# Informática Forense y Auditoría

## Grado en Ingeniería Informática del Software

### Escuela de Ingeniería Informática de Oviedo

**Práctica 4: Ejercicios de Práctica Forense III**

## Introducción

En muchas investigaciones forenses aparecen los móviles como elementos de evidencia. Este es un campo de investigación en continua evolución a medida que lo hace la tecnología. Cada día surgen nuevos retos, así como aparecen nuevas herramientas. En la investigación forense de un dispositivo móvil, el primer paso suele ser la adquisición del dispositivo, la cual, puede ser física (completa) o lógica (solamente de los datos de usuario). La primera dificultad es que un móvil actual es como un ordenador. En un ordenador, para adquirir evidencias cuando está encendido, necesitamos ejecutar determinados programas que generan nuevos procesos y entradas en los logs del sistema. No podemos utilizar **write-blockers** en una adquisición en vivo de un ordenador, por tanto, tampoco lo podemos hacer en una adquisición de un Smartphone. Esto plantea el problema de añadir entradas en el sistema correspondientes al propio proceso de adquisición forense. Además, a esta dificultad se añade que no es lo mismo realizar la adquisición de un smartphone Android o de un smartphone IOS. Dentro de los Smartphone que comparten SO, puede haber diferencias en los procedimientos de adquisición de un fabricante a otro. El siguiente paso a la adquisición es el análisis de los datos obtenidos y su relación con el caso. Para ello se suele utilizar software forense para facilitar la tarea del investigador. La mayoría del software (Oxygen, MagnetEngine, etc.) que facilita la tarea del investigador forense suele ser de pago.

## Objetivos

- Utilizar Autopsy para examinar imágenes físicas de móviles con SO Android.
- Utilizar ALEAPP para realizar un triaje rápido de imágenes de dispositivos móviles con SO Android.
- Examinar algunos de los artefactos presentes en un móvil Android y saber cómo interpretarlos.

## Instrucciones comunes a todos los ejercicios

**Deberá justificar la realización de los siguientes ejercicios con capturas de pantalla donde quede patente que el ejercicio se realiza bajo la autoría del alumno, así como los comandos empleados en la resolución de los mismos y las explicaciones que considere oportunas.**

## Instrucciones comunes a todos los ejercicicios

Abra la utilidad Autopsy. Cree un nuevo caso desde el interfaz de Autopsy. Llame al nuevo caso de la siguiente manera: **P4-EjercicioXX_SmartPhone**, donde XX es el número del ejercicio que está realizando en este momento. En el número de caso ponga DDMMAAAA-XX donde DD es el día en el que realiza el ejercicio, MM es el número del mes actual y AAAA es el año actual, siendo XX el número del ejercicio que está realizando. Ponga su nombre y sus datos en la información del examinador (ponga en el correo su dirección de email de uniovi). Añada al caso la evidencia, correspondiente al ejercicio que está realizando, como **Imagen de disco o fichero VM**. Conteste a las preguntas que se le formulan en cada ejercicio justificándolas con capturas de pantalla.

1. Descarga del campus virtual (**Recursos Prácticas->Práctica 4**), el fichero **ChipoffLGK7.raw**. Este fichero se corresponde con una imagen física de un teléfono móvil **LG-K7**. 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 siguientes: **Recent Activity, File Type Identification, Picture Analyzer, Keyword Search** (seleccione la búsqueda de números de teléfono, direcciones IP, emails, URLs y números de tarjeta de crédito), **Email Parser, Extension Mistmatch Detector, PhotorecCarver y Android Analyzer**. Con todos esos módulos de ingestión activados, el proceso de búsqueda de artefactos por parte de Autopsy puede demorarse un buen rato. Responda a las siguientes cuestiones:

   a) ¿Cuántos registros tiene la libreta de direcciones (Contactos)?
   b) ¿Qué conocido cantante de rock tiene una entrada en la agenda el propietario del teléfono?
   c) ¿Qué dirección de correo está vinculada a dicha entrada?
   d) ¿Cuál es el número de teléfono de dicho artista?

e) ¿Cuántas llamadas salientes detecta Autopsy?
f) ¿A qué números corresponden?
g) ¿Cuántos ficheros tienen registrados METADATOS EXIF?
h) ¿Cuántos de ellos tienen registradas coordenadas de posicionamiento GPS?
i) ¿Dónde fueron tomadas ambas imágenes?
j) Puede traducir las coordenadas polares a coordenadas GPS utilizando el comando ExifTool (preinstalado en CAINE). Indique la dirección que obtiene a través de Google Maps utilizando dichas coordenadas.
k) ¿Con qué modelo de cámara fue tomada la imagen existente en el fichero IMG_20181109_085135.jpg ?.
l) ¿En qué fecha-hora local fue tomada la imagen existente en el fichero IMG_20181109_085135.jpg?
m) ¿En qué fecha-hora GMT fue creado el fichero IMG_20181109_085135.jpg?
n) ¿Son iguales todos los MAC times del fichero IMG_20181109_085135.jpg?
o) ¿De qué color es el móvil que aparece en la imagen IMG_20181109_085135.jpg?
p) ¿Qué resolución en pixeles (anchoxalto) tiene la imagen IMG_20181109_085135.jpg?
q) ¿Con qué velocidad de obturación fue tomada la imagen IMG_20181109_085135.jpg?
r) ¿Se utilizó flash al capturar la imagen IMG_20181109_085135.jpg?
s) Compruebe si hay algún fichero **.jpg** en la carpeta de Descargas (userdata/Media/0/Download), y en caso de haber alguno, extráigalo a la carpeta de Export del proyecto. Pegue a continuación el contenido de dicho fichero.
t) ¿Cuántos ficheros en la carpeta son de tipo PDF?
u) ¿Cuántos están borrados?
v) Indique el nombre del fichero PDF que no está borrado y su ubicación.
w) Exporte dicho fichero a la carpeta Export del proyecto y pegue a continuación su contenido.
x) Localice en cuál de los mensajes SMS se encuentra el código de verificación de Whatsapp y pegue a continuación el valor de dicho código.

y) ¿Fue leído el mensaje donde se encuentra el código de verificación de Whatsapp?
z) ¿En qué fecha-hora se recibió dicho mensaje?
aa) ¿Cuántas cadenas con la forma de direcciones de correo ha detectado el plugin de búsqueda de cadenas?
bb) ¿Cuántos ficheros gif han sido detectados?
cc) Haga una captura del contenido de uno cualquiera de ellos e indique su nombre y ubicación.
dd) A la vista de las entradas existentes en la subcarpeta userdata/data, enumere las redes sociales con que trabajaba el usuario.
ee) Extraiga el fichero que contiene la lista de apps instaladas y almacénelo en la carpeta de Export.
ff) Examine el fichero con un visor XML y pegue las líneas del mismo donde figuran los permisos que tiene la aplicación de **whatsapp** instalada.
gg) A la vista de la información proporcionada en el fichero packages.xml, ¿en qué ubicación se encuentra el fichero de instalación de whatsapp?.
hh) Localice el fichero accounts.db que se encuentra en la carpeta userdata/system/users/0. Almacene dicho fichero en la carpeta Export. Abra dicho fichero con DB Browser for SQLite (se encuentra instalado en CAINE). ¿Cuántas cuentas hay asociadas con el dispositivo?
ii) ¿Cuál es la cuenta de Google?
jj) Explore dicha tabla y observe además que existe una columna que contiene la password asociada a cada cuenta. El campo password contiene la versión hasheada de la contraseña. Prueba a intentar craquearlas utilizando un sitio web como https://crackstation.net/ para copiar el hash de cada contraseña en el decodificador de hashes de contraseñas y comenzar a decodificarla.

2. Android almacena de forma predeterminada los datos del usuario en la partición userdata en el directorio /data. Dentro del directorio data hay directorios que contienen nombres de paquetes. Y dentro de cada directorio de paquete suele haber una subcarpeta denominada databases donde se encuentran ficheros .db de SQLite. Suele ser interesante, desde un punto de vista forense, la información existente en las siguientes ubicaciones:

- /userdata/data/com.android.email/databases/EmailProvider.db
- /userdata/data/com.android.email/databases/EmailProviderBody.db
- /userdata/data/com.android.providers.calendar/databases/calendar.db
- /userdata/data/com.android.providers.contacts/databases/contacts2.db
- /userdata/data/com.android.providers.downloads/databases/downloads.db

- /userdata/data/com.android.providers.settings/databases/settings.db
- /userdata/data/com.android.providers.telephony/databases/mmssms.db
- /userdata/data/com.android.providers.telephony/app_parts
- /userdata/data/com.facebook.katana/databases
- /userdata/data/ com.facebook.orca/databases

a) Explore la carpeta userdata/system/usagestats. Bien en ella o en sus subcarpetas encontrará diversos ficheros. ¿De qué tipo son?
b) Exporte alguno de ellos a la carpeta Export del caso. Observe su contenido. En ellos encontrará entradas de log correspondientes a eventos ocurridos en el sistema con sus tiempos asociados (expresados en milisegundos desde el EPOCH) para lo cual puede utilizar el conversor que encontrará en la página https://currentmillis.com/.

3. Si está examinando una imagen de un teléfono Android para un caso criminal y está instalado Facebook, puede que esta sea una buena razón para examinar los datos asociados con la aplicación de Facebook. Suele haber dos app vinculadas a Facebook. El nombre del paquete[1] de la aplicación principal es **com.facebook.katana**, por lo que los datos asociados con esta aplicación se almacenarán en la partición de datos en el directorio userdata/data/com.facebook.katana. La segunda app es la aplicación de mensajería de Facebook y el nombre de su paquete suele ser **userdata/data/com.facebook.orca**.

   a) Haga una de captura de pantalla de la aplicación Autopsy donde se vea que ha localizado la ubicación de ambos paquetes.
   b) Si queremos obtener información sobre los contactos de Facebook tendremos que exportar la carpeta **userdata/data/com.facebook.katana/databases** a la carpeta Export del caso. Hágalo a través del interfaz de Autopsy.

      En dicha carpeta se encuentra el fichero **contacts_db2**. Abra la BD con **DB Browser for SQLite** (se encuentra disponible en CAINE). Observe las tablas que contiene. Abra la tabla contacts. Esta tabla tiene, entre otras, las siguientes columnas que hay que tener en consideración:

      - **first_name**: autoexplicativo.
      - **last_name**: autoexplicativo.

[1] Dependiendo de la versión de Facebook instalada en el dispositivo, los nombres de los paquetes pueden ser ligeramente diferentes.

- **display_name**:  autoexplicativo.
- **small_picture_url**: Una URL a una versión pequeña de la imagen de perfil del usuario.
- **big_picture_url**: Una URL para una versión grande de la imagen de perfil del usuario.
- **huge_picture_url**: Una URL a una versión muy grande de la imagen de perfil del usuario.
- **communication_rank**: Un número que representa la frecuencia con la que el usuario se comunica con ese contacto en particular. Este número se calcula utilizando alguna fórmula de Facebook. Las comunicaciones incluyen: mensajes, publicaciones, me gusta, comentarios, etc. Un 0 en esta columna significa que no hay comunicación. Cuanto mayor sea el número, más comunicación. Desde una perspectiva forense, este número es una forma de determinar con qué frecuencia el usuario interactúa con otro usuario.
- **is_messenger_user**: Un campo booleano. Verdadero indica que el usuario usa una aplicación de mensajería móvil (como la aplicación **com.facebook.orca** para Android).
- **data**: Una larga cadena que describe la información del perfil del usuario.
- **bday_day**: Cumpleaños.
- **bday_month**: Cumpleaños.

c) ¿Cuántos contactos aparecen en la tabla?
d) Haga una captura de pantalla del contenido de la misma.

El campo data de la tabla anterior suele ser un campo que arroja una gran cantidad de información desde el punto de vista forense. Un ejemplo del contenido del mismo sería el siguiente:

**{"contactId":"Y2<redactado>k2","profileFbid":"62<redactado>09","graphApiWriteId":"contact_20<redactado>96","name":{"firstName":"<redactado>","lastName":"<redactado>","displayName":"<redactado>"},"phoneticName":{},"smallPictureUrl":"https://profile-a.<redactado>a40","bigPictureUrl":"https://profile-a.<redactado>26e","hugePictureUrl":"https://profile-a.<redactado>eea","smallPictureSize":160,"bigPictureSize":320,"hugePictureSize":466,"communicationRank":0.03445798,"withTaggingRank":0.3325288,"phones":[{"id":"62978<redactado>259","label":"Mobile","displayNumber":"(**

**6xx) 9xx-xxxx","universalNumber":"+16xx9xxxxxx","isVerified":true}],"nameSearchTokens":["<redactado>","<redactado>"],"canMessage":true,"isMobilePushable":"YES","isMessengerUser":true,"messengerInstallTime":1417438579000,"isMemorialized":false,"isOnViewerContactList":true,"addedTime":1419017431000,"friendshipStatus":"ARE_FRIENDS","subscribeStatus":"IS_SUBSCRIBED","contactType":"USER","timelineCoverPhoto":{"focus":{"x":0.5,"y":0.39435146443515},"photo":{"image_midres":{"uri":"https://fbcdn-sphotos-h-a.<redactado>201","width":320,"height":179},"image_lowres":{"uri":"https://fbcdn-sphotos-h-a.<redactado>817","width":500,"height":281}}},"nameEntries":[],"birthdayDay":"<redactado>","birthdayMonth":"<redactado>","cityName":"<redactado>, Ohio","isPartial":false}**

e) Este conjunto de datos puede parecer ininteligible, pero tiene estructura. En realidad, está en lenguaje JSON. Abra la URL de JSON Editor Online (https://jsoneditoronline.org/) y pegue el ejemplo anterior en el panel izquierdo. Haga una captura de pantalla de lo que aparece en el panel derecho y examínela con detenimiento.

f) ¿En qué estado se encuentra la ciudad del contacto en el campo de datos de ejemplo?

g) ¿Contiene este campo de datos números de teléfono?

4. Facebook tiene la capacidad de enviar mensajes privados a otros usuarios. Estos mensajes se almacenan en los servidores de Facebook y también se pueden almacenar en su teléfono. El archivo **userdata/data/com.facebook.orca/databases/threads_db2** almacena mensajes que el usuario ha enviado y recibido. Una de las tablas más interesantes es la tabla **messages**. Observe la tabla **messages**. Los principales campos de interés en dicha tabla son:

   - **text**: el texto del mensaje.
   - **sender**: El usuario que envió el mensaje. Puede usar esta columna para saber si el mensaje fue enviado o recibido.
   - **timestamp_ms**: la fecha y hora del mensaje expresada en milisegundos desde el Unix EPOCH.
   - **attachments**: cualquier archivo adjunto con el mensaje. El archivo adjunto puede incluir un enlace a una foto.

- **coordinates**: si el usuario envió el mensaje usando un dispositivo móvil y permitió el acceso a la ubicación del dispositivo cuando se envió el mensaje.
- **source**: si el mensaje proviene de una computadora o dispositivo o de cualquier otra fuente.

  El contenido del campo **sender** puede ser como el siguiente:

  **{"email":"2077777786@facebook.com","user_key":"FACEBOOK:2077777786","name":"Pepito Perez"}**

  Este campo tiene un formato similar al campo de datos en la tabla de contactos comentada anteriormente. Puede ver un campo para correo electrónico, que es básicamente el ID de usuario numérico @facebook.com. Si intentara enviar un correo electrónico a esta dirección desde su correo electrónico ese mensaje sería reenviado a la dirección de correo electrónico donde el usuario Pepito Perez recibe notificaciones de Facebook.

  El campo coordenadas almacena la latitud y longitud según lo informado por el dispositivo en el momento en que se envió el mensaje. Puede determinar dónde estaba una persona, o dónde estaba su dispositivo cuando se envió un mensaje. Esa puede ser información bastante útil porque permite determinar dónde estaba el dispositivo cuando se envió un mensaje en un momento específico. **Si puedes estar seguro de que el usuario y no otra persona estaba sosteniendo el dispositivo y enviando el mensaje, entonces sabemos dónde estaba la persona en un momento específico al enviar un mensaje**. Hay que tener en cuenta que en Android es muy fácil falsificar la ubicación (buscar en Google Play Fake GPS GO Location Spoofer Free).

5. La aplicación **com.facebook.orca** es solo una aplicación de mensajería. Básicamente también hay un archivo **threads_db2** dentro del directorio de bases de datos al igual que en **com.facebook.katana**. Estos archivos de base de datos almacenan básicamente la misma información. Lo importante es saber que si la aplicación **com.facebook.orca** está presente, el usuario está usando Facebook Messenger para Android.

   a) Extraiga el archivo **userdata/data/com.facebook.orca/databases/threads_db2** y almacénelo en la carpeta Export del caso. Abra el archivo con DB Browser for SQLite (está instalado en CAINE). Observe las tablas que contiene. Abra la tabla messages. Indique quién envió el mensaje de _id=21.
   b) ¿En qué momento se envió dicho mensaje? **Muestre la hora GMT**.

6. En las subcarpetas de **userdata/data/com.facebook.katana/cache** y de **userdata/data/com.facebook.orca/cache/image** se almacena también una gran cantidad de información en forma de ficheros. Algunos de ellos son ficheros con extensión **.cnt** que contienen imágenes. Estas son imágenes que en algún momento se guardaron en el dispositivo. En otras palabras, estas son imágenes públicas que un usuario publicó en línea. Dependiendo del caso pueden ser interesantes, con lo cual es necesario estudiarlas.

   a) En la carpeta **userdata/data/com.facebook.orca/cache/image/v2.ols100.1/39** extraiga el archivo **9i9MBNqF9i_eJF3289gU9c35YZE.cnt** a la carpeta Export del caso. Indique de qué tipo es el archivo.
   b) ¿Cuál fue la fecha de último acceso al archivo?
   c) ¿Qué imagen contiene dicho archivo?
   d) ¿Contiene el fichero que contiene la imagen metadatos de dónde fue tomada?

   Estos son algunos (no todos) los artefactos interesantes en una investigación forense de Facebook. Quedan otros como los posts publicados, las imágenes y los videos, etc. El dispositivo almacena muchos datos, pero Facebook es, en última instancia, un servicio en la nube, lo que significa que todos los datos de Facebook se almacenan en un servidor remoto. Si está en una investigación forense y necesita datos asociados con un usuario de los servidores de Facebook y tiene una orden judicial que permite el acceso a estos registros, hay una vía para obtener el acceso a dicha información (https://www.facebook.com/safety/groups/law/guidelines/).

7. ALEAPP (Android Logs Events And Protobuf Parser) es un conjunto de scripts python desarrollados en un esfuerzo colaborativo por la comunidad DFIR (Digital Forensics Incident Response) liderado por Alexis Brignoni, el cual trabaja como agente del FBI en Orlando (Florida). Podemos descargar e instalar ALEAPP desde GitHub (https://github.com/abrignoni/ALEAPP).

   a) Descarga el ejecutable ALEAPP para Windows o bien instala ALEAPP en CAINE.
   b) Extrae de **ChipoffLGK7.raw** (la imagen física del teléfono LG-K7) el volumen 42 correspondiente a la partición de **userdata** (datos de usuario). Para ello utiliza el comando dd teniendo en cuenta el sector de comienzo de la partición y el número de sectores que ocupa. Almacena la partición extraída de la imagen con el nombre **userdataLGK7.raw**.
   c) En CAINE, monta en solo lectura, sin modificar los tiempos de acceso a los inodos y en modo bucle la imagen (fichero **userdataLGK7.raw**) de la partición userdata extraída en el apartado anterior. (NOTA: Para realizar este ejercicio, repasa los

conceptos del montaje de imágenes de particiones en modo bucle vistos en la Práctica 2).

d) Ejecuta ALEAPP sobre el directorio en el que has montado la partición y responde a las siguientes cuestiones.
e) ¿Cuántos eventos tiene registrados el calendario?
f) ¿En qué fecha está registrado el evento "**Hendrix summer of love documentary**"?
g) ¿En qué zona horaria ocurre el evento identificado en el apartado anterior?
h) ¿Bajo qué identidad se registró el evento referido en el apartado f)?
i) ¿Tiene asociada una alarma el evento identificado en el apartado f)?
j) ¿En qué fecha/hora fue registrado el evento más antiguo del calendario?
k) ¿Qué título tiene el evento identificado en el apartado anterior?
l) ¿En qué fecha/hora fue registrado el evento más moderno del calendario?
m) ¿Cuántos contactos (entradas) tiene la libreta de direcciones (Contactos)?
n) ¿Cuántas entradas en la libreta de direcciones corresponden a contactos no duplicados?
o) ¿Cuántas de las entradas de la libreta de contactos son entradas que contienen información sobre el correo electrónico de un contacto?
p) ¿Cuál es la dirección de correo electrónico de Stevie Ray Vaughn?
q) ¿Cuántas llamadas entrantes se registraron en el teléfono?
r) ¿De qué número/s provenían?
s) ¿En qué fecha/hora se recibió la primera (más antigua) de dichas llamadas entrantes?
t) ¿Cuántos ficheros se descargaron al teléfono?
u) ¿En qué fecha/hora se descargó el fichero **chare.wav**?
v) ¿Cuántas búsquedas se realizaron desde Google Maps?
w) Indique las coordenadas del punto de origen de la primera de las búsquedas realizadas con Google Maps.
x) ¿A qué dirección corresponden las coordenadas identificadas en el apartado anterior?
y) ¿Cuál es el punto de destino de todas las búsquedas realizadas con Google Maps?
z) ¿Cuántos email registró la app de Gmail del teléfono?
aa) En qué fecha/hora se registró el email más antiguo registrado en la aplicación de Gmail del teléfono.
bb) ¿Quién es el remitente (dirección de correo) del email identificado en el apartado anterior?
cc) En qué fecha/hora se registró el email más reciente registrado en la aplicación de Gmail del teléfono.

dd) ¿Cuántos mensajes de correo fueron remitidos por Snapchat?
ee) ¿En qué fecha se remitió el más antiguo de los mensajes provenientes de Snapchat?
ff) ¿En qué fecha se remitió el más reciente de los mensajes provenientes de Snapchat?
gg) ¿Desde cuántos dispositivos hay avisos de inicio de sesión en Snapchat?
hh) Identifique el/los modelo/s de dispositivo/s desde el/los cual/es se inició sesión en SnapChat que sean distintos del modelo del teléfono investigado.
ii) Desde qué IP se produjo un intento de login en SnapChat desde el dispositivo identificado en el apartado anterior.
jj) En qué localidad aproximada tuvo lugar el inicio de sesión en SnapChat desde el dispositivo identificado en el apartado gg).
kk) ¿Cuántas imágenes de la Casa Blanca hay presentes en la caché de imágenes del dispositivo?
ll) ¿En qué fecha fueron registradas las imágenes anteriores?
mm) ¿Cuál fue la última fecha de actualización de la app de Whatsapp en el dispositivo investigado?
nn) ¿Cuál es la versión de código de la aplicación de Whatsapp instalada en el dispositivo investigado?
oo) ¿En qué fecha/hora se instaló la aplicación de mensajería de Facebook?
pp) ¿Cuántos mensajes MMS distintos hay registrados en el teléfono?
qq) ¿Cuántos de los mensajes MMS identificados eran entrantes?
rr) Los mensajes MMS entrantes, ¿de qué número provenían?
ss) De los mensajes salientes, ¿cuántos contenían un mensaje de audio?
tt) ¿A qué número/s fue enviado el mensaje/s saliente identificado en el apartado anterior?
uu) ¿En qué fecha fue enviado el/los mensaje/s saliente/s identificado/s en el apartado ss)?
vv) ¿Cuántos mensajes SMS distintos hay registrados en el teléfono?
ww) ¿Qué se puede inferir de los MSG ID de los SMSs registrados en el teléfono?
xx) ¿Cuántos mensajes SMS fueron entrantes?
yy) De los mensajes entrantes, ¿cuántos fueron leídos?
zz) ¿Desde qué número se envió el mensaje cuyo MSG ID es el número 5?
aaa) ¿Desde qué número fue enviado el mensaje con el código de activación de Whatsapp?
bbb) ¿Cuál es el nickname del usuario **Tammie Smith** en la lista de amigos de la aplicación Snap Chat?

ccc) ¿Cuántos contactos hay registrados en la lista de contactos de Whatsapp?

ddd) De los contactos de Whatsapp, ¿cuál es el único que no figura en la lista de contactos del teléfono?

eee) ¿Cuántos mensajes de Whatsapp salientes se registraron?

fff) ¿A qué número/s se enviaron los mensajes de Whatsapp?

ggg) ¿Cuál es el identificador para mostrar asociado al número 2402528734?

8. Descarga del campus virtual (**Recursos Prácticas->Práctica 4**), el fichero **JTAGSamsungS4.bin**. Este fichero se corresponde con una imagen física de un teléfono móvil **Samsung S4**. 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: **Recent Activity, File Type Identification, Picture Analyzer, Keyword Search** (seleccione la búsqueda de números de teléfono, direcciones IP, emails, URLs y números de tarjeta de crédito), **Email Parser, Extension Mistmatch Detector, PhotorecCarver y Android Analyzer**. Con todos esos módulos de ingestión activados, el proceso de búsqueda de artefactos por parte de Autopsy puede demorarse un buen rato. Responda a las siguientes cuestiones:

   a) ¿Cuántos registros tiene la libreta de direcciones (Contactos)?
   b) ¿Cuántas entradas en la tabla de contactos tienen un número de teléfono asociado?
   c) ¿Cuántos contactos corresponden a números telefónicos extranjeros?
   d) ¿A qué contacto (Nombre) corresponde un número de teléfono con prefijo de Francia?
   e) ¿Cuál es la entrada (Número de teléfono) que corresponde con un número de teléfono con prefijo internacional de China?
   f) ¿A qué entrada (Nombre) corresponde el número de teléfono con código de área (Area code) de Maryland?
   g) ¿A qué entrada (Nombre) corresponde el número de teléfono con código de área (Area code) de Mississippi?
   h) ¿Qué email está vinculado al número de teléfono **1234567890**?
   i) ¿Qué número de teléfono recibió más llamadas salientes?
   j) ¿Cuántas llamadas recibió el número identificado en el apartado h)?
   k) ¿En qué fecha/hora se realizó la primera de las llamadas salientes destinada al número identificado en el apartado h)?
   l) ¿En qué fecha/hora se realizó la última de las llamadas salientes destinada al número identificado en el apartado h)?

m) ¿Cuántas llamadas entrantes se recibieron en el teléfono?
n) ¿Cuántas llamadas salientes se realizaron desde el teléfono?
o) ¿Cuántas llamadas entrantes fueron llamadas perdidas?
p) ¿Desde qué número se realizó la llamada perdida?
q) ¿A qué hora se recibió la llamada perdida?
r) ¿A qué estado pertenece el número desde el cual se realizó la llamada perdida?
s) ¿Cuántas llamadas entrantes se recibieron desde el teléfono desde el que se realizó la llamada perdida?
t) ¿Cuántos mensajes MMS/SMS han sido detectados por la herramienta?
u) ¿Cuántos mensajes MMS/SMS son mensajes recibidos (entrantes)?
v) ¿De qué número provienen los mensajes MMS/SMS recibidos?
w) ¿En qué fecha/hora fue recibido el último mensaje MMS/SMS enviado desde el teléfono identificado en el apartado v)?
x) ¿Fueron leídos todos los mensajes MMS/SMS recibidos? Al ser esta una imagen forense destinada a probar las habilidades de los investigadores y las capacidades de las herramientas por ellos manejadas, observe el contenido de los mensajes antes de contestar a la pregunta y razone su respuesta.
y) ¿Cuántos mensajes MMS/SMS entrantes de más de 160 caracteres fueron detectados por Autopsy?
z) ¿Cuántos mensajes MMS/SMS fueron enviados desde el teléfono móvil intervenido?
aa) ¿Cuántos mensajes salientes borrados fueron detectados por Autopsy? Al ser esta una imagen forense destinada a probar las habilidades de los investigadores y las capacidades de las herramientas por ellos manejadas, observe el contenido de los mensajes antes de contestar a la pregunta y razone su respuesta.
bb) Abra el archivo de mensajes con un visor de SQLite y compruebe si la tabla **sms** del fichero **mmssms.db** tiene los mismos registros que los mostrados por Autopsy.
cc) ¿Cuántos ficheros registran metadatos EXIF?
dd) ¿Cón qué dispositivo (Modelo y Fabricante) fue tomada la imagen **face.jpg**?
ee) ¿En qué fecha-hora fue tomada la imagen **face.jpg**?
ff) ¿Cón qué dispositivo (Modelo y Fabricante) fue tomada la imagen **20181114_160845.jpg?**
gg) ¿En qué fecha-hora fue tomada la imagen **20181114_160845.jpg?**
hh) ¿Con qué dispositivo (Modelo y Fabricante) fue tomada la imagen **20181114_163605.jpg**?
ii) ¿En qué fecha-hora fue tomada la imagen **20181114_163605.jpg**?
jj) ¿En qué lugar fue tomada la imagen **20181114_163605.jpg**?
kk) ¿En qué lugar fue tomada la imagen **IMG_20181115_190903.jpg**?

ll) ¿Fue tomada con el flash activado la imagen **IMG_20181115_190903.jpg**?

mm) ¿Con qué valor de distancia focal fue tomada la imagen **IMG_20181115_190903.jpg**?

nn) ¿Con qué velocidad de disparo se tomó la imagen **IMG_20181115_190903.jpg**?

oo) ¿Qué dimensiones (anchoxalto) en pixeles tiene la imagen **IMG_20181115_190903.jpg**?

pp) ¿Con qué sensibilidad (ISO) fue tomada la imagen **IMG_20181115_190903.jpg**?

qq) ¿Cuál fue la fecha-hora local del sitio en que fue tomada la imagen **IMG_20181115_190903.jpg**?

rr) ¿Cómo se llama el documento que se está editando en la imagen **20181114_163605.jpg**?

ss) ¿Qué usuario parece tener abierto Word con el que se está editando el documento que aparece en la imagen **20181114_163605.jpg**?

tt) ¿Cuántos ficheros aparecen como borrados?

uu) ¿De todos los ficheros borrados, cuántos son ficheros del sistema?

vv) ¿Cuántos ficheros de vídeo de tipo mp4 fueron localizados por la herramienta?

ww) ¿En qué fecha-hora fue grabado el vídeo **PART_1542244092760_20181114_200004_001_001.mp4**? Razone la respuesta y tenga en cuenta que Autopsy está mostrando los datos en CET.

xx) ¿De qué marca es el ordenador portátil que aparece en el vídeo **20181114_163729.mp4**?

yy) ¿Cuál es la frase que aparece en el primer fotograma de **video_help.mp4**?

zz) Indique si el video **bubbly.mp4** es un video descargado o bien grabado desde el propio teléfono.

aaa) Identifique la cantante que aparece en el video **bubbly.mp4**. Para ello descargue e instale en Chrome o bien en Firefox el plugin **InVID** desde https://www.invid-project.eu/tools-and-services/invid-verification-plugin/. Extraiga el vídeo a la carpeta Export del caso y luego analícelo con el plugin mencionado, descomponiéndolo en fotogramas y buscando cada uno de ellos en **Google Images**, **TinEye** o **Yandex**.

bbb) ¿Cuántos ficheros de tipo imagen jpeg fueron localizados por Autopsy?

ccc) ¿Cuántos ficheros de tipo jpeg fueron creados, accedidos o modificados en el teléfono entre el **1 de Noviembre de 2018** y el **30 de Noviembre de 2018** inclusive?

ddd) ¿Cuántos ficheros de video de tipo **mp4** fueron creados en el teléfono entre el **1 de Noviembre de 2018** y el **30 de Noviembre de 2018** inclusive?

eee) ¿Cuántos ficheros de tipo **pdf** fueron creados en el teléfono entre el **1 de Noviembre de 2018** y el **30 de Noviembre de 2018** inclusive?

fff) Compruebe si hay algún fichero **.jpg** en la carpeta de Descargas (**userdata/Media/0/Download**), y en caso de haber alguno, extráigalo a la carpeta de Export del proyecto.

ggg) Indique si hay algún fichero **.pdf** en la carpeta de Descargas (**userdata/Media/0/Download**), y en caso de haber alguno, extráigalo a la carpeta de Export del proyecto y pegue a continuación su contenido.

hhh) Indique si hay algún fichero **.gif** en la carpeta de Descargas (**userdata/Media/0/Download**), y en caso de haber alguno, extráigalo a la carpeta de Export del proyecto y pegue a continuación su contenido.

iii) Enumere las redes sociales con que trabajaba el usuario.

jjj) Localice el fichero que contiene la lista de apps instaladas, extráigalo y almacénelo en la carpeta de Export del proyecto.

kkk) Examine el fichero anterior con un visor XML y pegue las líneas del mismo donde figuran los permisos que tiene la aplicación de twitter instalada.

lll) A la vista de la información proporcionada en el fichero **packages.xml**, en qué ubicación se encuentra el fichero de instalación de whatsapp.

mmm) Localice el fichero **accounts.db**. Indique en qué carpeta se encuentra. Almacene dicho fichero en la carpeta Export. Abra dicho fichero con DB Browser for SQLite. ¿Cuántas cuentas hay asociadas con el dispositivo?

nnn) Según la información obtenida en el apartado mmm), ¿cuál es la cuenta de Google?

ooo) 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**.

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

qqq) Muestre una captura de pantalla de la página de inicio de Facebook cada uno de los contactos localizados en el apartado anterior. Utilice para ello el ID de usuario en Facebook.

rrr) Averigüe el mes y el día de nacimiento del primero de los contactos de Facebook almacenados en el móvil intervenido.

sss) Averigüe el mes y el día de nacimiento del último de los contactos de Facebook almacenados en el móvil intervenido.

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?

uuu) ¿Cuántos mensajes registrados por la aplicación de mensajería de Facebook tuvieron como remitente el usuario con id **100007218342184**?.

vvv) ¿Cómo se llama el usuario/s de Facebook que remitió los mensajes indicados en el apartado uuu)?

www) En función de los mensajes de Facebook recibidos registrados en el teléfono, ¿quién sería el/la usuario@ vinculad@ a la cuenta de Facebook destinatari@ de dichos mensajes?

xxx) ¿Cuántos de los mensajes recibidos con la aplicación de mensajería de Facebook tienen registrados coordenadas de posicionamiento GPS?

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

zzz)¿Cuál es la fecha/hora GMT del mensaje de id 5?

aaaa) ¿Cuántos mensajes de Facebook registrados en el teléfono tienen como remitente el usuario identificado en el apartado www)?

bbbb) En la carpeta **userdata/data/com.facebook.orca/cache/image/v2.ols100.1/98** extraiga el archivo **5BR9nUc39Mt_DL5iMb6AtdFFcjw.cnt** a la carpeta Export del caso. Indique de qué tipo es el archivo.

cccc) ¿Cuál fue la fecha de último acceso al archivo del apartado bbbb)?

dddd) ¿Cuántos frames tiene el archivo bbbb)?

eeee) ¿Cuántas iteraciones de animación tiene el archivo del apartado bbbb)?

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:
   a) ¿Qué versión de sistema operativo Android tenía el teléfono intervenido?
   b) ¿A qué build corresponde la versión del sistema operativo Android identificada en el apartado anterior?
   c) ¿Cuál es la cuenta principal del teléfono y en qué momento fue creada?
   d) Compruebe si hay una cuenta secundaria (perfil secundario) en el teléfono y en ese caso, indique cómo se llama y cuándo fue creada.
   e) ¿Cuál es la MAC de la conexión BlueTooth del dispositivo?
   f) ¿Cuántas conexiones vía BlueTooth se establecieron con otros dispositivos?
   g) ¿En qué fecha/hora se estableció la conexión con el dispositivo Forerunner 35?
   h) ¿Cuántas entradas almacena la caché del navegador Firefox?
   i) ¿En qué ubicación del sistema de ficheros de Android se encuentran los ficheros almacenados en la caché del navegador Firefox?

j) ¿Cuántas entradas tiene el log de llamadas telefónicas?
k) ¿Cuántas llamadas fueron salientes?
l) ¿Cuántas llamadas fueron entrantes?
m) ¿Cuántas llamadas perdidas hubo?
n) ¿Cuántas llamadas fueron rechazadas?
o) ¿Cuántas llamadas dejaron mensaje en el buzón de voz?
p) ¿Cuánto duró la llamada saliente de mayor duración?
q) ¿A qué número corresponde el destinatario de la llamada saliente identificada en el apartado anterior?
r) ¿En qué fecha/hora se produjo la llamada saliente de mayor duración?
s) ¿Cuánto duró la llamada entrante de mayor duración?
t) ¿De qué número provenía la llamada entrante identificada en el apartado anterior?
u) ¿De qué localidad/estado provenía la llamada identificada en el apartado anterior?
v) ¿En qué fecha/hora se produjo la llamada referida en el apartado anterior?
w) ¿Cuántas entradas tiene la libreta de contactos del teléfono?
x) ¿A cuántos contactos únicos pertenecen las entradas anteriores?
y) ¿Cuántos perfiles de autocompletar tiene registrados la app de Chrome?
z) ¿A qué usuario (nombre y apellidos) corresponde cada perfil?
aa) ¿Cuántos marcadores (bookmarks) tiene registrados Chrome?
bb) ¿A qué página/s corresponden?
cc) ¿Qué expresiones o cadenas de búsqueda se han empleado en la app de Chrome?
dd) ¿Cuántas veces se ha buscado la expresión “Cult of Mac”?
ee) ¿Cuántas entradas tiene la lista de sitios más visitados desde la app de Chrome?
ff) ¿Cuáles fueron los sitios más visitados?
gg) ¿Cuántas entradas tiene el historial de sitios visitados en la app de Chrome?
hh) ¿Cuál es la URL más reciente visitada desde la app de Chrome?
ii) ¿Qué URL fue la más visitada desde la app de Chrome?
jj) En qué fecha/hora se realizó la última visita a la URL https://www.starwars.com/ desde la app de Chrome.
kk) ¿En qué momento (fecha/hora) tuvo lugar la última (más reciente) carga rápida del teléfono?
ll) ¿En qué zona horaria se encontraba el teléfono en el momento de su última carga rápida?
mm) ¿Cuántas tarjetas SIM estuvieron insertadas en el teléfono?

nn) ¿A qué proveedor de telefonía está asociado el Carrier ID 1989?
oo) ¿En qué momento (fecha/hora) se reanudó por última vez la aplicación de whatsapp?
pp) ¿En qué fecha/hora se tomó la fotografía más reciente con la cámara del teléfono?
qq) ¿En qué fecha/hora se grabó el vídeo más reciente con la cámara del teléfono?
rr) ¿Qué fichero se encuentra almacenado en el locker de ficheros multimedia encriptados?
ss) ¿Qué actividad estaba realizando el usuario que portaba el móvil a partir de las 12:49 del 13-09-2020?
tt) ¿Cuántos kilómetros recorrió?
uu) En la primera de las búsquedas de Google Maps, ¿cuál es el punto de origen?
vv) ¿Cuál es el punto de destino?
ww) ¿Cuánto tiempo se tarda en llegar entre ambos puntos por la ruta más corta en coche?
xx) ¿Cuándo fue (fecha/hora) la última conexión registrada del teléfono con el dispositivo Forerunner 35?
yy) ¿Estaba el usuario del teléfono durmiendo entre las 3:30AM GMT y las 10:15AM GMT del día 2-10-2020?
zz) ¿Cuántas entradas tiene la tabla de contactos de Google Duo?
aaa) ¿Cuántas de las entradas anteriores identifican a un único contacto?
bbb) ¿Cuántas llamadas se realizaron a través de Google Duo el 4-10-2020?
ccc) ¿Cuántas de las llamadas realizadas a través de Google Duo el 4-10-2020 fueron entrantes?
ddd) ¿A qué contacto de Google Duo se realizaron las llamadas salientes el 4-10-2020?
eee) ¿Confirman los registros de Google Fit que el usuario del teléfono estaba durmiendo entre las 3:30AM GMT y las 10:15AM GMT del día 2-10-2020?
fff) ¿En qué fecha/hora se solicitó al asistente de conducción de Google la dirección del hospital veterinario de Holly Springs?
ggg) ¿Qué carpetas con imágenes y capturas de pantalla han sido backapeadas por Google Photos?
hhh) ¿Cuántas búsquedas de aplicaciones se realizaron desde Google Play?
iii) ¿Está la aplicación de pagos Venmo instalada en el teléfono?
jjj) ¿Cuántas llamadas de vídeo salientes se realizaron a través de la app Line?
kkk) ¿Qué usuario de la app Line fue el iniciador de la llamada identificada en el apartado anterior?

lll) ¿Puede la app de Garmin acceder a la localización del teléfono cuando dicha app está funcionando en background?

mmm) ¿Cuántos contactos existen en la libreta de direcciones de Proton Mail?

nnn) ¿Desde qué cuenta de correo electrónico de Proton Mail se remite el correo recibido el 2020-10-04?

ooo) ¿Cuántos mensajes MMS se enviaron desde el teléfono?

ppp) ¿A qué número/s se enviaron dichos mensajes?

qqq) ¿Figura dicho número en la lista de contactos del teléfono?

rrr) ¿Cuántos mensajes SMS se enviaron desde el teléfono?

sss) ¿A qué número/s se enviaron dichos mensajes?

ttt) ¿Figura dicho número en la lista de contactos del teléfono?

uuu) ¿Cuántos mensajes SMS se recibieron en el teléfono?

vvv) ¿En qué fecha/hora se recibió el mensaje SMS con el código de verificación de Whatsapp?

www) ¿Cuántas cuentas de amigos (Friends) tiene registrada la app de SnapChat?

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

yyy) ¿Cuántas llamadas salientes se realizaron a través de la app de Text Now?

zzz) ¿A qué número/s se realizaron dichas llamadas?

aaaa) ¿Figura/n dicho/s números entre la lista de contactos de la app Text Now?

bbbb) ¿Figura/n el/los número/s identificado/s en el apartado zzz) entre la lista de contactos del teléfono?

cccc) ¿Cuántos contactos de Tik-Tok hay registrados?

dddd) ¿Cuál es el Nickname del propietario del teléfono en la app de Tik-Tok?

eeee) ¿En qué fecha/hora publicó su primer mensaje en la app de Tik-Tok el propietario del teléfono?

ffff) Dados los eventos de uso del teléfono, cuál fue el último momento (fecha/hora más reciente) en que se movió a segundo plano la entrada escrita en la aplicación de Whatsapp?

gggg) ¿Cuántos contactos distintos tiene la app de Viber?

hhhh) ¿Cuántas llamadas quedaron registradas en el log de la app de Viber?

iiii) ¿Cuántas de ellas se dirigieron al usuario **This Is DFIR Two**?

jjjj) ¿En qué fecha/hora se envió el primer mensaje de texto desde la app de Viber con destino al usuario **This Is DFIR Two**?

kkkk) ¿Cuántos contactos aparecen en la libreta de contactos de Whatsapp?

llll) ¿Cuántas entradas de la libreta de contactos de Whatsapp corresponden al usuario **Josh Hickman**?

mmmm) ¿Cuál es el mensaje de estado de Whatsapp de la cuenta **This Is DFIR**?

nnnn) ¿Qué contiene el cuerpo del mensaje de Whatsapp que se le envía al usuario **This Is DFIR Two** el 2020-09-23 a las 14:09:03?

oooo) ¿Cuánto duró la videollamada de Whatsapp que realizó el usuario **This Is DFIR Two** a la cuenta del usuario del teléfono?

pppp) ¿Cómo se identifica el hot-spot wifi ofrecido por el teléfono?

qqqq) ¿Cuál es la passphrase del hot-spot indicado en el apartado anterior?

rrrr) ¿Cuál es la clave precompartida de la red wifi con SSID **CcookiesDcastleR5 Guest**?

ssss) ¿En qué fecha/hora se restauró el teléfono a los valores de fábrica por última vez?

Firmado por GARCIA TAMARGO, MARCO ANTONIO (FIRMA) el día 22/10/2024 con un certificado emitido por AC DNIE 006