

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

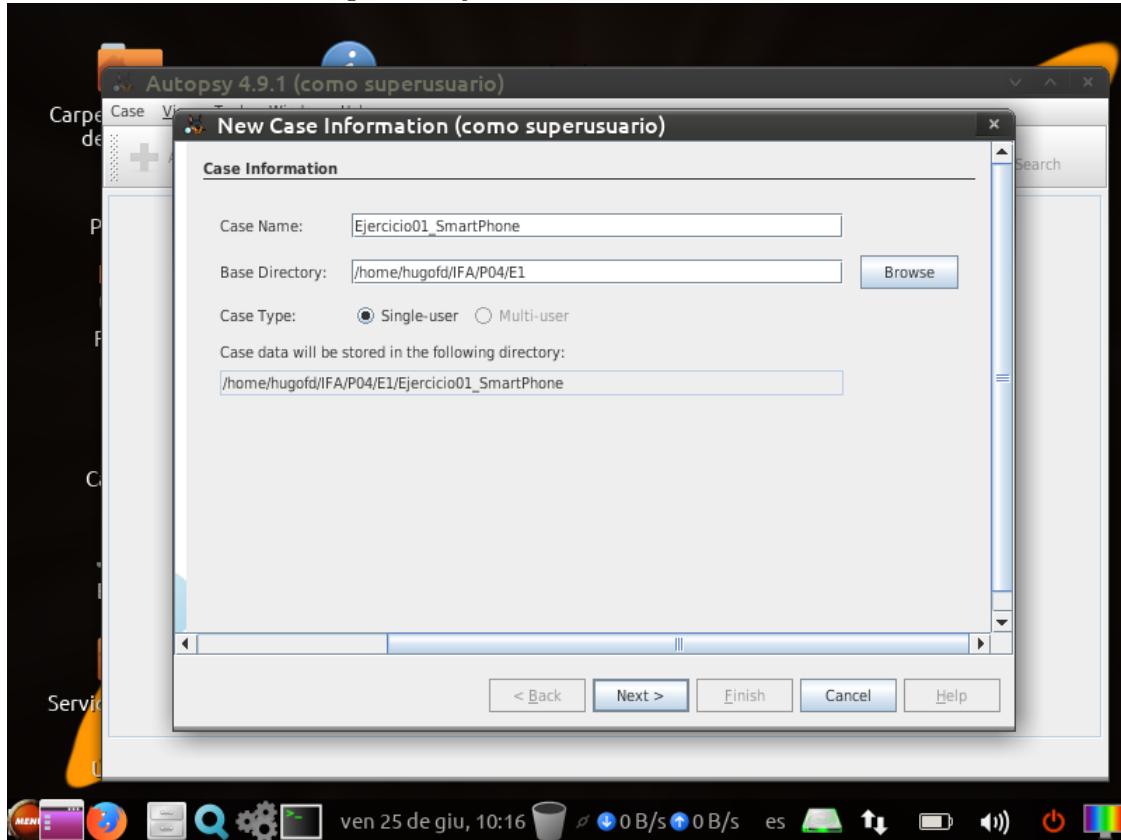
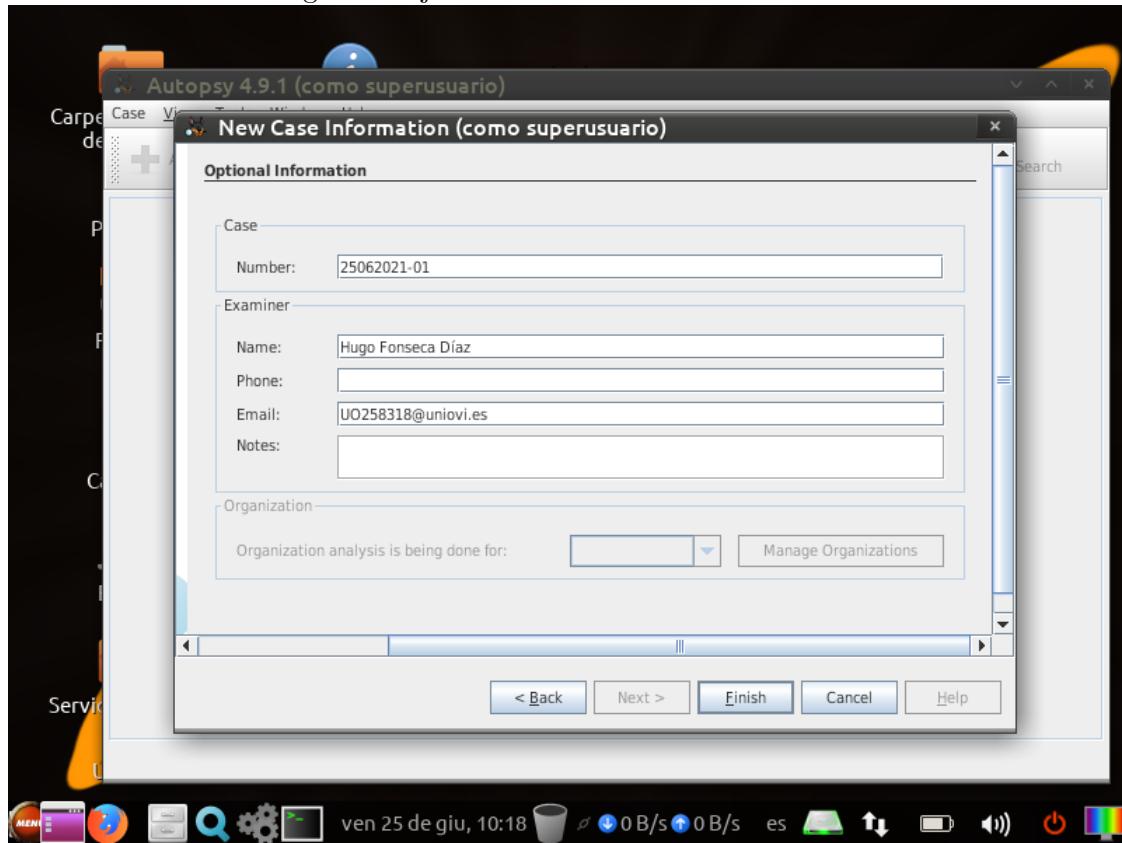
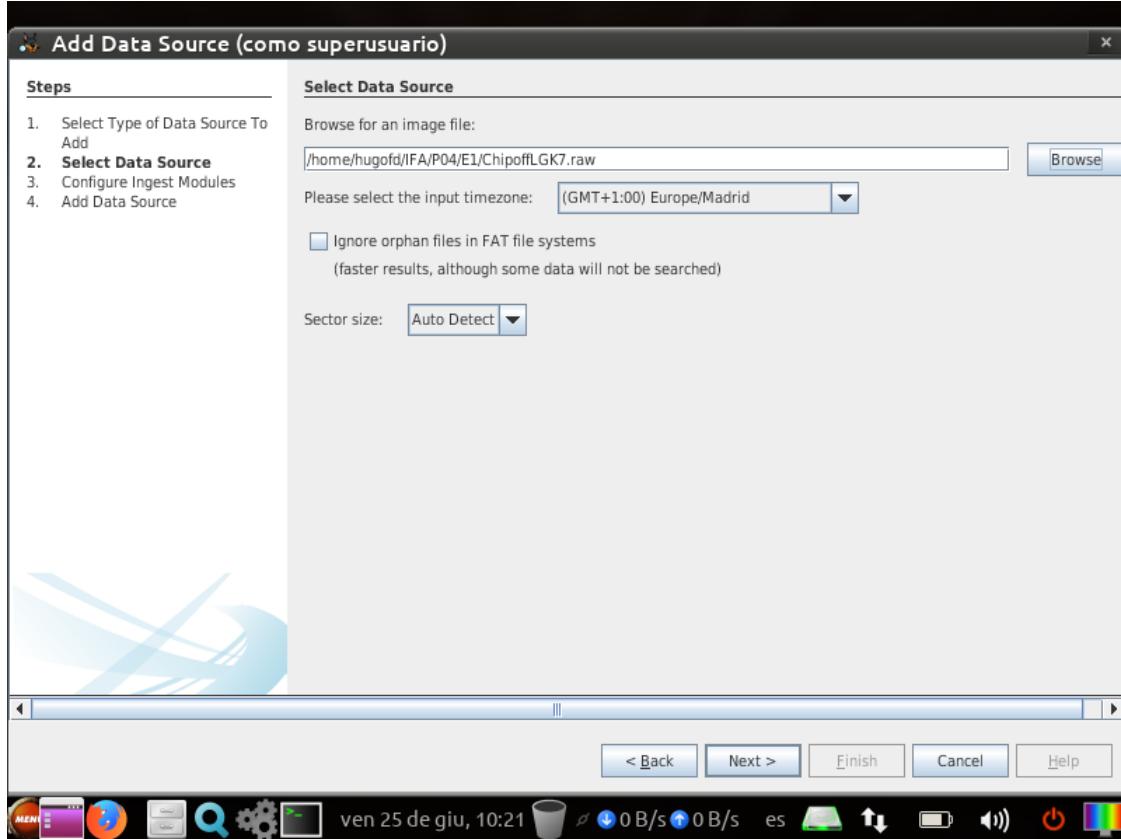


Figura 2: Ejercicio 1: Detalles del examinador



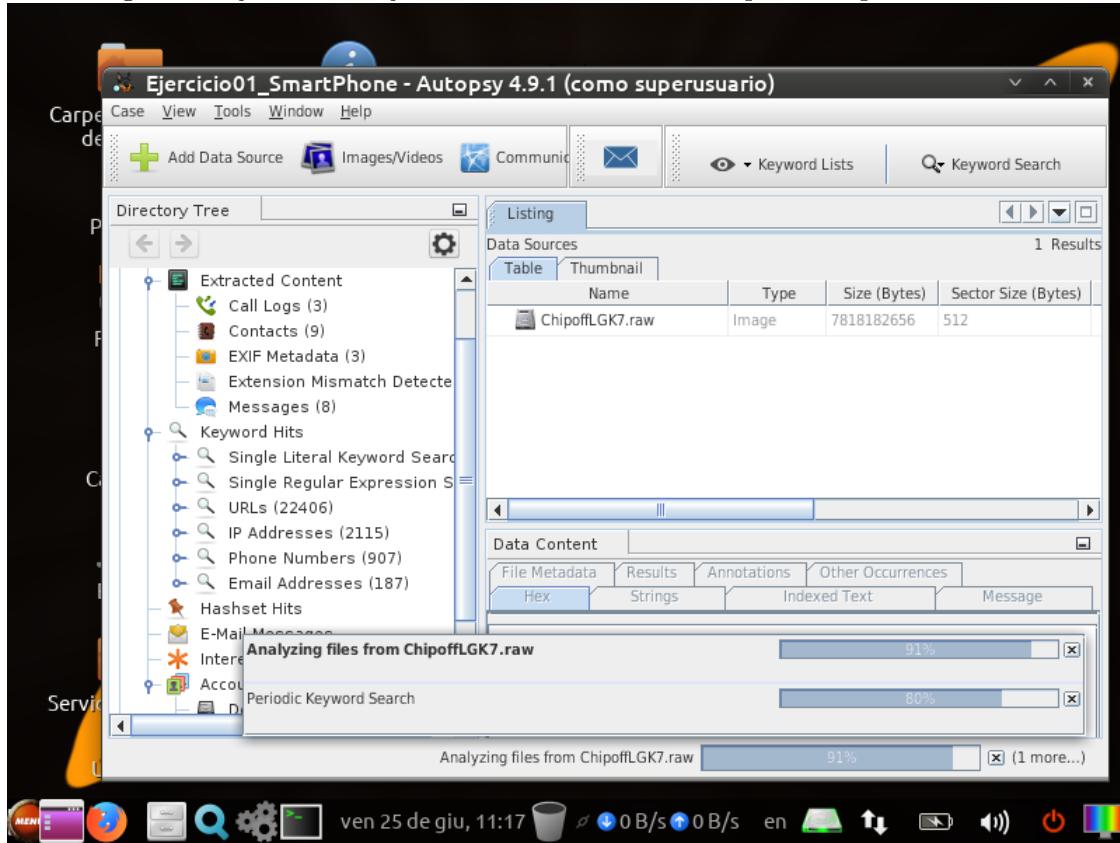
Añadimos la imagen a analizar.

Figura 3: Ejercicio 1: Selección de la imagen



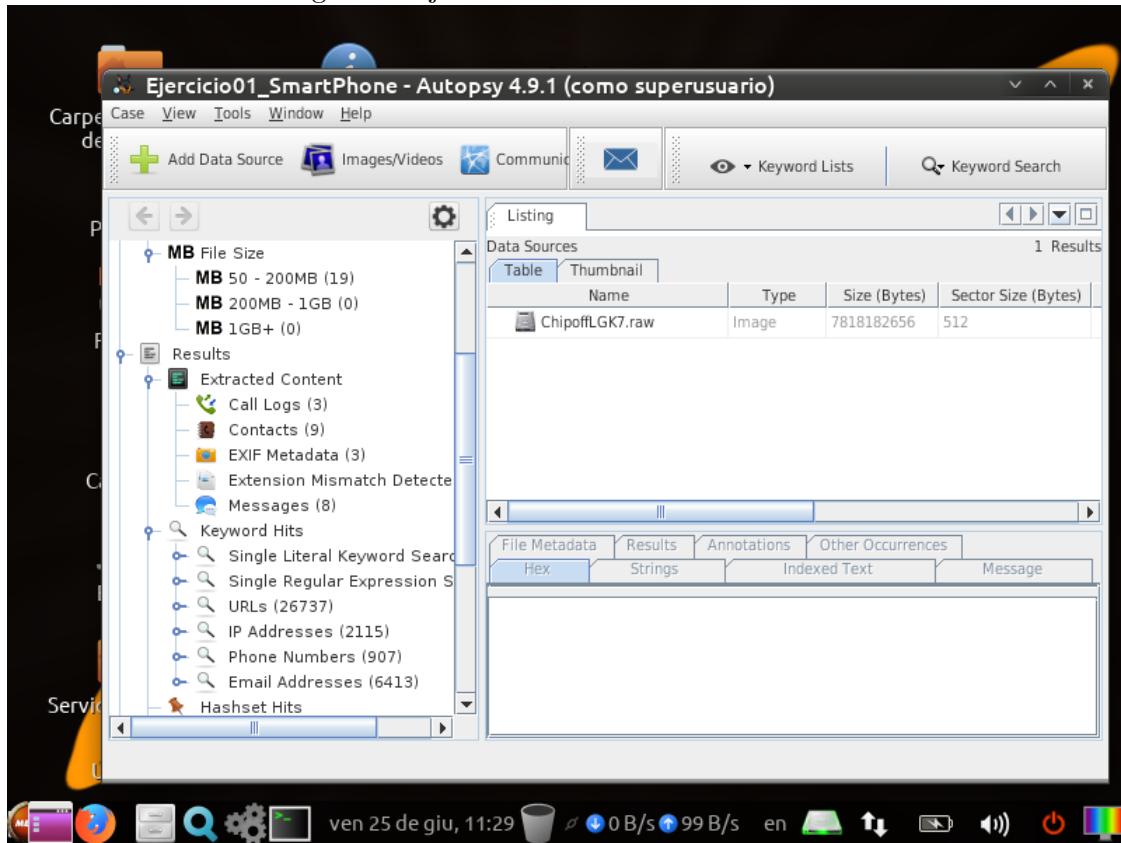
Se ejecutan los módulos de uno en uno para que el cómputo no sea excesivo. El que más tarda en ejecutarse es el módulo de búsqueda de palabras clave, el cual se ha dejado para el final.

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



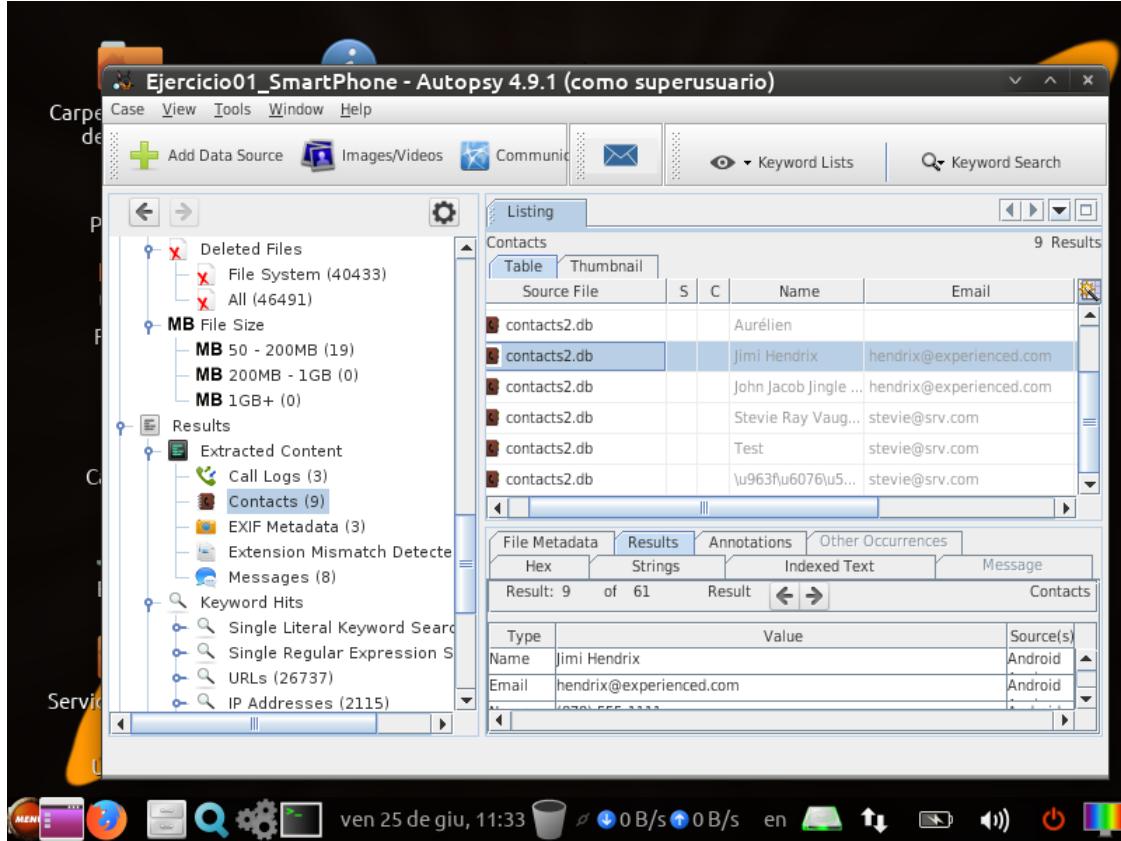
Una vez finalizada la ejecución de los módulos, se tienen los datos necesarios para responder a las cuestiones del ejercicio.

Figura 5: Ejercicio 1: Resultados del análisis



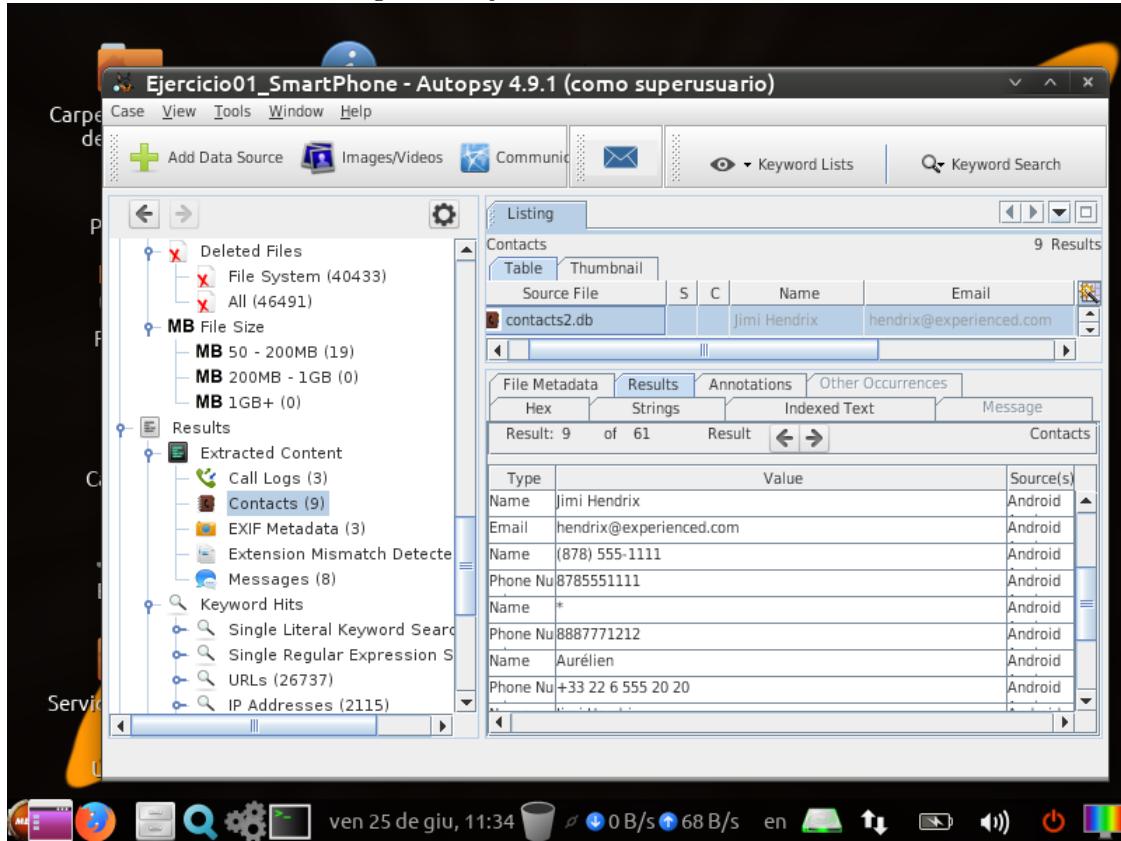
a) Como se puede observar en la siguiente imagen, hay un total de 9 entradas en el apartado de contactos.

Figura 6: Ejercicio 1: Contactos



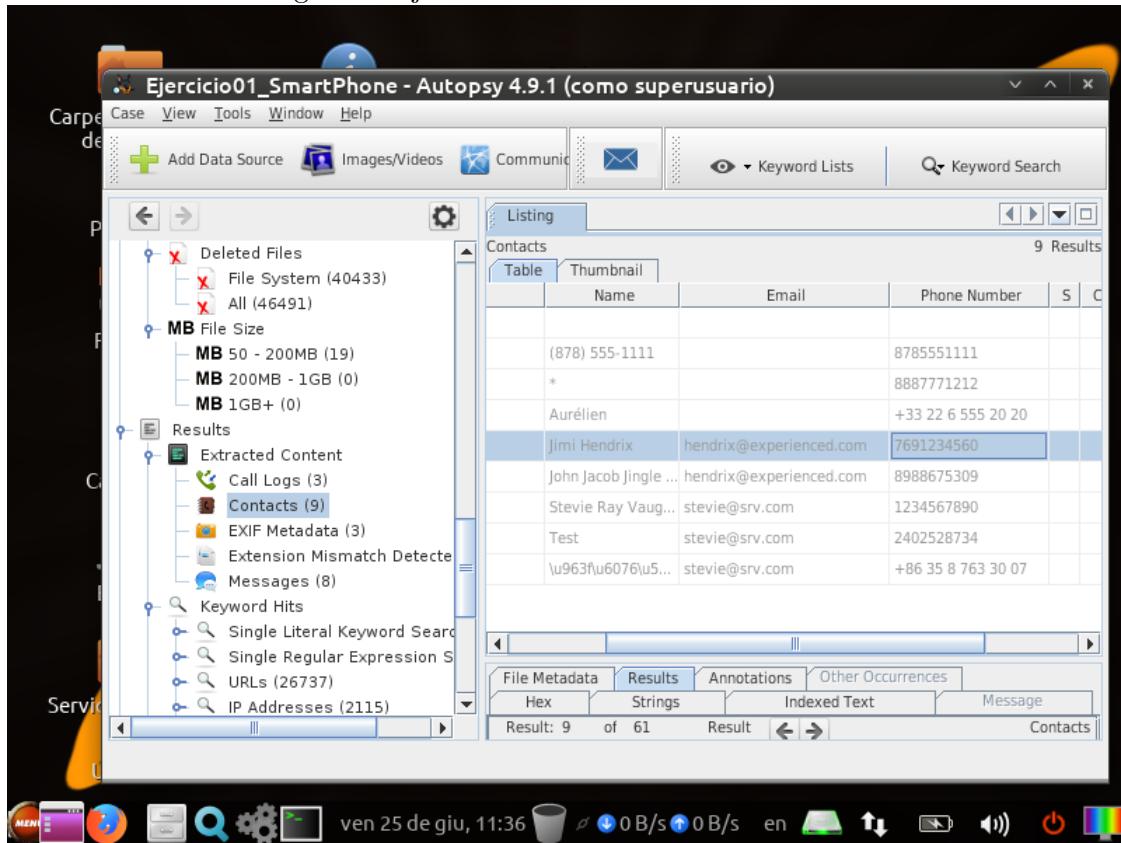
b) Jimi Hendrix, como se puede ver en la siguiente captura.

Figura 7: Ejercicio 1: Jimi Hendrix



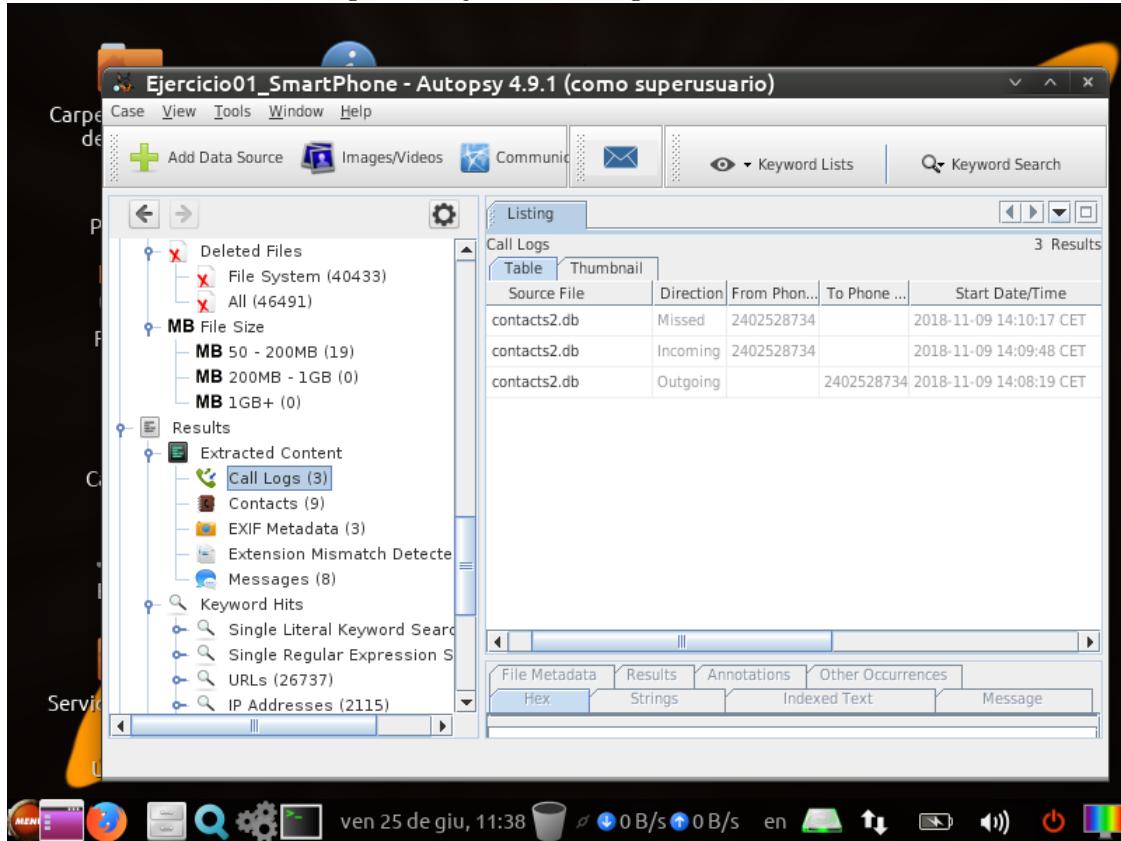
- c) *hendrix@experienced.com*, como se puede observar en la anterior captura.
- d) El correo aparece dos veces, cada vez con un número distinto, pero si se tiene en cuenta el nombre del contacto, 7691234560.

Figura 8: Ejercicio 1: Teléfono de Jimi Hendrix



e) Hay una llamada saliente.

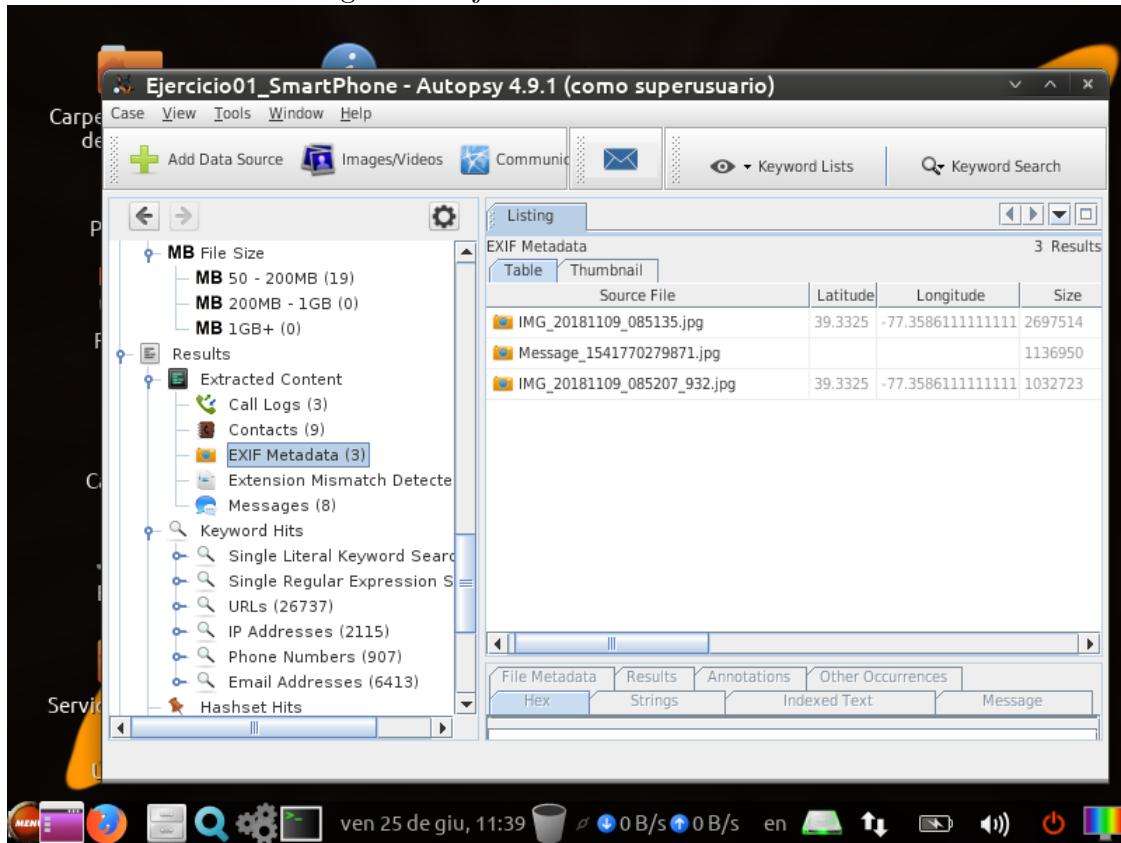
Figura 9: Ejercicio 1: Logs de llamadas



f) Del teléfono analizado al número de teléfono 2402528734.

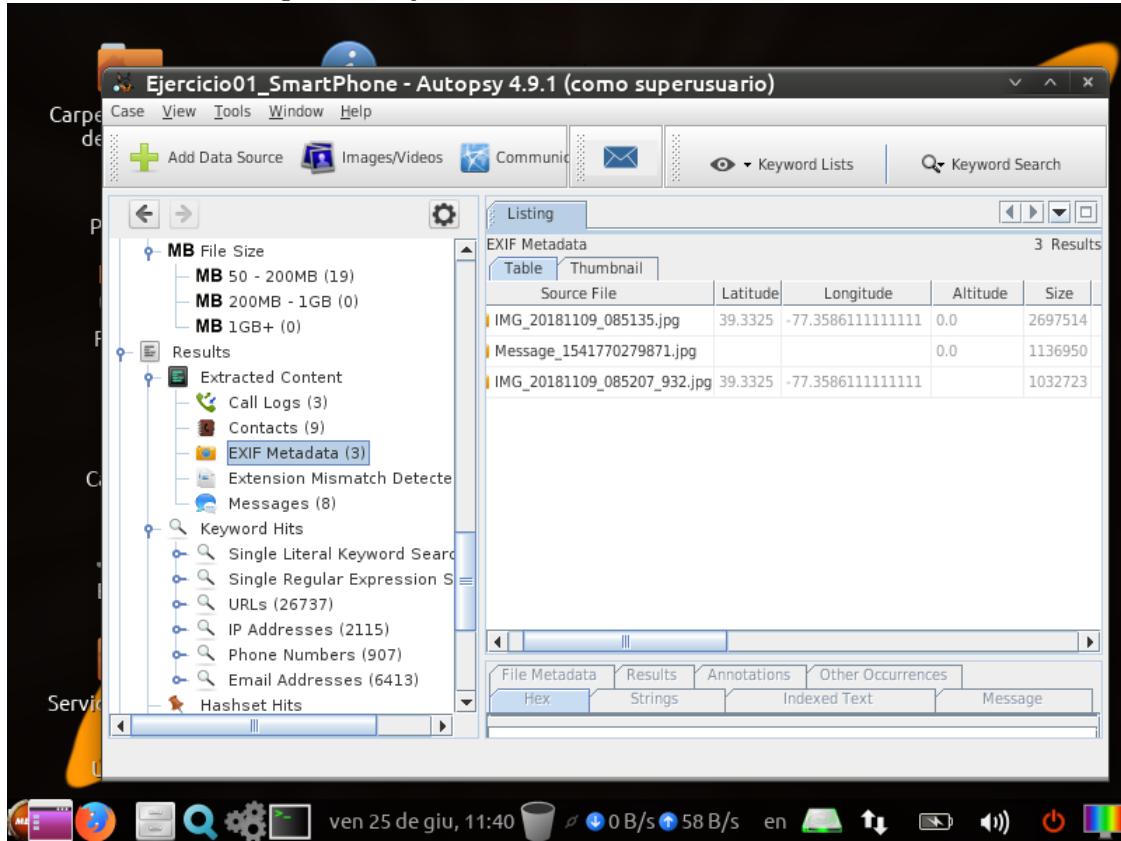
g) Tres ficheros.

Figura 10: Ejercicio 1: Metadatos EXIF



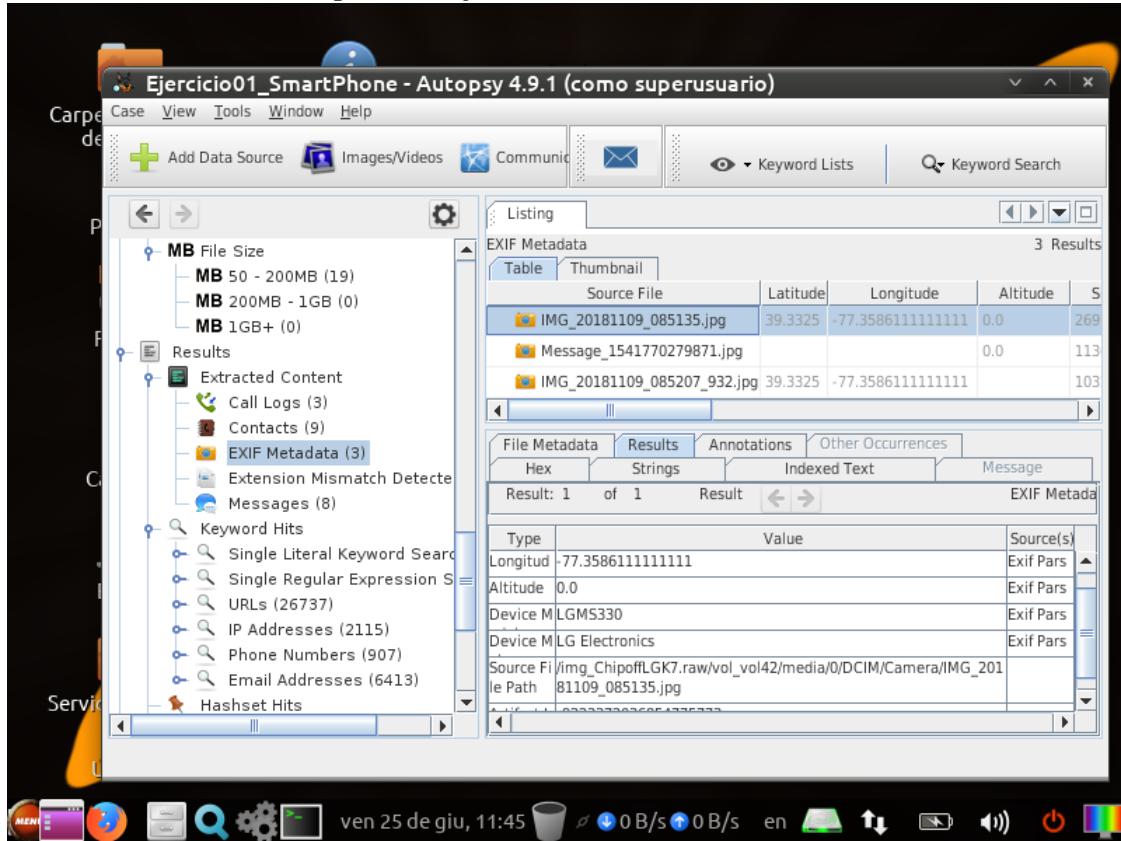
h) Dos de ellos tienen longitud y latitud (y uno de esos dos altitud). El tercero solo tiene la altitud.

Figura 11: Ejercicio 1: Metadatos de coordenadas



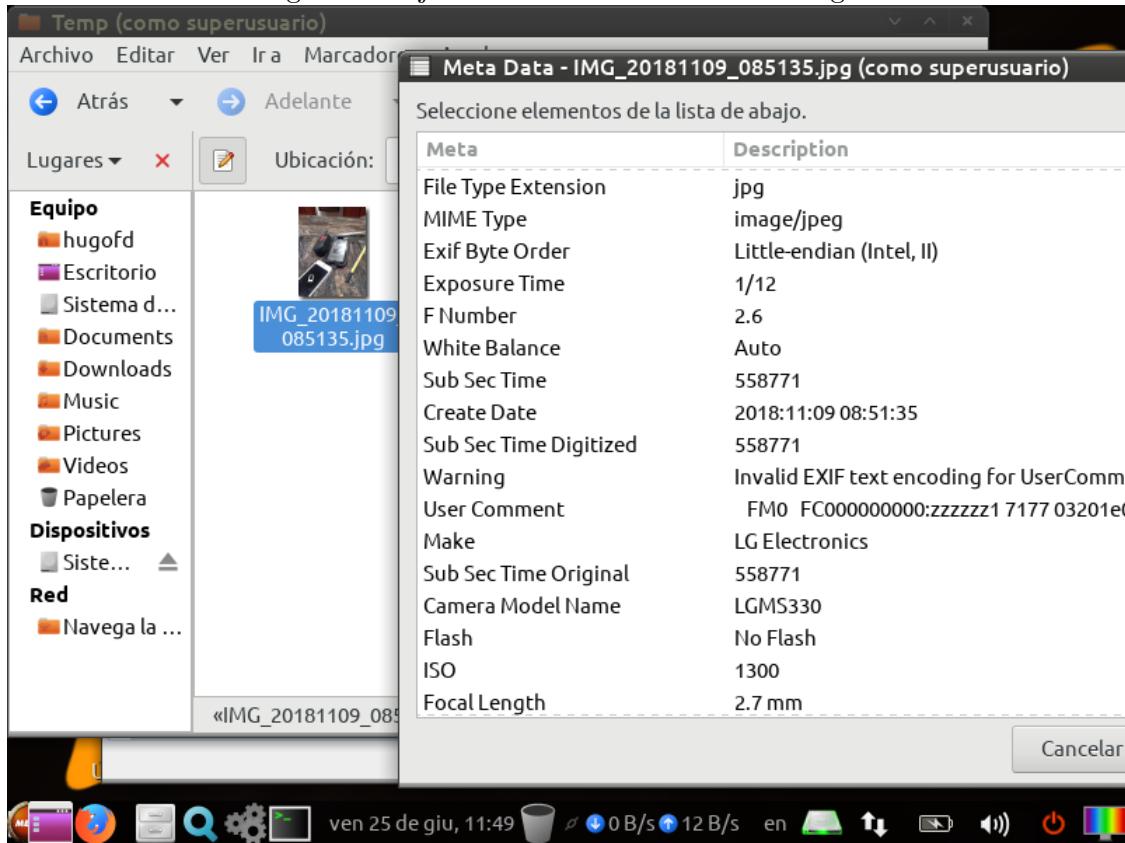
- i) TBD GOOGLE MAPS
- j) TBD GOOGLE MAPS
- k) Con la cámara LGMS330 de un dispositivo LG.

Figura 12: Ejercicio 1: Modelo de cámara



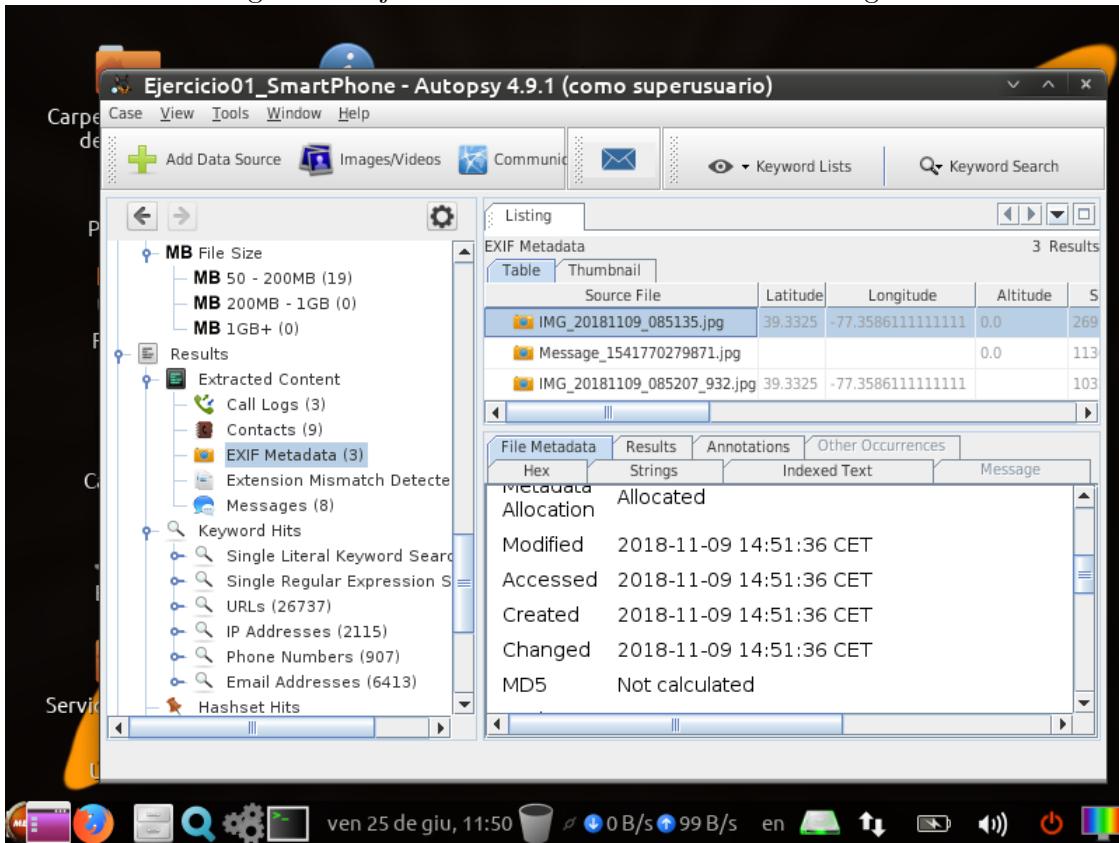
l) 2018/11/09 08:51:35

Figura 13: Ejercicio 1: Información de la imagen



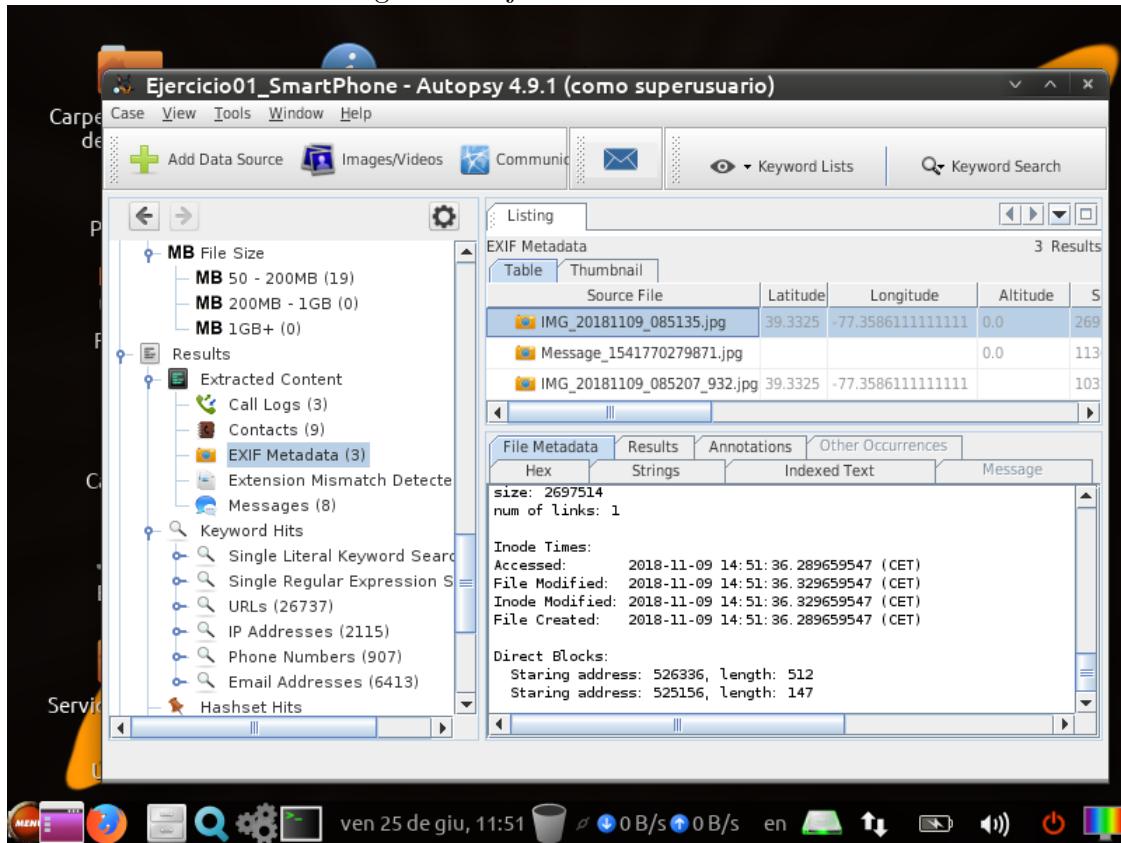
m) 2018/11/09 13:51:36

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



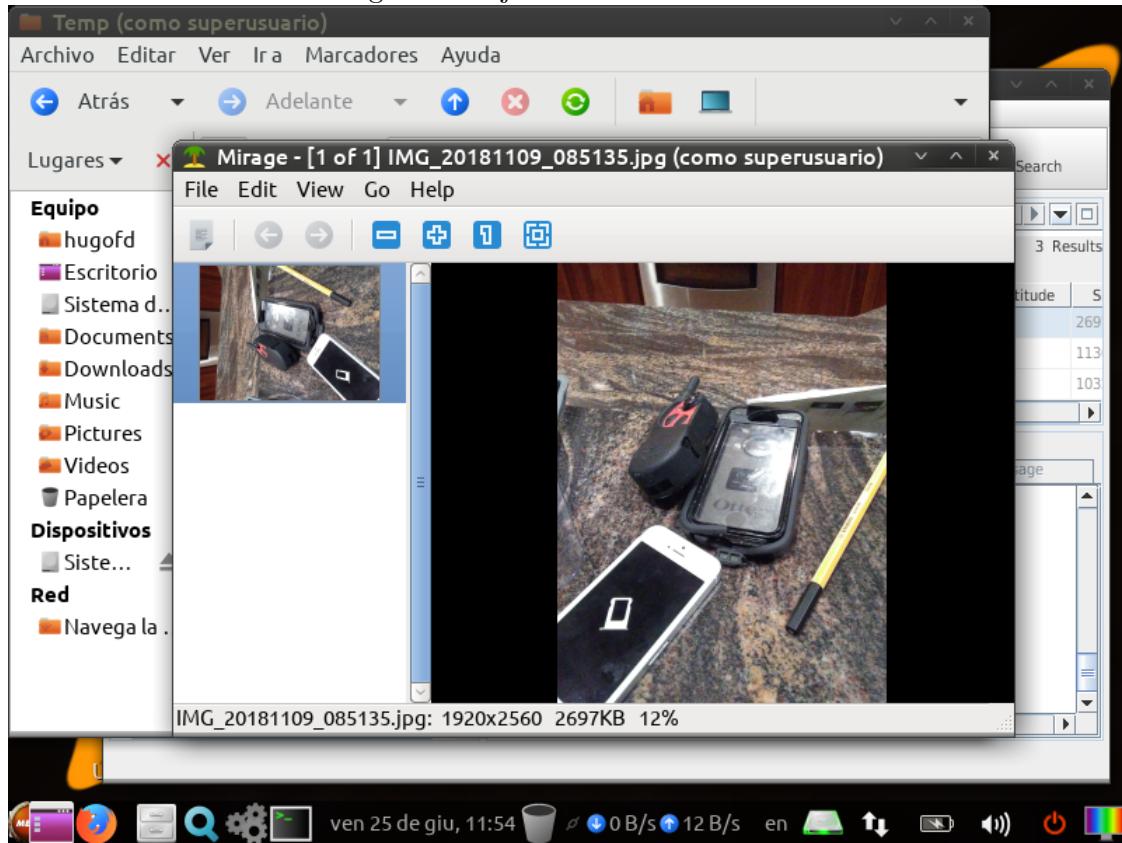
- n) No, hay diferencias entre la hora de modificación del inodo y del fichero y la hora de creación y de acceso del fichero.

Figura 15: Ejercicio 1: MAC times



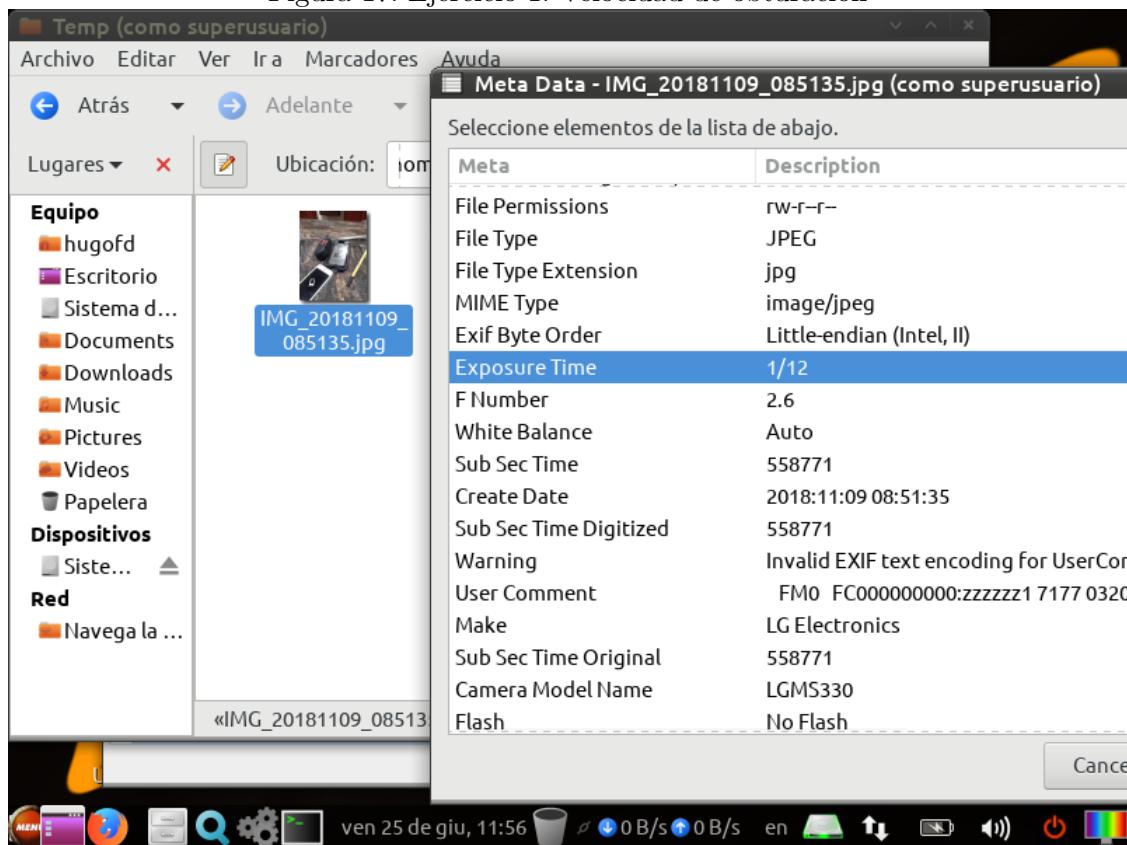
- o) Hay dos móviles, uno de color blanco y otro oscuro con funda negra.

Figura 16: Ejercicio 1: Foto móviles



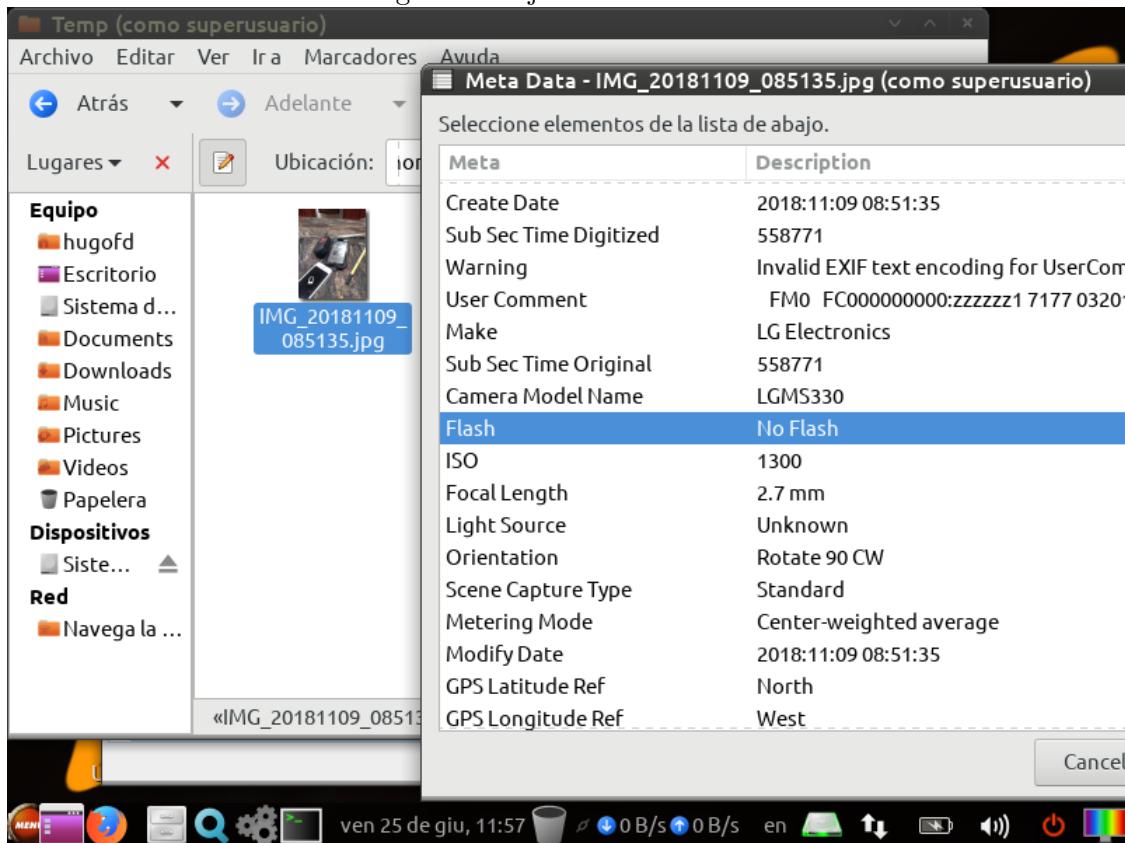
- p) Se puede ver en la captura anterior, 1920x2560.
- q) Una velocidad de obturación de 1/12.

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

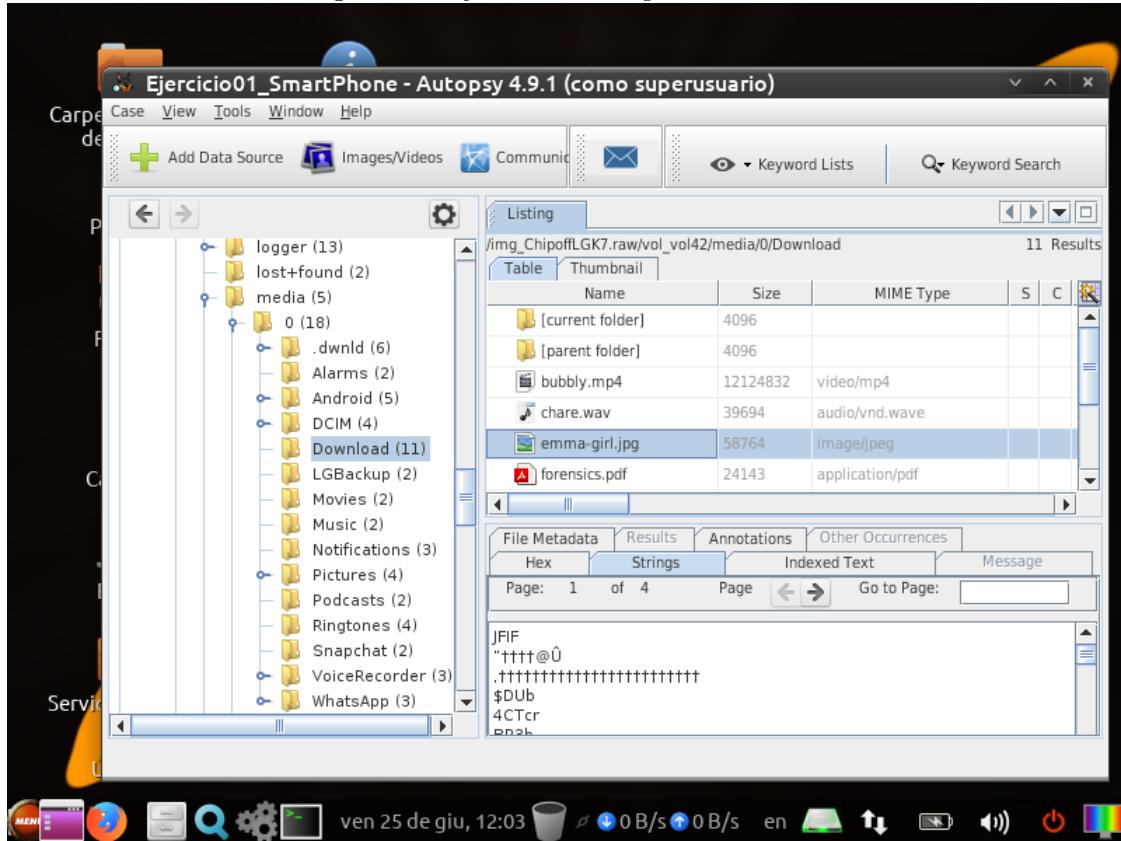
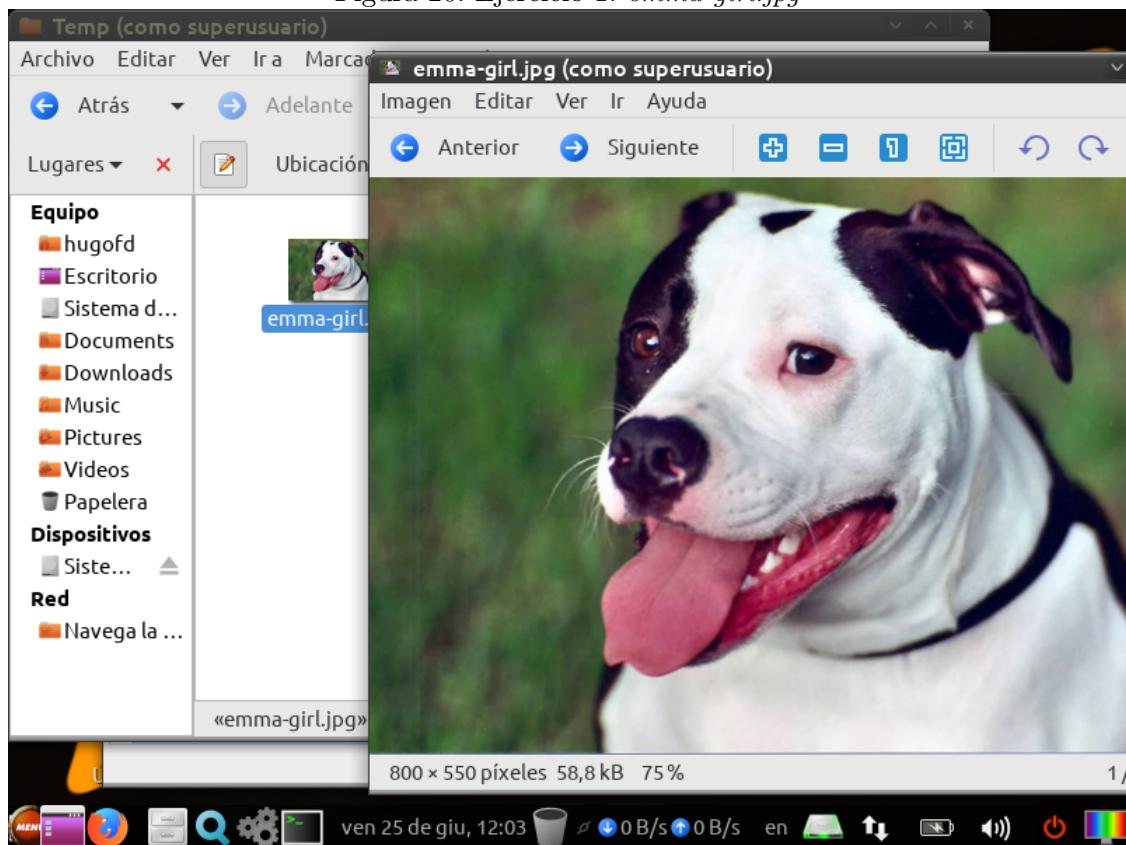
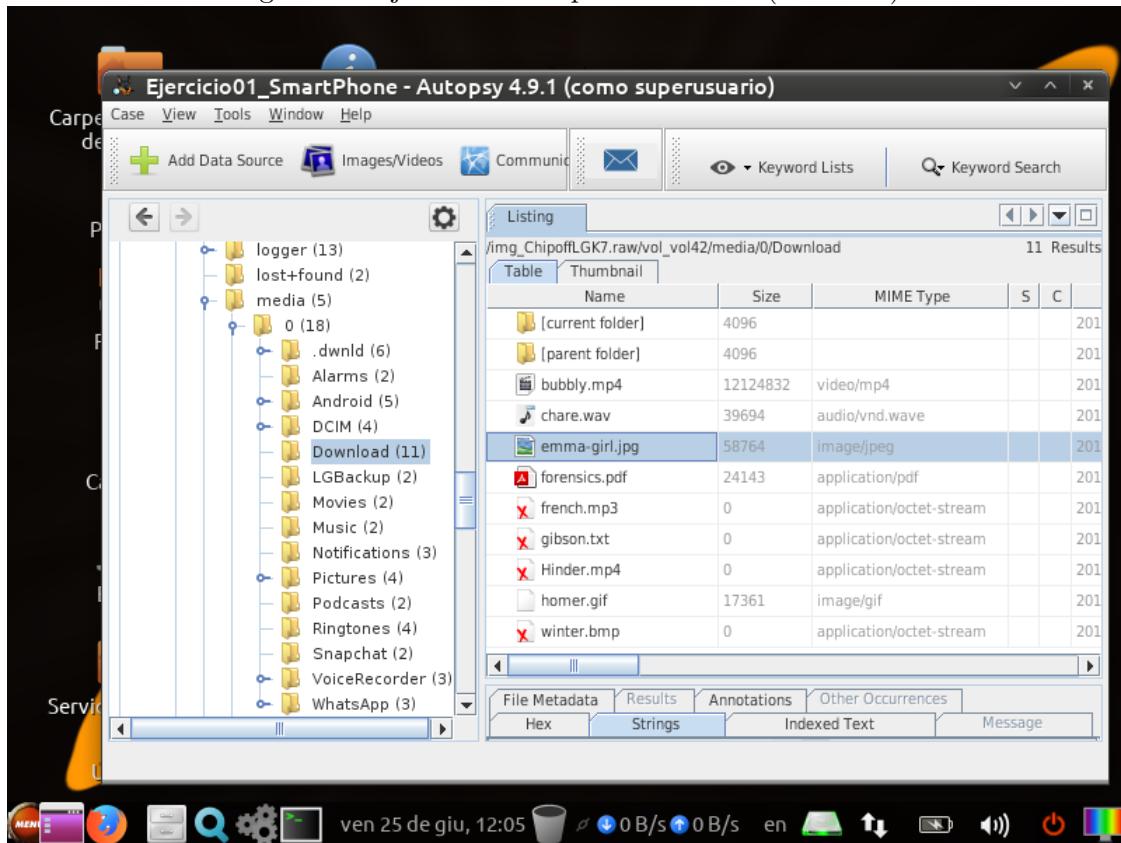


Figura 20: Ejercicio 1: *emma-girl.jpg*



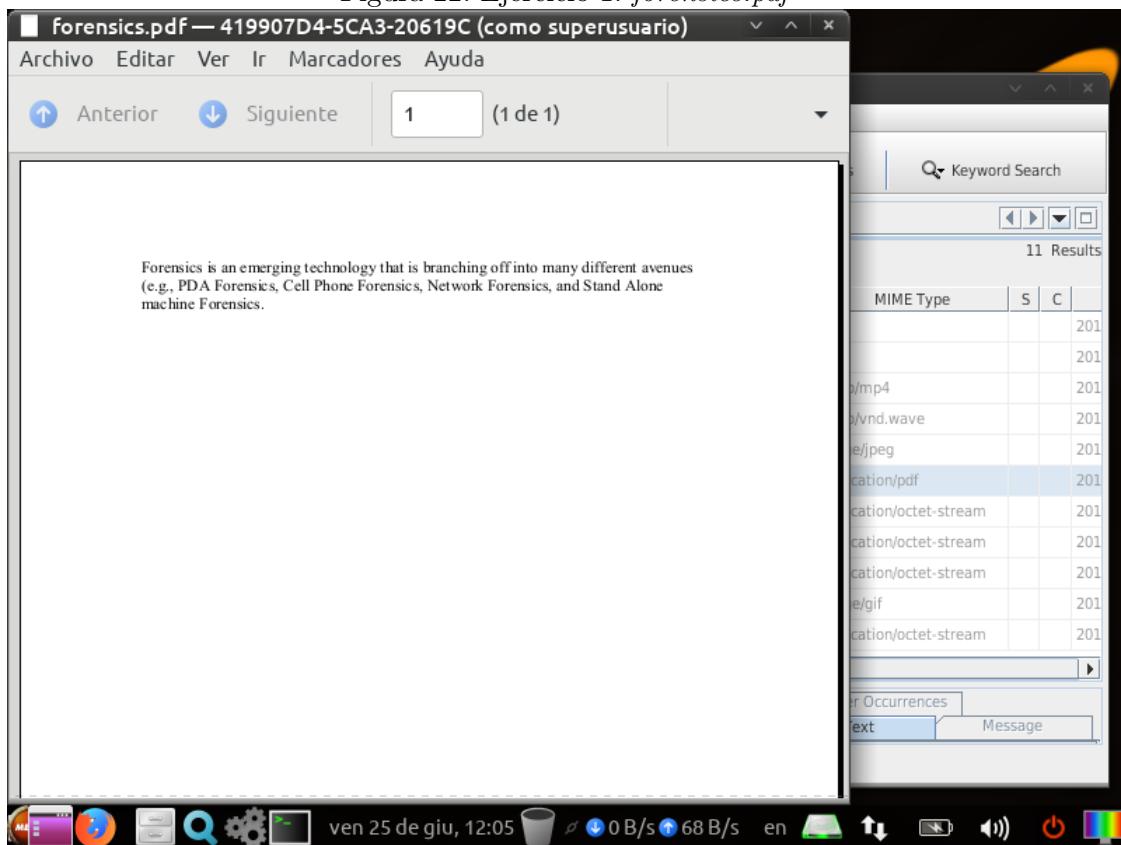
t) Uno, llamado *forensics.pdf*.

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



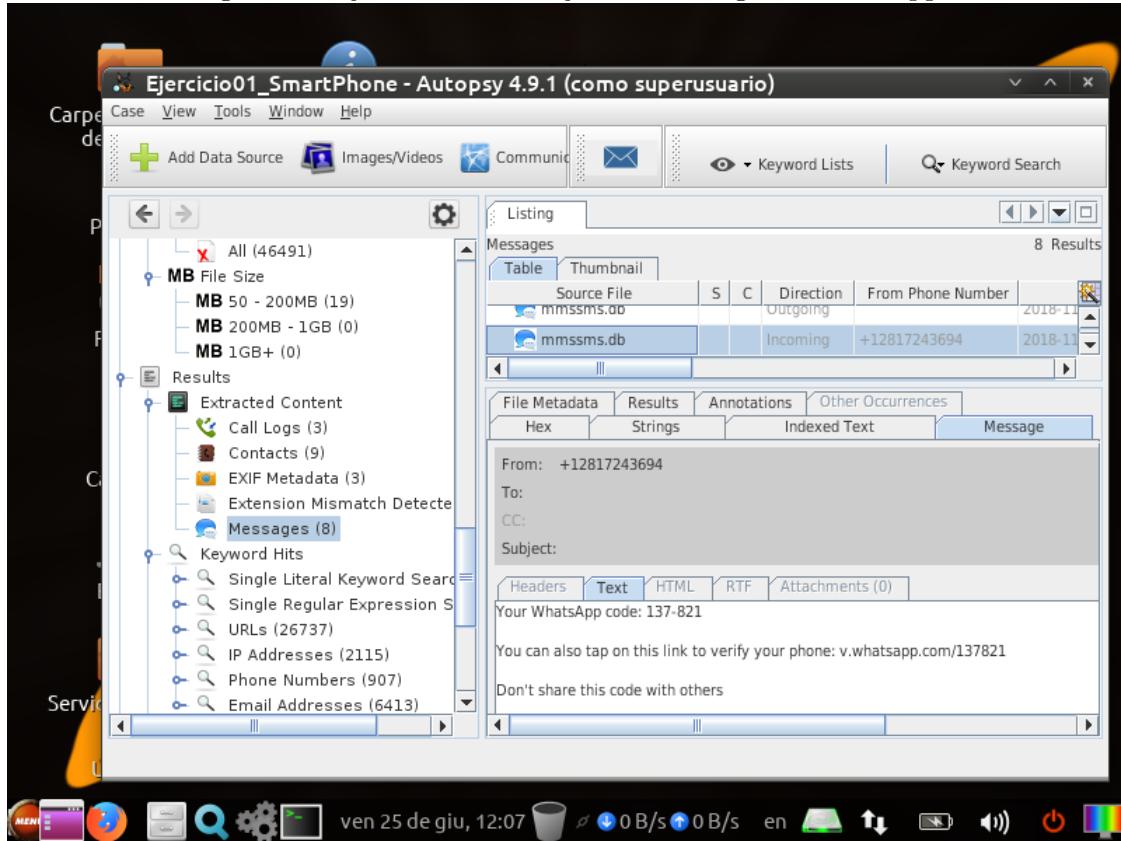
- u) Cuatro, como se ve en la anterior captura.
- v) En la carpeta download hay un fichero pdf llamado *forensics.pdf*.
- w) Se muestra su contenido en la siguiente captura.

Figura 22: Ejercicio 1: *forensics.pdf*



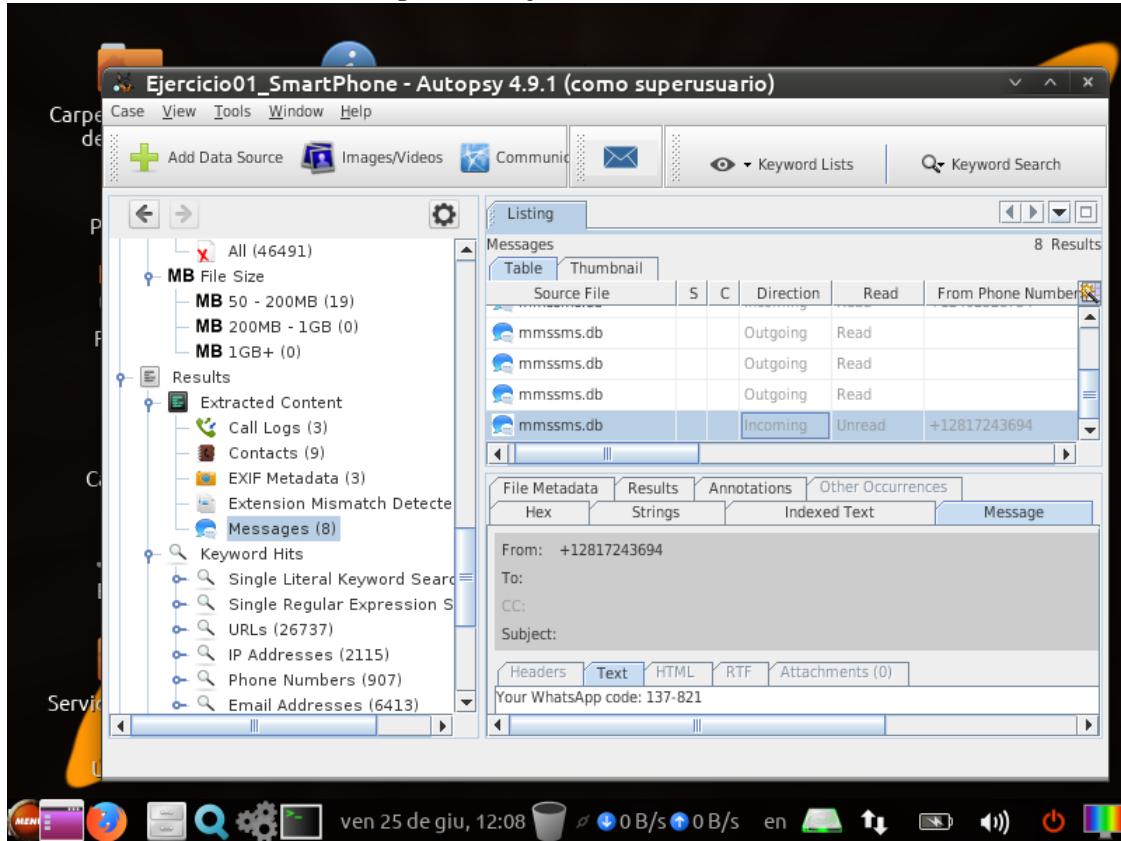
- x) Los mensajes pueden encontrarse en Extracted Content, Messages. El mensaje con el código de Whatsapp se muestra a continuación.

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



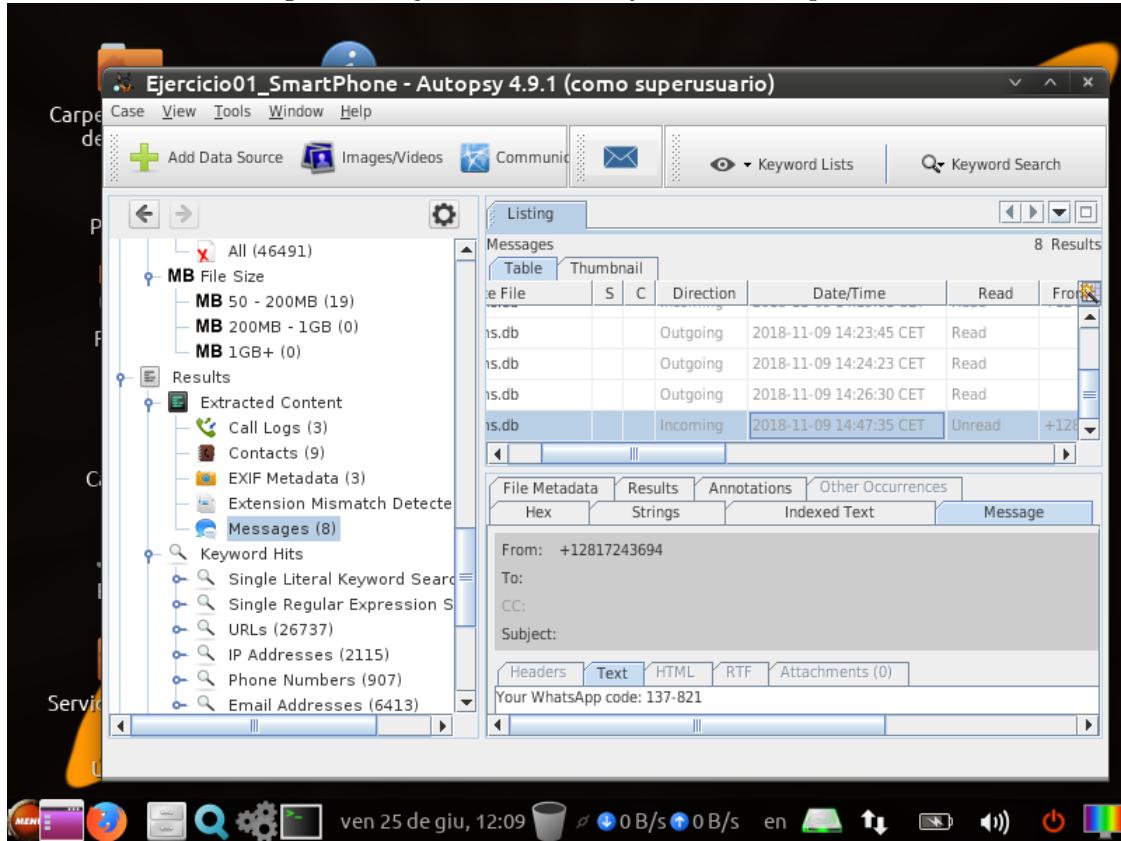
y) El mensaje aparece como *No leído*.

Figura 24: Ejercicio 1: No leído



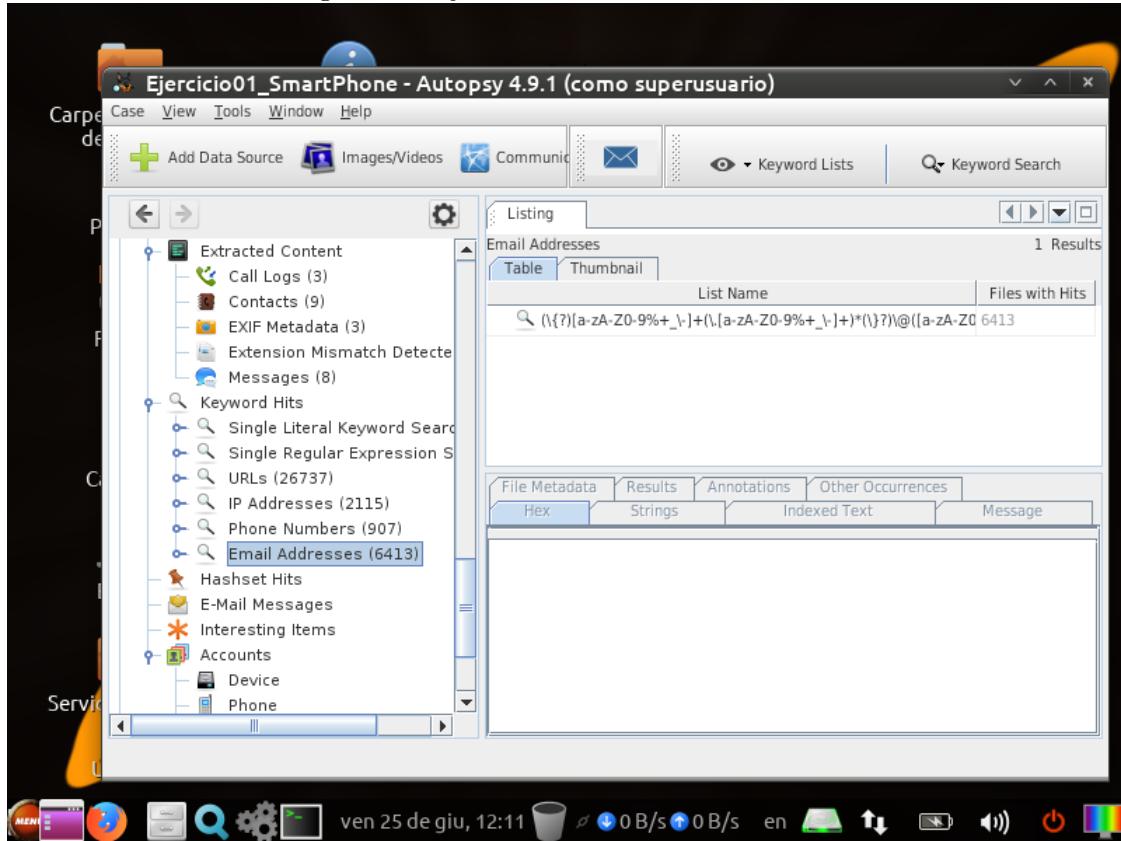
z) El mensaje se recibió el 2018/11/09 a las 14:47:35 CET.

Figura 25: Ejercicio 1: Fecha y hora de recepción



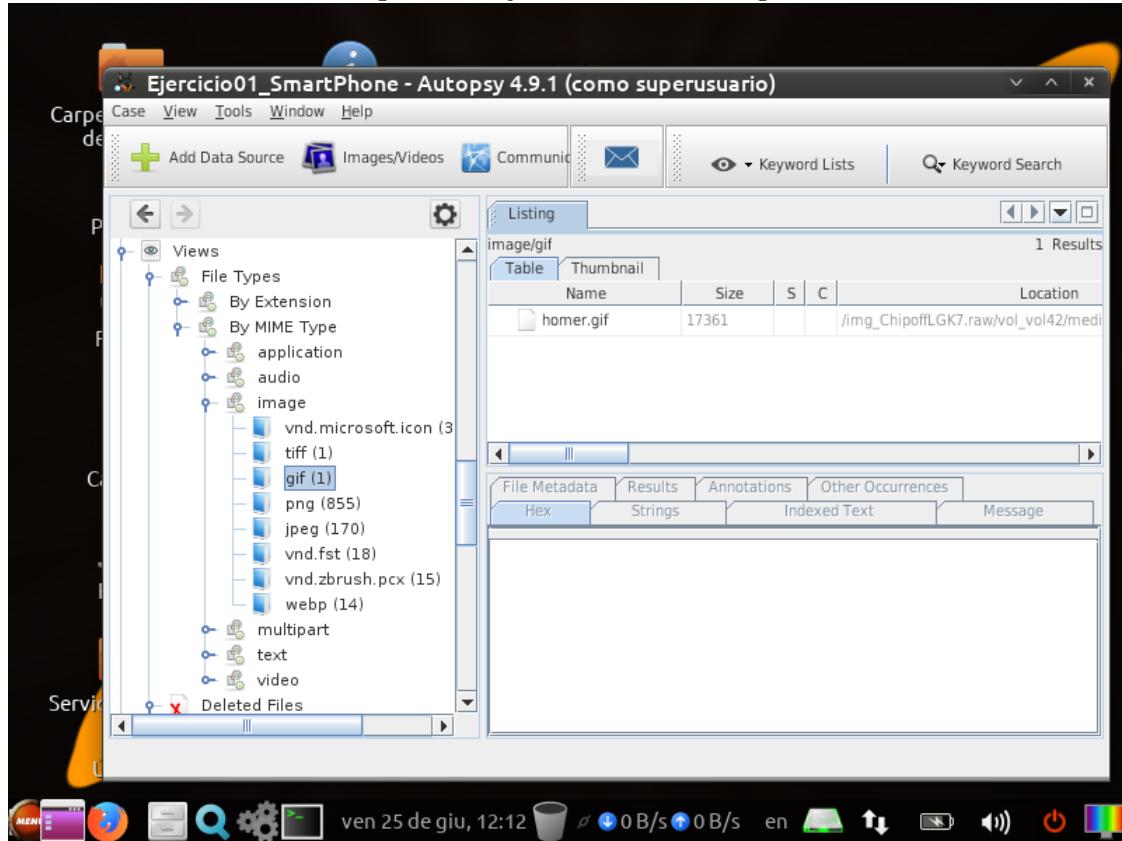
aa) El módulo de búsqueda de cadenas detectó 6413 direcciones de email.

Figura 26: Ejercicio 1: Direcciones de email



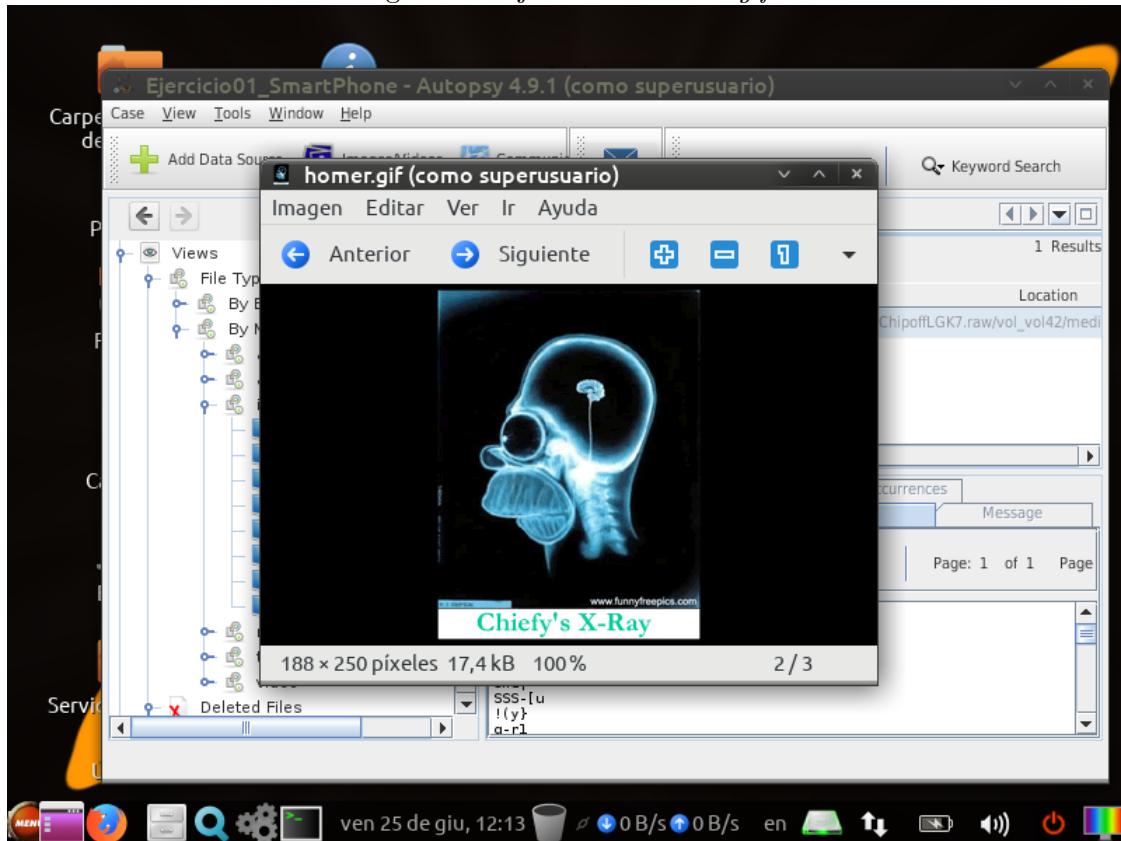
bb) Se puede buscar en el apartado Views por tipo MIME, se observa que hay un único fichero gif detectado, llamado *homer.gif*.

Figura 27: Ejercicio 1: Ficheros gif



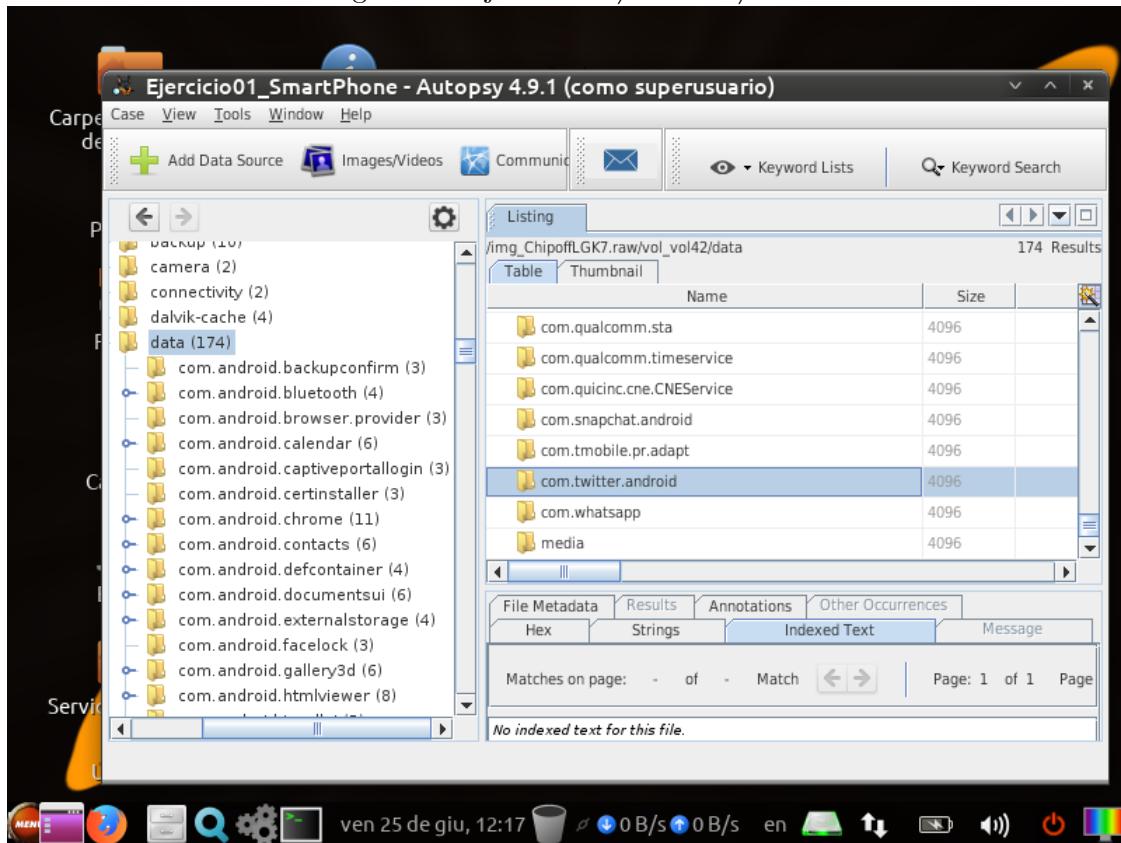
cc) Se muestra a continuación una captura del fichero *homer.gif*.

Figura 28: Ejercicio 1: *homer.gif*



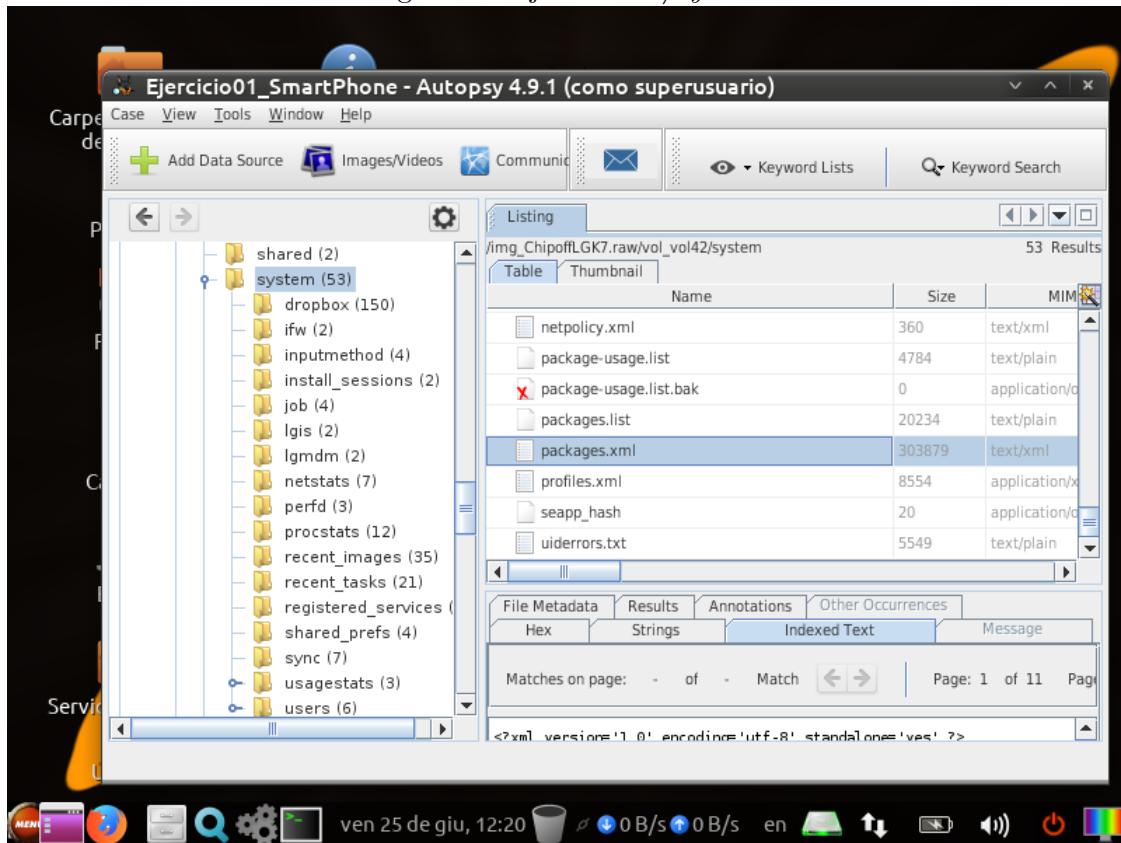
dd) Se busca entre las subcarpetas de */userdata/data* (en la partición 42) las posibles redes sociales que maneja el usuario. Se encuentran *Facebook*, *Instagram*, *LinkedIn*, *Pinterest*, *Snapchat*, *Twitter*, *Whatsapp* y *Youtube*.

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



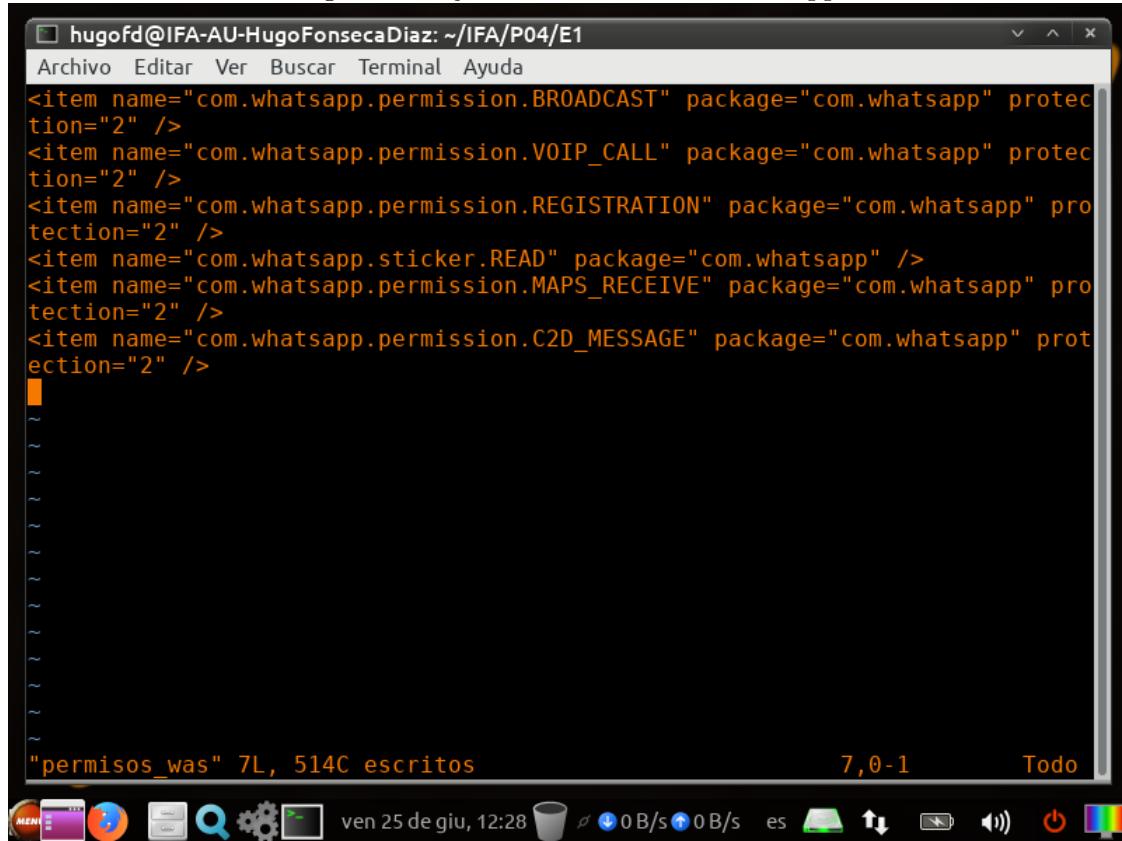
ee) Se extrae el fichero *packages.xml*, encontrado en la carpeta */system* del volumen 42.

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 followed by the message: "permisos_was" 7L, 514C escritos. In the bottom right corner of the terminal window, it says "7,0-1" and "Todo". The terminal window has a dark background with white text. At the bottom of the screen, there is a dock with various icons, including a menu icon, a browser icon, a file manager icon, a search icon, a settings gear icon, and a terminal icon. The date and time "ven 25 de giu, 12:28" are also visible 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*

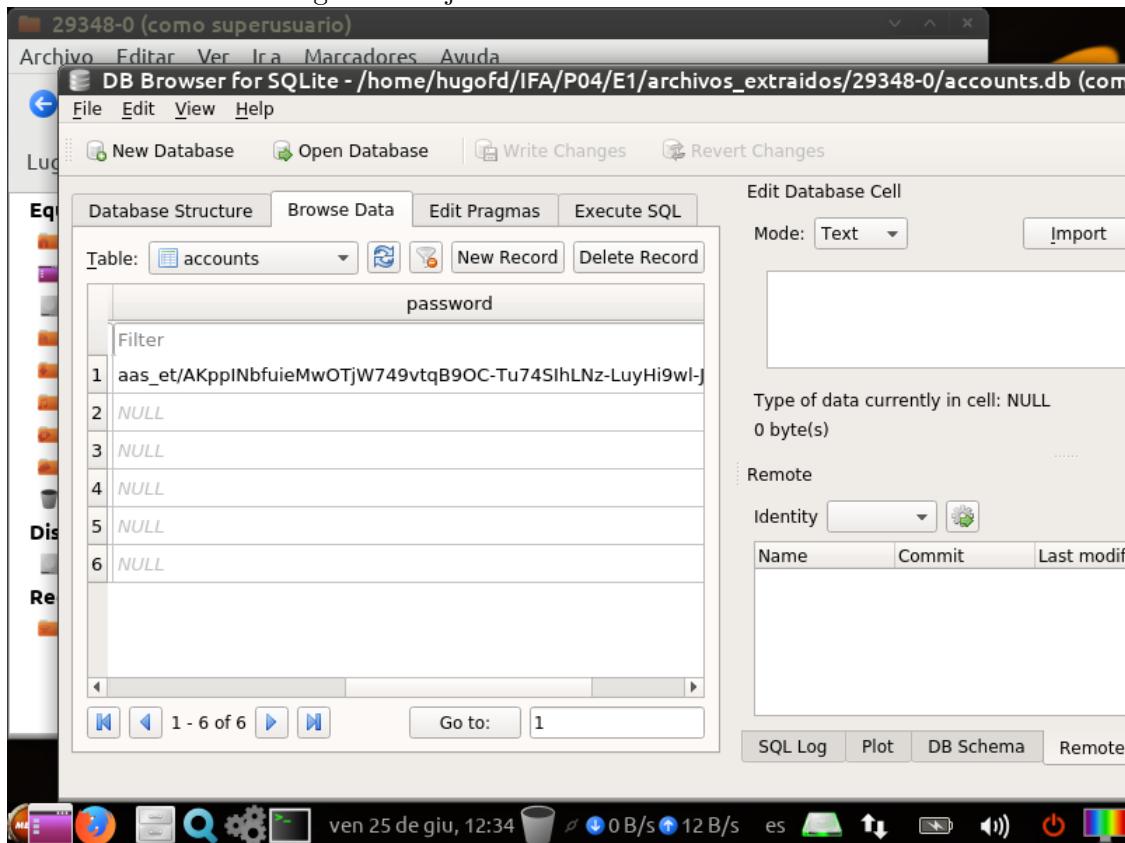
The screenshot shows the DB Browser for SQLite interface. The title bar reads "29348-0 (como superusuario)" and "DB Browser for SQLite - /home/hugofd/IFA/P04/E1/archivos_extraidos/29348-0/accounts.db (com)". The main window displays the "accounts" table with the following data:

	_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

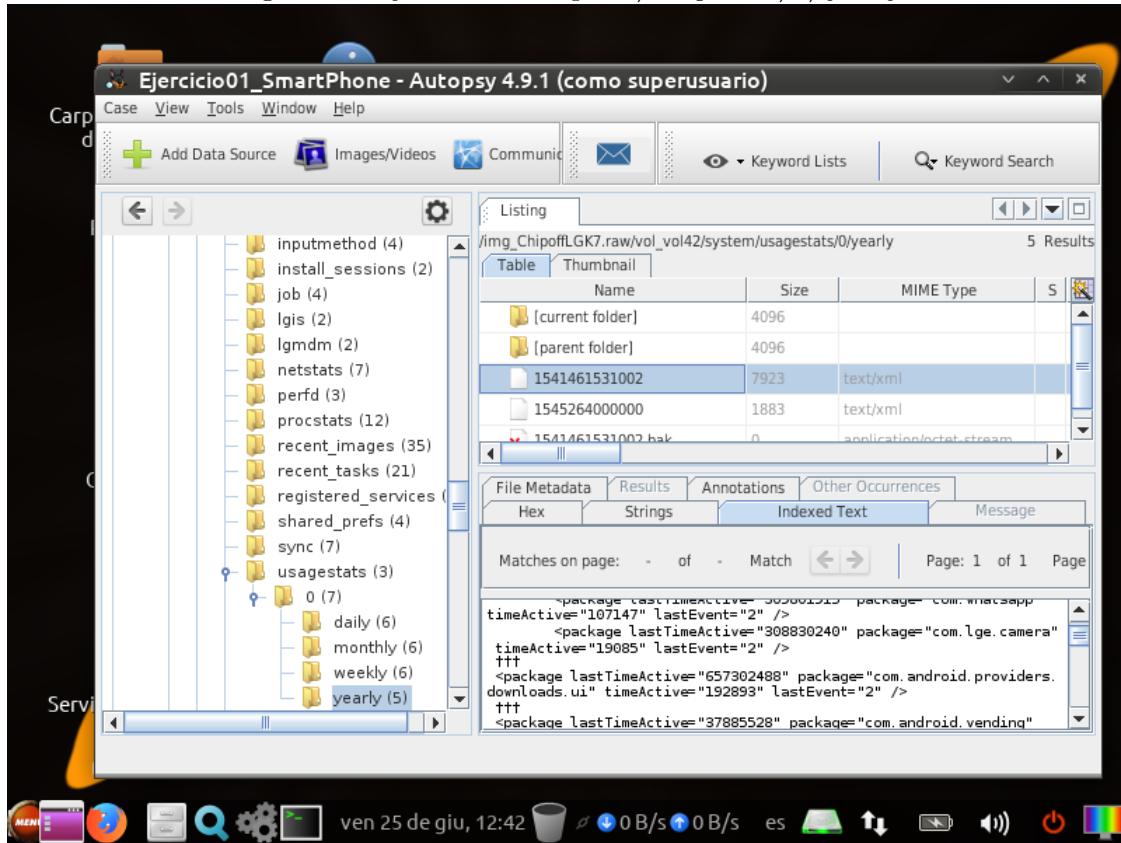


2. Ejercicio 2

Se responden a continuación a las dos preguntas del ejercicio.

- a) Los archivos sin borrar encontrados en subcarpetas de la carpeta *usagestats* son de tipo *text/xml*.

Figura 34: Ejercicio 2: Carpeta */usagestats/0/yearly*



- b) Se exporta uno de los archivos, su contenido se muestra en la siguiente captura.

Figura 35: Ejercicio 2: Contenidos del fichero xml

The screenshot shows the Geany 1.32 interface with two tabs open: 'packages.xml' and '1541461531002'. The 'packages.xml' tab contains the following XML code:

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<usagestats version="1" endTime="657450629">
  <packages>
    <package lastTimeActive="8394839233" package="com.android.LGSetupWizard" timeActive="107">
      <package lastTimeActive="308811774" package="com.android.documentsui" timeActive="107">
        <package lastTimeActive="657265536" package="com.android.htmlviewer" timeActive="107">
          <package lastTimeActive="309801915" package="com.whatsapp" timeActive="107">
            <package lastTimeActive="308830240" package="com.lge.camera" timeActive="107">
              <package lastTimeActive="657302488" package="com.android.providers.downloads" timeActive="107">
                <package lastTimeActive="37885528" package="com.android.vending" timeActive="107">
                  <package lastTimeActive="657450629" package="com.lge.shutdownmonitor" timeActive="107">
                    <package lastTimeActive="657183486" package="com.android.contacts" timeActive="107">
                      <package lastTimeActive="657239416" package="com.android.mms" timeActive="107">
                        <package lastTimeActive="310013080" package="com.instagram.android" timeActive="107">
                          <package lastTimeActive="309889077" package="com.pinterest" timeActive="82">
                            <package lastTimeActive="310188193" package="com.lge.settings.easy" timeActive="82">
                            <package lastTimeActive="307730495" package="com.google.android.gm" timeActive="82">
                            <package lastTimeActive="657092341" package="com.android.calendar" timeActive="82">
                            <package lastTimeActive="8394819191" package="com.google.android.setupwizard" timeActive="82">
    
```

The status bar at the bottom displays system information and a terminal log:

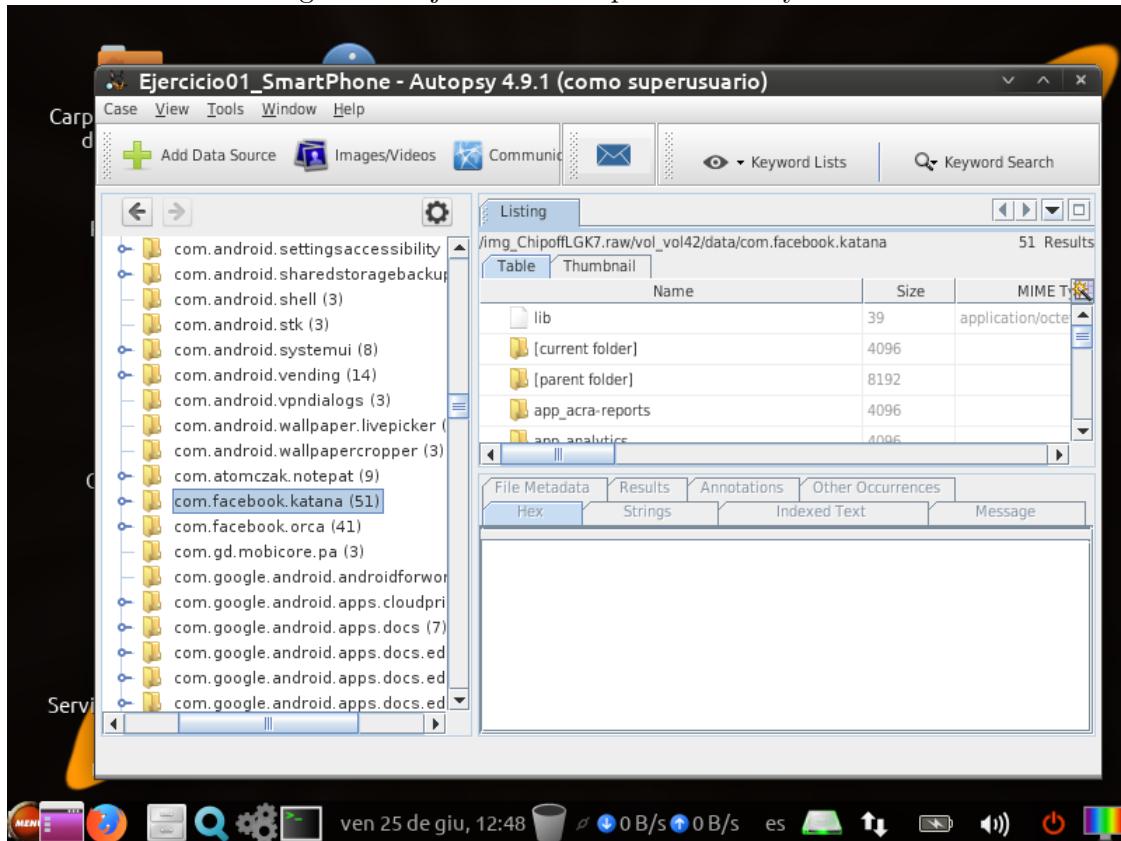
```
12:44:11: Esto es Geany 1.32.
12:44:11: Archivo /home/hugofd/IFA/P04/E1/Ejercicio01_SmartPhone/Temp/packages.xml abierto(1)
12:44:11: Archivo /home/hugofd/IFA/P04/E1/archivos_extraidos/1541461531002 abierto(2)
```

The terminal log also includes the message "Esto es Geany 1.32."

3. Ejercicio 3

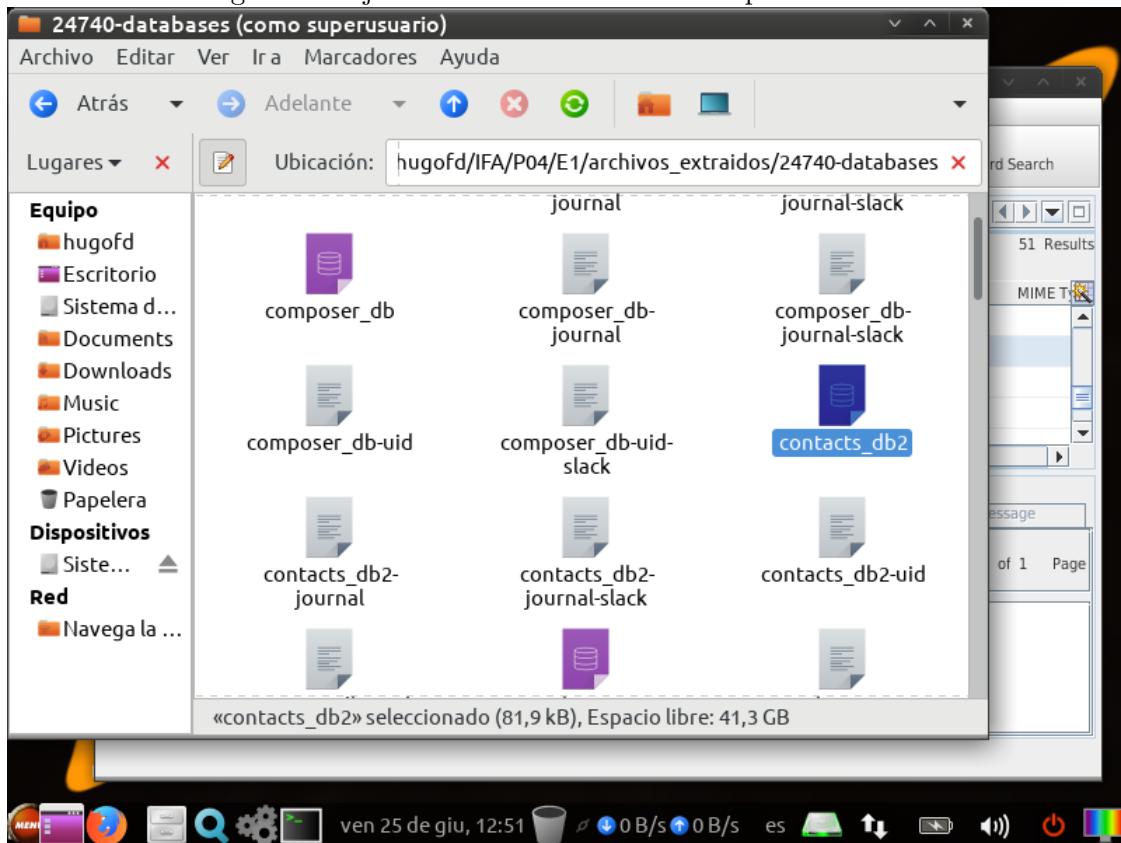
a)

Figura 36: Ejercicio 3: Carpetas *katana* y *orca*



- b) Se extrae la carpeta *databases* de *katana*.

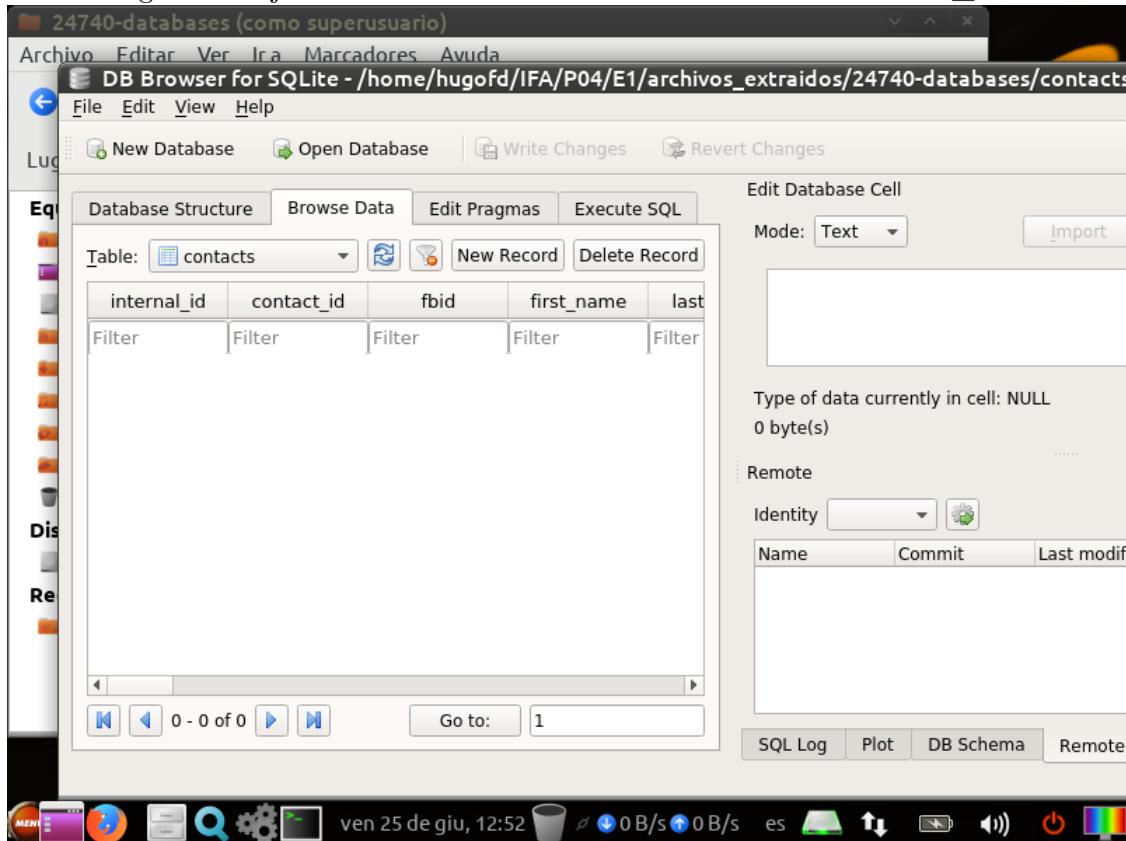
Figura 37: Ejercicio 3: Contenido de la carpeta *databases*



Se busca la base de datos *contacts_db2* y se abre con el programa *DB Browser for SQLite*.

- c) No aparece ningún contacto en la tabla.
- d) Se hace una captura de la tabla.

Figura 38: Ejercicio 3: Tabla *contacts* de la base de datos *contacts_db2*

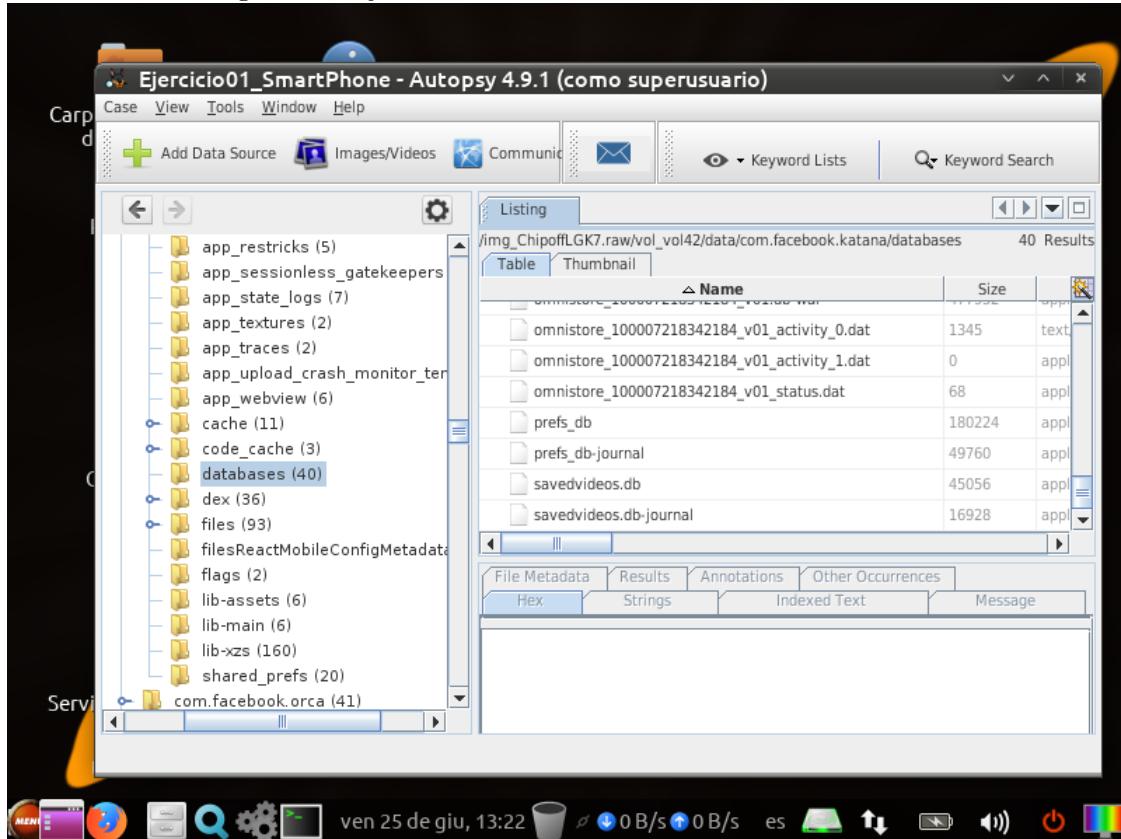


- e) TBD JSON
- f) TBD
- g) TBD

4. Ejercicio 4

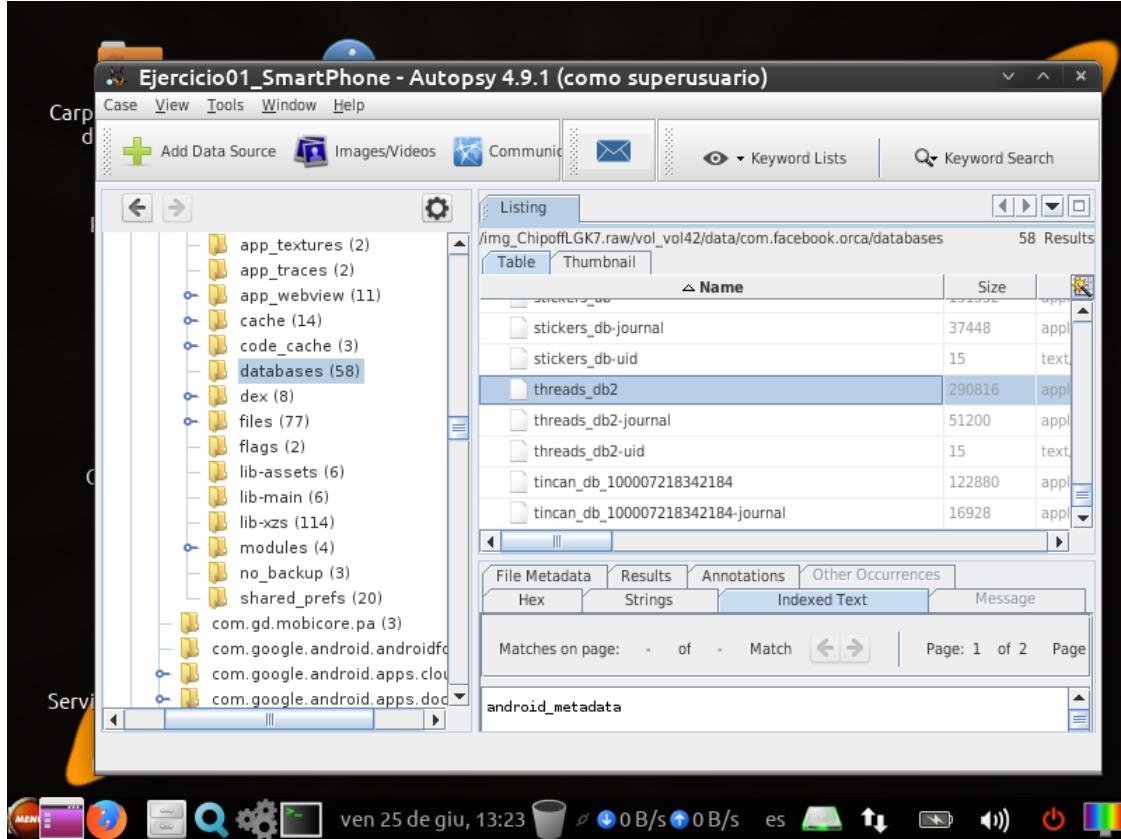
Al buscar el fichero descrito en el enunciado se observa que no existe en la carpeta *com.facebook.katana/databases*.

Figura 39: Ejercicio 4: Buscando *threads_db2* en *katana*



Al buscar el fichero equivalente en la carpeta *orca* se ve que existe, por lo que se realizará el ejercicio con ese fichero.

Figura 40: Ejercicio 4: Buscando *threads_db2* en *orca*



Se abre la tabla *messages* de la base de datos comentada previamente con el programa *DB Browser for SQLite*.

Figura 41: Ejercicio 4: Tabla *messages* de la base de datos *threads_db2*

The screenshot shows the DB Browser for SQLite interface. The title bar reads "archivos_extraidos (como superusuario)" and "DB Browser for SQLite - /home/hugofd/IFA/P04/E1/archivos_extraidos/thread... (como superu)". The main window displays the "messages" table with the following data:

	_id	msg_id	thread_key	text	ser
1	21	mid.\$cAAAAA...	ONE_TO_ON...	Hey Jane thi...	{"user...
2	22	mid.\$cAAAAA...	ONE_TO_ON...	Hey Jane thi...	{"user...
3	23	mid.\$cAAAAA...	ONE_TO_ON...		{"user...
4	24	mid.\$cAAAAA...	ONE_TO_ON...		{"user...
5	25	mid.\$cAAAAA...	ONE_TO_ON...	Hey Jane thi...	{"user...
6	26	mid.\$cAAAAA...	ONE_TO_ON...		{"user...
7	27	mid.\$cAAAAA...	ONE_TO_ON...		{"user...
8	28	mid.\$cAAAAA...	ONE_TO_ON...		{"user...
9	29	mid.\$cAAAAA...	ONE_TO_ON...	Hey Jane thi...	{"user...

The status bar at the bottom shows: ven 25 de giu, 13:26 0 B/s 0 B/s es

Se verán a continuación los diferentes campos del mensaje con ID 25.

Figura 42: Ejercicio 4: Campo *text* del mensaje con ID 25

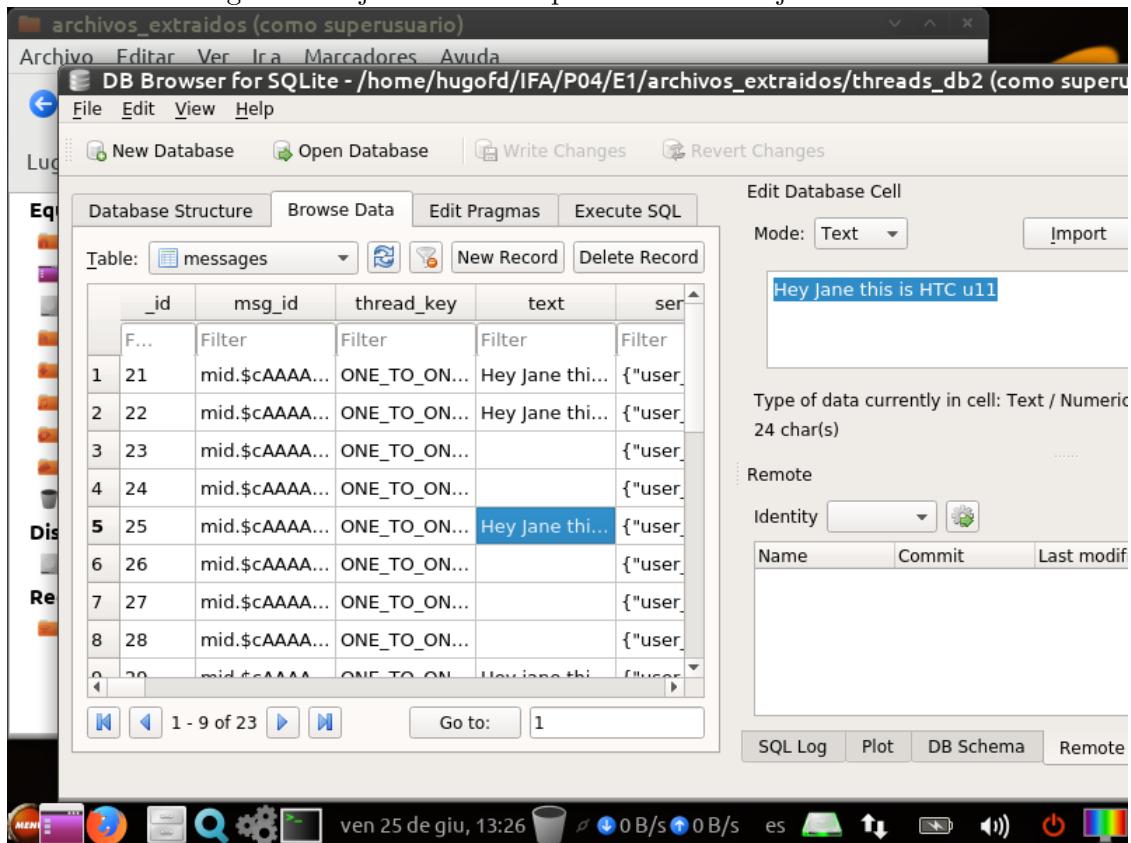


Figura 43: Ejercicio 4: Campo *sender* del mensaje con ID 25

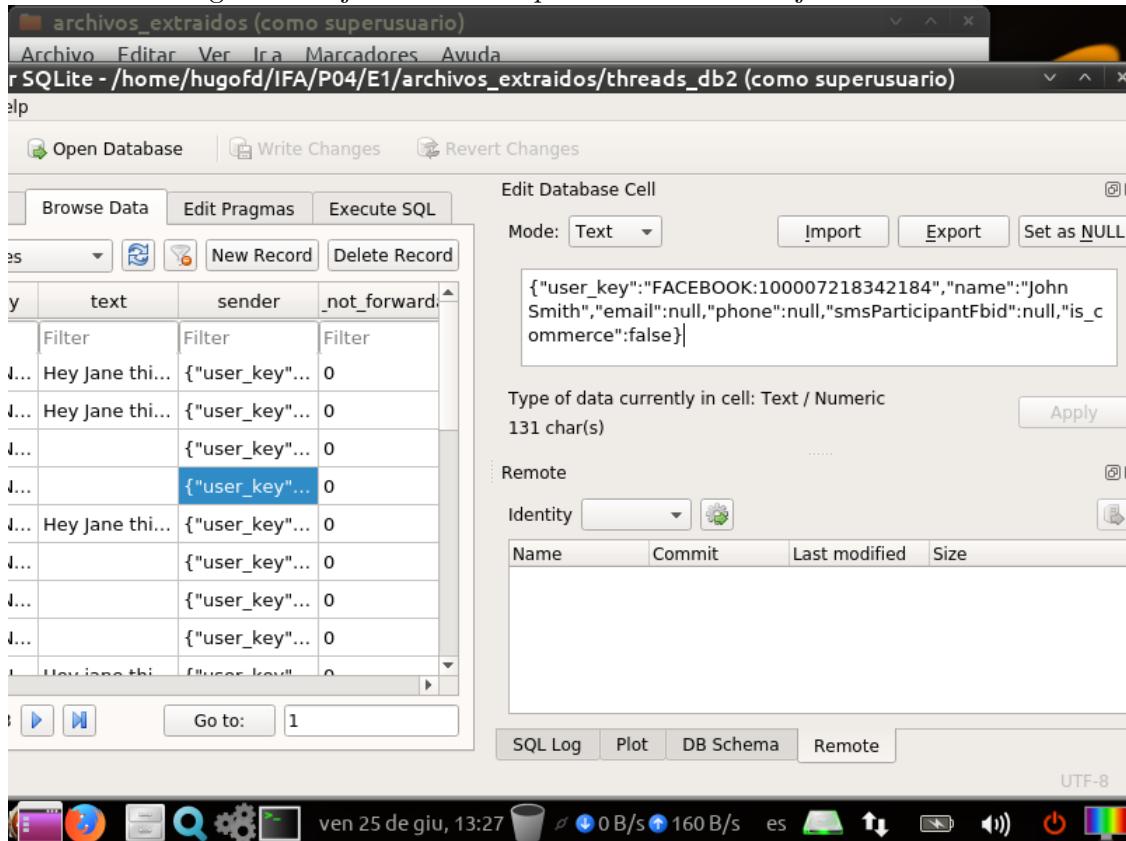


Figura 44: Ejercicio 4: Campo *timestamp_ms* del mensaje con ID 25

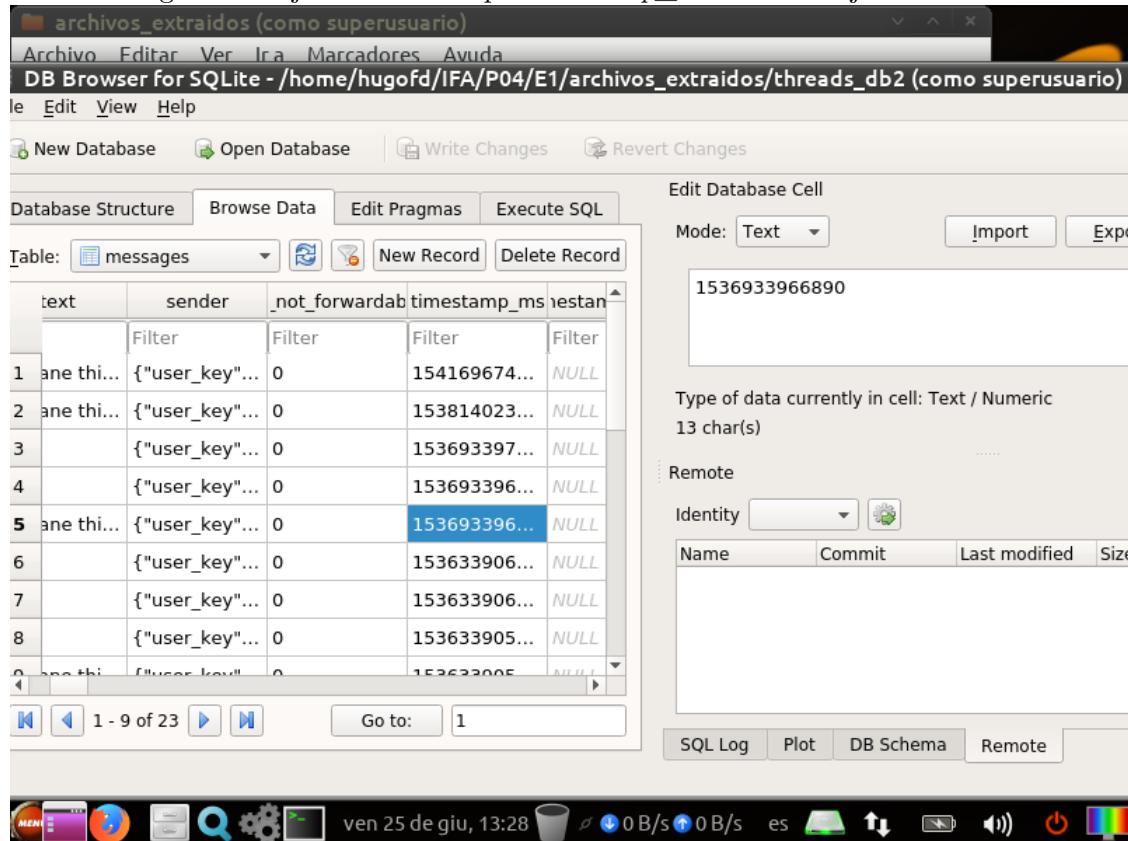


Figura 45: Ejercicio 4: Campos *coordinates* y *source* del mensaje con ID 25

The screenshot shows the DB Browser for SQLite interface. The title bar reads "archivos_extraidos (como superusuario)" and "DB Browser for SQLite - /home/hugofd/IFA/P04/E1/archivos_extraidos/thread_db2 (como superusuario)". The main window displays the "messages" table with the following data:

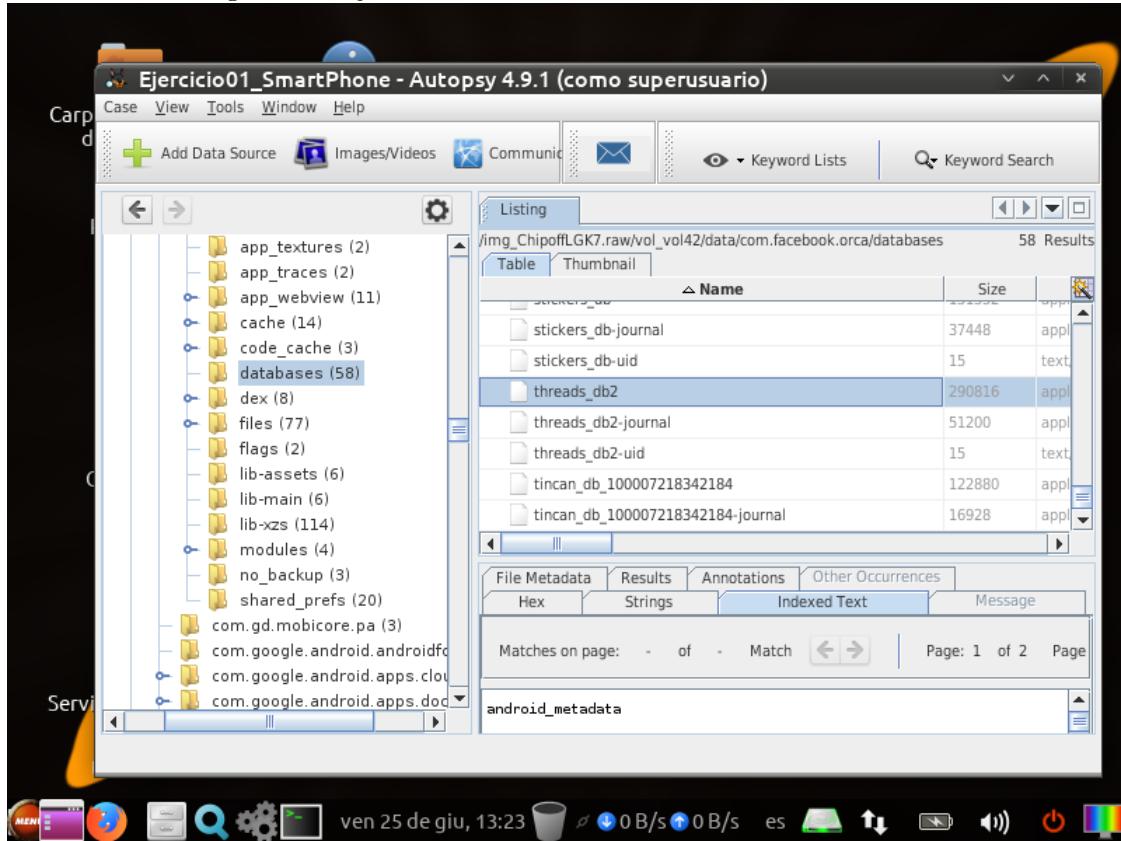
	coordinates	line_threading	source	channel_source
1	NULL	646634480...	NULL	A
2	NULL	645142775...	NULL	A
3	NULL	644636832...	NULL	A
4	NULL	644636829...	NULL	A
5	NULL	644636828...	NULL	A
6	NULL	644387308...	NULL	A
7	NULL	644387306...	NULL	A
8	NULL	644387304...	NULL	A
9	NULL	644387303...	NULL	A

The "coordinates" column for the 25th row is currently selected, indicated by a blue highlight. The status bar at the bottom shows the date and time as "ven 25 de giu, 13:29".

5. Ejercicio 5

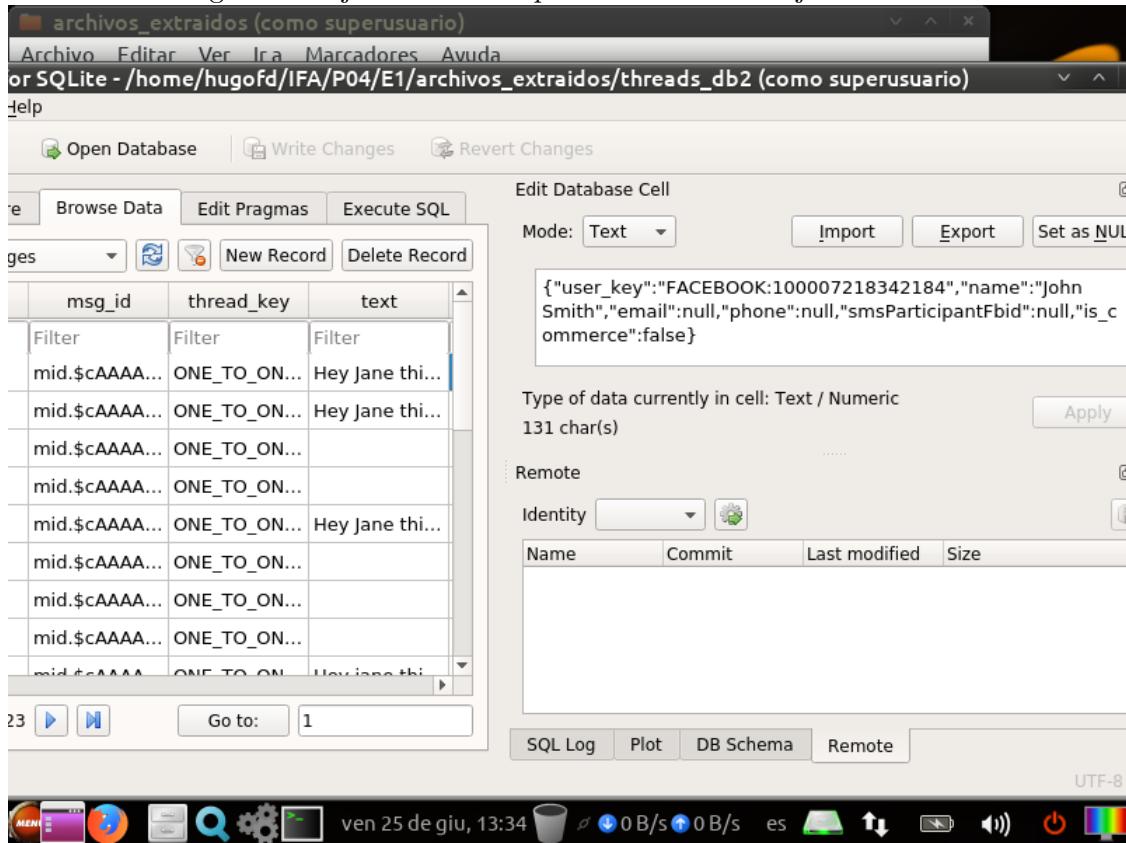
Como la base de datos se había utilizado en el ejercicio 4, ya está extraída. Se procede a abrirla y a examinar los contenidos de la tabla *messages*. La fila que se analizará es la del mensaje con ID 21.

Figura 46: Ejercicio 5: Base de datos *threads_db2* en *orca*



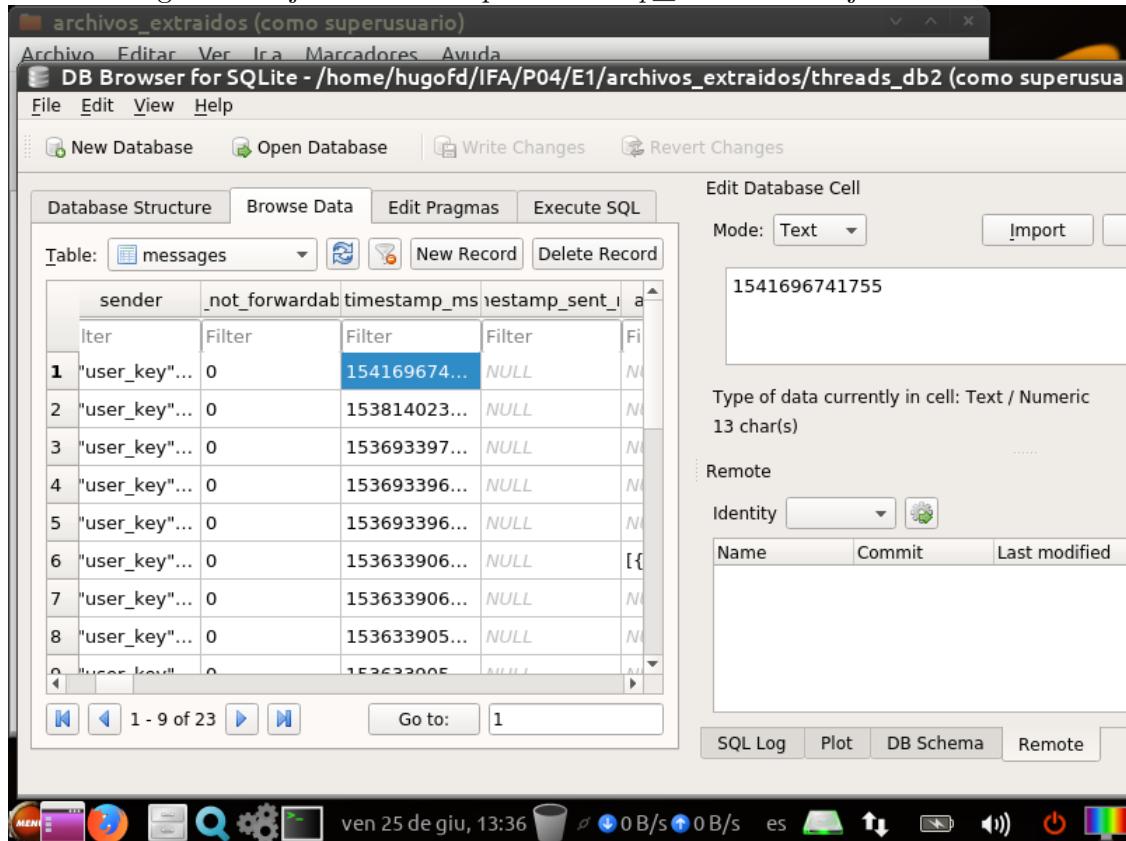
- a) Se procede a buscar el emisor del mensaje.

Figura 47: Ejercicio 5: Campo *sender* del mensaje con ID 21



- b) Se busca ahora la hora de emisión del mensaje, para ello se mira el campo *timestamp_ms*.

Figura 48: Ejercicio 5: Campo *timestamp_ms* del mensaje con ID 21

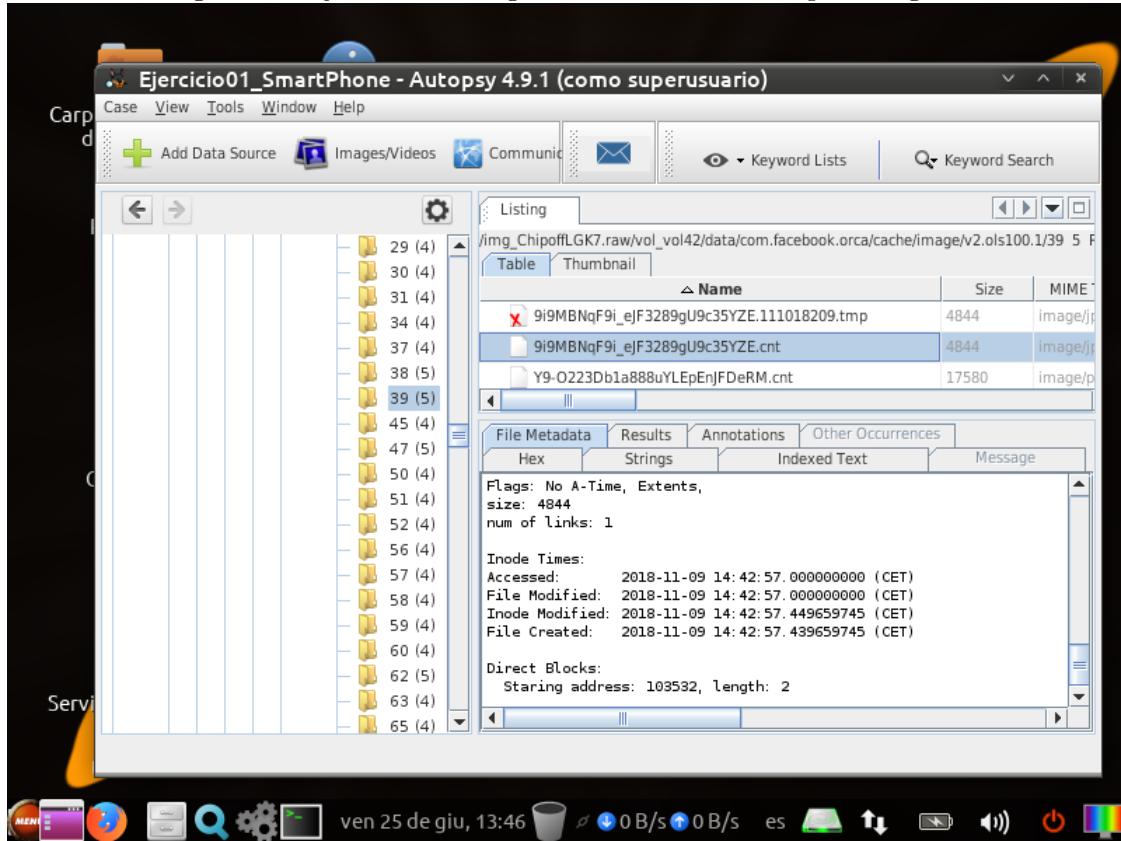


TBD Conversor EPOCH

6. Ejercicio 6

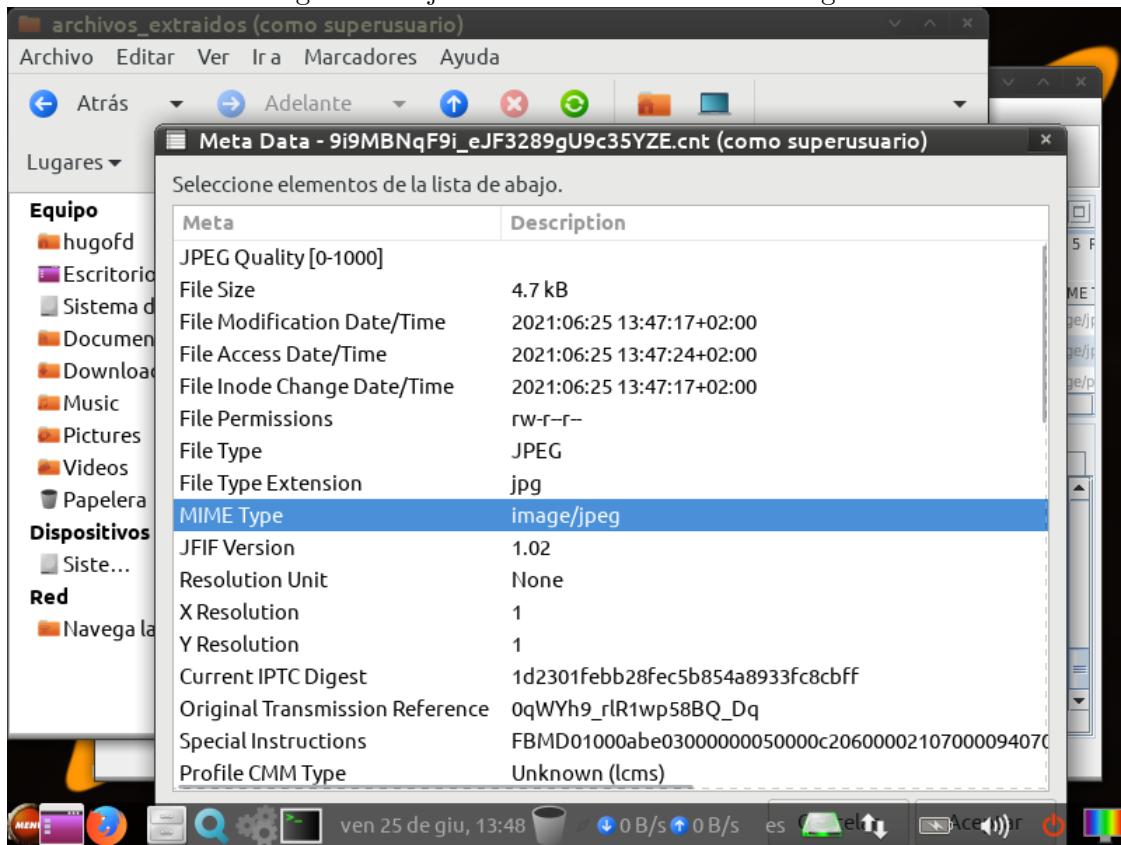
- a) Se encuentra el archivo en la carpeta indicada y se extrae a una carpeta para su análisis.

Figura 49: Ejercicio 6: Imagen a analizar en su carpeta original



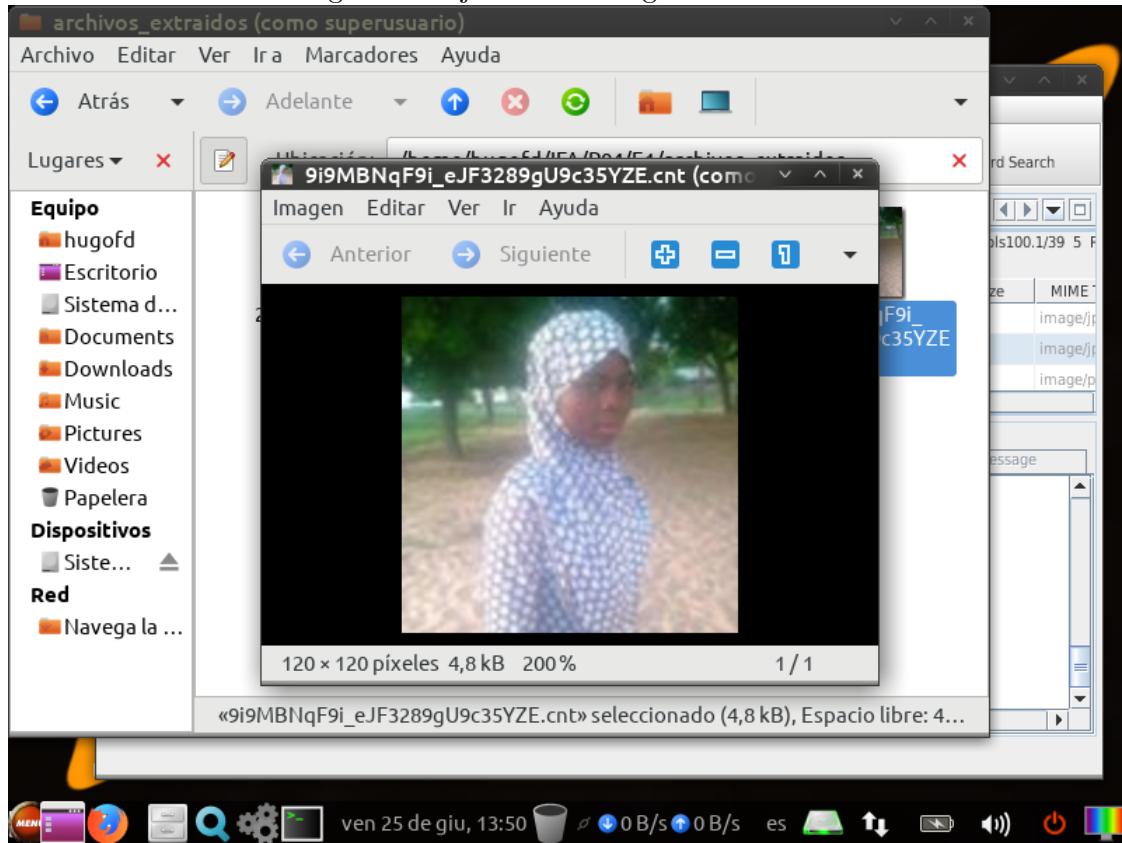
A continuación se observa la salida del script *FileInfo* de la imagen extraída. Se puede observar que su tipo MIME es *image/jpeg*.

Figura 50: Ejercicio 6: Metadatos de la imagen



- b) La fecha del último acceso al archivo puede observarse en una de las anteriores capturas, 2018/11/09 14:42:57 (CET).
- c) Se muestra la imagen del archivo a continuación.

Figura 51: Ejercicio 6: Imagen del archivo



- d) Ni *FileInfo* ni *MediaInfo* contienen metadatos de la localización de la imagen. Autopsy tampoco los muestra, por lo que se concluye que dichos metadatos no están disponibles.

Referencias