



ENERO 2024

# CARLOS SÁNCHEZ RODRÍGUEZ

INFORMÁTICA FORENSE Y AUDITORÍA

CARLOS SÁNCHEZ RODRÍGUEZ

UO282621

UO282621@uniovi.es



## índice

Práctica 2 .....	3
Ejercicio 21 .....	3
Ejercicio 23 .....	5
Ejercicio 34 .....	6
Práctica 3 .....	7
Ejercicio 7 .....	7
Ejercicio 12 .....	11
Apartado a .....	12
Apartado b .....	12
Apartado c .....	13
Apartado d .....	13
Ejercicio 17 .....	14
Apartado a .....	15
Práctica 4 .....	16
Ejercicio 8 .....	16
Apartado ddd .....	16
Apartado ooo .....	17
Apartado ppp .....	18
Apartado ttt .....	19
Apartado yyy .....	20
Ejercicio 9 .....	20
Apartado g .....	21
Apartado mm .....	21
Apartado ss .....	21
Apartado yy .....	22
Apartado xxx .....	22
Práctica 5ª .....	23
Ejercicio 28 .....	23
Apartado b .....	23
Apartado d .....	24
Apartado f .....	24
Apartado l .....	24
Apartado m .....	25
Apartado q .....	25
Ejercicio 34 .....	26

Ejercicio 35 .....	28
Ejercicio 43 .....	29
Apartado a .....	30
Apartado b .....	30
Apartado f .....	31
Apartado i .....	31
Apartado q .....	32
Ejercicio 46 .....	32
Apartado m .....	32
Apartado n .....	32
Apartado o .....	33
Apartado s .....	33
Práctica 5b .....	34
Ejercicio 7 .....	34
Apartado d .....	34
Apartado e .....	34
Apartado f .....	35
Apartado j .....	35
Apartado s .....	36

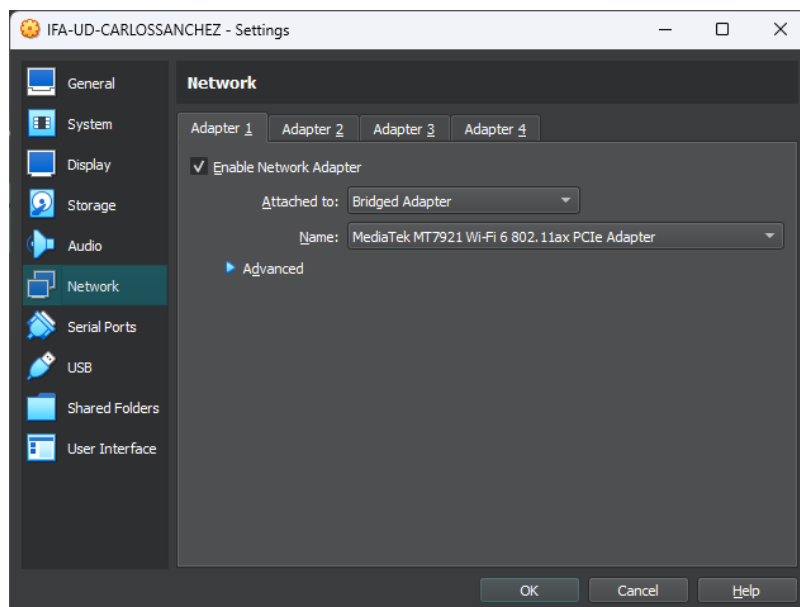
## Práctica 2

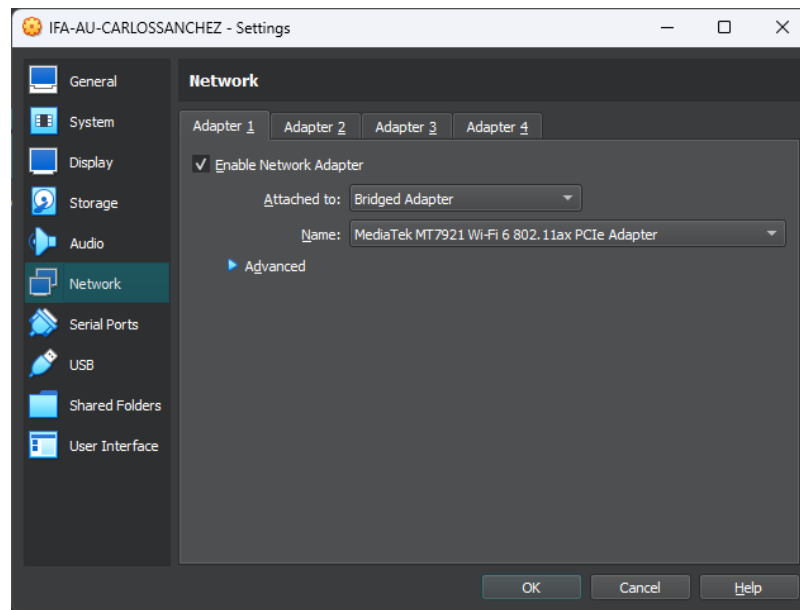
### Ejercicio 21

En algunas ocasiones es necesario adquirir las evidencias de un sistema utilizando un disco de arranque y una conexión de red a la cual está conectada la plataforma de recolección de evidencias. El ordenador del cual crearemos la imagen lo llamaremos ordenador “objetivo” y en el que almacenaremos la imagen lo llamaremos ordenador “recolector de evidencias”. Para poder realizar la imagen a través de la red necesitaremos en primer lugar hacer que el “recolector de evidencias” escuche el flujo de datos proveniente del ordenador “objetivo”. Esto puede hacerse mediante el comando `netcat (nc)`. El primer paso será abrir una conexión de escucha en el “recolector de evidencias” y redirigir todos los datos recibidos en dicha conexión al comando `dd`. En la computadora objetivo debemos ejecutar el comando `dd` tomando como fichero de entrada el fichero que representa el disco (o la partición) del cual queremos hacer la imagen y en lugar de suministrar un fichero de salida canalizaremos la salida al comando `nc` en la dirección IP y puerto en la que está esperando el comando homónimo en la máquina “recolector de evidencias”.

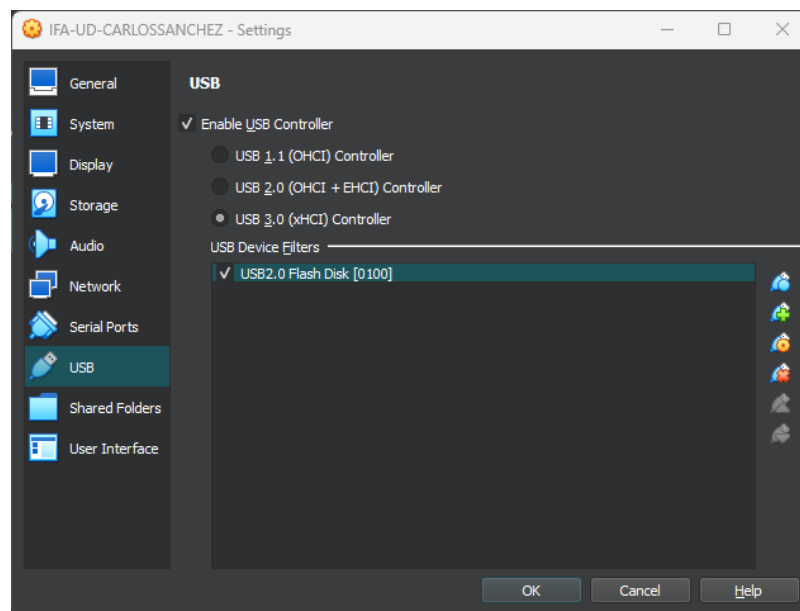
Para probar esta técnica, vamos a hacer una imagen de un dispositivo conectado a su máquina virtual IFA-UD-XX en su máquina virtual IFA-AU-XX. Para ello modifique los interfaces de red de ambas máquinas y colóquelos en modo “adaptador puente”. En segundo lugar, añada un filtro para el lápiz USB que va a conectar a la máquina IFA-UD-XX. Si ya tenía un filtro creado para dicho dispositivo en la máquina IFA-AU-XX, elimínelo primero. Una vez añadido el filtro, conecte dicho dispositivo a la máquina IFA-UD-XX y compruebe que ha sido detectado por el Sistema Operativo de dicha máquina. Haga un hash del dispositivo del cual va a crear la imagen antes de realizarla. Luego haga la imagen utilizando el procedimiento descrito anteriormente para lo cual tendrá que averiguar la IP de la máquina que asume el rol de “recolector de evidencias”. Una vez concluido el proceso de realización de la imagen, haga un hash en destino del fichero de imagen y compruebe si coincide con el hash del dispositivo del cual ha realizado la imagen en origen.

En primer lugar, modificamos las interfaces de red de ambas máquinas, configurándolas del modo **Bridge adapter**.





En segundo lugar, añadimos un filtro de USB a la máquina máquina **IFA-UD-CARLOSSANCHEZ**.



Arrancamos la máquina y tras asegurarnos de que el USB ha sido reconocido por ella, le hacemos un hash tal y como se muestra a continuación:

```
carlossr@carlossr-VirtualBox:~$ sudo sha1sum /dev/sdb
[sudo] contraseña para carlossr:

58012b8556b17edb42e274d1bebc08cdf61ffbf8 /dev/sdb
carlossr@carlossr-VirtualBox:~$
```

A continuación, iniciamos la máquina **IFA-UD-CARLOSSANCHEZ** y consultamos su dirección IPv4 con el comando **ipconfig**. El cual nos la indica como se muestra en la siguiente captura:

```
carlossr@carlossr-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1492
    inet 192.168.1.113 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe82:7139 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:82:71:39 txqueuelen 1000 (Ethernet)
    RX packets 1550 bytes 1915299 (1.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1128 bytes 107593 (107.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Acto seguido ejecutamos en la misma maquina el comando **nc -l -p 5000 | dd of=./ejer21**. Donde **nc** corresponde a netcat, abre el servidor, y las opciones **-l**, que activa el modo escucha, y **-p** para indicar el puerto que queremos usar. Todo ello pasado mediante un pipe al comando **dd** al que se le especifica donde guardar lo recibido con la opción **of=./ejer21**.

```
carlossr@carlossr-VirtualBox:~/Documents$ nc -l -p 5000 | dd of=./ejer21
```

En la maquina donde se ha conectado el USB, se ejecuta el comando mostrado a continuación, donde **dd** crea una imagen del input file especificado por **if=/dev/sdb**. Y mediante un pipe, su salida se envía a la dirección IPv4 mostrada a continuación en el puerto **5000**.

```
carlossr@carlossr-VirtualBox:~$ sudo dd if=/dev/sdb | nc 192.168.1.113 5000
1988608+0 registros leídos
1988608+0 registros escritos
1018167296 bytes (1,0 GB, 971 MiB) copied, 72,836 s, 14,0 MB/s
```

Por último, tras comprobar que el paso anterior ha sido completado, en la maquina de recolección de evidencias hacemos un hash a la información recibida y comprobamos que es equivalente al hecho en la otra maquina antes de su envío (mostrado en anteriores capturas).

```
carlossr@carlossr-VirtualBox:~/Documents$ sudo shasum ./ejer21
58012b8556b17edb42e274d1bebc08cdf61ffbf8 ./ejer21
```

## Ejercicio 23

Reensamble las imágenes creadas en el ejercicio 22 en un único archivo denominado **imagen\_nueva.dd**. Calcule el hash SHA1 de la imagen reensamblada y compáralo con el hash del lápiz obtenido en el ejercicio 17. ¿Son iguales?

Teniendo las imágenes creadas en la carpeta **ejer22**, nos situamos en dicho directorio y ejecutamos los comandos mostrados a continuación. Donde en el primero, **cat** concatena todos los archivos que le siguen, en este caso gracias al **\*** tras el nombre, concatena todos los que hay en el directorio cuyo nombre empiece por **trozo\_pen** y lo guardamos como un nuevo archivo **imagen\_nueva.dd**. Tras ello ejecutamos el comando **sha1sum** que hace un hash al archivo recién creado **imagen\_nueva.dd**

```
carlossr@carlossr-VirtualBox:~/Documents/ejer22$ cat trozo_pen* > imagen_nueva.dd
carlossr@carlossr-VirtualBox:~/Documents/ejer22$ sudo shasum imagen_nueva.dd
5f0f18cf92bb717b35f32a33ac808cd4ea7b64a4 imagen_nueva.dd
```

Por último, comparamos el hash que acabamos de obtener con el obtenido en el ejercicio 17, el cual se muestra a continuación y que como era de esperar, coinciden.

```
141 SHA1 hash : 5f0f18cf92bb717b35f32a33ac808cd4ea7b64a4
```

## Ejercicio 34

Descargue del campus virtual el fichero denominado Recursos de Prácticas->Práctica 2->logs.v3.tar.gz. Destarea y descomprime el anterior archivo en una carpeta denominada logs. Deberás ver 5 ficheros de log de diferentes sistemas Unix. Estos ficheros de log contienen entradas correspondientes a una gran variedad de fuentes, incluyendo el kernel y otras aplicaciones. Crea un pipeline que muestre las fechas (mes y día) en las que ha habido apuntes en los respectivos logs de forma descendente (de más reciente a menos reciente) y que elimine las entradas múltiples (las repetidas para una misma fecha).

Utilizamos el comando **tar -xzf logs.v3.tar.gz** para extraer los ficheros. Donde la opción **-x** sirve para extraer el contenido del archivo, **-z** el tipo de descompresión a utilizar, **-v** para que nos muestre el progreso de la operación y **-f** para especificar el nombre del archivo.

```
carlossr@carlossr-VirtualBox:~/Documents/ej34$ tar -xzf logs.v3.tar.gz
messages
messages.1
messages.2
messages.3
messages.4
```

A continuación, usamos el comando **tac messages\* | awk '{print \$1" "\$2}' | uniq** donde **tac messages\*** nos muestra el contenido de los ficheros cuyo nombre empieza por **messages** ordenados de final a principio. Esa salida se pasa como entrada mediante un pipe al comando **awk '{print \$1" "\$2}'** que procesará cada línea e imprimirá la columna uno y dos separadas por un espacio. Por último, esa salida se le pasa como entrada al comando **uniq** el cual eliminara las filas repetidas.

```
carlossr@carlossr-VirtualBox:~/Documents/ej34$ tac messages* | awk '{print $1" "$2}' | uniq
Nov 23
Nov 22
Nov 21
Nov 20
Nov 19
Nov 18
Nov 17
Nov 13
Nov 12
Nov 11
Nov 10
Nov 7
Nov 6
```

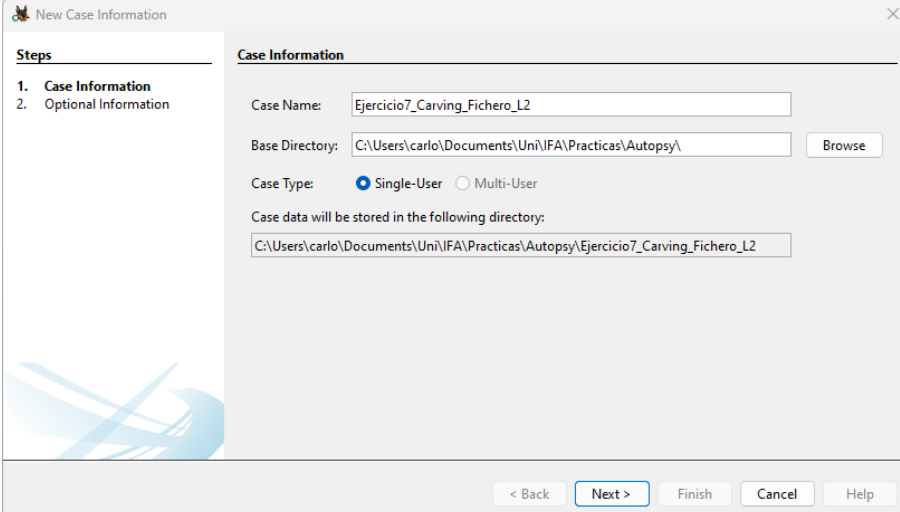
## Práctica 3

### Ejercicio 7

En este ejercicio aplicaremos técnicas de carving sobre ficheros comprimidos (7z, zip, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L0\_Archive.dd.bz2**. Almacénalo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Investigue las posibilidades que le ofrece el módulo de ingestión **Embedded File Extractor**. Añada además al caso los módulos de ingestión que ha utilizado en los ejercicios anteriores. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla. Indique por cada fichero comprimido carveado la siguiente información: Nombre del fichero en Autopsy, Tamaño del fichero (en Bytes) y Tipo MIME

En este ejercicio, al ser el primero a entregar en el que se usa Autopsy, se mostrarán todos los pasos que se deben seguir para crear un nuevo caso. Y puesto que es un proceso repetitivo y similar en todos los ejercicios, las capturas y explicaciones de muchos de estos pasos se obviarán en futuros ejercicios.

En primer lugar, debemos de proporcionar información básica del nuevo caso como son el nombre y donde se almacenará. Tal y como se indica en la siguiente captura:



Continuamos proporcionando información acerca del número de caso y los datos relativos al examinador.



New Case Information

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number: 10012024-7

Examiner

Name: Carlos Sanchez

Phone:

Email: uo282621@uniovi.es

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

Una vez empezamos a configurar con que tipo de datos vamos a trabajar, seleccionaremos **Fichero de Imagen de Espacio no Asignado**.

Add Data Source

**Steps**

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

**Select Data Source Type**

Disk Image or VM File

Local Disk

Logical Files

☒ Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

< Back Next > Finish Cancel Help

A continuación, se selecciona el archivo que queremos examinar y la zona horaria en la que se encuentra el examinador.

Add Data Source

**Steps**

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

**Select Data Source**

Browse for an unallocated space image file:

C:\Users\carlo\Documents\Unif\FA\Practicas\Evidencias\L0\_Archive.dd Browse

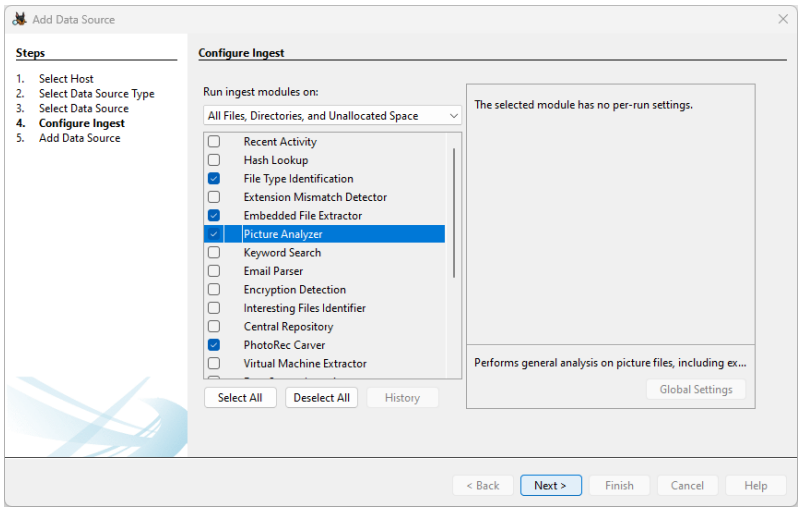
Please select the input timezone: (GMT+1:00) Europe/Madrid

Break image up into:

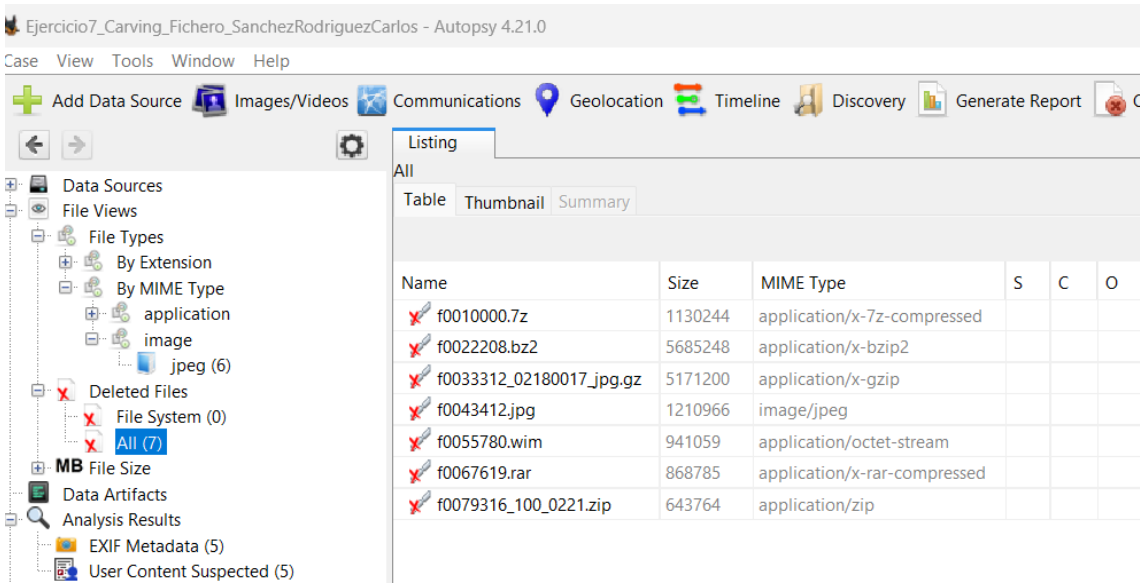
☐ 2GB chunks ☒ Do not break up

< Back Next > Finish Cancel Help

Por último, se seleccionan los módulos de ingestión deseados, que en este caso son los marcados en la siguiente captura.

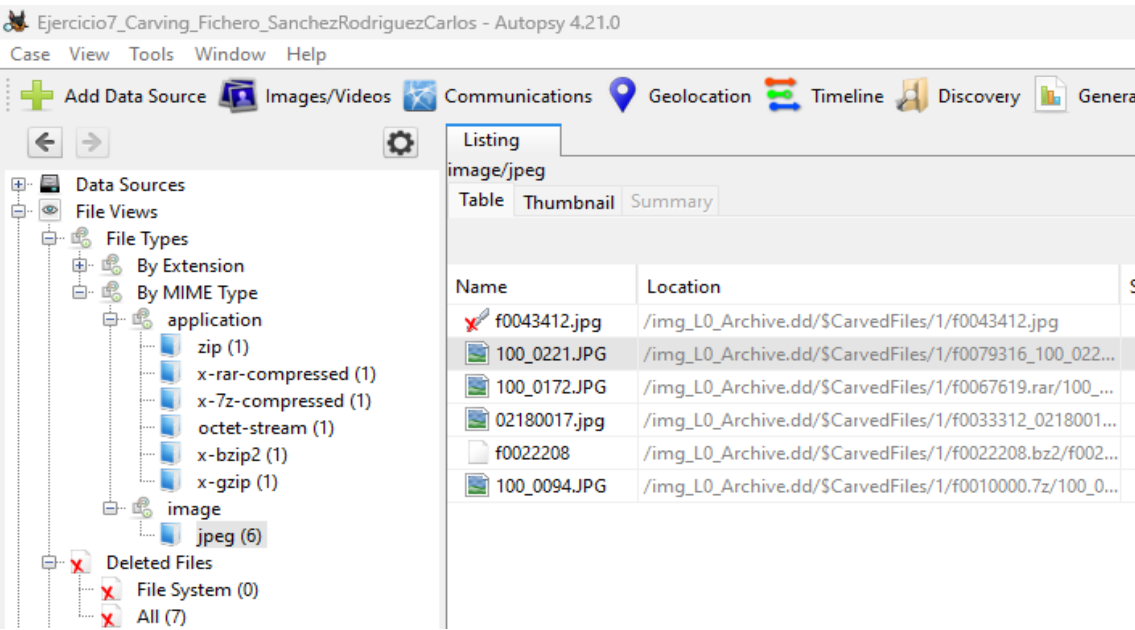


Se encuentran 7 carved files, pero únicamente 6 son ficheros comprimidos ya que uno es una imagen JPG. Toda la información requerida en la primera parte del ejercicio la podemos sacar directamente del panel principal como muestra la siguiente captura:

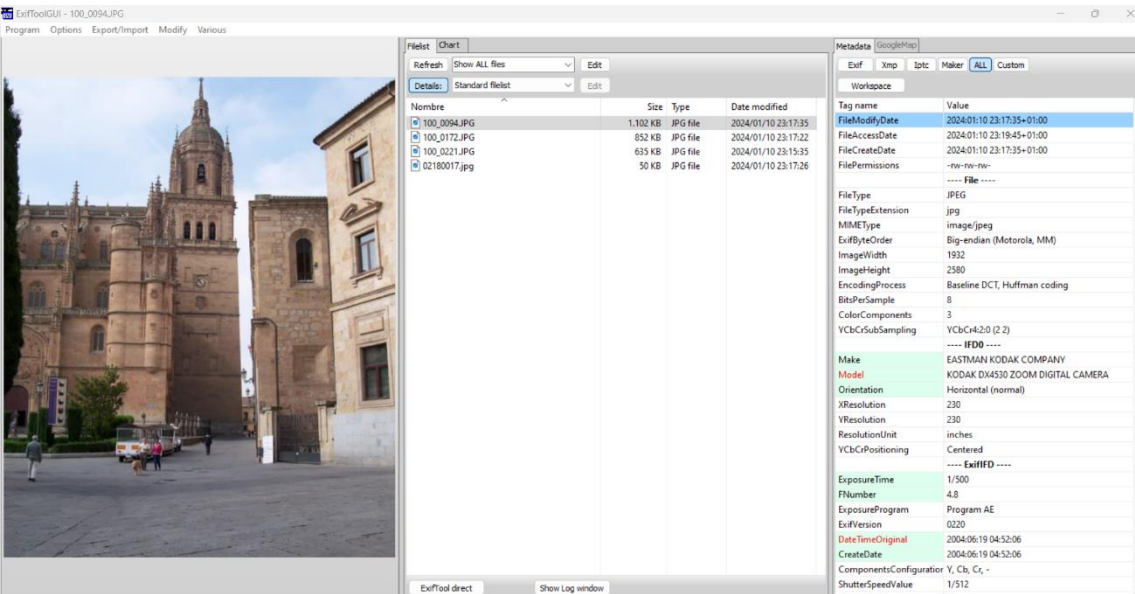


Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME
f0010000.7z	1130244	application/x-7z-compressed
f0022208.bz2	5685246	application/x-bzip2
f0033312_02180017_jpg.gz	5171200	application/x-gzip
f0055780.wim	941059	application/octet-stream
f0067619.rar	868785	application/x-rar-compressed
f0079316_100_0221.zip	643764	application/zip

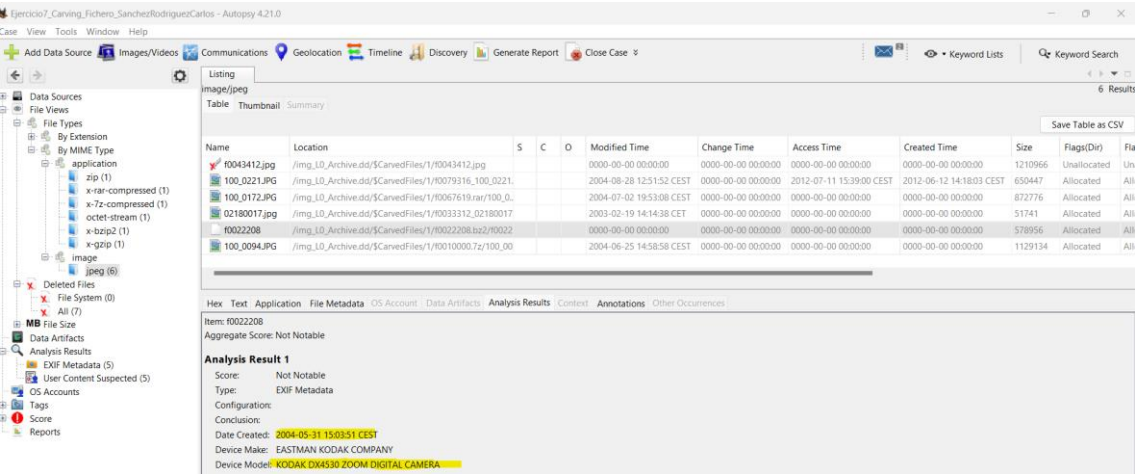
Del contenido de los ficheros comprimidos se pueden extraer 5 ficheros JPG



Exportando los archivos y examinándolos con exifTool obtenemos la información necesaria. En la parte izquierda se puede observar una previsualización del archivo, y en la parte derecha los datos de este. En rojo, marcados los requeridos por el ejercicio. Se muestra únicamente la captura para uno de los archivos, pues para el resto a excepción de un archivo, se seguiría el mismo procedimiento.



Para el archivo, el cual exifTool no detecta, usamos el propio panel de resultados de Autopsy.



Nombre del fichero en Autopsy	Fecha y hora de la imagen	Dispositivo con el que se tomó la imagen	Descripción de la imagen
100_0221.jpg	2004-08-28 07:32:22 CEST	KODAK DX4530 ZOOM DIGITAL CAMERA	Bambú
100_0172.jpg	2004-07-02 19:42:41 CEST	KODAK DX4530 ZOOM DIGITAL CAMERA	Flor roja
021810017.jpg	2003-02-18 10:46:51 CEST	No se logra recabar información al respecto	Casa nevada
f0022208	2004-05-31 15:03:51 CEST	KODAK DX4530 ZOOM DIGITAL CAMERA	Flor blanca
100_0094.jpg	2004-06-19 04:52:06 CEST	KODAK DX4530 ZOOM DIGITAL CAMERA	Calle con edificios

Ejercicio 12

Descarga del campus virtual (Recursos Prácticas- Práctica 3), el dfr-01-gbu.dd.bz2. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada como módulos de ingestión de evidencia asociados al proyecto los módulos siguientes: File Type Identification, PhotorecCarver.

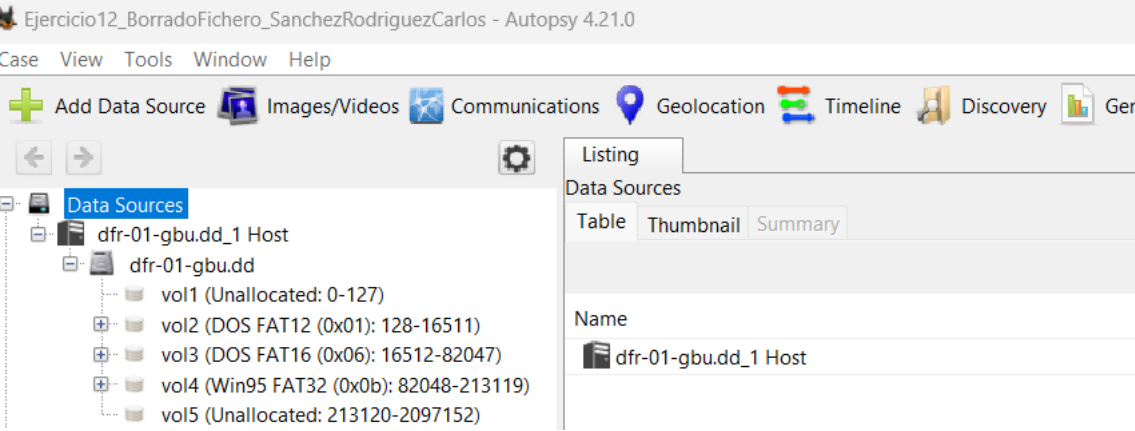
El procedimiento de creación del nuevo caso es similar al ejercicio anterior y por ello, con el fin de no saturar el documento de información repetida, se obvia su explicación en este. Las únicas diferencias son el **data source type** que en este caso será **disk image or VM file**, y los módulos de ingestión, en este caso **file type identification** y **photorecCarver**.

Apartado a

Responda a las siguientes cuestiones:

Número de partición	Sector de comienzo	Sector de finalización	Tipo de sistemas de ficheros
1	0	127	Unallocated
2	128	16511	DOS FAT12
3	16512	82047	DOS FAT16
4	82048	213119	Win95 FAT32
5	213120	2097152	Unallocated

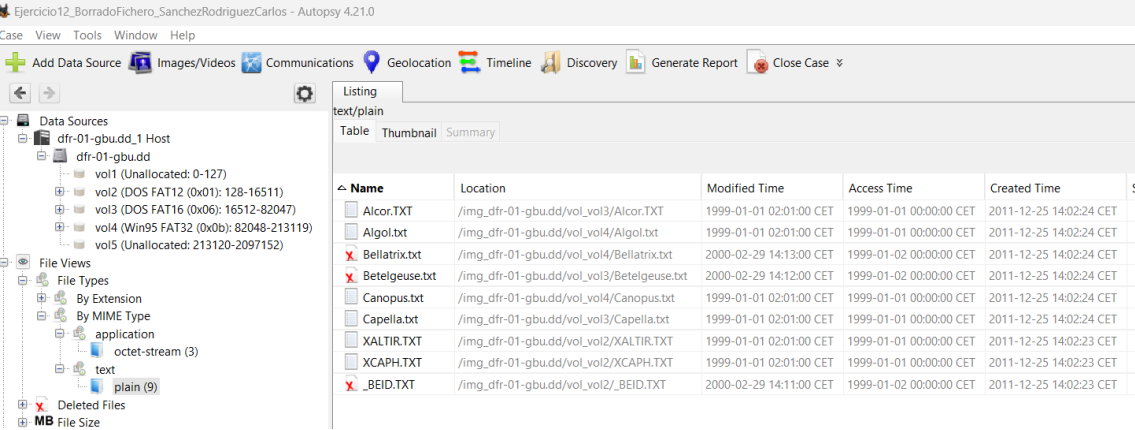
Toda la información detallada en la tabla anterior se puede obtener fácilmente del panel de navegación izquierdo de Autopsy, tal y como se muestra en la siguiente captura:



Apartado b

¿Cuántos ficheros de texto (borrados o no) se encuentran en las particiones detectadas en la imagen?

Como se muestra en la siguiente imagen, se encuentran 9 ficheros de texto.



Apartado c

Por cada fichero borrado indique la siguiente información:

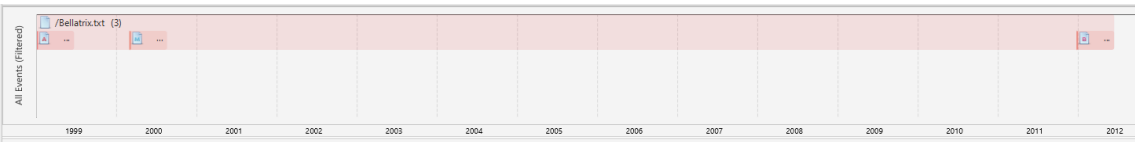
				MAC times por cada fichero antes del borrado (GMT)		
Nombre	Tamaño (bytes)	Sector relativo	Partición	Acceso	Modificación	Creación
Bellatrix.txt	712	8195	4	1999-01-01 23:00:00	2000-02-29 13:13:00	2011-12-25 13:02:24
Betelgeuse.txt	712	546	3	1999-01-01 23:00:00	2000-02-29 13:12:00	2011-12-25 13:02:24
_BEID.TXDT	712	170	2	1999-01-01 23:00:00	2000-02-29 13:11:00	2011-12-25 13:02:23

Para rellenar la tabla anterior, se ha extraído la información del panel central de Autopsy (en la captura anterior se pueden ver por ejemplo las MAC times). Las MAC times se han convertido del huso horario CEST al GMT, restando una hora, provocando que la fecha de acceso sea en el día anterior al que muestra la captura. La única información no disponible en este panel es el sector relativo el cual se ha obtenido observando el apartado de File Metadata.

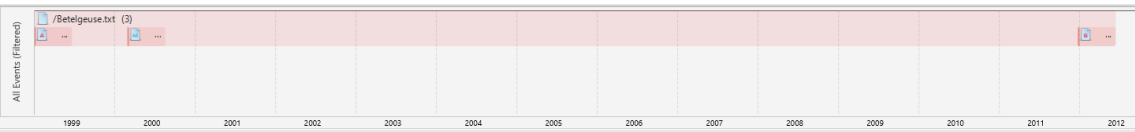
Apartado d

Muestre la línea temporal de cada uno de los ficheros borrados localizados por la herramienta.

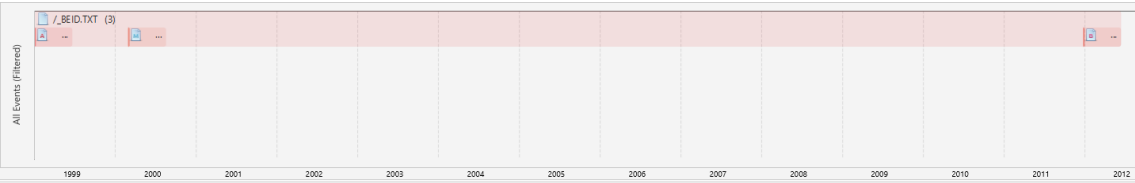
Bellatrix.txt



Betelgeuse.txt



\_BEID.TXDT



## Ejercicio 17

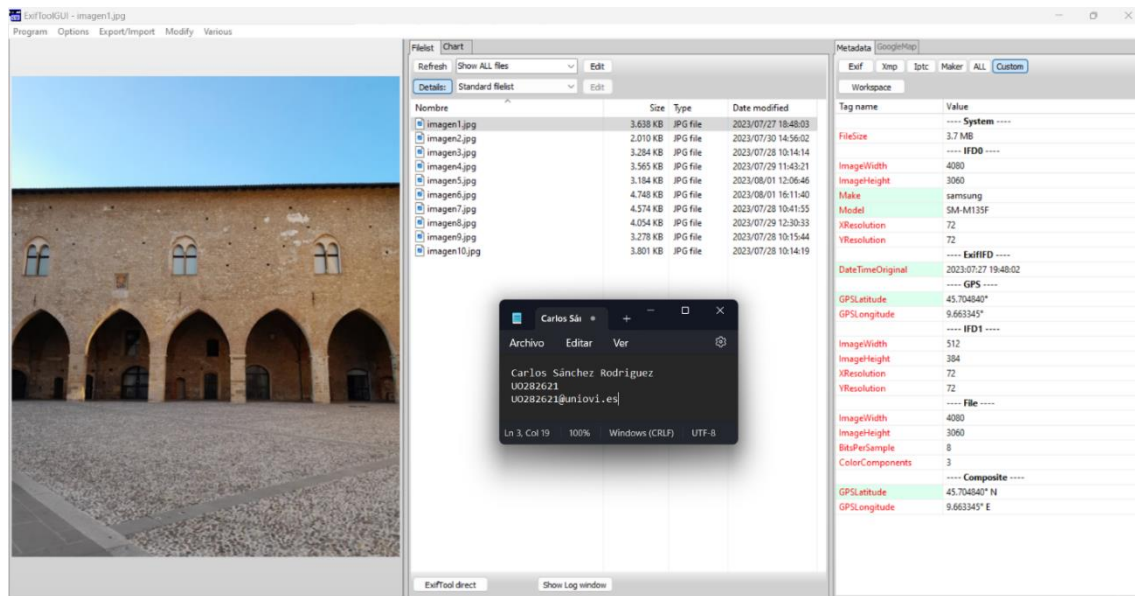
Descarga del campus virtual (Recursos Prácticas- Práctica 3), el fichero imagenesEXIF.zip. Almacénalo en una carpeta de Evidencias. Descomprime dicho archivo y, ayudado por las herramientas instaladas en los dos ejercicios anteriores, obtén para cada archivo la siguiente información a partir de sus etiquetas:

- Fecha en la que fue tomada la imagen
- Marca de la cámara.
- Modelo de la cámara.
- Características de la imagen:
  - Ancho y alto de la imagen en pixeles.
  - Resolución en el eje X (ppp o dpi).
  - Resolución en el eje Y (ppp o dpi).
  - Bits de color por píxel.
- Tamaño del archivo.
- Ubicación GPS (si disponible)
- Lugar correspondiente a la ubicación. A partir de coordenadas de posicionamiento GPS utilizando Google Maps.
- 

	Imagen 1	Imagen 2	Imagen 3	Imagen 4	Imagen 5
Fecha captura de la imagen (AAAA-MM-DD hh:mm:ss)	2023-07-27 19:48:02 +2:00	2023-07-30 15:56:00 +2:00	2023-07-28 11:14:14 +2:00	2023-07-29 12:43:20 +2:00	2023-08-01 13:06:45 +2:00
Marca cámara	Samsung	Samsung	Samsung	Samsung	Samsung
Modelo cámara/dispositivo	SM-M135F	M135F	M135F	M135F	M135F
AnchoxAlto	4080x3060	4080x3060	4080x3060	4080x3060	4080x3060
Resolución horizontal (ppp)	72	72	72	72	72
Resolución vertical (ppp)	72	72	72	72	72
Bits de color por píxel	24	24	24	24	24
Tamaño archivo (KB)	3638	2010	3284	3565	3184
Ubicación GPS (Latitud y Longitud)	45.704840°N – 9.663345°E	43.767867°N – 11.255473°E	45.466312°N – 9.197347°E	43.717990°N – 10.399654°E	41.8932595°N – 12.482768°E
Lugar correspondiente a la ubicación	Bérgamo	Florenia	Milán	Pisa	Roma

Todos los datos se han obtenido mediante la herramienta ExifTool. Con el fin de aglutinar todos los datos en una sola captura se han seleccionado y añadido todos los datos

necesarios (de la pestaña All en Metadata) a una lista customizada tal y como se indica en la siguiente imagen:



Cabe destacar que los bits de color por píxel, no se muestran como tal, pero se calculan como  $\text{ColorComponents} * \text{BitsPerSample}$ .

## Apartado a

Suponiendo que las fotos fueron adquiridas de un mismo dispositivo, ¿qué sitios visitó su propietario en orden cronológico?

Suponiendo que todas las fotos son de un mismo dispositivo, el dispositivo ha visitado en orden cronológico: Bérgamo, Milán, Pisa, Florencia y Roma





El panel de navegación nos muestra cómo se encuentran 10 fichero de video de tipo mp4. Entrando en la lista de estos y comprobando cuando han sido creados, se puede observar que son 6 los que se han creado entre el 1 y 30 de noviembre de 2018 tal y como se muestra en la siguiente captura:

Directory Tree

- Data Sources
  - JTAGsamsungS4.bin\_1 Host
    - JTAGsamsungS4.bin
- File Views
  - By Extension
    - Images (2093)
    - Videos (20)
    - Audio (226)
    - Archives (860)
    - Databases (362)
    - Documents
    - Executable
  - By MIME Type
    - application
    - audio
    - image
    - message
    - multipart
    - text
    - video

Listing

Name	Created Time	Size	Location
custom_sticker_onboarding_10_6.mp4	2018-11-16 01:20:25 CET	123798	/img_JTAGsamsungS4.bin/vol_vol32/data/com.snapc...
FB_VIDEO_FOR_UPLOAD_1542245053243.mp4	2018-11-15 02:24:13 CET	552836	/img_JTAGsamsungS4.bin/vol_vol32/data/com.facebo...
PART_1542244092760_20181114_200004_001.mp4	2018-11-15 02:08:12 CET	294864	/img_JTAGsamsungS4.bin/vol_vol32/data/com.androi...
20181114_163729.mp4	2018-11-14 22:37:29 CET	29457814	/img_JTAGsamsungS4.bin/vol_vol32/media/0/DCIM/...
bubbly.mp4	2018-11-14 22:14:40 CET	12124832	/img_JTAGsamsungS4.bin/vol_vol32/media/0/Downlo...
20181114_160934.mp4	2018-11-14 22:09:34 CET	13737829	/img_JTAGsamsungS4.bin/vol_vol32/media/0/DCIM/...
video_help.mp4	1971-03-28 13:15:53 CET	8411614	/img_JTAGsamsungS4.bin/vol_vol19/media/video/vid...
camera.mp4	1970-05-05 10:54:23 CET	5936965	/img_JTAGsamsungS4.bin/vol_vol19/media/video/ca...
group_play.mp4	0000-00-00 00:00:00	2374174	/img_JTAGsamsungS4.bin/vol_vol19/media/video/gro...
motion.mp4	0000-00-00 00:00:00	6250562	/img_JTAGsamsungS4.bin/vol_vol19/media/video/mo...

## Apartado 000

Localice el fichero `usage-history.xml` e indique dónde lo ha localizado. Almacene dicho fichero en la carpeta Export del caso. Abra dicho archivo con un visor XML. Indique en qué fecha-hora (GMT+1) se produjo el evento `LoginActivity`.

El fichero **usage-history.xml** se encuentra en la partición encargada de almacenar el **userdata**. La ruta específica es: **vol\_vol32/system/usegestats**. A continuación, se muestra una captura donde se puede observar esta información.

Directory Tree

- audio (4)
- backup (8)
- bcmnfc (6)
- clipboard (6)
- connectivity (5)
- dalvik-cache (176)
- data (314)
- dontpanic (2)
- drm (4)
- fota (2)
- hostapd (2)
- knox (7)
- local (3)
- log (15)
- lost+found (2)
- media (5)
- mediadrmm (3)
- misc (77)

Listing

Name	Size	MIME Type	S	C	O	Modified Time
usage-history.xml.bak	10236	application/octet-stream				2018-11-09 06:26:59 CET
usage-history.xml	13865	text/xml				2018-11-08 14:42:19 CET
usage-20181116	7088	application/octet-stream				2018-11-16 21:49:41 CET
usage-20181115	7408	application/octet-stream				2018-11-16 01:05:42 CET
usage-20181114	8496	application/octet-stream				2018-11-14 22:40:06 CET
usage-20181111	0	application/octet-stream				2018-11-11 16:11:58 CET
usage-20181109	0	application/octet-stream				2018-11-09 06:23:34 CET
usage-20181108.bak	0	application/octet-stream				2018-11-11 16:16:23 CET
[parent folder]	4096					2018-11-11 16:32:59 CET
[current folder]	4096					2018-11-11 16:11:58 CET

Una vez localizado y extraído el fichero .XML, lo analizamos y podemos observar como como el **LoginActivity** se produjo en la fecha **2018-11-15 14:31:58 GMT+1**. Fecha que obtenemos de traducir el timestamp **1542245518015**.

```

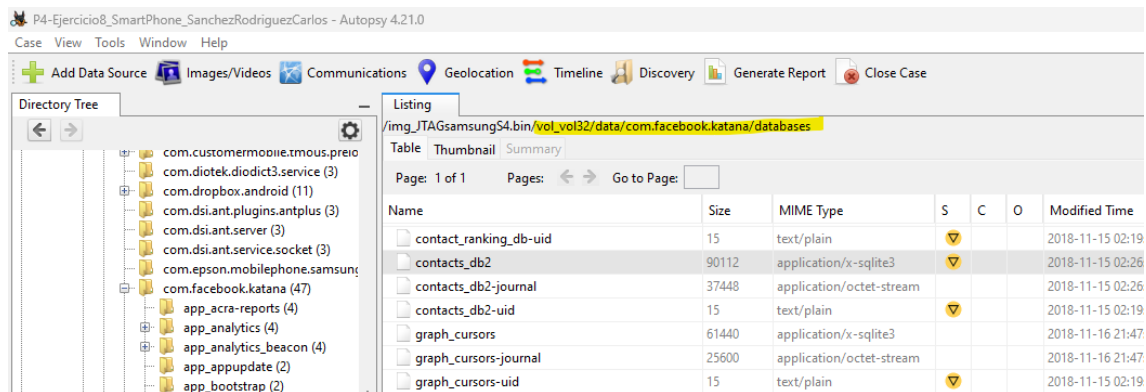
102 <comp name="com.twitter.app.onboarding.common.OcfInvisibleSubtaskActivity" lrt="1542245494014" />
103 <comp name="com.twitter.app.onboarding.signup.SignUpSplashActivity" lrt="1542245511149" />
104 <comp name="com.twitter.app.dm.DMAActivity" lrt="1542245658991" />
105 <comp name="com.twitter.android.AuthorizeAppActivity" lrt="1542245545048" />
106 <comp name="com.twitter.app.onboarding.loading.OcfStartFlowActivity" lrt="1542245493125" />
107 <comp name="com.twitter.android.LoginActivity" lrt="1542245518015" />
108 <comp name="com.twitter.app.onboarding.signup.SignUpStepFormActivity" lrt="1542245494470" />
109 <comp name="com.twitter.android.StartActivity" lrt="1542327683151" />
110 </pkg>

```

## Apartado ppp

Obtenga información sobre los contactos de Facebook almacenados por dicha aplicación. ¿Cuántos contactos hay? ¿Cuáles son sus nombres?

Esta información se encuentra en la base de datos **contacts\_db2** la cual se sitúa en la ruta **userdata/data/com.facebook.katana/databases/contacts\_db2** (siendo userdata equivalente a vol\_vol32) tal y como se muestra a continuación:



Una vez localizada la base datos, la exportamos al equipo y la analizamos con la herramienta **DBbrowserForSQLite**.

internal_id	contact_id	fbid	first_name	last_name	display_name	small_picture_url
Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	2	Y29udGFjdDoxMDAwMDcyNDYxODQxNDM6MTAw...	John	Smith	John Smith	https://scontent-iad3-1.xx.fbcdn.net/v/t1.0-1/...
2	1	Y29udGFjdDoxMDAwMDcyNDYxODQxNDM6MTAw...	Jane	Smith	Jane Smith	https://scontent-iad3-1.xx.fbcdn.net/v/t1.0-1/...

Editar celda

Modo: Texto

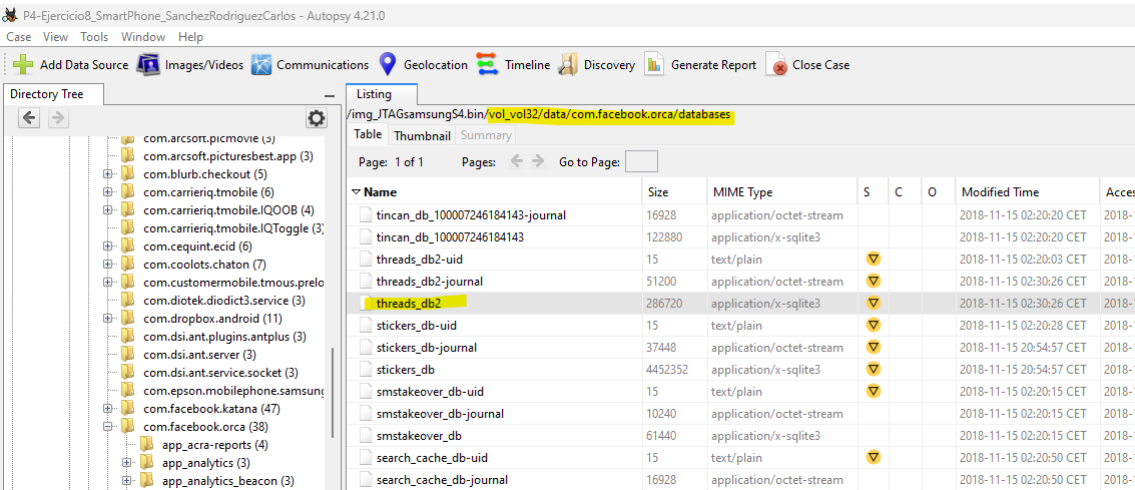
NL Carlos Sánchez Rodríguez  
UO282621  
UO282621@uniovi.es

Se observa claramente como únicamente existen dos contactos y sus nombres son **John Smith** y **Jane Smith**.

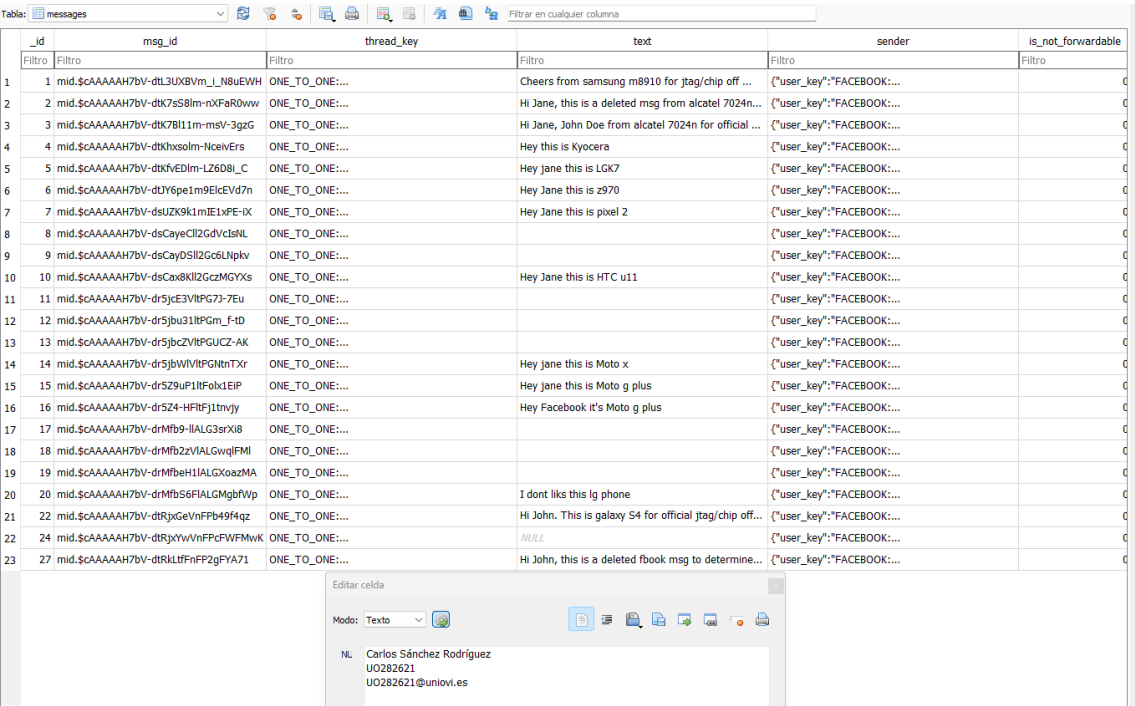
Apartado ttt

Obtenga información sobre los mensajes de Facebook enviados/recibidos por el usuario desde/en su teléfono móvil a través de la aplicación de mensajería de Facebook. ¿Cuántos mensajes fueron enviados/recibidos por el usuario desde/en el teléfono móvil a través de la aplicación de mensajería de Facebook?

Al igual que en el anterior apartado, esta información se encuentra en una base de datos. Esta vez la **threads\_db2** en la ruta **userdata/data/com.facebook.orca/databases/threads\_db2**.



Como anteriormente, exportamos dicha base de datos y la analizamos con **DBbrowserForSQLite**. Podemos observar que el usuario envió/recibió 23 mensajes.



## Apartado yyy

¿En cuántos mensajes recibidos remitidos por el usuario de Facebook de id 100007218342184 aparece la palabra Moto?

Siguiendo con la herramienta **DBbrowserForSQLite** y esta vez haciendo uso de sus filtros por columnas (en la columna texto: “Moto”), se observa 3 mensajes en los que aparece la palabra Moto.

Tabla: messages

_id	msg_id	thread_key	text	sender	is_not_forwa
Filtro	Filtro	Filtro	Moto	Filtro	Filtro
1	14 mid.\$CAAAA7bV-dr5jbWVlTPGNtTxr	ONE_TO_ONE:...	Hey jane this is Moto x	{"user_key": "FACEBOOK:..."}	
2	15 mid.\$CAAAA7bV-dr5Z9uP1lIFolk1EIP	ONE_TO_ONE:...	Hey jane this is Moto g plus	{"user_key": "FACEBOOK:..."}	
3	16 mid.\$CAAAA7bV-dr5Z4-HFtFj1tnvjy	ONE_TO_ONE:...	Hey Facebook it's Moto g plus	{"user_key": "FACEBOOK:..."}	

Editar celda

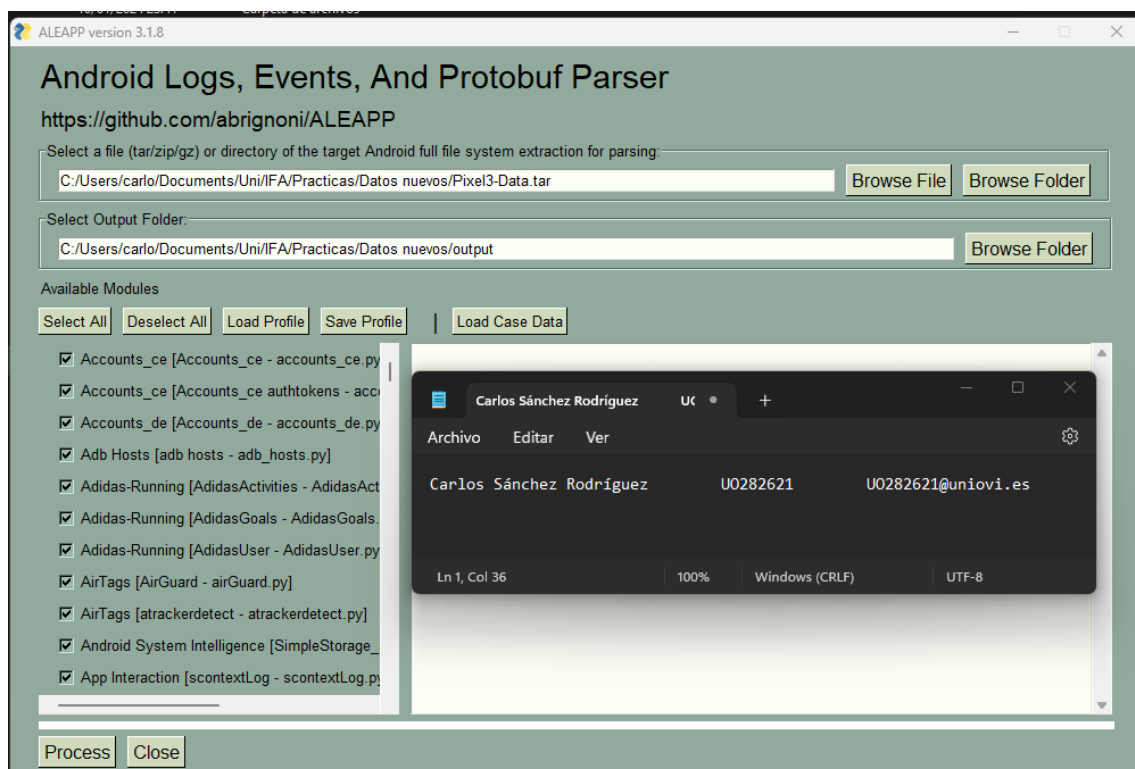
Modo: Texto

Carlos Sánchez Rodríguez  
U0282621  
U0282621@uniovi.es

## Ejercicio 9

Descarga del campus virtual (Recursos Prácticas->Práctica 4), el fichero Pixel3-Data.tar. Este fichero se corresponde con un tar de la carpeta data de un móvil modelo Google Pixel 3. Utiliza ALEAPP GUI para hacer un triaje rápido de dicho fichero y responde a las siguientes cuestiones:

En primer lugar, se ha procedió con hacer el triaje al fichero tal y como se muestra en la siguiente captura de pantalla.



Apartado g

¿En qué fecha/hora se estableció la conexión con el dispositivo Forerunner 35?

Esta información se encuentra en el apartado de Bluetooth Connections, en la que como se muestra en la siguiente captura, la conexión se estableció en la fecha **2020-10-02** y hora **03:51:17 UTC**.

Show 15 entries

Search:

First Connected Timestamp	Device Name	MAC Address	Link Key
	Charge 3	C4:B4:5E:16:B5:E9	
	Rouge	B4:EC:02:73:FF:93	d21126cc7d7652ba2378325c68a9347f
2020-09-14 17:51:33	iHome B66	90:C6:82:02:43:F6	bae21b8cf965dfdaa92b2a596c85fc4
2020-09-16 14:09:08	TicWatch E2 0018	98:28:A6:D4:93:BB	6bfc9a814a337d49ff92b8f45864a9f2
2020-10-02 03:51:17	Forerunner 35	C1:D1:71:67:AC:4E	
First Connected Timestamp	Device Name	MAC Address	Link Key

Archivo

Editar

Ver

Carlos Sánchez Rodríguez

U0282621

U0282621@uniovi.es

Ln 3, Col 1

100%

Windows (CRLF)

UTF-8

Apartado mm

¿Cuántas tarjetas SIM estuvieron insertadas en el teléfono?

Tal y como se muestra a continuación, en el teléfono han estado insertadas 3 tarjetas SIM.

DEVICE INFO

Partner Settings

SIM\_info\_0

Settings\_Secure\_0

Settings\_Secure\_10

DIGITAL WELLBEING

Account Data

Events

DOWNLOADS

Native Downloads

EMULATED STORAGE METADATA

Emulated Storage Metadata - Au

Show 15 entries

Search:

Number	IMSI	Display Name	Carrier Name	ISO Code	Carrier ID	ICC ID
		Google Fi			1952	89015801000029277699
2313604902	310260976111372	Google Fi	No service	us	1989	8901260971161113723
19195794674	310260974867669	Google Fi	Emergency calls only – Google Fi	us	1989	8901260971148676693
+19195794674	310120406713246	Google Fi	Google Fi	us	1989	89011203004067132462
Number	IMSI	Display Name	Carrier Name	ISO Code	Carrier ID	ICC ID

Showing 1 to 4 of 4 entries

Previous

1

Next

Carlos Sánchez Rodríguez

U0282621

U0282621@uniovi.es

Apartado ss

¿Qué actividad estaba realizando el usuario que portaba el móvil a partir de las 12:49 del 13-09-2020?

El usuario se encontraba corriendo tal y como nos muestra el registro de Fibit Activity.

Fitbit Activity

Fitbit Heart Rate Summary

Fitbit Sleep Detail

Fitbit Sleep Summary

Fitbit User Profile

GEO LOCATION

Google Search History Maps

GARMIN

Garmin - Devices

Garmin - GCM Cache Activities

Garmin - Notifications

Garmin - Close Activities

Show 15 entries

Search: 2020-09-13 12:49

Timestamp	Time Created	Name	Log Type	Active Duration	SPEED	Pace	Elevation Gain	Avg Heart Rate	Distance	Distance Unit
2020-09-13 12:49:16	2020-09-24 16:30:28	Run	tracker	1270	11.545625196850393	311.8064148645729	42.672	156	4.073039	Kilometer
Timestamp	Time Created	Name	Log Type	Active Duration	SPEED	Pace	Elevation Gain	Avg Heart Rate	Distance	Distance Unit

Showing 1 to 1 of 1 entries (filtered from 14)

Previous

1

Next

Carlos Sánchez Rodríguez

U0282621

U0282621@uniovi.es

Apartado yy

¿Estaba el usuario del teléfono durmiendo entre las 3:30AM GMT y las 10:15AM GMT del día 2-10-2020?

El usuario se encontraba durmiendo entre dichas horas. Y así nos lo muestran los registros de **Garmin – Sleep Activities**. El uso horario dado (**UTC**) y el pedido (**GMT**) son equivalentes por lo que no hay que hacer ninguna conversión.

GEO LOCATION

Google Search History Maps

GARMIN

Garmin - Devices

Garmin - GCM Cache Activities

Garmin - Notifications

Garmin - Sleep Activities

Garmin - Weather

GARMIN-CACHE

Activities

Dailies

Polyline

Sleep

Show 15 entries

Search:

Sleep Start Timestamp (UTC)	Sleep End Timestamp (UTC)	Auto Sleep Start Timestamp (UTC)	Auto Sleep End Timestamp (UTC)	Total Sleep Time	Deep Sleep	Light Sleep	REM Sleep	Awake Sleep	Average SpO2	Lowest SpO2	Average Breaths/mi
2020-10-02 03:16:00	2020-10-02 10:40:00	2020-10-02 03:16:00	2020-10-02 10:40:00	07:24:00	02:21:00	05:03:00	00:00:00	00:00:00	-1	-1	-1.0
2020-10-03 02:56:00	2020-10-03 10:54:00	2020-10-03 02:56:00	2020-10-03 10:54:00	07:58:00	02:20:00	05:38:00	00:00:00	00:00:00	-1	-1	-1.0
2020-10-04 03:38:00	2020-10-04 10:44:00	2020-10-04 03:38:00	2020-10-04 10:44:00	07:01:00	02:07:00	04:54:00	00:00:00	00:05:00	-1	-1	-1.0
Sleep Start Timestamp (UTC)	Sleep End Timestamp (UTC)	Auto Sleep Start Timestamp (UTC)	Auto Sleep End Timestamp (UTC)	Total Sleep Time	Deep Sleep	Light Sleep	REM Sleep	Awake Sleep	Average SpO2	Lowest SpO2	Average Breaths/mi

Apartado xxx

La imagen transmitida a través de Snapchat el 4-10-2020, ¿dónde fue tomada?

Haciendo uso de las columnas **latitude** y **longitude** que observamos en el apartado **Snapchat – Snap Media**, y tras filtrar por la fecha indicada, obtenemos que la imagen fue tomada en Holly Springs en Carlina del Norte, EEUU.

SNAPCHAT

Snapchat - Feeds

Snapchat - Friends

Snapchat - Identity Persistent

Snapchat - Login Signup

Snapchat - Memories

Snapchat - Messages

Snapchat - Snap Media

Snapchat - User Session Shared

TEXT NOW

Search: 2020-10

uration	Has Overlay	Overlay Size	Overlay Info	Front Facing	Size	Has Location Info	Latitude	Longitude	Snap User Agent	Thumbnail Size	Thumbnail Info
.0	NO			NO	4302448	YES	35.6712338	-78.8778653	Snapchat/11.0.6.82 (Pixel 3; Android 11#6720564#30; gzip) V/MUSHROOM		
uration	Has Overlay	Overlay Size	Overlay Info	Front Facing	Size	Has Location Info	Latitude	Longitude	Snap User Agent	Thumbnail Size	Thumbnail Info



## Práctica 5ª

### Ejercicio 28

Descargue del campus virtual (Recursos Prácticas->Práctica 5) el fichero denominado windowsram.zip. Se trata de una captura de la memoria RAM de una máquina Windows. Descomprima dicho archivo. Vamos a intentar buscar en la captura de memoria trazas de malware. Utilice la herramienta Volatility y realice los siguientes apartados sobre dicha imagen:

Se prueba la autoría en observando la ruta en la que estamos (users/carlo -> Carlos Sánchez Rodríguez)

### Apartado b

Obtenga la lista de procesos que se encontraban en ejecución cuando se obtuvo el volcado de memoria. ¿Son todos los procesos svchost.exe hijos del proceso services.exe?

Para obtener la lista de procesos ejecutamos el comando que se muestra en la siguiente captura. Donde **.\volatility\_2.6\_win64\_standalone.exe** indica el ejecutable a utilizar y la opción **-f** nos permite especificar que archivo analizar (**.\windowsRAM.vmem**) Por último especificamos el tipo de perfil del Sistema Operativo (previamente averiguado) con **--profile=WinXPSP2x86** y para finalizar, indicamos que nos muestre la lista de los procesos con **pslist**.

```
PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\windowsRAM.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                Exit
-----
0x810b1660 System                4    0     58   379  -----  0
0xff2ab020 smss.exe             544    4      3    21  -----  0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe           608   544    10   410    0    0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe        632   544    24   536    0    0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe       676   632    16   288    0    0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe             688   632    21   405    0    0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe          844   676     1    37    0    0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe           856   676    29   336    0    0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe           936   676    11   288    0    0 2010-08-11 06:06:24 UTC+0000
```

Para ver visualmente si todos los procesos svchost.exe son hijos de services.exe, ejecutamos el comando mostrado a continuación, donde esta vez indicamos **pslist** para que nos muestre el árbol de procesos. Como se puede observar, si que son todos hijos de services.exe



```
PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\windowsRAM.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
```

Name	Pid	PPid	Thds	Hnds	Time
0x810b1660: System	4	0	58	379	1970-01-01 00:00:00 UTC+0000
. 0xff2ab020: smss.exe	544	4	3	21	2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978: winlogon.exe	632	544	24	536	2010-08-11 06:06:23 UTC+0000
... 0xff255020: lsass.exe	688	632	21	405	2010-08-11 06:06:24 UTC+0000
... 0xff247020: services.exe	676	632	16	288	2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28: vmtoolsd.exe	1668	676	5	225	2010-08-11 06:06:35 UTC+0000
..... 0xff224020: cmd.exe	124	1668	0	-----	2010-08-15 19:17:55 UTC+0000
..... 0x80ff88d8: svchost.exe	856	676	29	336	2010-08-11 06:06:24 UTC+0000
..... 0xff1d7da0: spoolsv.exe	1432	676	14	145	2010-08-11 06:06:26 UTC+0000
..... 0x80fbf910: svchost.exe	1028	676	88	1424	2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0: wuauc.lt.exe	1732	1028	7	189	2010-08-11 06:07:44 UTC+0000
..... 0x80f94588: wuauc.lt.exe	468	1028	4	142	2010-08-11 06:09:37 UTC+0000
..... 0xff364310: wscntfy.exe	888	1028	1	40	2010-08-11 06:06:49 UTC+0000
..... 0xff217560: svchost.exe	936	676	11	288	2010-08-11 06:06:24 UTC+0000
.... 0xff143b28: TPAutoConnSvc.e	1968	676	5	106	2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8: TPAutoConnect.e	1084	1968	1	68	2010-08-11 06:06:52 UTC+0000
.... 0xff22d558: svchost.exe	1088	676	7	93	2010-08-11 06:06:25 UTC+0000
.... 0xff218230: vmacthlp.exe	844	676	1	37	2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0: alg.exe	216	676	8	120	2010-08-11 06:06:39 UTC+0000
.... 0xff203b80: svchost.exe	1148	676	15	217	2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88: VMUpgradeHelper	1788	676	5	112	2010-08-11 06:06:38 UTC+0000
.. 0xff1ecd0: csrss.exe	608	544	10	410	2010-08-11 06:06:23 UTC+0000
0xff3865d0: explorer.exe	1724	1708	13	326	2010-08-11 06:09:29 UTC+0000
. 0xff374980: VMwareUser.exe	452	1724	8	207	2010-08-11 06:09:32 UTC+0000
. 0xff3667e8: VMwareTray.exe	432	1724	1	60	2010-08-11 06:09:31 UTC+0000

## Apartado d

Indique la/s direcciones IPs de la/s máquina/s remotas con las cuales existían conexiones abiertas.

Para ello utilizamos la orden **connscan** (ya que el tipo de perfil del sistema utilizado no dispone de netscan). Se observa que la dirección IP con la que existía conexión es la **193.104.41.75**.

```
PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\windowsRAM.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
```

Offset(P)	Local Address	Remote Address	Pid
0x02214988	172.16.176.143:1054	193.104.41.75:80	856
0x06015ab0	0.0.0.0:1056	193.104.41.75:80	856

## Apartado f

¿Qué PID/s tenían el/los proceso/s que había establecido dichas conexiones?

Basándonos en la captura del apartado anterior, el PID del proceso era el 856.

## Apartado l

Obtenga la firma hash de el/los fichero/s donde ha almacenado el volcado de/los proceso/s. Utilice para ello HashMyFiles que puede encontrar en la subcarpeta Nirsoft del CD de Caine.

En primer lugar, volcamos los procesos indicados. Gracias al comando **memdump** la opción **-p** (para indicar que proceso), **856** (PID del proceso) y **--dump-dir=./** para indicar que los vuelque en la propia ruta en la que nos encontramos.

```
PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\windowsRAM.vmem --profile=WinXPSP2x86 memdump -p 856 --dump-dir=./
Volatility Foundation Volatility Framework 2.6
*****
Writing svchost.exe [ 856] to 856.dmp
PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone>
```

Ahora con ayuda de la herramienta HashMyFiles de Nirsoft, obtenemos los diferentes tipos de hashes de dicho volcado. Por ejemplo, 75220fcf84669aa6e3098605833d0c1fd4dc3f82.

HashMyFiles			
File Edit View Options Help			
Filename	Full Path	MD5	SHA1
856.dmp	C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\...	f39a96816d9fa30b69d1c809f671c052	75220fcf84669aa6e3098605833d0c1fd4dc3f82

## Apartado m

Compruebe en la página Web de VirusTotal (<https://www.virustotal.com/gui/home/search>) si se reconoce la firma hash del/los fichero/s volcados como software malicioso.

Efectivamente, como se puede ver a continuación, lo reconoce como malware.

3ae9ea250966b3a061ce2d5e001f338e811288dc64a52f01238ae7bba8e3a15f

2 / 56

2 security vendors and no sandboxes flagged this file as malicious

3ae9ea250966b3a061ce2d5e001f338e811288dc64a52f01238ae7bba8e3a15f

856.dmp

Size: 60.87 MB

Last Analysis Date: 19 hours ago

Community Score: 2

DETECTION DETAILS COMMUNITY 2

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Avast	Sf:Crypt-BT [Trj]	AVG	Sf:Crypt-BT [Trj]
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Baidu (on cloud)	Undetected	Baidu	Undetected

Do you want to automate checks?

## Apartado q

Compruebe si el Firewall está deshabilitado ya que o bien lo tenía deshabilitado el usuario o bien fue deshabilitado por un software malicioso. Para ello compruebe el valor de la clave de registro "ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile". ¿Estaba el Firewall de Windows deshabilitado?

Se ejecuta el comando **printkey** con la opción **-K** para especificar la clave de registro. Se puede observar en la siguiente imagen, como el Firewall estaba desactivado.

```

PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\windowsRAM.vmem --profile=WinXPSP2x86 printkey -K ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: StandardProfile (S)
Last updated: 2010-08-15 19:17:24 UTC+0000

Subkeys:
(S) AuthorizedApplications

Values:
REG_DWORD EnableFirewall : (S) 0
PS C:\Users\carlo\Documents\Uni\IFA\Practicas\DatosDiversos\volatility_2.6_win64_standalone>

```

## Ejercicio 34

En este ejercicio vamos a tratar de obtener los metadatos de las fotografías existentes en los ficheros imagenXX.jpg resultado de descomprimir el fichero imagenesP5.zip (Recursos Prácticas->Práctica 5). Para cada una de dichas imágenes trate de obtener la siguiente información:

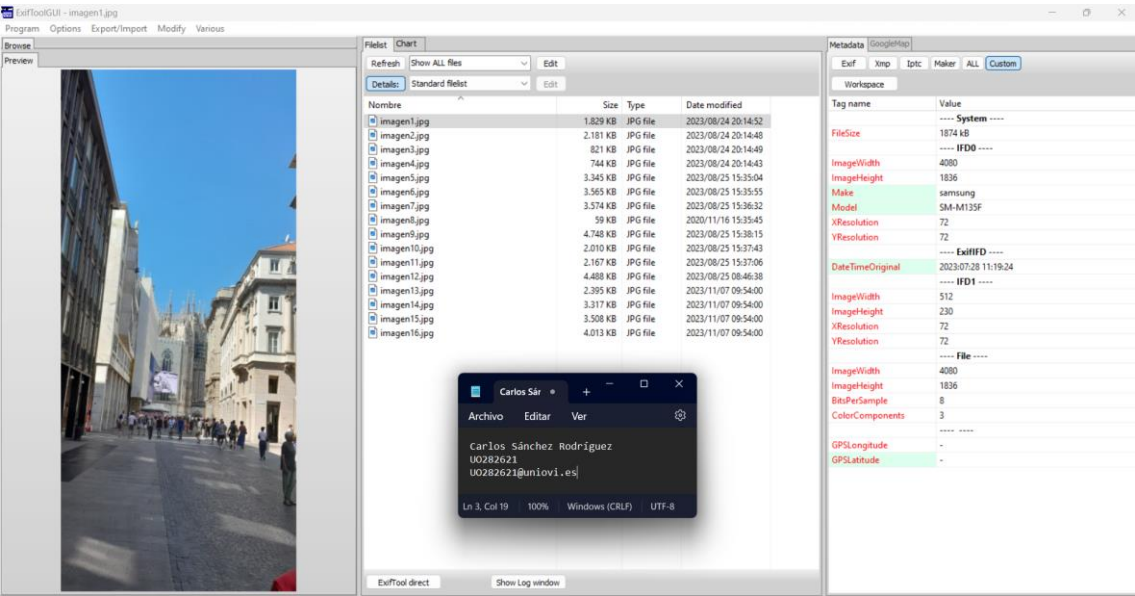
- Fecha en la que fue tomada la imagen.
- Ubicación. En caso de que dicha información no esté presente en los metadatos, trate de averiguarla a través de la búsqueda inversa de imágenes.
- Marca de la cámara.
- Modelo de la cámara.
- Modelo del teléfono en caso de haberse realizado con un Smartphone.
- Año de lanzamiento del teléfono.
- Características de la imagen:
  - Dimensión (ancho x alto) de la imagen en pixeles.
  - Resolución.
  - Bits de color por píxel.
- Tamaño del archivo.

Para obtener los metadatos EXIF de dichas imágenes puede utilizar bien la herramienta EXIFToolGUI o bien desde la página <http://metapicz.com/>.

	Imagen 1	Imagen 4	Imagen 6	Imagen 16
Fecha en la que fue tomada	2023-07-28 11:19:24+02:00	2023-08-02 16:10:08+02:00	2023-07-29 12:43:20+02:00	2023-07-13 18:36:13+02:00
Ubicación	Milán	Trastevere	Pisa	Luxemburgo
Marca de la cámara	Samsung	Samsung	Samsung	Samsung
Modelo de la cámara	SM-M135F	SM-M135F	SM-M135F	SM-A505FN
Modelo del teléfono si es el caso	Galaxy M13	Galaxy M13	Galaxy M13	Galaxy A50
Año de lanzamiento del teléfono	2022	2022	2022	2019
Dimensión (AnchoxAlto)	4080x1836	2560x1152	4080x3060	4032x3024

Resolución	72x72	72x72	72x72	72x72
Bits de color por píxel	24	24	24	24
Tamaño del archivo (kB)	1874	762	3700	4100

Para la obtención de la información se usa ExifTool, donde tras navegar por el apartado all de la pestaña Metadata, se ha incluido información al apartado Custom, con el fin de que toda la requerida entrase en una única captura de pantalla. Se muestra una captura para únicamente una de las fotografías, pues el procedimiento es el mismo para las demás.



Además, para averiguar la ubicación se ha hecho una búsqueda operativa a través de Google, contrastando la ubicación de fotografías similares. Por otra parte, el modelo de teléfono móvil y año de lanzamiento se ha hecho uso de la página Web <https://www.movilcelular.es/> como se muestra a continuación:

Características del modelo	
	Galaxy A50 (SM-A505FN/DS 128GB)
Cambiar modelo	SM-A505FN/DS 128GB
Modelo	Galaxy A50 (SM-A505FN/DS 128GB)
Otros nombres del modelo	Galaxy A50 SM-A505FN/Dual-Sim (128GB + 4GB RAM) NFC
Región o país donde se vende	(Europa)
Marca	Samsung
Fecha lanzamiento	15/3/2019
Grosor / Espesor	7,7 milímetros
Dimensiones (anchura x altura)	74,7 x 158,5 milímetros
Peso	166 gramos
Construcción, materiales	Cuerpo de plástico, pantalla de cristal
Protección frente al agua y otros	No compatible

## Ejercicio 35

En este ejercicio vamos a tratar de obtener los metadatos existentes en los ficheros resultado de descomprimir el archivo ficherosP5.zip (Recursos Prácticas->Práctica 5). Para obtener dichos metadatos utilice la página información que le proporcionará la página Web <https://www.metadata2go.com/>. Para cada uno de los ficheros indicados, trate de obtener la siguiente información:

- Aplicación con la que se creó el archivo.
- Versión de la aplicación con la que se creó el fichero.
- Autor.
- Empresa/organización donde se crea el documento.
- Fecha/hora de creación.
- Fecha/hora modificación.
- Fecha/hora modificación metadatos.
- Número de páginas.
- Tamaño del archivo.

	Fichero2.pdf	Fichero4.xlsx	Fichero7.doc	Fichero9.pptx
<b>Aplicación con la que se creó el archivo</b>	Microsoft Word	Microsoft Excel Online	Microsoft Office Word	Microsoft Office PowerPoint
<b>Versión de la aplicación con la que se creó el fichero</b>	Microsoft 365	16.03	16	16
<b>Autor</b>	Irene Cid Rico	Alberto Núñez	X	Joaquín Entrialgo Castaño
<b>Empresa/organización donde se crea el documento</b>	Desconocido	Desconocido	Desconocido	Desconocido
<b>Fecha/hora de creación</b>	2023-05-30 16:42:47 +02:00	2022-12-11 09:20:45 UTC	2021-07-21 12:32:00	2021-04-21 16:31:20 UTC
<b>Fecha/hora modificación</b>	2023-05-30 16:42:47+02:00	2023-11-14 10:38:22 UTC	2023-01-12 10:16:00	2023-01-10 07:37:28 UTC
<b>Fecha/hora modificación metadatos</b>	Desconocido	Desconocido	Desconocido	Desconocido
<b>Número de páginas</b>	5	3 hojas de calculo	2	1
<b>Tamaño del archivo (kB)</b>	478	22	115	4400

Para la obtención de la información arriba detallada, se ha usado la página Web <https://www.metadata2go.com/>. A continuación, se muestra una demo para el archivo **fichero4.xlsx**. Para el resto se procedería de manera similar por lo que no se adjuntan capturas de estas.

file_name	fichero4.xlsx
file_size	22 kB
file_type	XLSX
file_type_extension	xlsx
mime_type	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
zip_required_version	20
zip_bit_flag	0x0006
zip_compression	Deflated
zip_modify_date	1980:01:01 00:00:00
zip_crc	0xb5119142
zip_compressed_size	453
zip_uncompressed_size	2132

Carlos Sá

ArchivoEditarVer

Carlos Sánchez Rodríguez  
U0282621  
U0282621@uniovi.es

Ln 3, Col 1100%Windows (CRLF)UTF-8

creator	Alberto Núñez
keywords	
description	
last_modified_by	MARCO ANTONIO GARCIA TAMARGO
revision_number	
create_date	2022:12:11 09:20:45Z
modify_date	2023:11:14 10:38:22Z
category	application
content_status	
application	Microsoft Excel Online
manager	
company	

Carlos Sá

ArchivoEditarVer

Carlos Sánchez Rodríguez  
U0282621  
U0282621@uniovi.es

Ln 3, Col 1100%Windows (CRLF)UTF-8

app_version	16.03	Carlos Sánchez Rodríguez U0282621 U0282621@uniovi.es
-------------	-------	--

Ejercicio 43

Analice las cabeceras de correo que se encuentran en el fichero CabecerasMensajeSospechoso-3.txt el cual puedes descargar desde Recursos Prácticas->Práctica 5. Para analizar las cabeceras puedes utilizar la página tanto la página web <https://mha.azurewebsites.net/> como

<https://mxtoolbox.com/public/tools/emailheaders.aspx>. Averiguar las IPs (<https://centralops.net/co/>, <https://viewdns.info/>, <https://research.domaintools.com/>) de los servidores de correo que aparecen en las cabeceras por los cuales ha pasado el mensaje y comprueba si se trata de IPs de sitios calificados como maliciosos (<https://www.abuseipdb.com>). Para averiguar si la dirección del remitente del mensaje ha sido comprometida utilice el siguiente URL <https://Haveibeenpwned.com>. En base a su investigación, responda a las siguientes preguntas.

## Apartado a

¿Desde qué dirección IP se envió el mensaje?

Utilizando la página web <https://mha.azurewebsites.net/>, la dirección IP desde la que se envió el mensaje es **94.177.224.44** que es la que se corresponde con el primer salto.

Hops	Submitting host	Receiving host	Time	Delay	Type
1	powercollect.com (server8.atimoproducto.com.br <b>94.177.224.44</b> )	mx02.puc.rediris.es	6/25/2019 6:02:53 AM		ESMTP
2	mx02.puc.rediris.es (130.206.19.178)	edge.uniovi.es (156.35.11.136)	6/25/2019 6:02:54 AM	1 second	Microsoft SMTP Server
3	Front1.idem.uniovi.es (172.22.11.144)	NMail01.idem.uniovi.es (172.22.11.131)	6/25/2019 6:02:55 AM	1 second	Microsoft SMTP Server (TLS)
4	NMail01.idem.uniovi.es (172.22.11.131)	NMail02.idem.uniovi.es (172.22.11.132)	6/25/2019 6:02:55 AM	0 seconds	Microsoft SMTP Server (TLS)
5	NMail02.idem.uniovi.es (172.22.11.132)		6/25/2019 6:02:56 AM	1 second	Microsoft SMTP Server (TLS)
6	micorreouniovi.es (156.35.11.135)		6/25/2019 6:03:04 AM	8 seconds	Microsoft SMTP Server (version=TLS1_0, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
7	DBSEURO1FT021.eap-EUR01.prod.pro		6/25/2019 6:03:05 AM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

## Apartado b

¿Qué ISP gestiona el rango de IPs en el que está incluida dicha IP?

Haciendo uso esta vez de la página web <https://whois.domaintools.com/>, obtenemos que el ISP es **Germany Frankfurt Am Main Cloud Services Dc05**.

[Home](#) > [Whois Lookup](#) > 94.177.224.44

### IP Information for 94.177.224.44

#### Quick Stats

IP Location	Germany Frankfurt Am Main Cloud Services Dc05
ASN	AS200185 XANDMAIL-ASN Aruba SAS, FR (registered Sep 13, 2013)
Resolve Host	host44-224-177-94.static.arubacloud.de
Whois Server	whois.ripe.net
IP Address	94.177.224.44

% Abuse contact for '94.177.224.0 - 94.177.224.255'

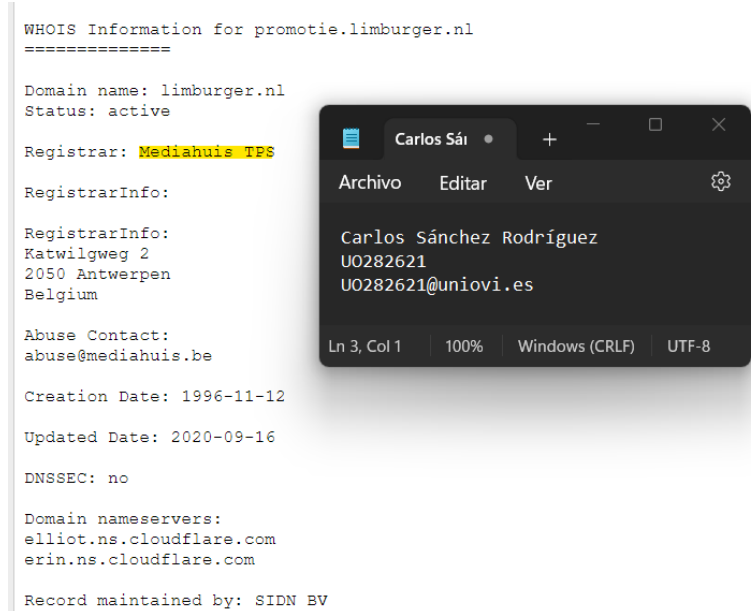
**DomainTools Iris**  
The gold-standard internet intelligence platform  
[Learn More](#)

Carlos Sánchez Rodríguez	U0282621	U0282621@uniovi.es
--------------------------	----------	--------------------

## Apartado f

¿A qué organización está asociada la IP del dominio desde la cual se remite en primera instancia el correo investigado?

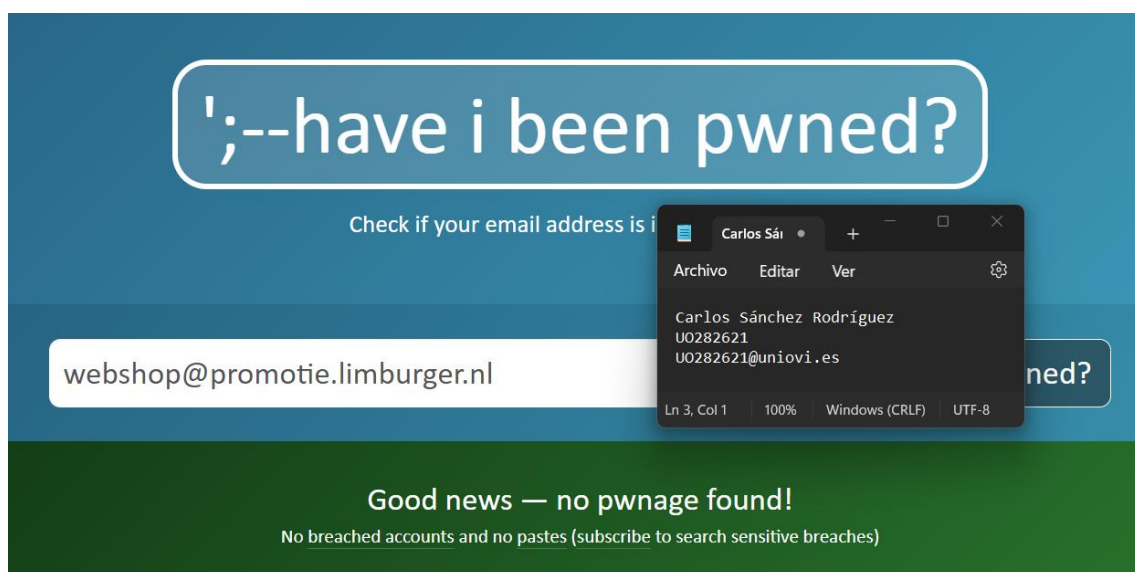
La IP del dominio promotie.limburger.nl, está asociada la organización **Mediahuis TPS**.



## Apartado i

¿Puede haber sido comprometida la dirección de correo que figura como remitente del mensaje?

En principio no hay evidencias de que haya sido comprometida.





Apartado q

En vista de los retardos en la transmisión del mensaje entre los diferentes MTAs por los que ha pasado, ¿se puede decir que ha sido manipulado?

En vista de los retardos en la transmisión y puesto que el máximo retraso entre saltos es de únicamente 8 segundos, aparentemente no parece haber sido manipulado, aunque no se debería de descartar al cien por cien.

Hop#	Submitting host	Receiving host	Time	Delay	
1	powercollecte.com (server8.otimoproduto.com.br [94.177.224.44])	mx02.puc.rediris.es	6/25/2019 6:02:53 AM		ESMTP
2	mx02.puc.rediris.es (130.206.19.178)	edge.uniovi.es (156.35.11.136)	6/25/2019 6:02:54 AM	1 second	Microsoft SMTP Server
3	Front1.ident.uniovi.es (172.22.11.144)	NMail01.ident.uniovi.es (172.22.11.131)	6/25/2019 6:02:55 AM	1 second	
4	NMail01.ident.uniovi.es (172.22.11.131)	NMail02.ident.uniovi.es (172.22.11.132)	6/25/2019 6:02:55 AM	0 seconds	
5	NMail02.ident.uniovi.es (172.22.11.132)	edge.uniovi.es (172.22.11.145)	6/25/2019 6:02:56 AM	1 second	
6	micoreo.uniovi.es (156.35.11.135)	DB5EURO1FT021.mail.protection.outlook.com (10.152.4.245)	6/25/2019 6:03:04 AM	8 seconds	
7	DB5EURO1FT021.eop-EURO1.prod.protection.outlook.com (2a01:111f400:7e02:202)	DB6PR0802CA0039.outlook.office365.com (2603:10a6:4a3:25)	6/25/2019 6:03:05 AM	1 second	
8	DB6PR0802CA0039.eurprd08.prod.outlook.com (2603:10a6:4a3:25)	AM4PR08MB2642.eurprd08.prod.outlook.com (2603:10a6:205:e:19)	6/25/2019 6:03:05 AM	0 seconds	
9	AM4PR08MB2642.eurprd08.prod.outlook.com (2603:10a6:800:7e:23)	V11PR08MB2654.eurprd08.prod.outlook.com	6/25/2019 6:03:06 AM	1 second	HTTPS

Ejercicio 46

Con el mismo contexto de inicio que indica el ejercicio anterior analizar el fichero p5\_tr\_cell\_bis.xlsx y responder a las siguientes preguntas.

Se utilizará la siguiente captura para la resolución del ejercicio:

	A	B	C	D	E	F	G	H	I	J	K	L
1	imsi	imei	icc	radio	mcc	net	area	cell	lon	lat	date	local time
2	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	361	19861051 -0.671539	38.601837	22/07/2019	20:16:03
3	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	361	19861051 -0.671539	38.601811	22/07/2019	23:45:01
4	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	361	19861849 -0.617499	38.526061	23/07/2019	3:41:10
5	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	361	19868528 -0.651234	38.570153	25/07/2019	18:33:17
6	214072222222222	356513043210360	8934072345678900000	UMTS		214	7	404	13390007 -2.621941	36.811991	15/07/2019	9:46:23
7	214072222222222	356513043210360	8934072345678900000	UMTS		214	7	404	13390835 -2.442398	36.909943	16/07/2019	21:23:59
8	214072222222222	356513043210360	8934072345678900000	UMTS		214	7	404	13389450 -2.465131	36.83991	17/07/2019	6:00:09
9	214072222222222	356513043210360	8934072345678900000	UMTS		214	7	404	13390006 -2.616806	36.806717	18/07/2019	16:33:14
10	214072222222222	356513043210360	8934072345678900000	UMTS		214	7	404	13389876 -2.441742	36.871835	19/07/2019	20:41:02
11	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	762	26703020 1.5923309326172	39.01725769043	24/07/2019	8:00:42
12	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	762	26695333 1.422654	38.906571	24/07/2019	13:48:16
13	214072222222222	862551036005121	8934071234567890000	UMTS		214	7	762	26702314 1.42183	38.90601	24/07/2019	20:01:53
14	214072222222222	356513043222324	8934072345678900000	UMTS		214	7	860	52955649 2.0221710205078	41.563339233398	24/07/2019	9:15:15
15	214072222222222	356513043222324	8934072345678900000	UMTS		214	7	860	79176280 2.0977020263672	41.417770385742	24/07/2019	11:15:23

Apartado m

Indicar, a la vista de los registros, si se trata de un servicio SIM o multi SIM. Razónese la respuesta.

Si que se trata de un servicio multi SIM puesto que como observamos en la captura anterior en verde, para un solo IMSI existen dos ICC.

Apartado n

Indicar las ternas IMSI/IMEI/ICC que resultan distinguibles

Tal y como se muestra en la anterior captura en amarillo, resultan distinguibles las tres ternas (IMSI, IMEI, ICC):

(2140722222222, 862551036005121, 8934071234567890000)

(2140722222222, 356513043210360, 8934072345678900000)

(2140722222222, 356513043222324, 8934072345678900000)

## Apartado o

Indicar si en algún momento se utilizaron redes 4G

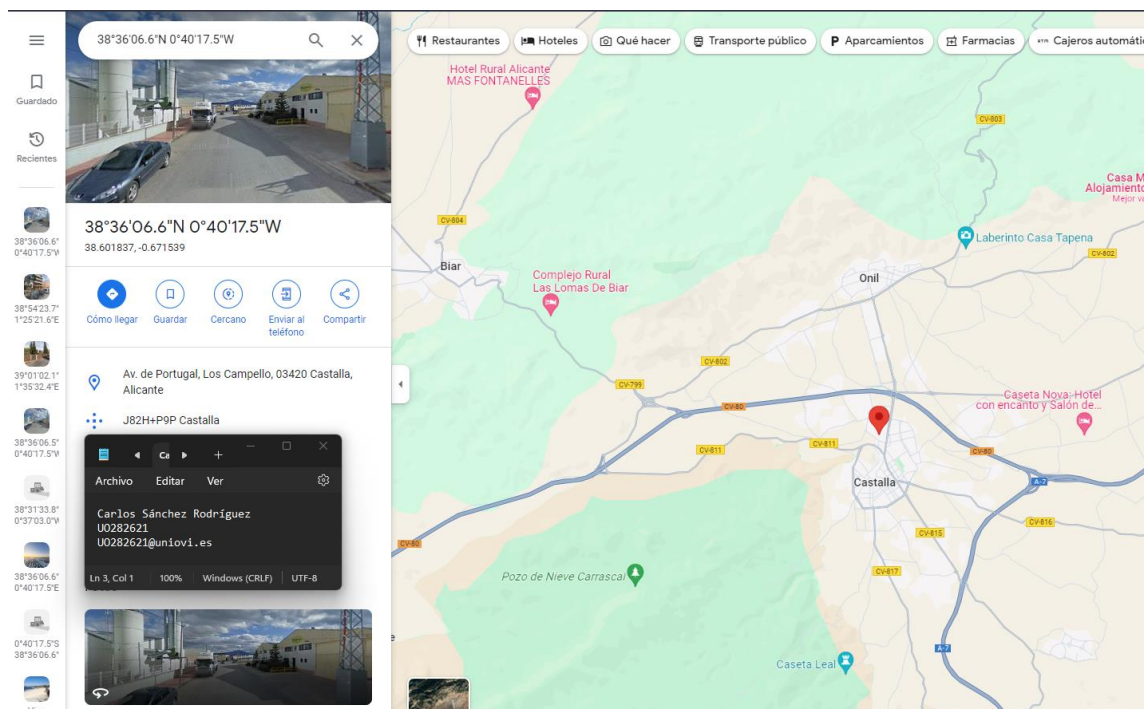
En ningún momento se usa la red 4G. Esto se puede comprobar observando la columna **radio** en la que claramente se ve que únicamente utiliza **UMTS** (red 3G).

## Apartado s

Indicar el desplazamiento geográfico, en términos provinciales y secuencia temporal creciente, que corresponde a todos los registros incluidos en el fichero para el IMEI 862551036005121.

Para ello hacemos uso de las columnas **lon** y **lat**, y mediante búsqueda operativa como puede ser el uso de Google Maps, podemos observar que se ha estado moviendo por Alicante, después por Ibiza y para terminar de vuelta a Alicante.

Se muestra a continuación un ejemplo de como se ha hecho la búsqueda para la primera provincia.



## Práctica 5b

### Ejercicio 7

Los ataques de inyección SQL permiten que los hackers maliciosos escriban sentencias SQL en un sitio web y reciban una respuesta de la base de datos. Esto permite a los atacantes manipular los datos actuales de la base de datos, suplantar identidades y modificar o destruir información.

Objetivos de la práctica:

En este ejercicio examinaremos un archivo PCAP para que veamos un ataque anterior a una base de datos SQL.

### Apartado d

¿A cuánto tiempo (en segundos) corresponde la captura?

La captura corresponde a 441 segundos. Tal y como nos muestra WireShark en el apartado estadísticas, propiedades del archivo, son 7 minutos 21 segundos.

The screenshot shows the Wireshark interface with the 'Archivo' (File) pane open. The file details show the file name 'C:\Users\carlo\Documents\Univ\FA\Practicas\Datos nuevos\SQL\_Lab.pcap', size '25 kB', and other metadata. The 'Intervalo' (Interval) section shows the capture time from '2017-02-06 15:15:27' to '2017-02-06 15:22:49', with a duration of '00:07:21' highlighted in red. The 'Estadísticas' (Statistics) pane shows the following data:

Medida	Capturado	Mostrado	Marcado
Paquetes	30	30 (100.0%)	—
Espacio de tiempo, s	441.807	441.807	—
Promedio pps	0.1	0.1	—
Promedio de tamaño de paquete, B	835	835	—
Bytes	25049	25049 (100.0%)	0
Promedio de bytes/s	56	56	—
Promedio de bits/s	453	453	—

### Apartado e

¿Cuántos paquetes fueron capturados?

Esta información se puede ver tanto en el panel principal de WireShark, o siguiendo con el menú propiedades del archivo como se muestra en la captura anterior. De ambas formas se puede observar que han sido 30 los paquetes capturados.

## Apartado f

En función de la información que proporcionan los paquetes capturados, ¿cuáles son las dos direcciones involucradas en este ataque de inyección SQL?

Como se muestra a continuación, las dos direcciones involucradas en el ataque son la 10.0.2.4 y la 10.0.2.15

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 M
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 L
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (applicat
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=303
8	0.014383	10.0.2.4	10.0.2.15	HTTP		
9	0.015485	10.0.2.15	10.0.2.4	HTTP		
10	0.015485	10.0.2.4	10.0.2.15	TCP		
11	0.068625	10.0.2.4	10.0.2.15	HTTP		
12	0.070400	10.0.2.15	10.0.2.4	HTTP		
13	174.254430	10.0.2.4	10.0.2.15	HTTP		
14	174.254581	10.0.2.15	10.0.2.4	TCP		
15	174.257989	10.0.2.15	10.0.2.4	HTTP		
16	220.490531	10.0.2.4	10.0.2.15	HTTP		
17	220.490637	10.0.2.15	10.0.2.4	TCP		
18	220.493085	10.0.2.15	10.0.2.4	HTTP		
19	277.727722	10.0.2.4	10.0.2.15	HTTP		
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 L
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=236 L
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dvwa/vulnerabilities/sqli/?id=1%27+
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Win=236 L
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?id=1%27+
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 L
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

## Apartado j

Indique cuántas cuentas de usuario se han descubierto.

Se han descubierto un total de 5 cuentas.

HTML output from a web application showing a list of discovered users:

```

<input type="text" size="15" name="id">
<input type="submit" name="Submit" value="Submit">
</p>
</form>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: ad
min</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre><pre>
ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 uni
on select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select da
tabase(), user()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select database(), user()
#<br />First name: dvwa<br />Surname: root@localhost</pre>
</div>
<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/se">http://www.securiteam.com/se
</li>
<li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html">a</li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection">a</li>
<li><a href="http://ferruh.mavituna.com/le">http://ferruh.mavituna.com/le
</li>
<li><a href="http://pentestmonkey.net/ch">a</li>


```

Paquete 21.1 cliente pkt(s), 1 server pkt(s), 1 turn(s). Clic para seleccionar.

Conversación completa (6532 bytes)    Mostrar datos como ASCII    Secuencia 3

Buscar:    Buscar siguiente

Filtrar secuencia    Imprimir    Guardar como...    Atrás    Cerrar    Ayuda

Apartado s

Utilice un sitio web como <https://crackstation.net/> para copiar el hash de la contraseña en el decodificador de hashes de contraseñas y comenzar a decodificarlo. ¿Cuál es la contraseña en texto plano?

La contraseña en texto plano es **charley**.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

8d3533d75ae2c3966d7e0d4fcc69216b

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Carlos Sán

Archivo Editar Ver

Carlos Sánchez Rodríguez  
U0282621  
U0282621@uniovi.es

Ln 3, Col 1 100% Windows (CRLF) UTF-8