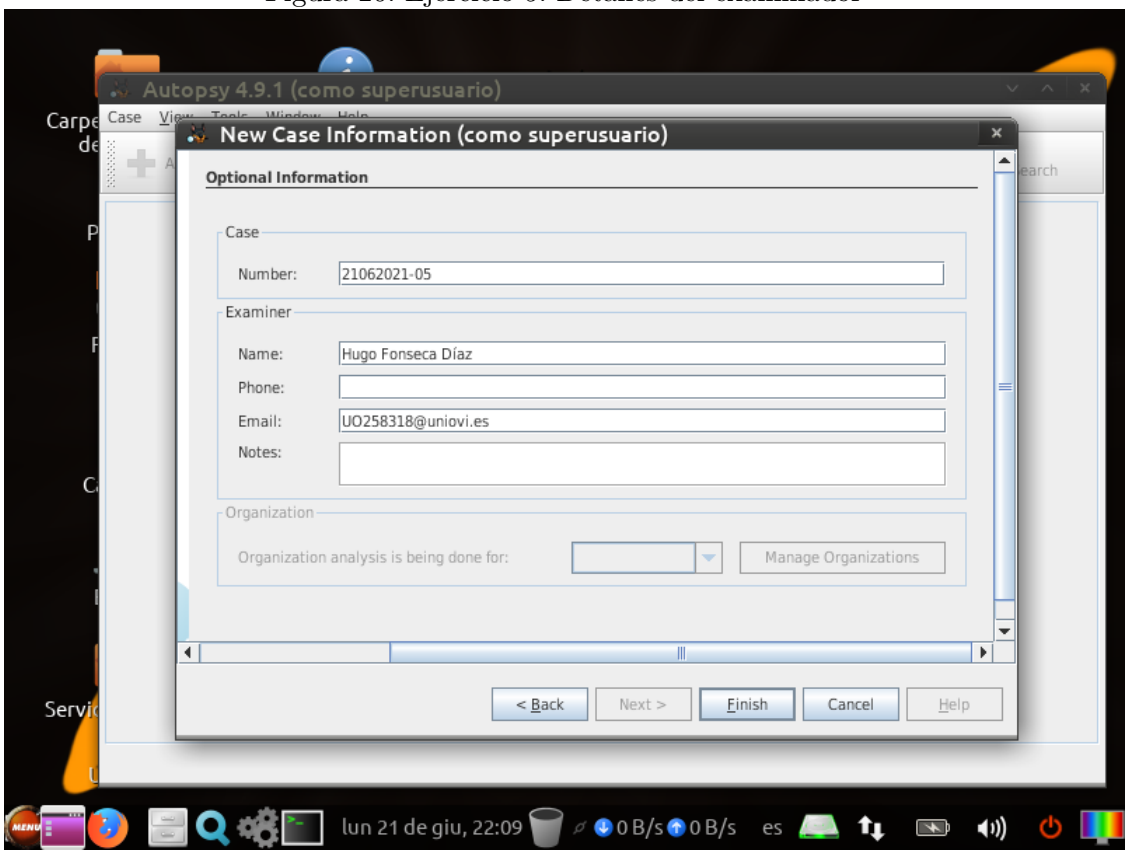
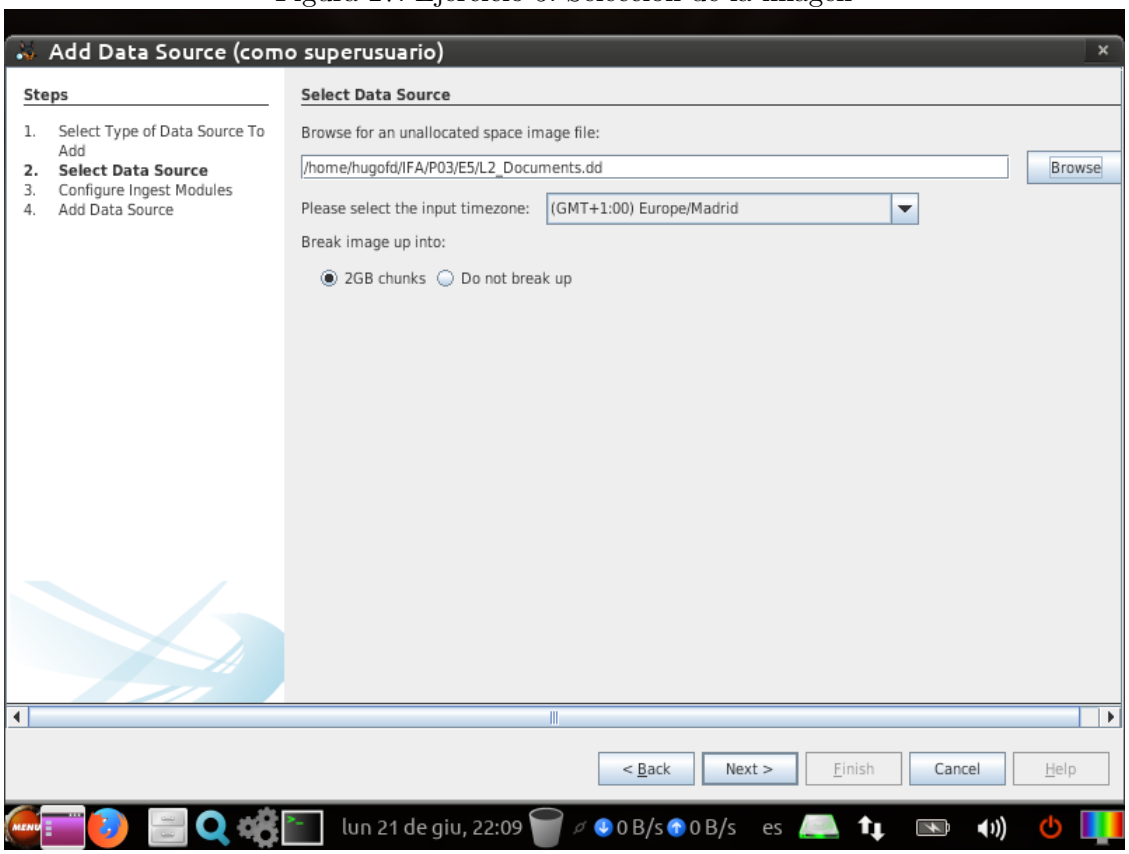


Figura 26: Ejercicio 5: Detalles del examinador



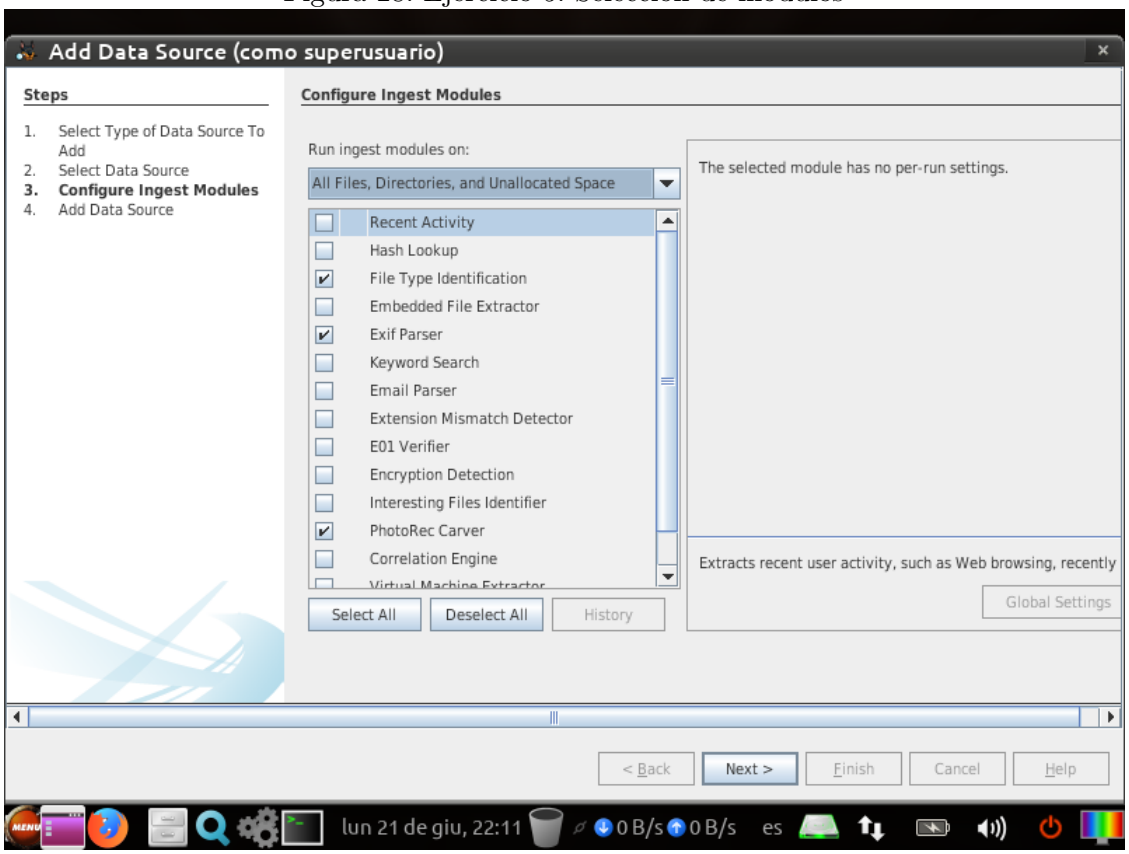
Añadimos la imagen a analizar.

Figura 27: Ejercicio 5: Selección de la imagen



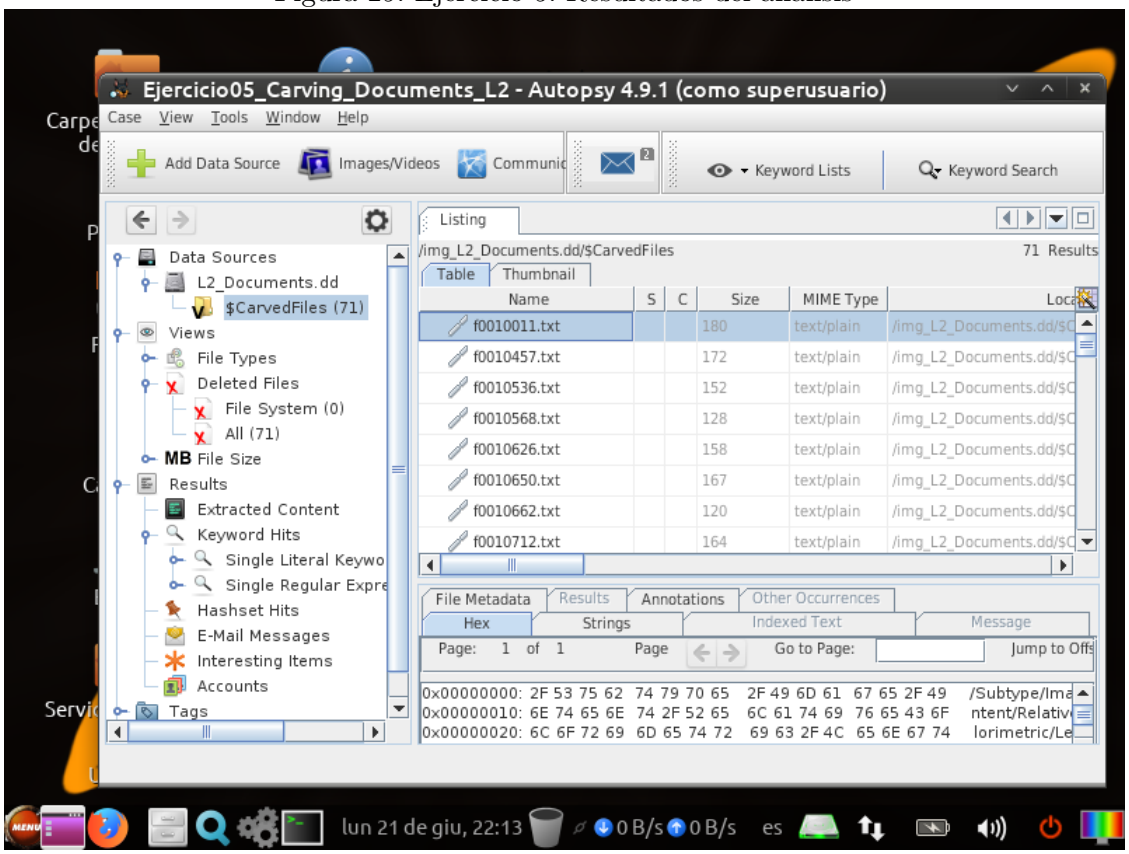
Se seleccionan los módulos de identificación de tipos de fichero, parseador de Exif y *PhotoRec Carver*.

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.

Referencias