

# IFA. Práctica de laboratorio 04

Hugo Fonseca Díaz  
email uo258318@uniovi.es

*Escuela de Ingeniería Informática. Universidad de Oviedo.*

25 de junio de 2021

## 1. Ejercicio 1

Se crea el caso en Autopsy con los datos solicitados.

Figura 1: Ejercicio 1: Creación del caso

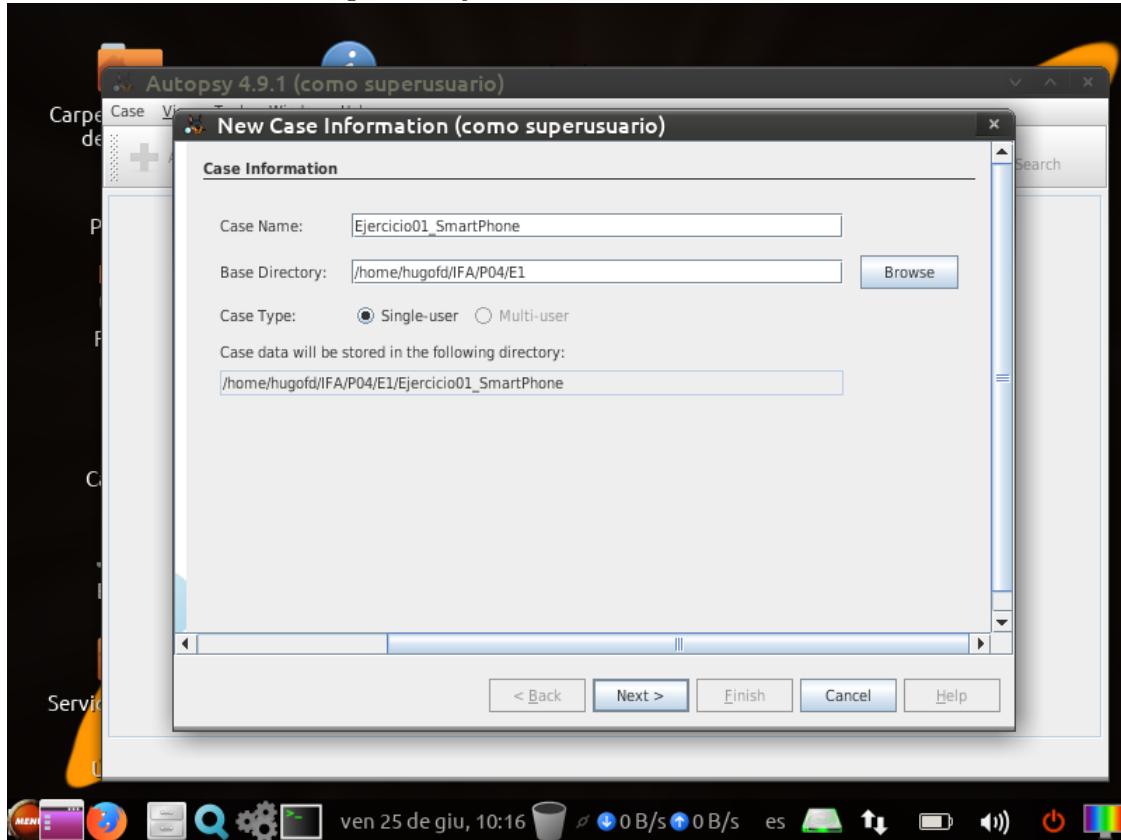
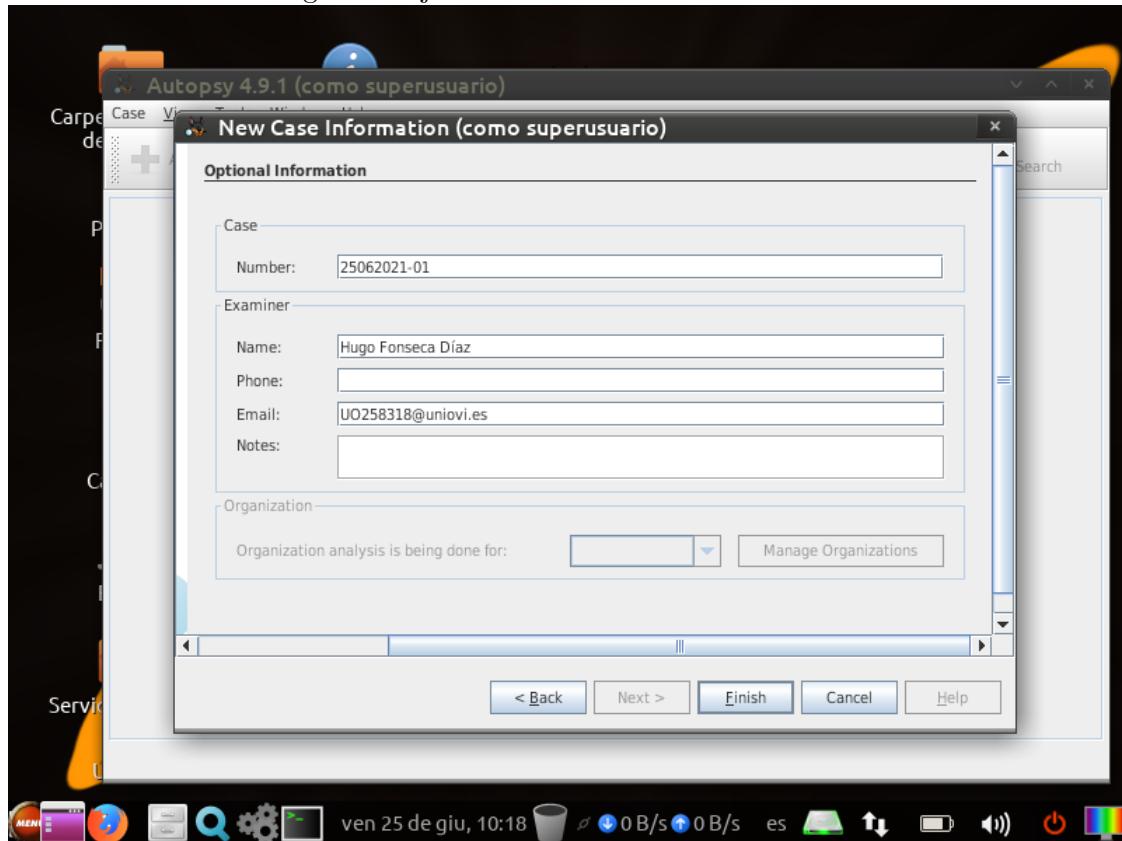
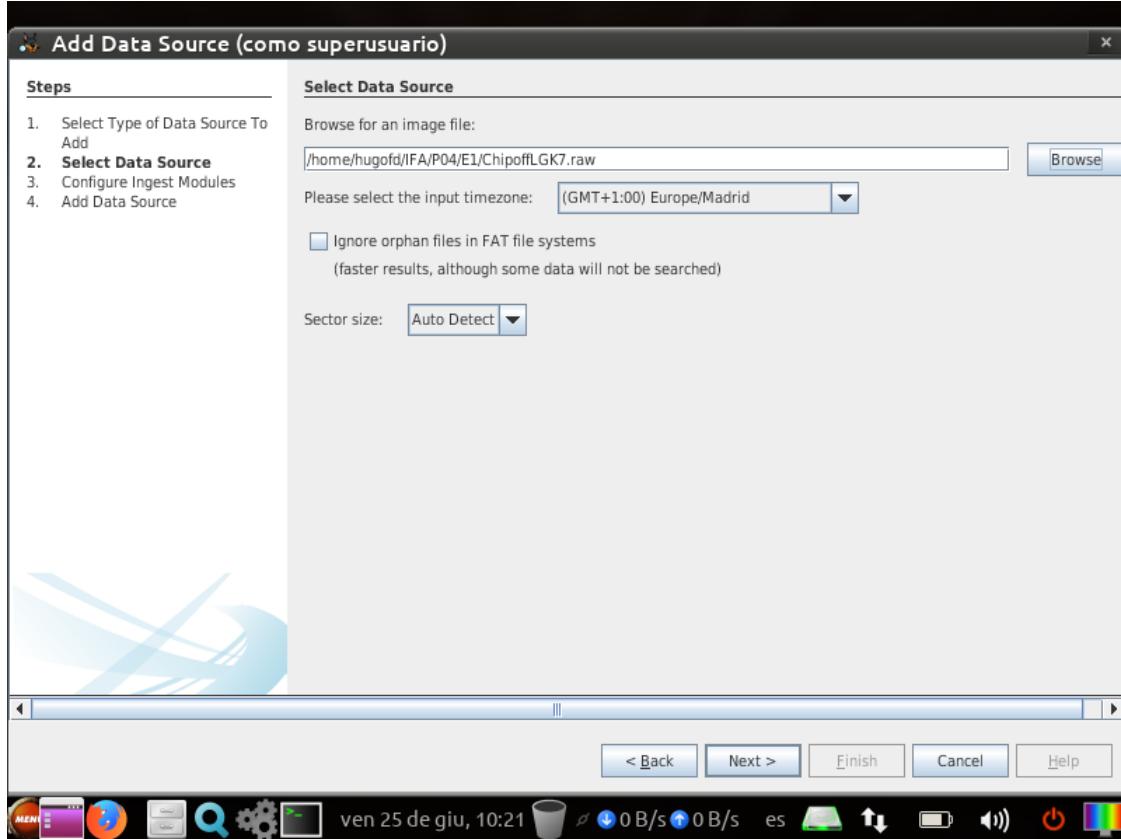


Figura 2: Ejercicio 1: Detalles del examinador



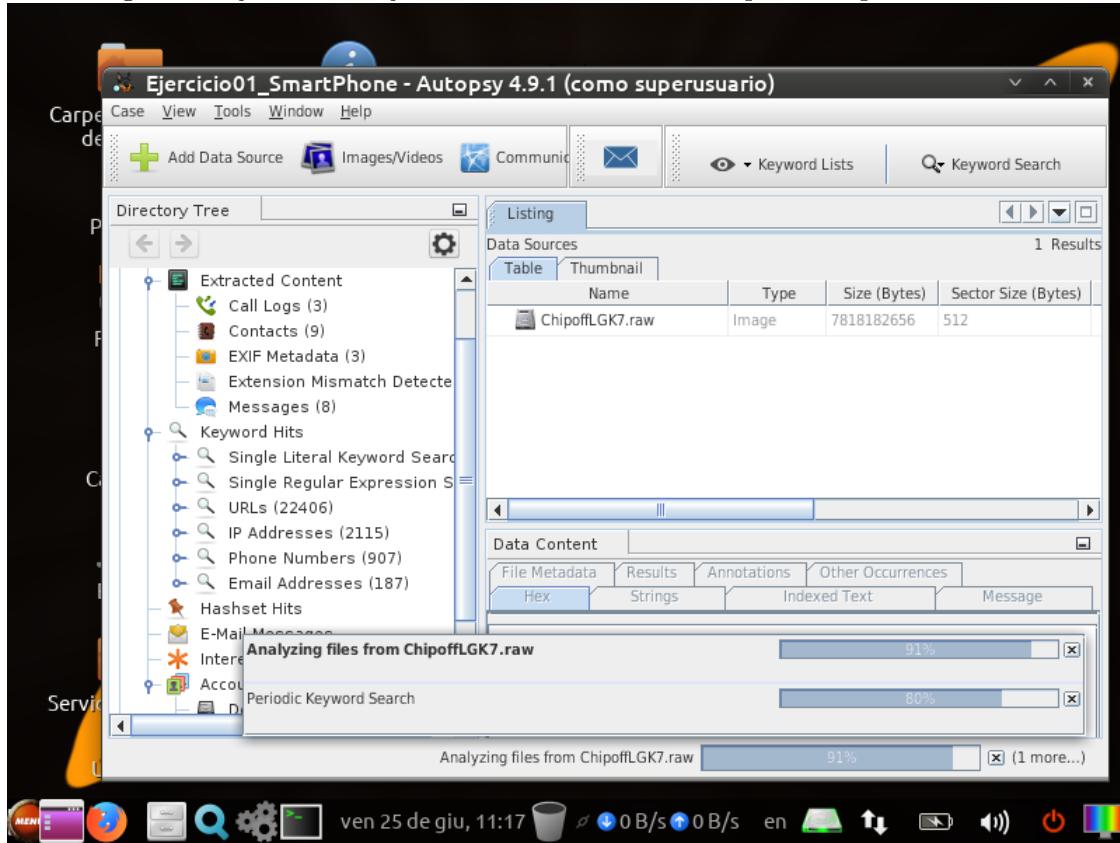
Añadimos la imagen a analizar.

Figura 3: Ejercicio 1: Selección de la imagen



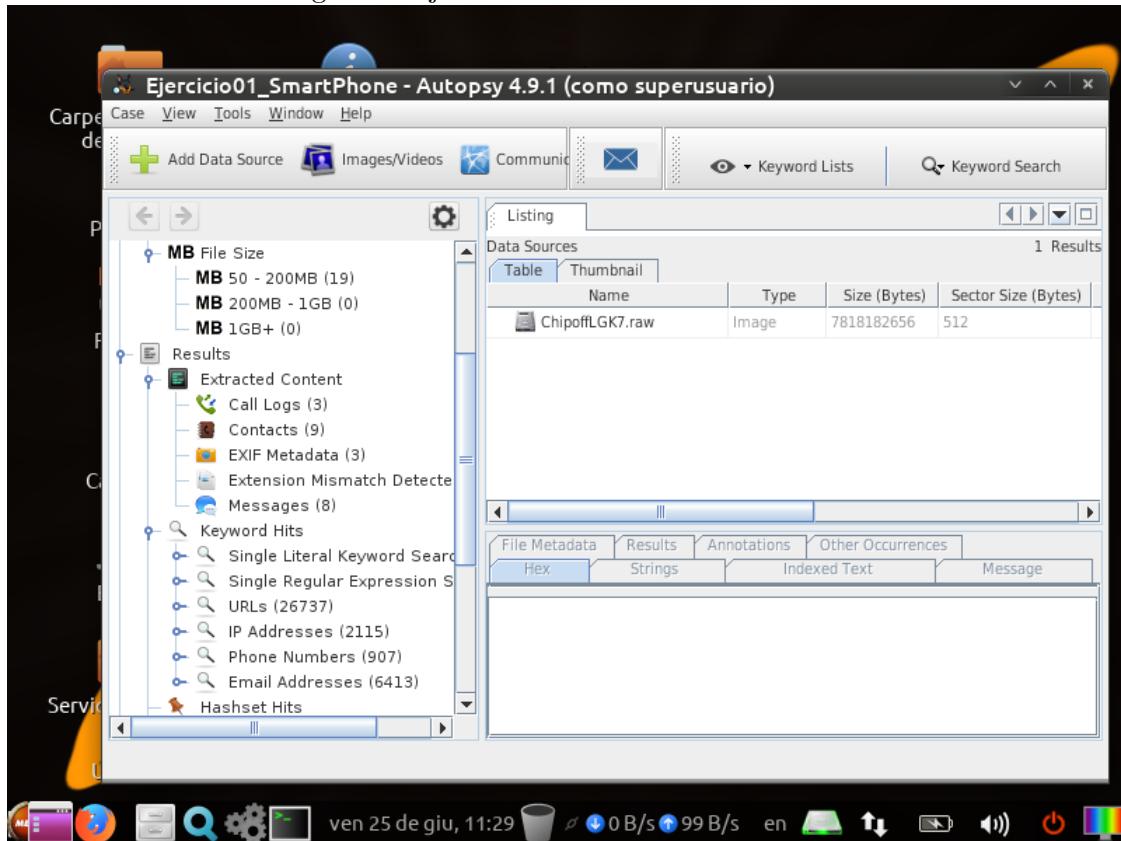
Se ejecutan los módulos de uno en uno para que el cómputo no sea excesivo. El que más tarda en ejecutarse es el módulo de búsqueda de palabras clave, el cual se ha dejado para el final.

Figura 4: Ejercicio 1: Ejecución del módulo de búsqueda de palabras clave



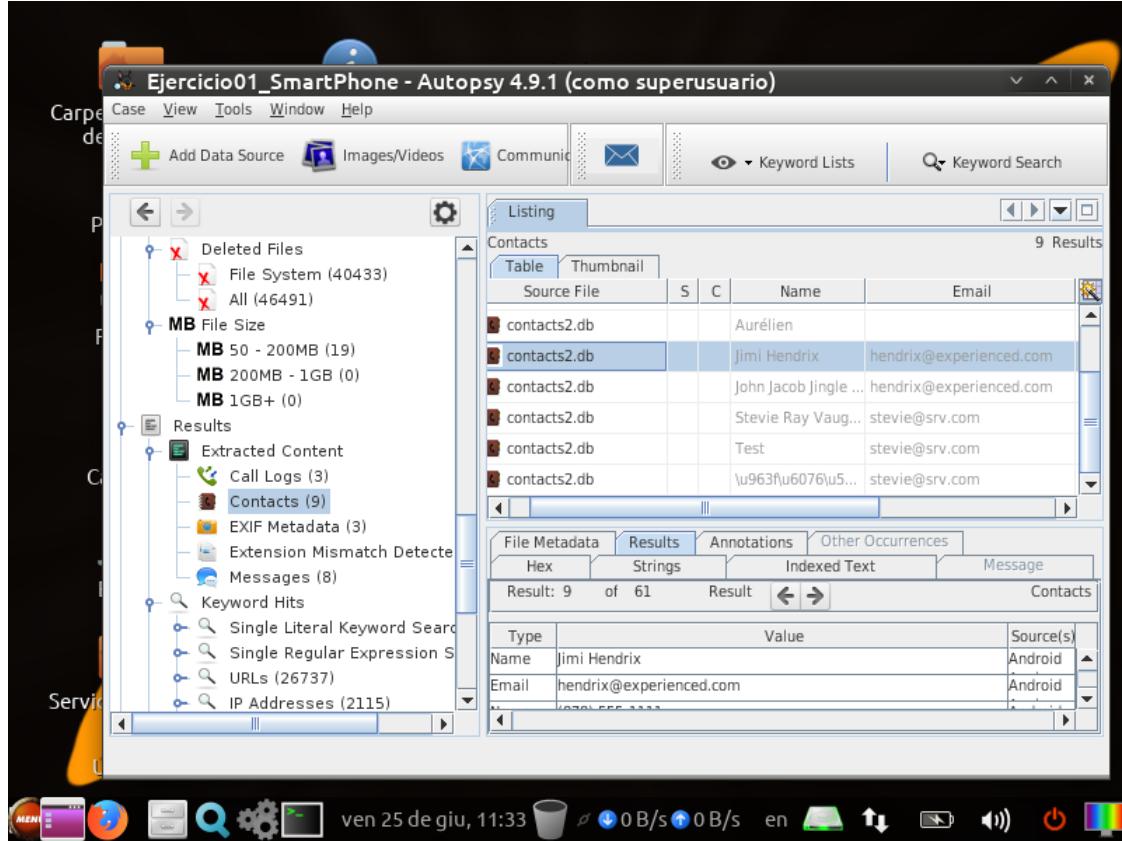
Una vez finalizada la ejecución de los módulos, se tienen los datos necesarios para responder a las cuestiones del ejercicio.

Figura 5: Ejercicio 1: Resultados del análisis



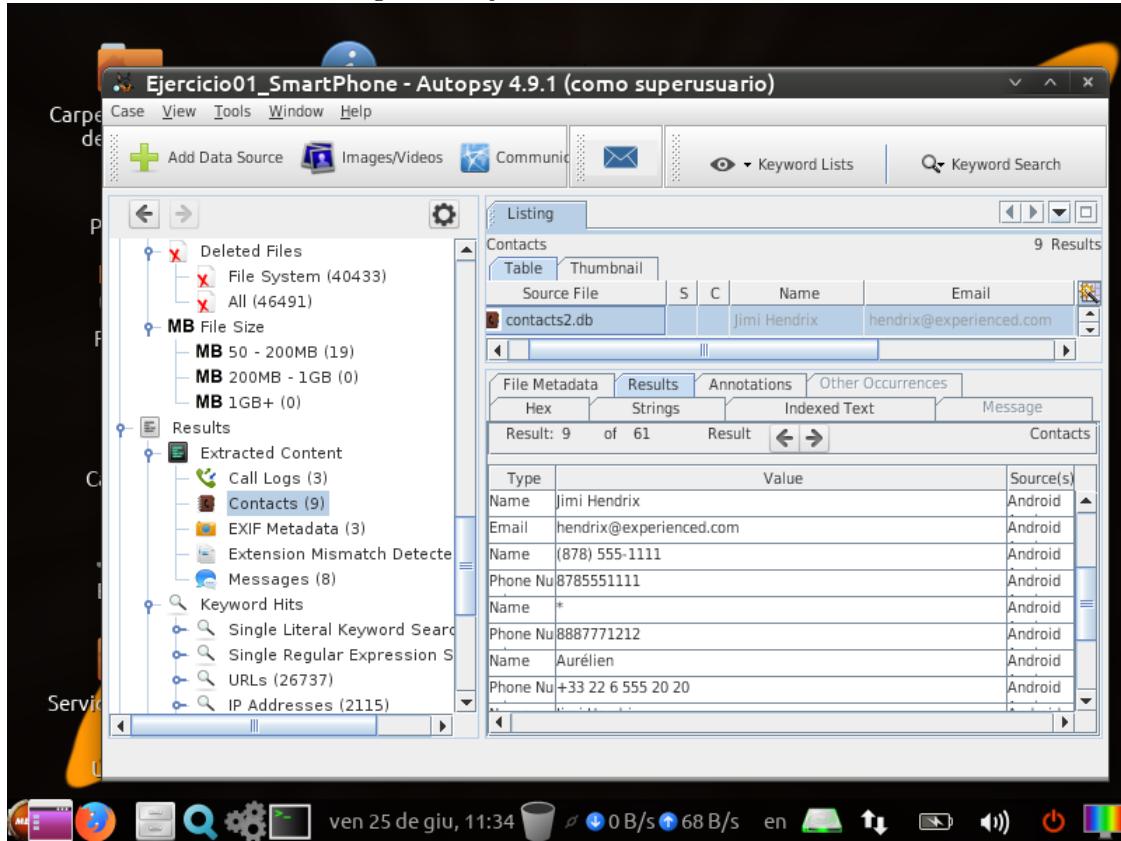
a) Como se puede observar en la siguiente imagen, hay un total de 9 entradas en el apartado de contactos.

Figura 6: Ejercicio 1: Contactos



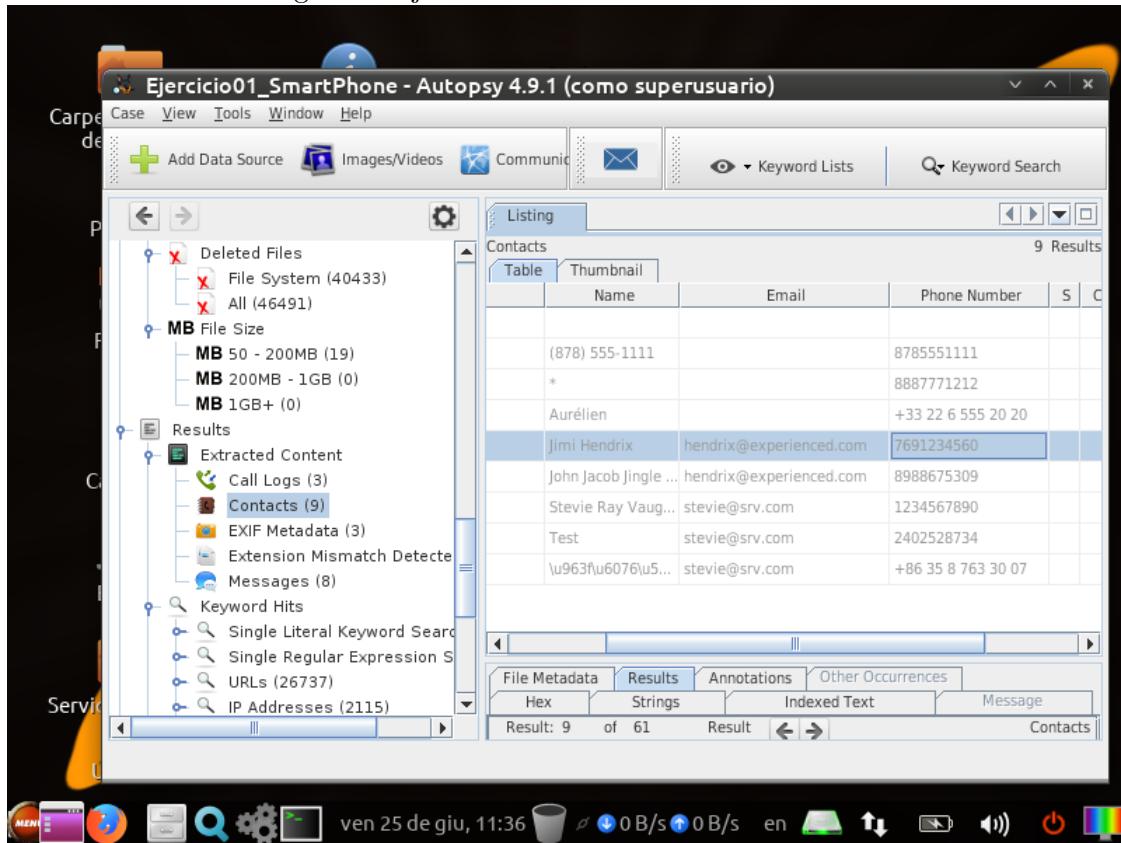
b) Jimi Hendrix, como se puede ver en la siguiente captura.

Figura 7: Ejercicio 1: Jimi Hendrix



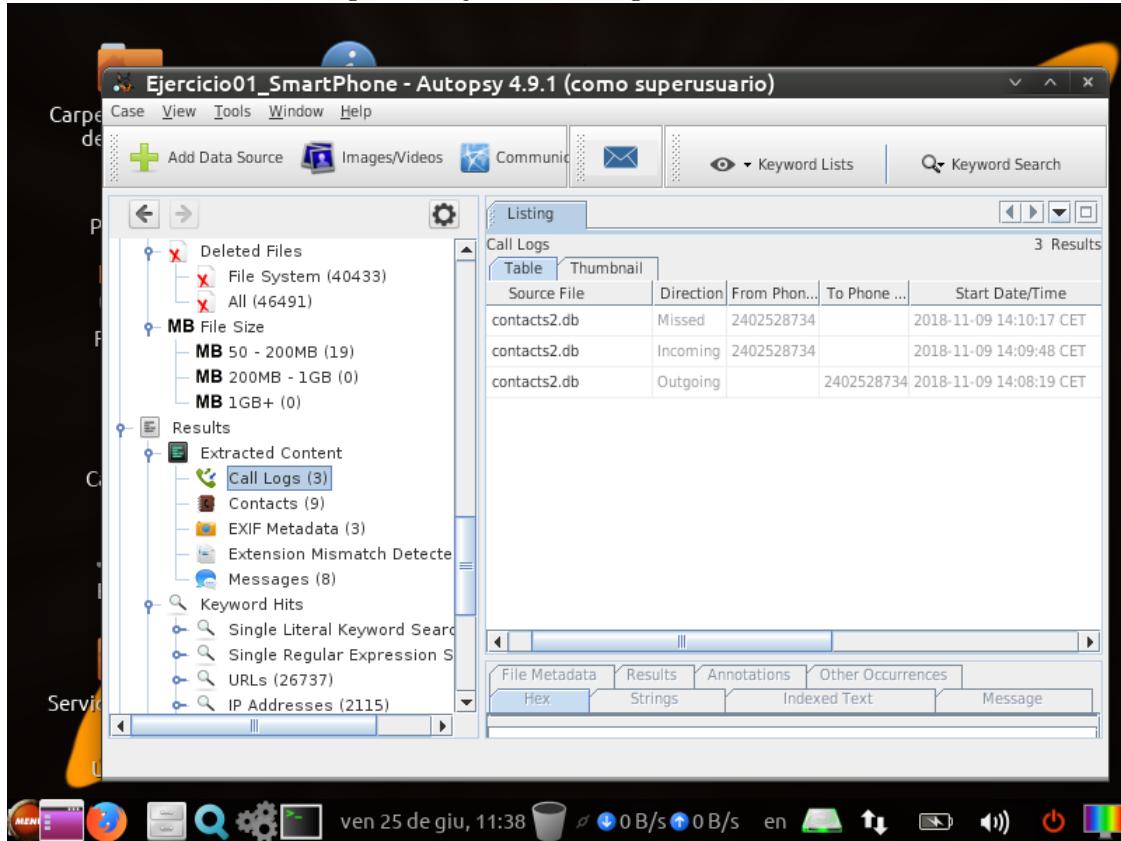
- c) *hendrix@experienced.com*, como se puede observar en la anterior captura.
- d) El correo aparece dos veces, cada vez con un número distinto, pero si se tiene en cuenta el nombre del contacto, 7691234560.

Figura 8: Ejercicio 1: Teléfono de Jimi Hendrix



e) Hay una llamada saliente.

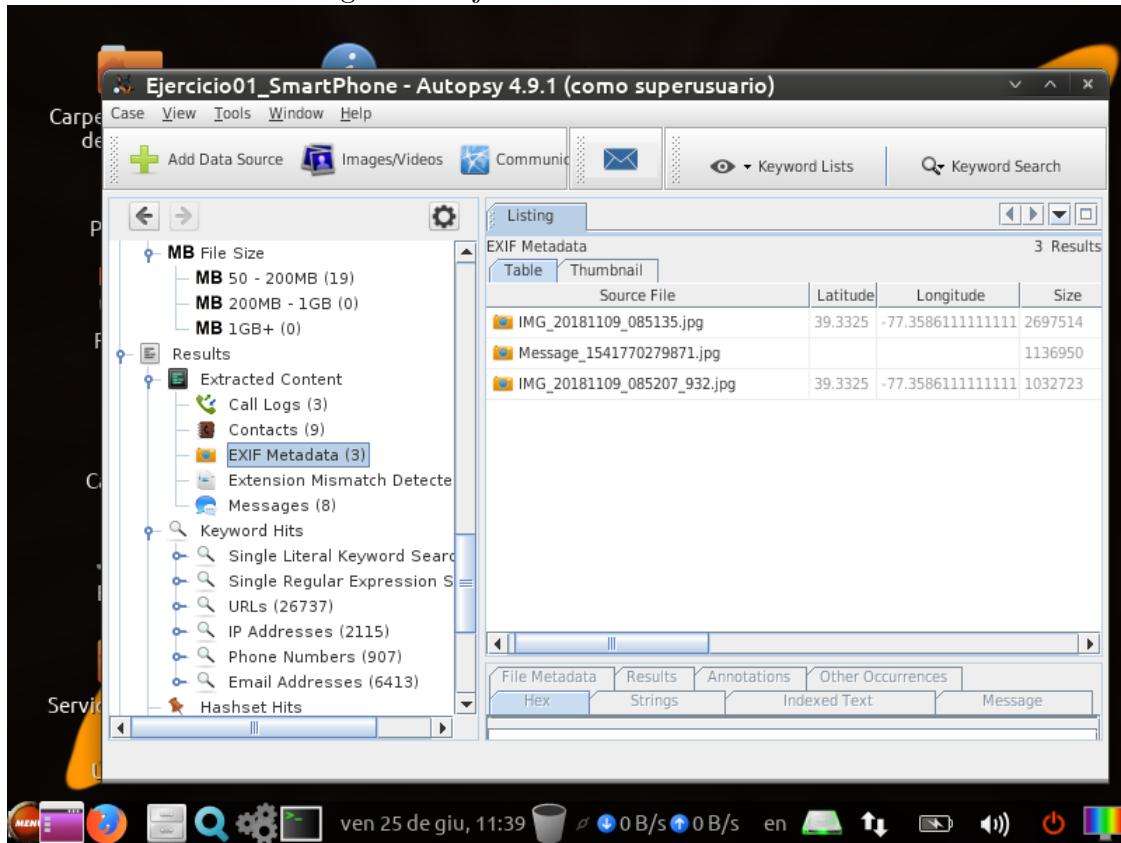
Figura 9: Ejercicio 1: Logs de llamadas



f) Del teléfono analizado al número de teléfono 2402528734.

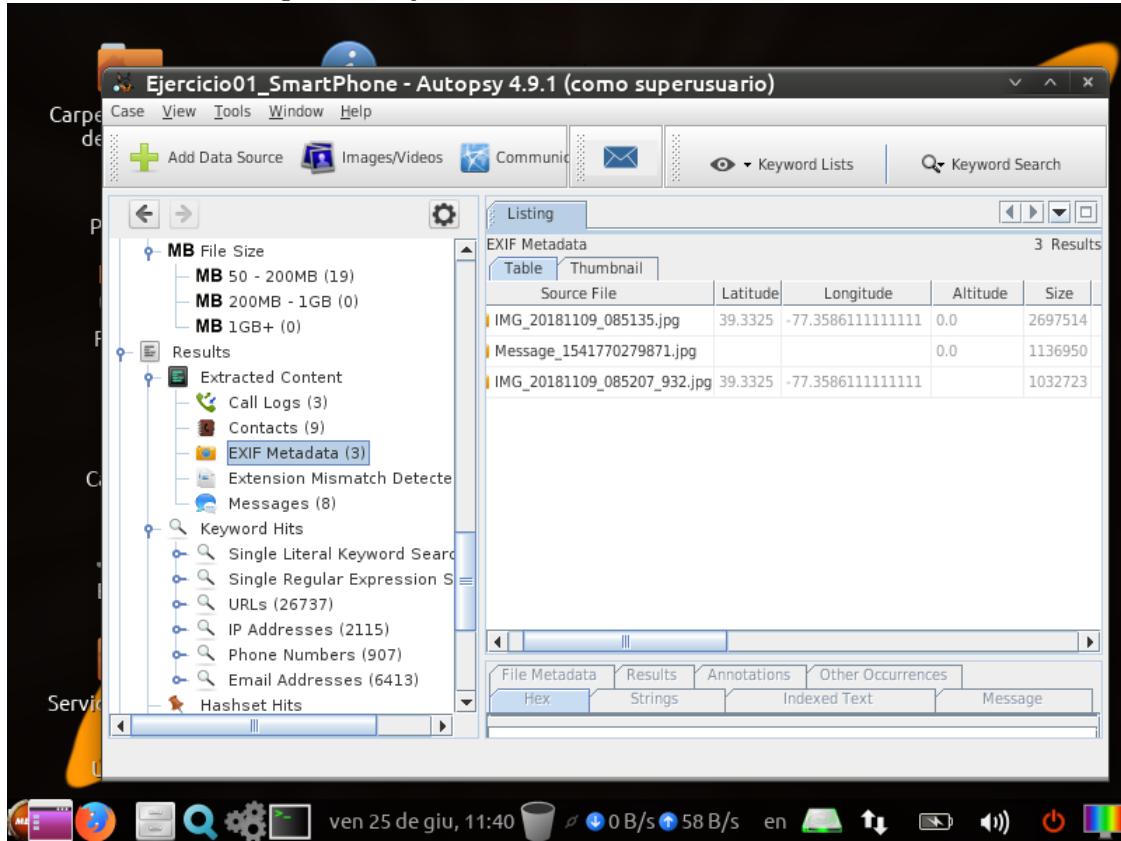
g) Tres ficheros.

Figura 10: Ejercicio 1: Metadatos EXIF



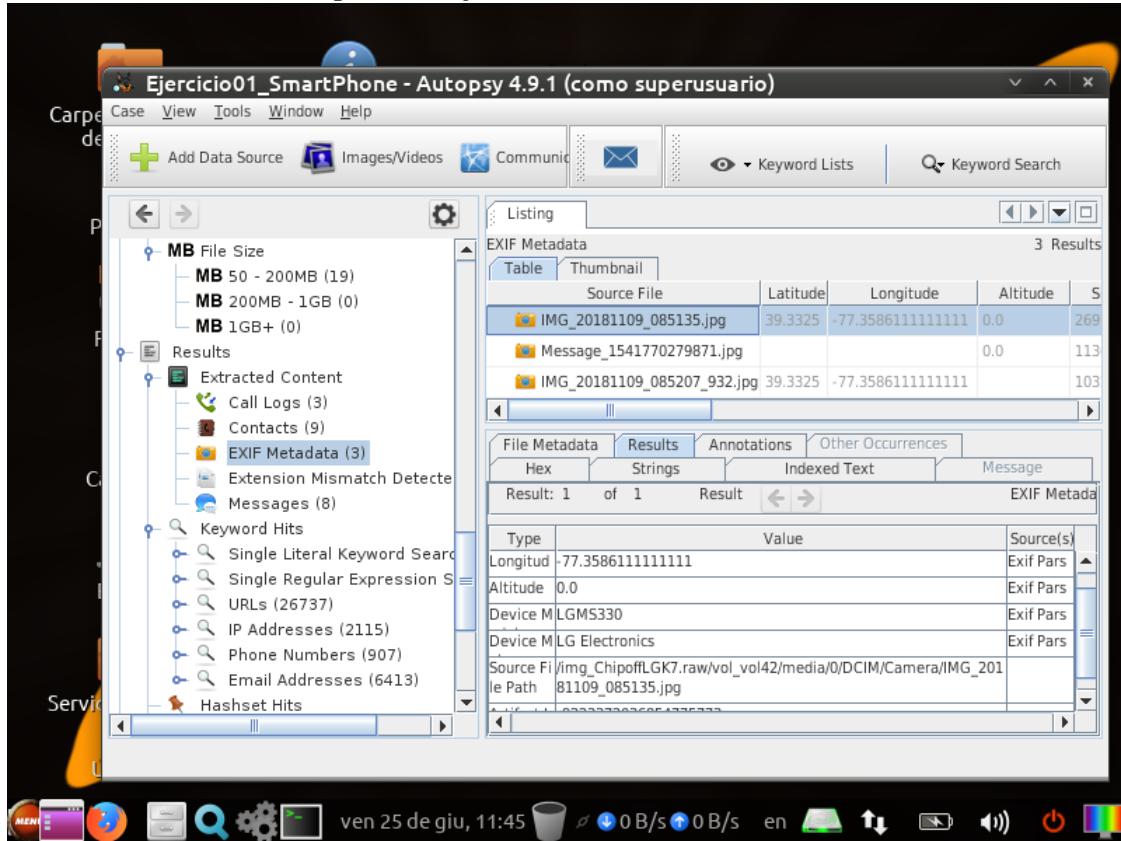
h) Dos de ellos tienen longitud y latitud (y uno de esos dos altitud). El tercero solo tiene la altitud.

Figura 11: Ejercicio 1: Metadatos de coordenadas



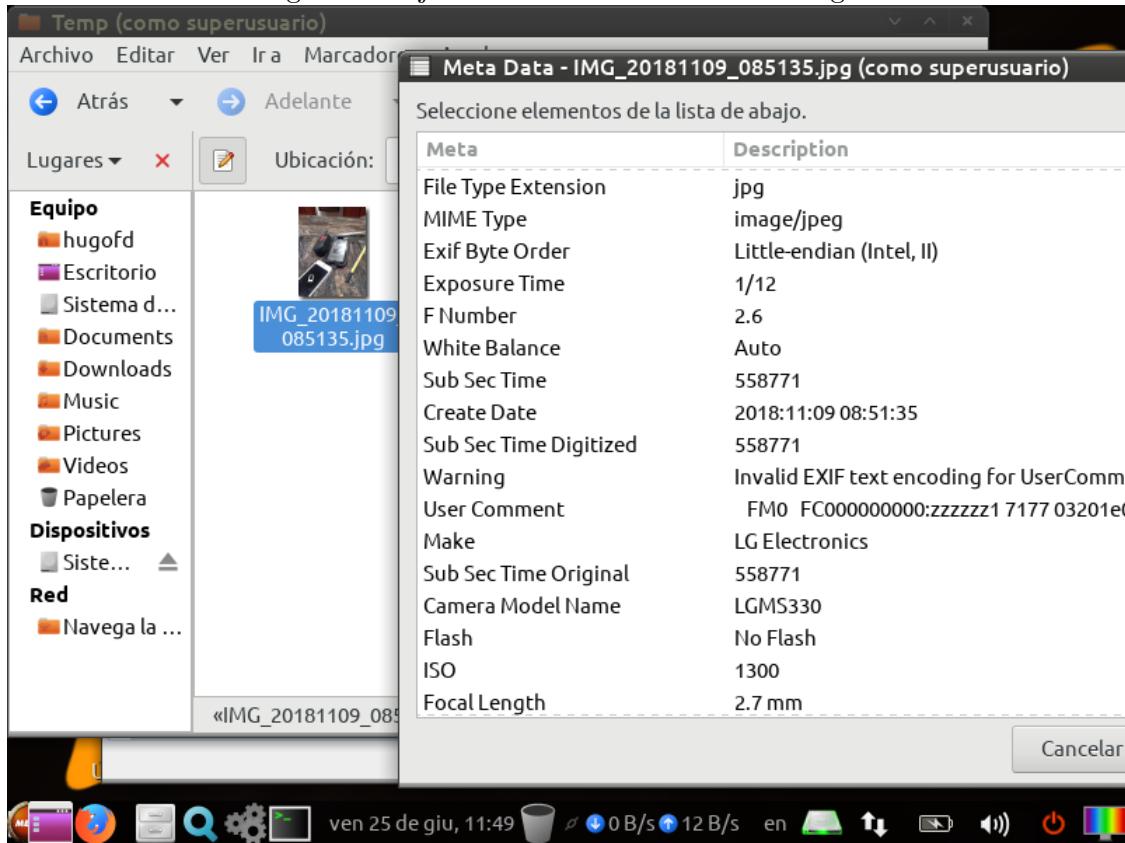
- i) TBD GOOGLE MAPS
- j) TBD GOOGLE MAPS
- k) Con la cámara LGMS330 de un dispositivo LG.

Figura 12: Ejercicio 1: Modelo de cámara



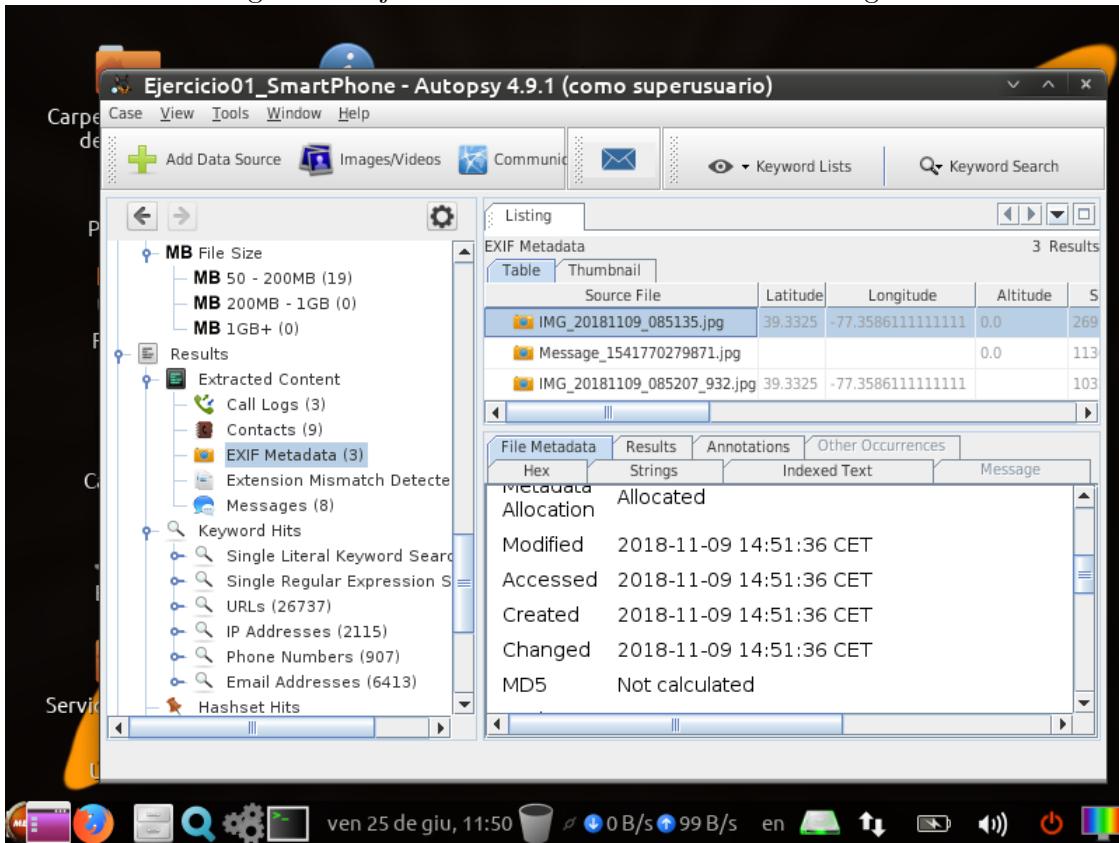
l) 2018/11/09 08:51:35

Figura 13: Ejercicio 1: Información de la imagen



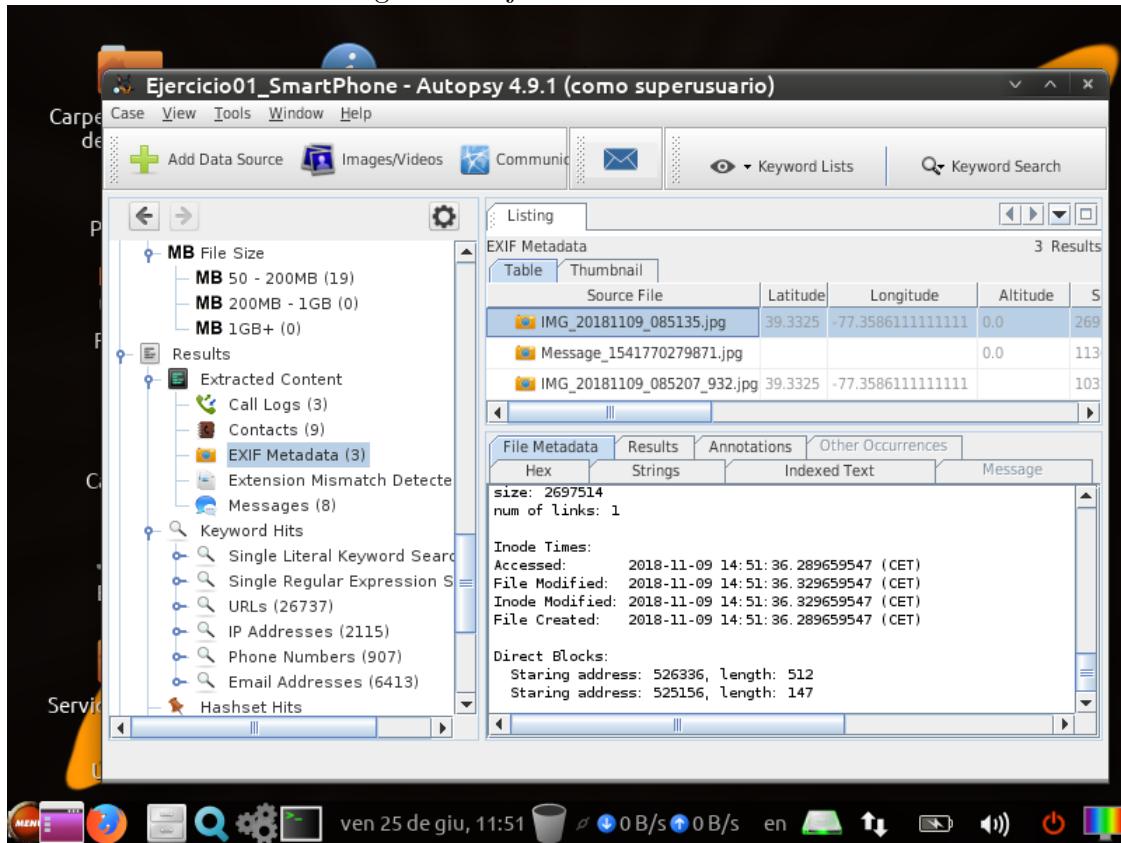
m) 2018/11/09 13:51:36

Figura 14: Ejercicio 1: Fecha de creación de la imagen



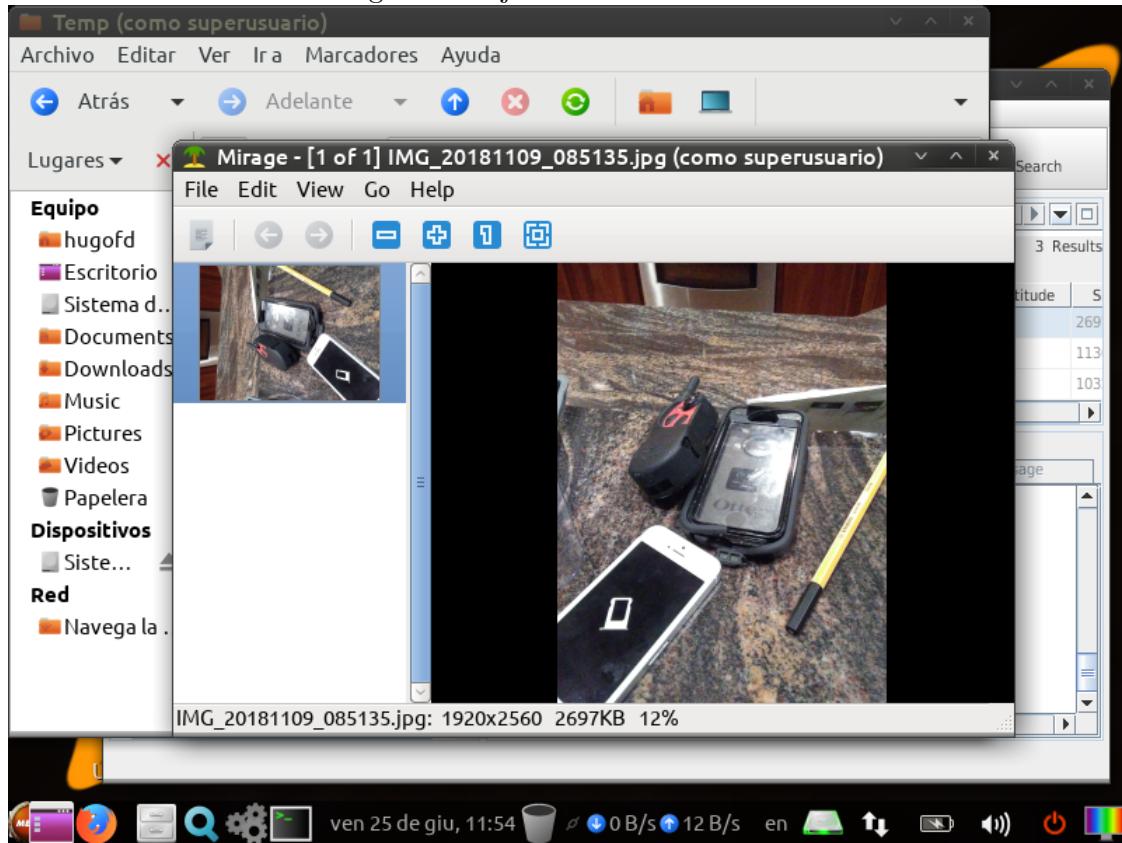
- n) No, hay diferencias entre la hora de modificación del inodo y del fichero y la hora de creación y de acceso del fichero.

Figura 15: Ejercicio 1: MAC times



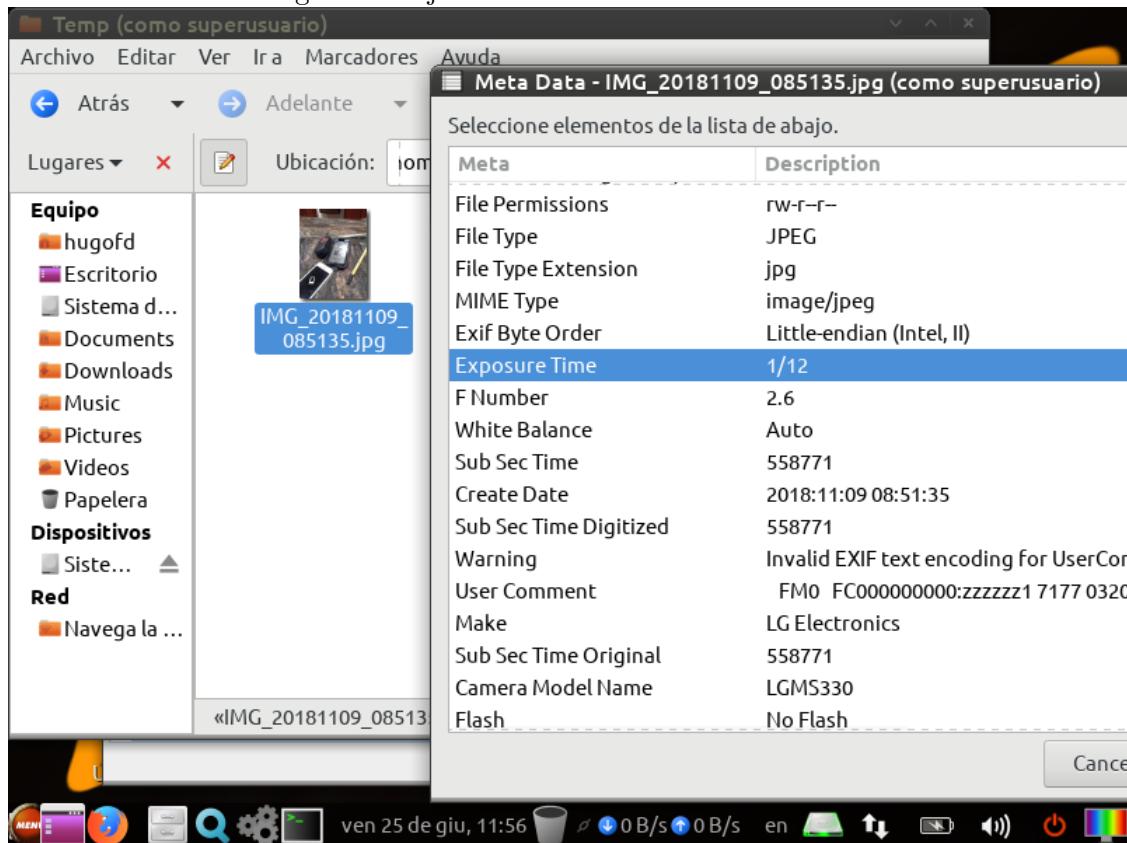
- o) Hay dos móviles, uno de color blanco y otro oscuro con funda negra.

Figura 16: Ejercicio 1: Foto móviles



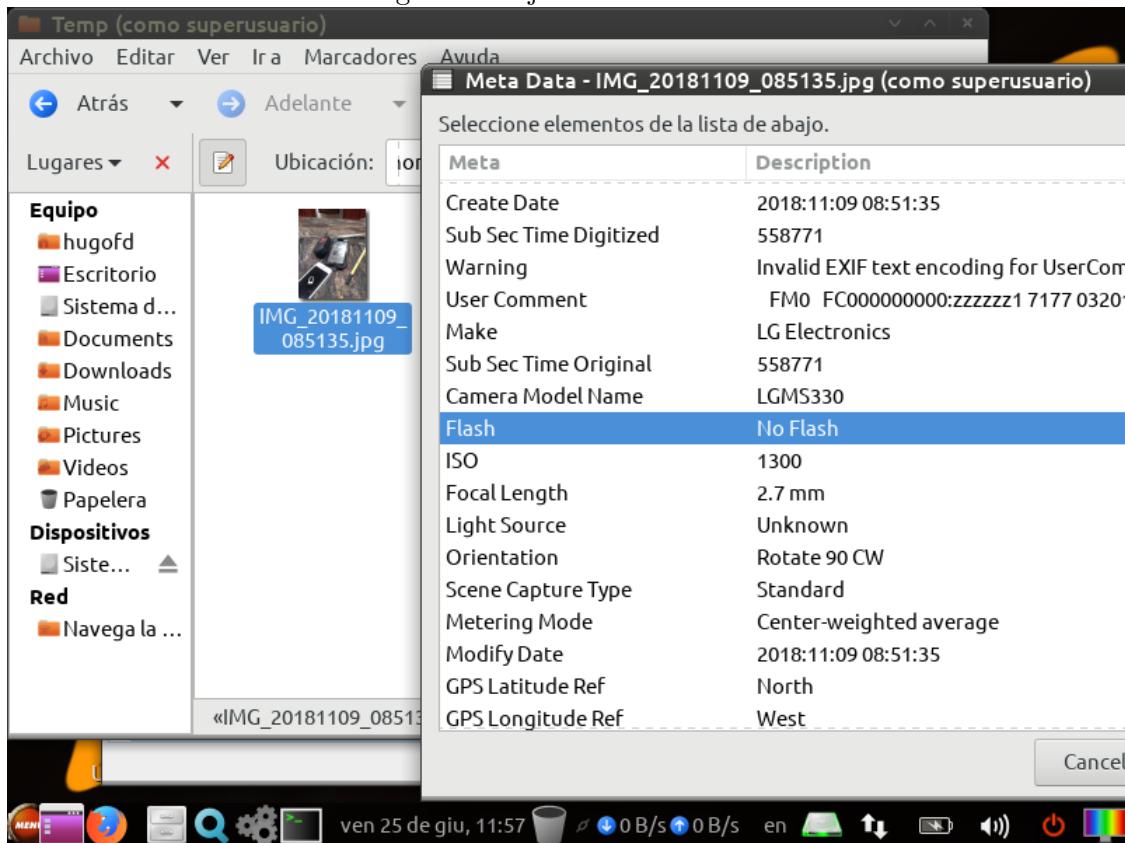
- p) Se puede ver en la captura anterior, 1920x2560.
- q) Una velocidad de obturación de 1/12.

Figura 17: Ejercicio 1: Velocidad de obturación



r) No se utilizó flash.

Figura 18: Ejercicio 1: No flash



s) Hay un fichero *emma-girl.jpg*.

Figura 19: Ejercicio 1: Carpeta download

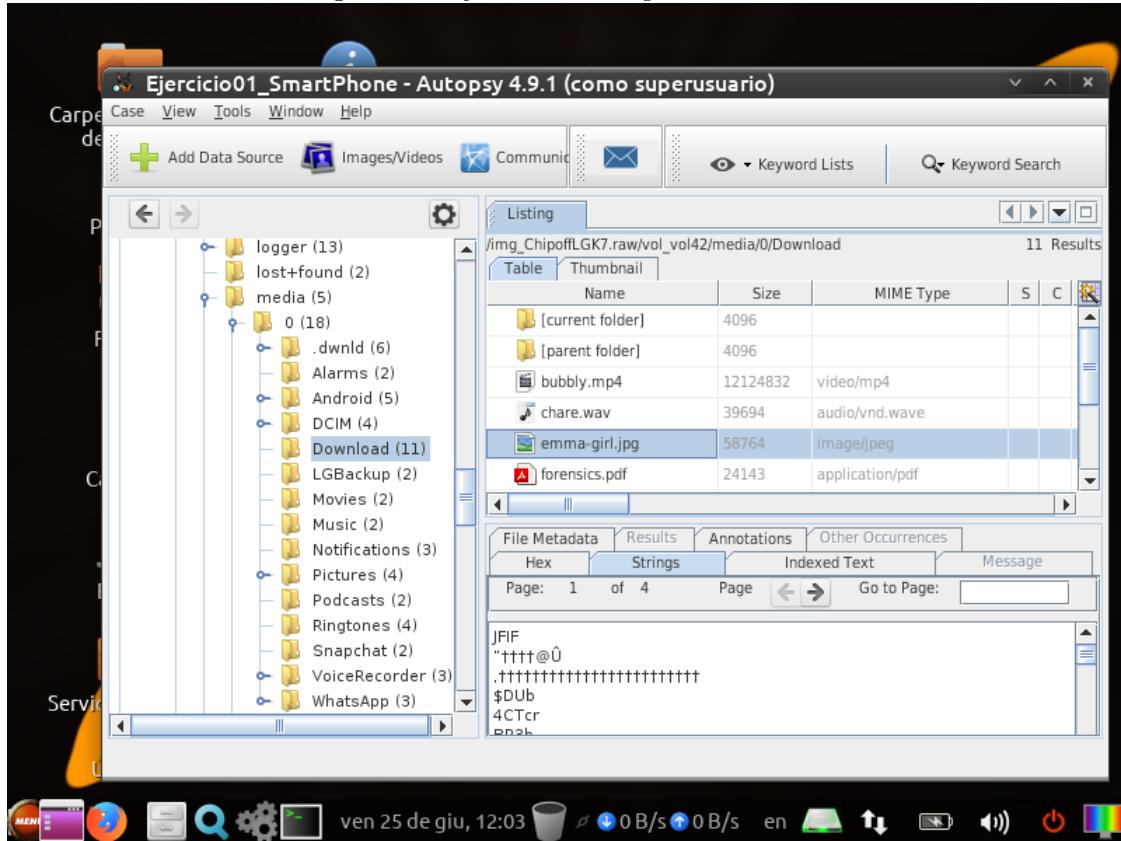
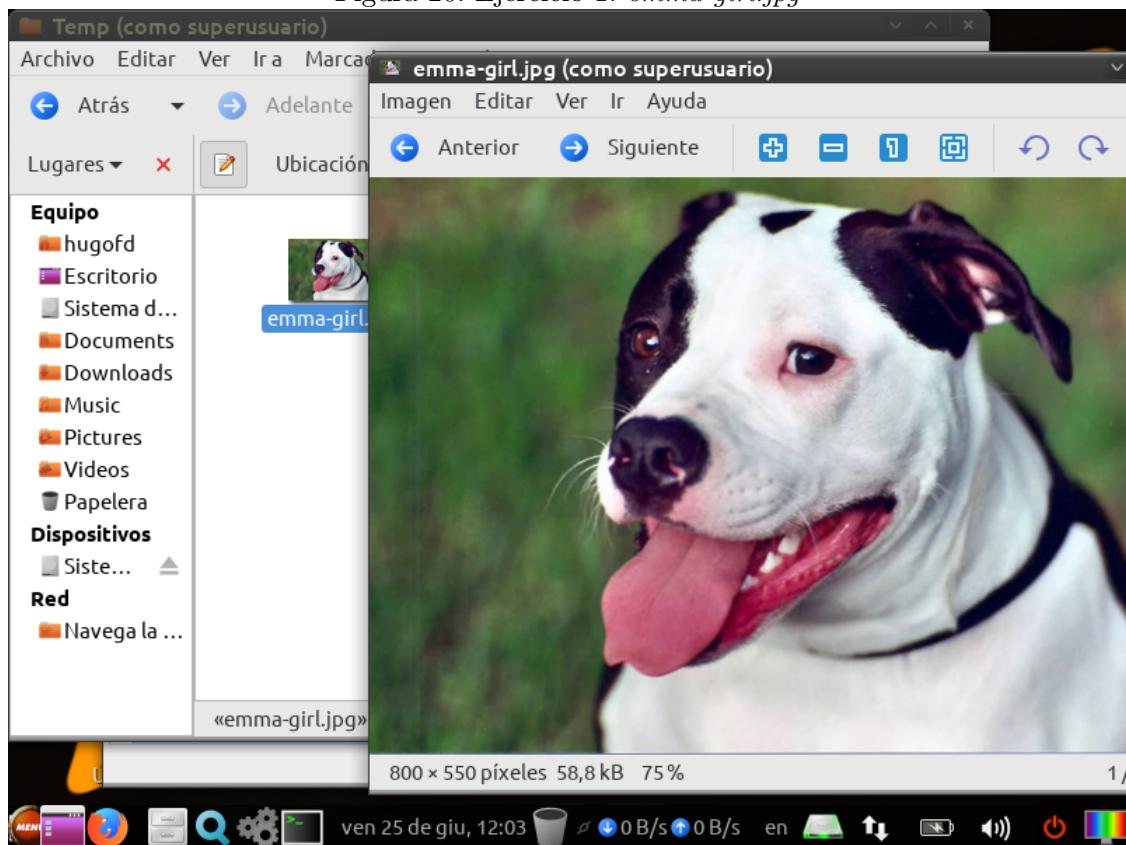
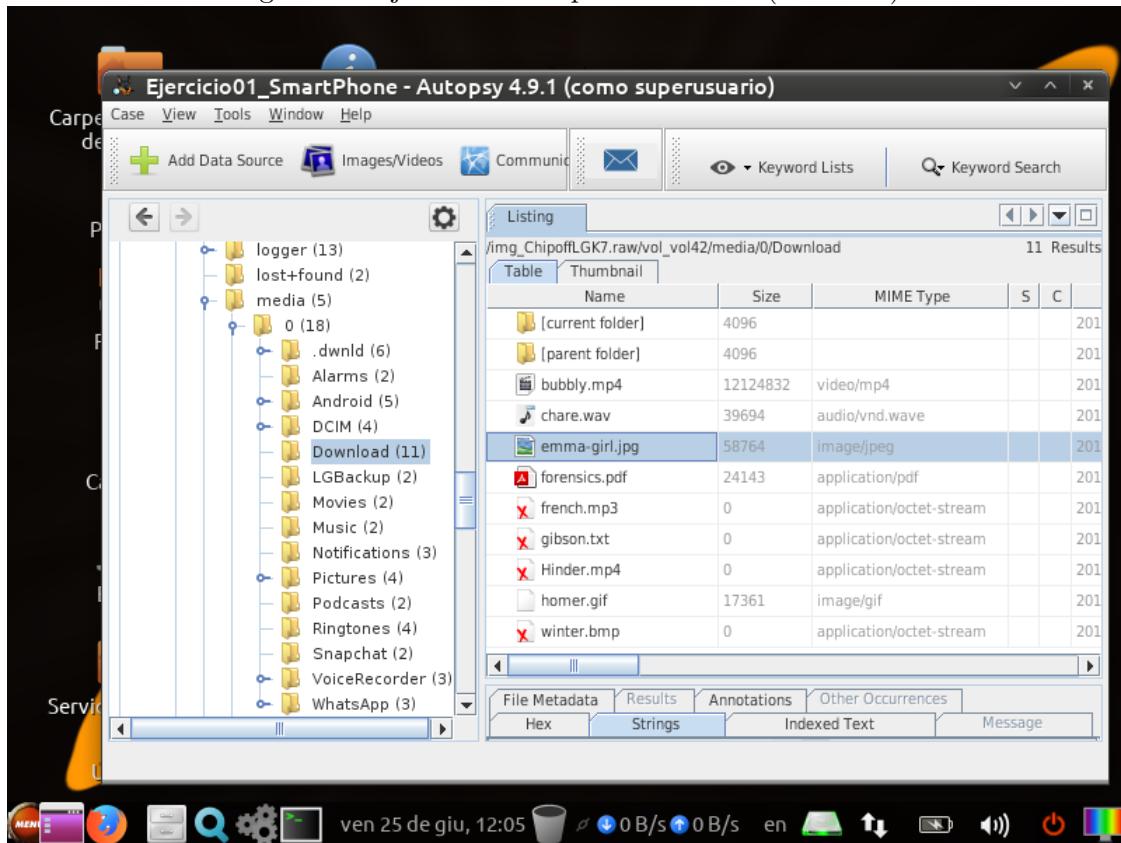


Figura 20: Ejercicio 1: *emma-girl.jpg*



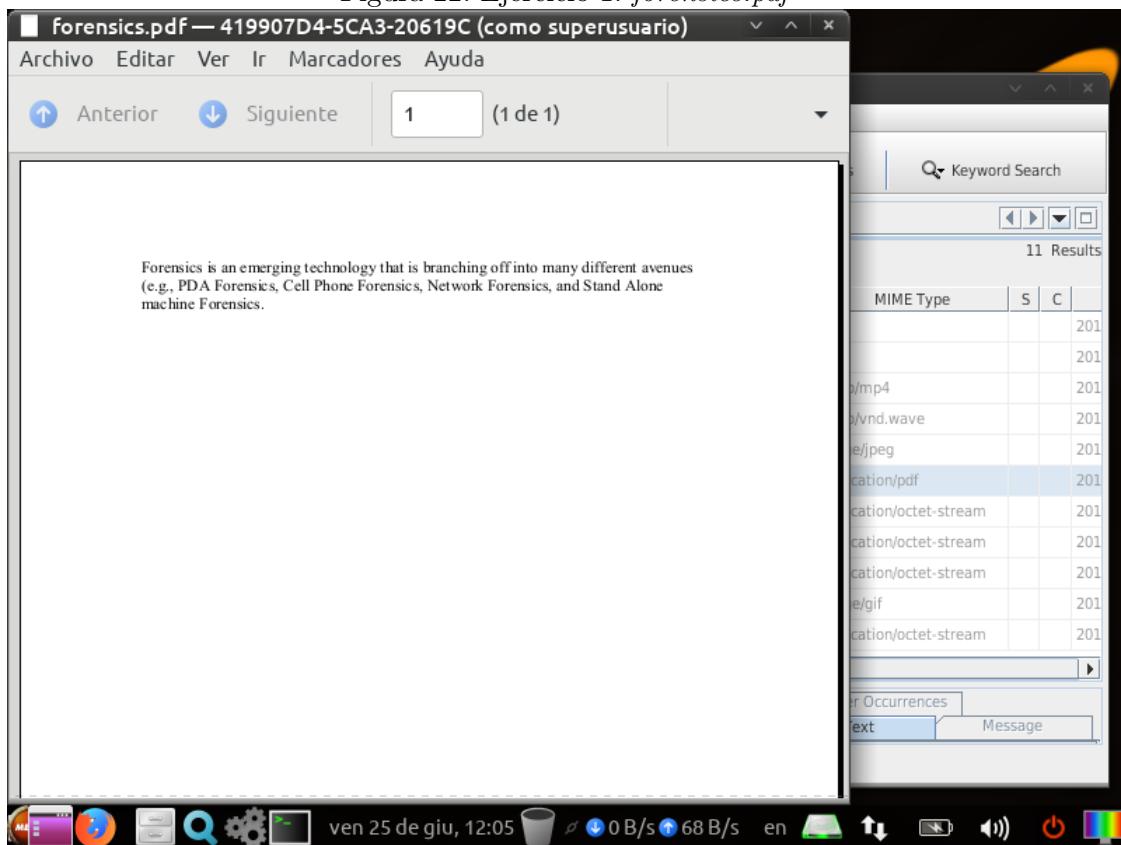
t) Uno, llamado *forensics.pdf*.

Figura 21: Ejercicio 1: Carpeta download (de nuevo)



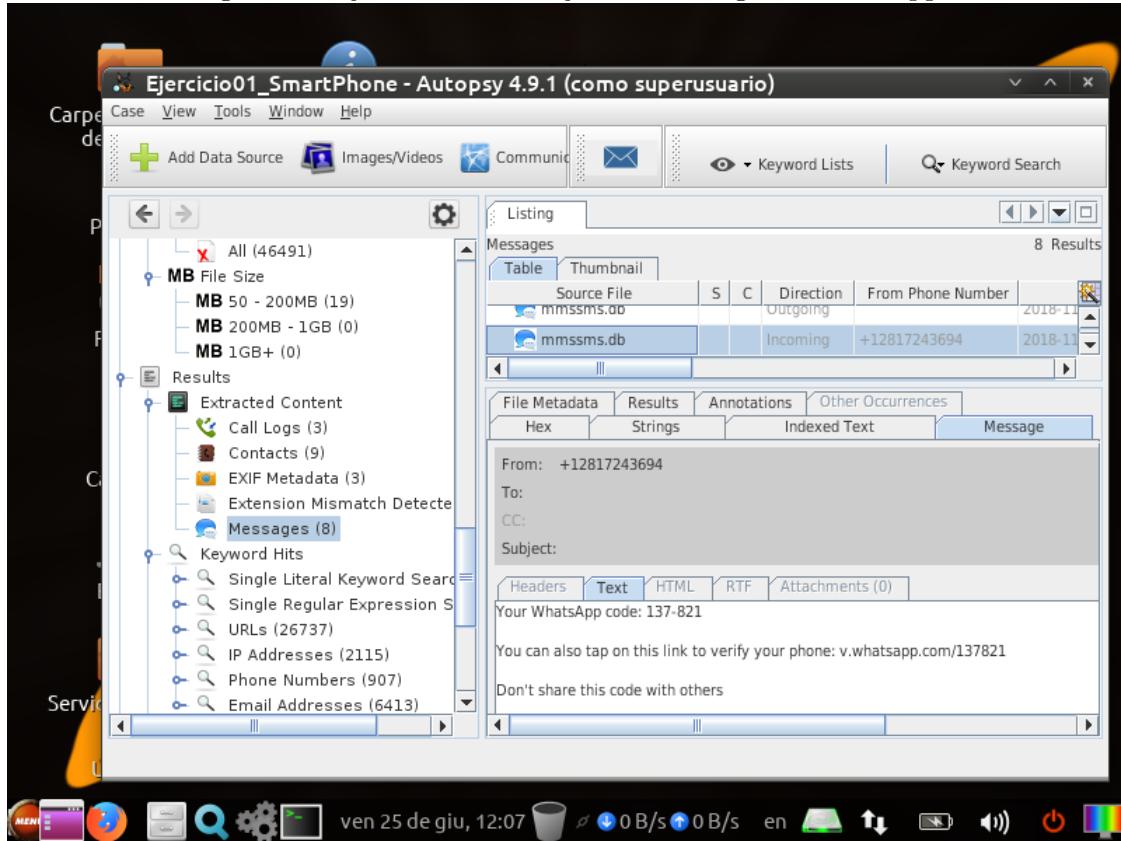
- u) Cuatro, como se ve en la anterior captura.
- v) En la carpeta download hay un fichero pdf llamado *forensics.pdf*.
- w) Se muestra su contenido en la siguiente captura.

Figura 22: Ejercicio 1: *forensics.pdf*



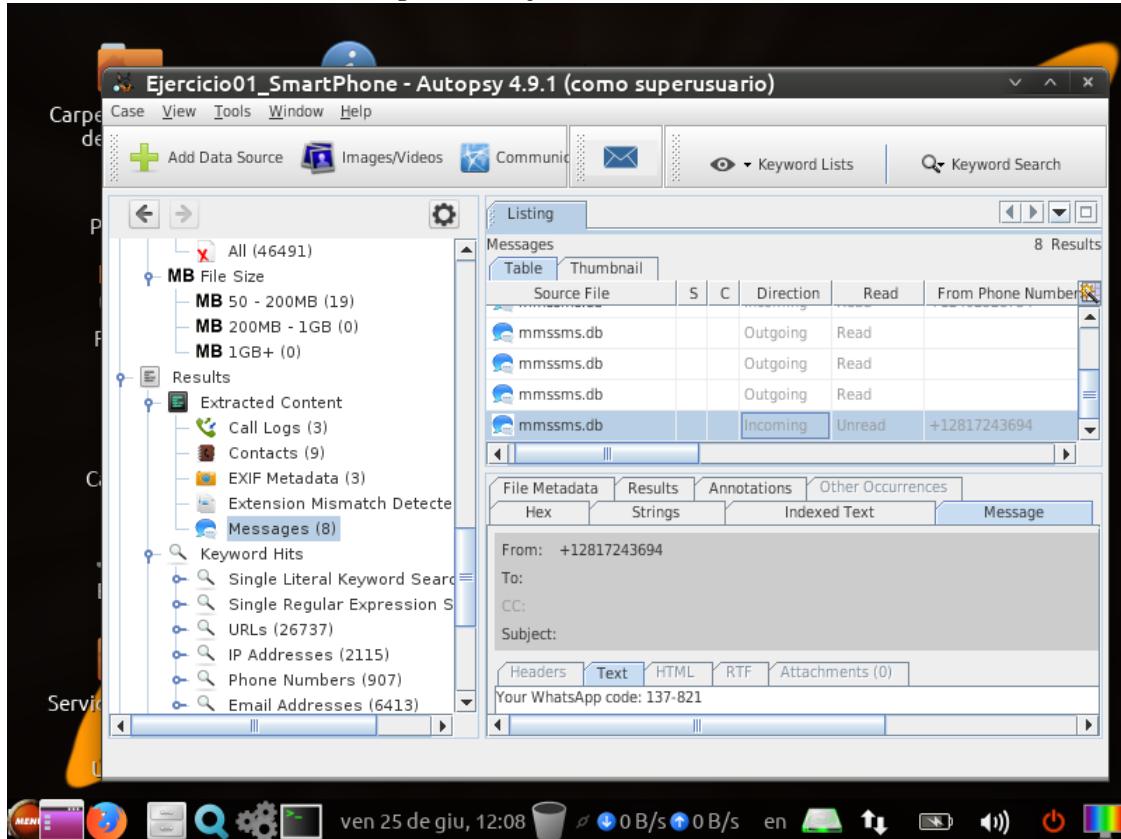
- x) Los mensajes pueden encontrarse en Extracted Content, Messages. El mensaje con el código de Whatsapp se muestra a continuación.

Figura 23: Ejercicio 1: Mensaje con el código de Whatsapp



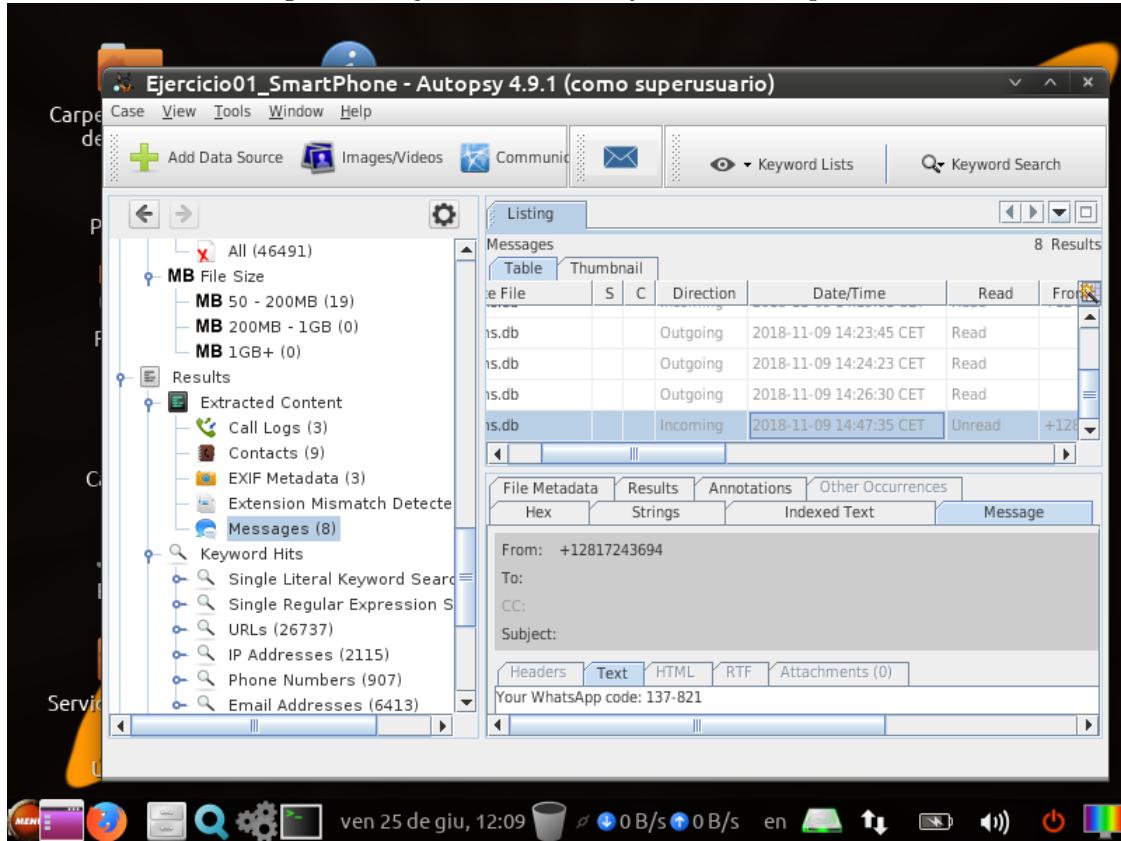
y) El mensaje aparece como *No leído*.

Figura 24: Ejercicio 1: No leído



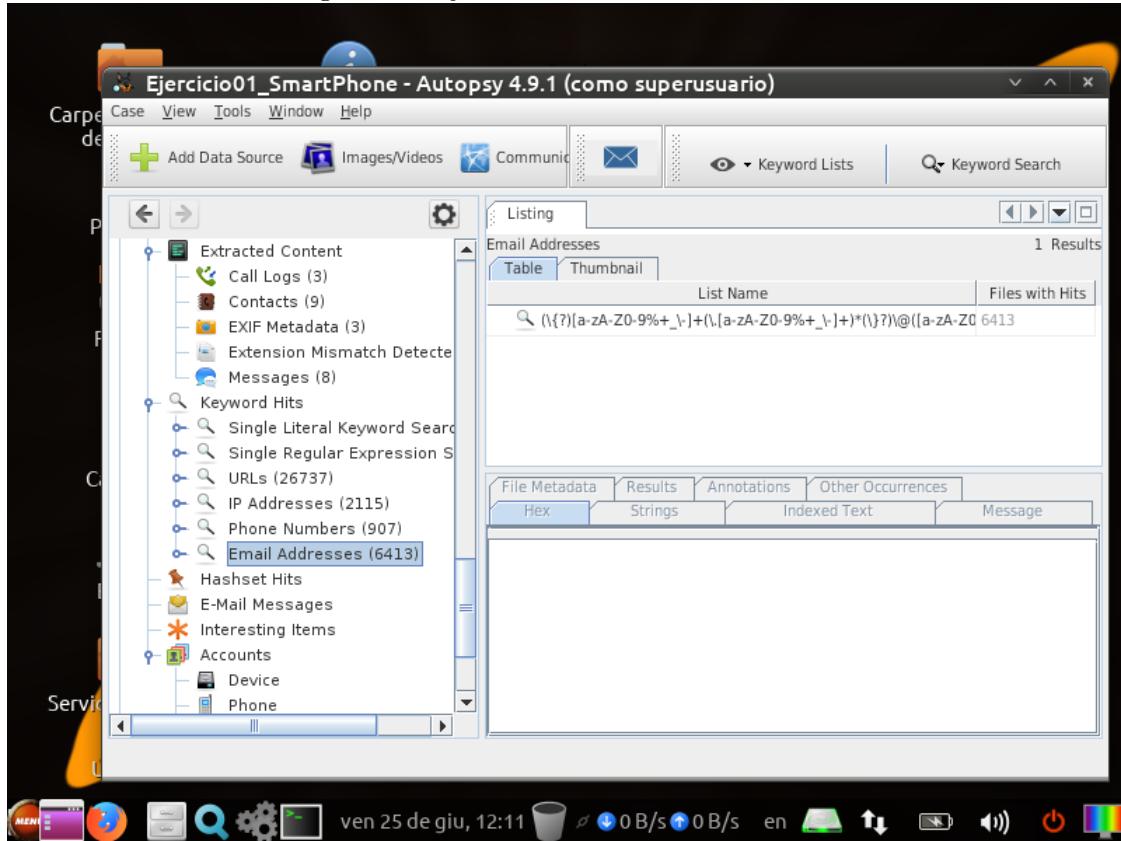
z) El mensaje se recibió el 2018/11/09 a las 14:47:35 CET.

Figura 25: Ejercicio 1: Fecha y hora de recepción



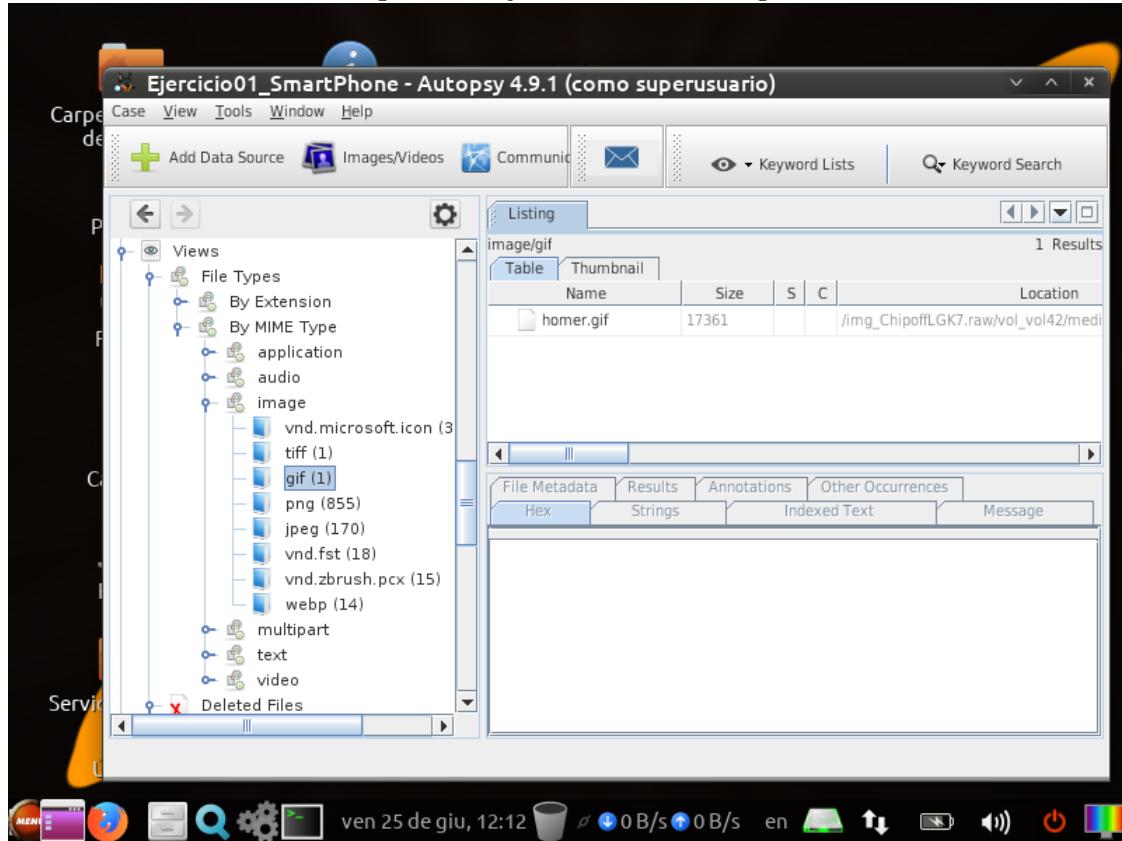
aa) El módulo de búsqueda de cadenas detectó 6413 direcciones de email.

Figura 26: Ejercicio 1: Direcciones de email



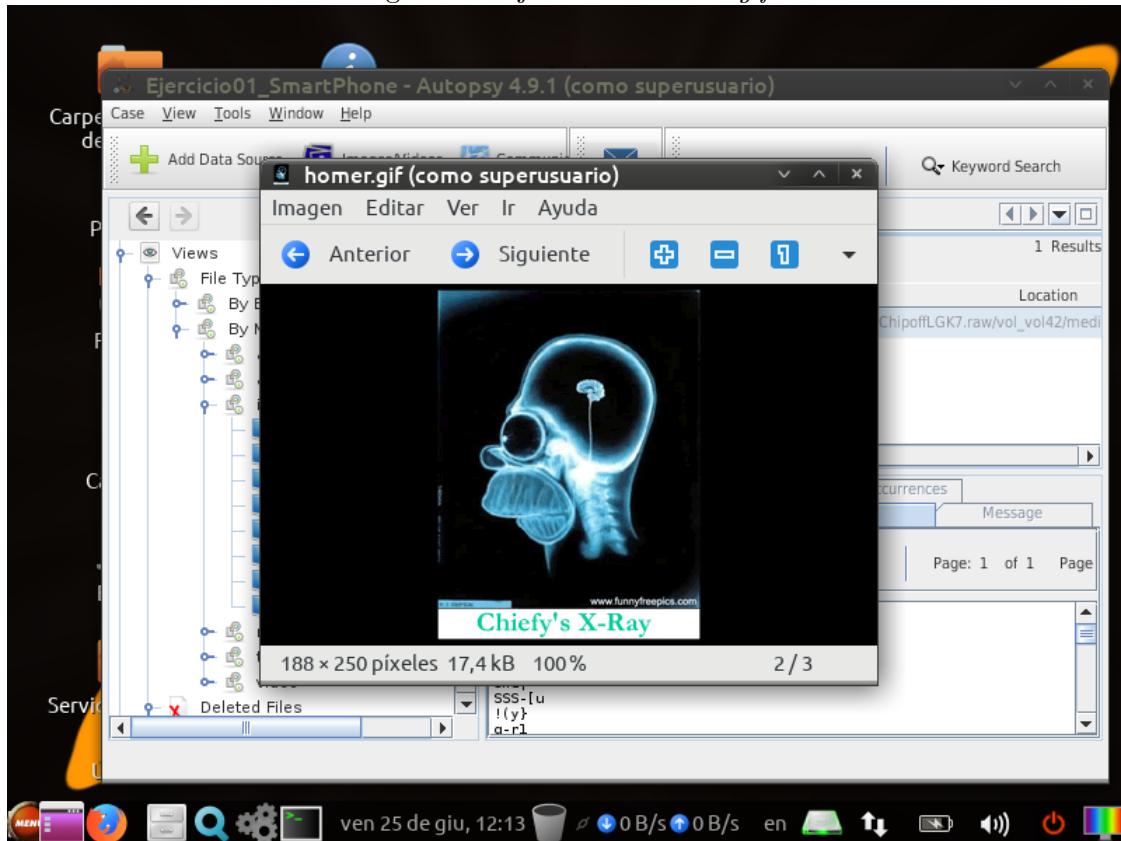
bb) Se puede buscar en el apartado Views por tipo MIME, se observa que hay un único fichero gif detectado, llamado *homer.gif*.

Figura 27: Ejercicio 1: Ficheros gif



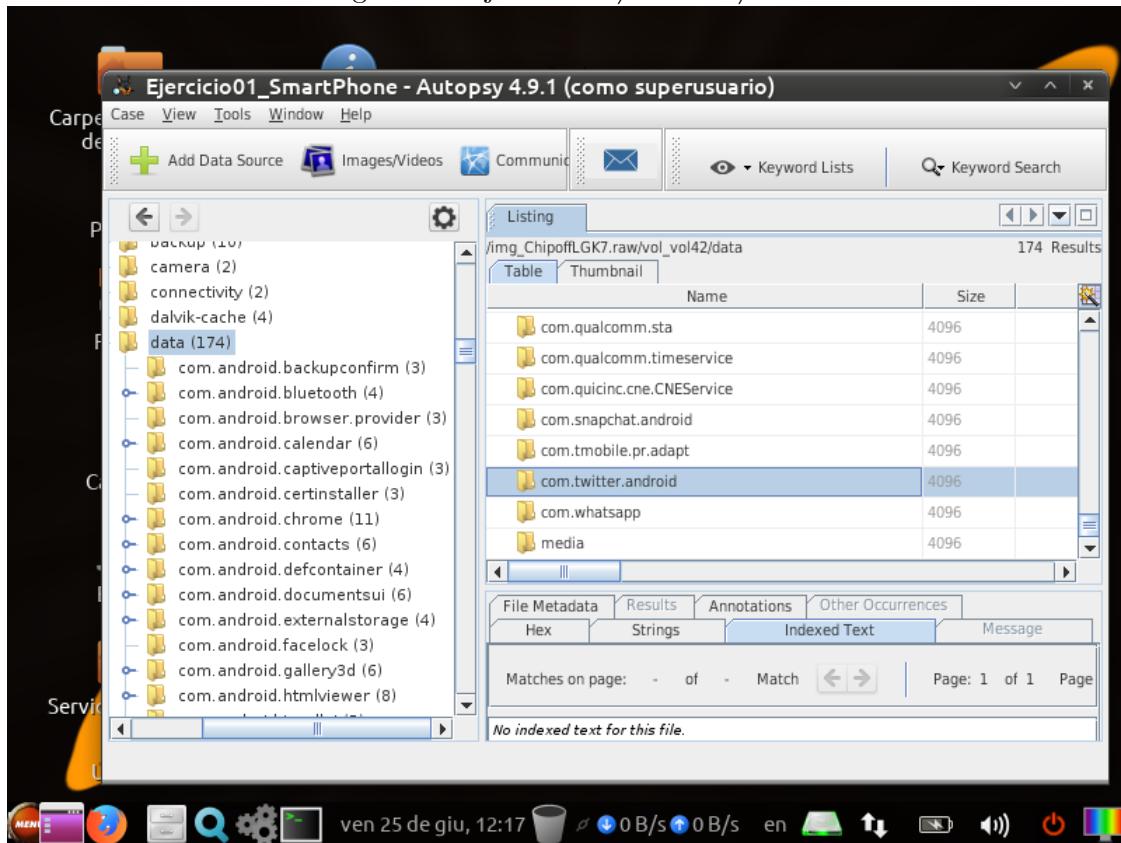
cc) Se muestra a continuación una captura del fichero *homer.gif*.

Figura 28: Ejercicio 1: *homer.gif*



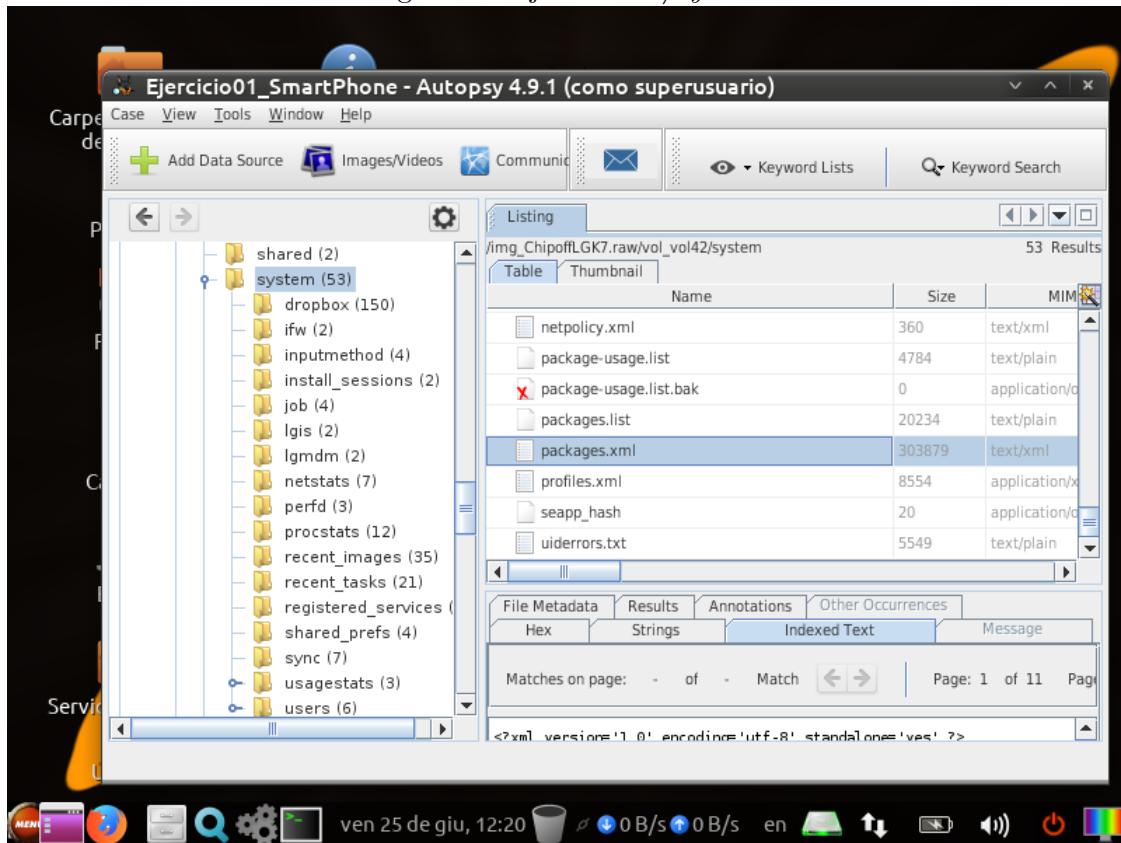
dd) Se busca entre las subcarpetas de */userdata/data* (en la partición 42) las posibles redes sociales que maneja el usuario. Se encuentran *Facebook*, *Instagram*, *LinkedIn*, *Pinterest*, *Snapchat*, *Twitter*, *Whatsapp* y *Youtube*.

Figura 29: Ejercicio 1: */userdata/data*



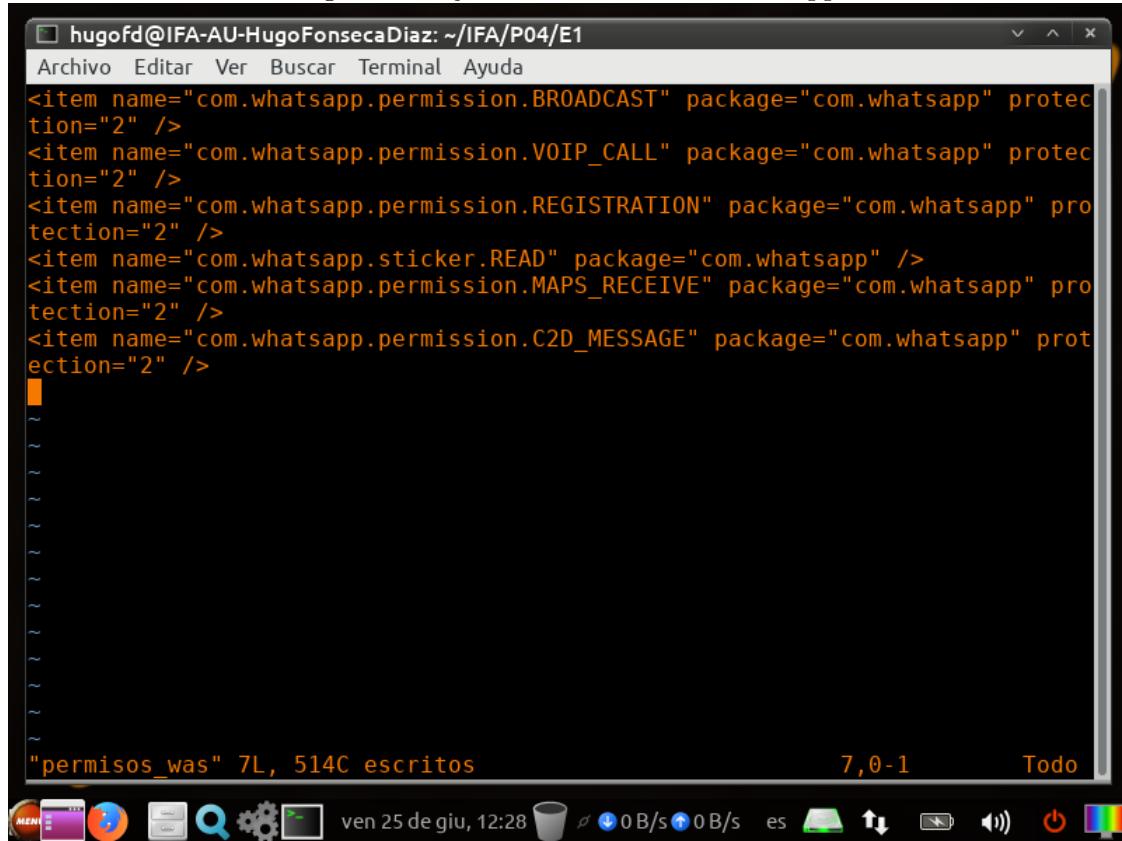
ee) Se extrae el fichero *packages.xml*, encontrado en la carpeta */system* del volumen 42.

Figura 30: Ejercicio 1: */system*



ff) Se muestran a continuación las líneas de los permisos de *Whatsapp* en el editor Vim.

Figura 31: Ejercicio 1: Permisos Whatsapp



The screenshot shows a terminal window titled "hugofd@IFA-AU-HugoFonsecaDiaz: ~/IFA/P04/E1". The window contains XML code listing various permissions for the WhatsApp application (com.whatsapp). The permissions listed include:

```
<item name="com.whatsapp.permission.BROADCAST" package="com.whatsapp" protection="2" />
<item name="com.whatsapp.permission.VOIP_CALL" package="com.whatsapp" protection="2" />
<item name="com.whatsapp.permission.REGISTRATION" package="com.whatsapp" protection="2" />
<item name="com.whatsapp.sticker.READ" package="com.whatsapp" />
<item name="com.whatsapp.permission.MAPS_RECEIVE" package="com.whatsapp" protection="2" />
<item name="com.whatsapp.permission.C2D_MESSAGE" package="com.whatsapp" protection="2" />
```

Below the XML code, there are several tilde (~) characters, likely indicating a continuation of the file or a placeholder. At the bottom of the terminal window, the status bar displays the command "permisos\_was", the file size "7L, 514C escritos", the version "7.0-1", and the word "Todo". The terminal window is part of a desktop environment, with icons for various applications visible in the taskbar at the bottom.

- gg) El instalador de *Whatsapp* se encuentra en *com.android.vending*, dentro de la carpeta */data*.  
hh) Hay seis cuentas asociadas.

Figura 32: Ejercicio 1: *Accounts.db* - Tabla *accounts*

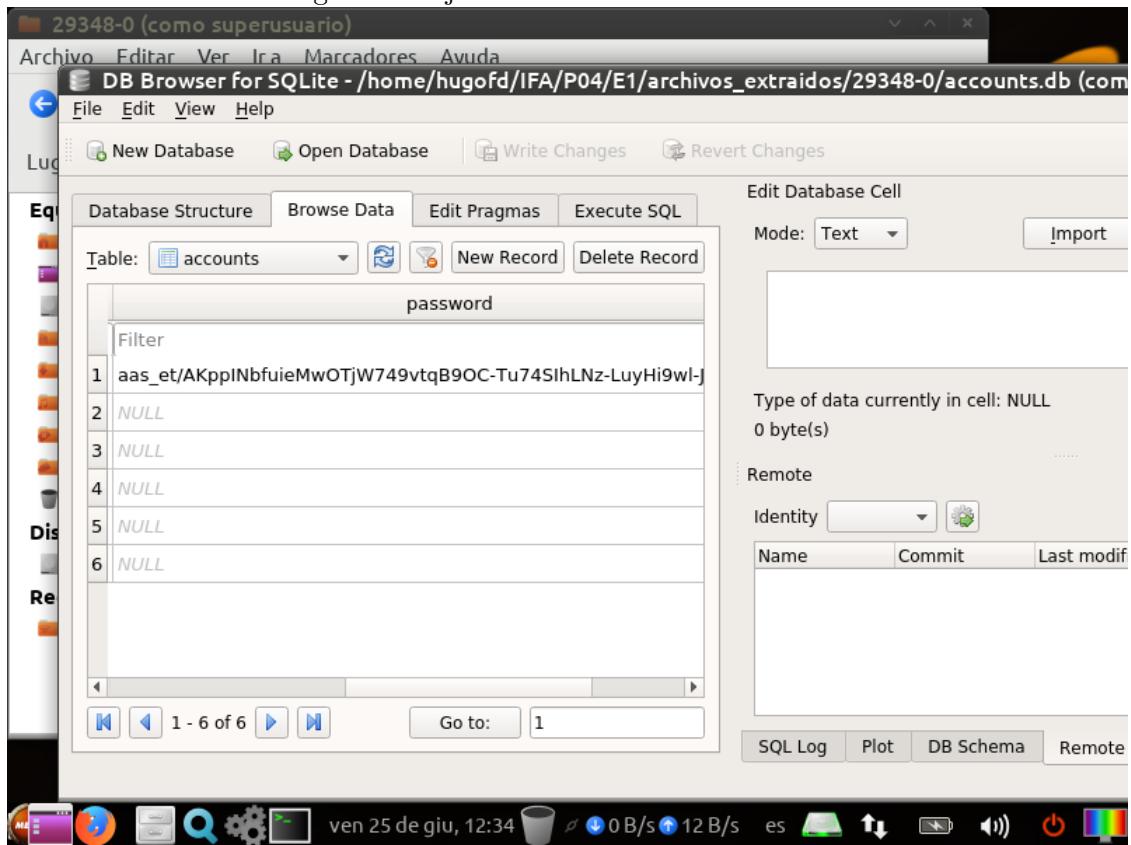
The screenshot shows the DB Browser for SQLite interface. The title bar reads "29348-0 (como superusuario)" and "DB Browser for SQLite - /home/hugofd/IFA/P04/E1/archivos\_extraidos/29348-0/accounts.db (com)". The main window displays the "accounts" table with the following data:

	_id	name	type
		Filter	Filter
1	1	cfttmobile1@gmail.com	com.google
2	4	cfttmobile1	com.twitter.android.auth.login
3	6	WhatsApp	com.whatsapp
4	3	Messenger	com.facebook.messenger
5	5	LinkedIn	com.linkedin.android
6	2	Facebook	com.facebook.auth.login

Below the table, there is a message: "Type of data currently in cell: NULL 0 byte(s)". On the right side, there is a "Edit Database Cell" panel with "Mode: Text" and an "Import" button. At the bottom, there are tabs for "SQL Log", "Plot", "DB Schema", and "Remote". The status bar at the bottom shows the date and time: "ven 25 de giu, 12:33".

- ii) La cuenta de Google es *cfttmobile1@gmail.com*. Puede observarse en la anterior captura.
- jj) Puede observarse la contraseña hasheada en la siguiente captura.

Figura 33: Ejercicio 1: Contraseña hasheada



## Referencias