

Análisis forense de entornos móviles

Introducción

Unidad 4

Contenidos

- 1 Introducción al análisis forense
- 2 Metodología
 - Etapas del análisis forense
 - El informe forense
- 3 Herramientas básicas
- 4 Métodos de adquisición de datos
 - Tipos de adquisición de datos
 - Maximizando la adquisición de datos
 - Adquisición en Android
 - Adquisición en iOS
 - Adquisición en Windows Phone
 - Adquisición en BlackBerry

Contenidos

- 5 Laboratorio de adquisición de datos
 - Imagen forense de un dispositivo Android
 - Imagen de una tarjeta SD
 - Imagen forense de un dispositivo iOS
 - Adquisición lógica de un dispositivo Android
 - Adquisición de memoria de un dispositivo Android
- 6 Análisis de datos
- 7 Laboratorio de análisis
 - Introducción al laboratorio
 - Presentación del caso
 - Creación del caso
 - Extracción de información
 - Análisis
 - Informe
- 8 Ejercicios de investigación
 - Test de evaluación



A person wearing a light blue button-down shirt is seated at a dark wooden desk. They are holding a black pen and writing in a white notebook. A laptop is partially visible to the right. The background is a warm, orange-toned wall. A semi-transparent dark blue banner is overlaid across the middle of the image, containing the title text.

Introducción al análisis forense

◆◆◇ Introducción al análisis forense

Principio de Intercambio de Locard

Cualquier interacción física entre dos objetos implica la transferencia de material de uno a otro

- El principio de Locard fue desarrollado por Edmond Locard en 1934.
- Este principio es el precursor del análisis forense como campo científico.
 - El criminal deja pruebas en el escenario durante la consecución del delito.
 - El analista puede modificar las pruebas durante el proceso de adquisición o análisis.



Definición

- ¿Qué es el análisis forense en entornos informáticos?
 - Es el conjunto de procedimientos de recopilación y análisis de evidencias que se realizan con el fin de conocer las causas a un incidente en el que hay un sistema informático envuelto.
- Dependiendo del tipo de incidente, el proceso de análisis forense se realiza con diferentes objetivos:
 - Si el incidente está relacionado con un hecho delictivo e intervienen las fuerzas de seguridad y cuerpos judiciales, el objetivo del análisis forense es la presentación de las pruebas en un tribunal.
 - Si se trata de un incidente de seguridad informática, los diferentes procedimientos ejecutados como el análisis tendrán como objetivo la respuesta eficiente ante el incidente.
- El proceso de análisis forense llevado a cabo dentro de una organización en caso de incidente informático es compatible con el proceso legal que se pueda derivar del propio incidente, y en muchos casos ayuda a esclarecer los hechos y atribución del mismo.

Objetivos

- De forma general, los objetivos del análisis forense se dividen en dos:
 - Conocer realmente lo que ha sucedido en un sistema informático, dependiendo del tipo de investigación los hechos a estudiar pueden ser diferentes:
 - En el caso de una intrusión informática, conocer el procedimiento que se llevó a cabo para acceder al sistema y el alcance de los daños generados.
 - Para delitos que no han sido ejecutados por medios informáticos, sirve para averiguar información sobre la persona dueña del dispositivo (ej. comprobar una coartada).
- Conocer el responsable de cada acción o evento descubierto durante el análisis , por cada hecho identificado es necesario identificar el responsable del mismo:
 - Para delitos cometidos a través de medios informáticos esta tarea es en ocasiones muy compleja debido a la existencia de técnicas para proveer anonimato a los atacantes (utilización de *botnets*, Tor, etc.).

◆◆◇ Introducción al análisis forense

Motivación

- La informática forense es una parte integral de los procedimientos de respuesta ante incidentes:
 - Se aplica después de que un delito o incidente de seguridad haya sucedido.
 - Permite reconstruir los sucesos o acciones que han llevado a un incidente de seguridad para mejorar los procesos de protección existentes en una organización.
- La informática forense también se puede utilizar de forma activa en el contexto de una organización para:
 - Auditar las propiedades de seguridad de un sistema (mantenimiento de privacidad, envío de datos sensible)
 - Revisar el cumplimiento de normativas y estándares de seguridad.
 - Asegurar que se cumplen los procedimientos para la destrucción de datos sensibles en un sistema.



Particularidades del entorno móvil I

- Uno de los principales problemas de la informática forense es que debe adaptarse a la constante aparición de nuevos dispositivos:
 - Durante sus inicios, la informática forense trababa delitos que se cometían a través de medios informáticos. Por lo tanto, las investigaciones se concentraban en estaciones de trabajo, servidores y redes.
 - La aparición de teléfonos móviles ofreció nuevos datos (SMS y llamadas) y empezó a acercar la informática forense a delitos que suceden fuera de los medios telemáticos.
 - La aparición de los *smartphones* amplió el abanico de información a recolectar de un dispositivo (mensajes, correos electrónicos, localización, etc.).
 - Los nuevos dispositivos conectables (*wearables*, vehículos, domótica, etc.) ofrecen aún más información que pueden ser de gran importancia durante una investigación judicial.
- Cada uno de estos tipos de dispositivos tiene un conjunto de particularidades que hacen del análisis forense una tarea compleja y dificultosa.

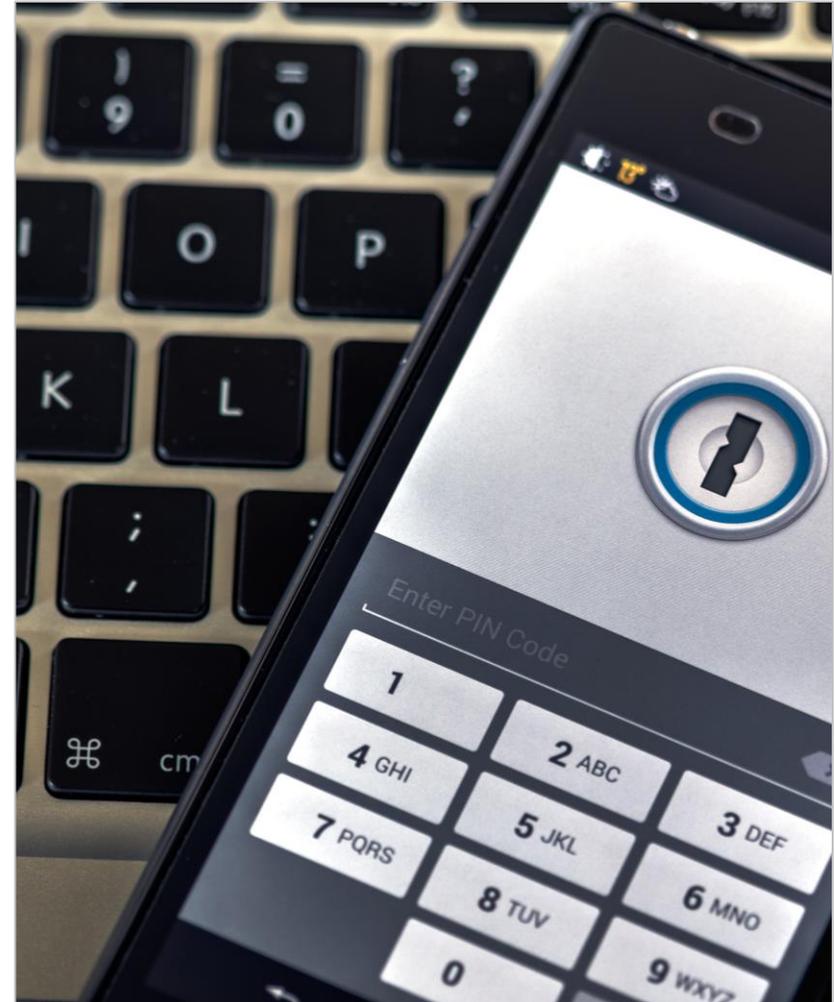
Particularidades del entorno móvil II

- En particular, el análisis de los entornos móviles y *smartphones* supone un desafío por las siguientes razones:
 - **Diferentes sistemas operativos:** pese a que Android es el sistema operativo móvil de uso mayoritario existen otros que también tienen una importante cuota de mercado y que por tanto deben ser conocidos en profundidad para poder llevar a cabo el proceso de toma de evidencias, iOS, Windows Phone y BlackBerry OS son algunos de ellos.
 - **Consideraciones legales:** durante el proceso es fundamental cumplir en todo momento con la normativa vigente, con el fin de mantener la validez legal de las pruebas en el caso de que se requiera.
 - **Técnicas anti-forense:** al igual que sucede con otros dispositivos como en el caso de los ordenadores, es posible realizar diferentes acciones para dificultar la identificación de pruebas en un proceso forense, como por ejemplo: destrucción, ocultación o falsificación de las evidencias.

◆◆◆ Introducción al análisis forense

Particularidades del entorno móvil III

- Los sistemas operativos móviles ofrecen por defecto sistemas de protección y cifrado que dificultan la adquisición y análisis de datos:
 - El **bloqueo por código** de un terminal evita el acceso al dispositivo, incluso por cable en algunos sistemas.
 - El **borrado remoto** permite eliminar todas las pruebas de un dispositivo sin tener acceso físico al mismo.
 - El **cifrado de disco** imposibilita la lectura de las memorias a través del acceso físico al chip.
- Existen millones de aplicaciones disponibles para cada dispositivo, cada una con un mecanismo de almacenamiento de información diferente.



◆◆◆ Introducción al análisis forense

Evidencias relevantes en el entorno móvil

Contactos	Correos electrónicos	Archivos de música
Historial de llamadas	Historial de navegación	Documentos
SMS	Fotografías	Calendario
MMS	Vídeos	Redes conocidas
Historial de búsquedas	Caché del teclado	Historial de localizaciones
Conversaciones de aplicaciones de mensajería	Post en redes sociales	Datos borrados del teléfono
Cuentas	Aplicaciones instaladas	Datos de los sensores del dispositivo



Metodología

A close-up, slightly blurred photograph of a person's hand holding a blue pen, poised to write on a document. The hand is wearing a grey, textured sweater. The desk is made of light-colored wood and has a laptop, a white mug of coffee on a brown coaster, and some papers. The background is softly out of focus, showing a wooden chair and a wall.

Etapas del análisis forense

◆◆◇ Etapas del análisis forense

Introducción

- El proceso de análisis forense se basa en el seguimiento de una metodología y la utilización de unas herramientas aceptadas por la comunidad.
- La metodología utilizada durante el análisis forense de sistemas informáticos ha sido heredada de los procesos forenses tradicionales.
- Las herramientas deben cumplir dos requisitos principales:
 - **Repetibilidad:** capacidad para repetir exactamente los mismos resultados a partir de las mismas condiciones iniciales, en ejecuciones sucesivas separadas, utilizando el mismo método y herramientas.
 - **Reproducibilidad:** capacidad de obtener los mismos resultados a partir de las mismas condiciones iniciales, utilizando el mismo método, pero medios diferentes (utilizando otras herramientas o creándolas de cero).
- Se dice que un procedimiento forense es “*forensically sound*” si el proceso para la recogida, manejo, almacenamiento y análisis de evidencias puede asegurar que no han sido modificadas o destruidas durante el proceso de análisis.

◆◆◆ Etapas del análisis forense

Guías

- Pese a no existir una metodología estandarizada que se centre en el análisis forense de dispositivos móviles, existen diferentes guías que pueden orientar el proceso:
 - [Guidelines on Mobile Device Forensics](#) del NIST.
 - [Developing Process for Mobile Device Forensics](#) del SANS.
 - [Best Practices for Mobile Phone Forensics](#) del Scientific Working Group on Digital Evidence (SWGDE).
 - [Good Practice Guide for Mobile Phone Seizure & Examination](#) de la Interpol.
 - [ISO/IEC 27037:2012](#), *Guidelines for identification, collection, acquisition and preservation of digital evidence*.
 - [RFC 3227](#), no hace mención directa a los dispositivos móviles, pero es un estándar de facto en el proceso forense de ordenadores.

◆◆◆ Etapas del análisis forense

Esquema

El proceso de análisis forense se divide en cinco etapas.



Para la correcta consecución del proceso de análisis se recomienda la toma de notas durante cada una de las fases del análisis.

Las notas, cuanto más detalladas mejor, pueden incluir:

Capturas de pantalla.

Localización de evidencias encontradas.

Notas manuscritas.

Utilización de sistemas de anotación dentro de la propia aplicación forense.

Preparación

Adquisición

Gestión de
evidencias

Examen

Análisis

Presentación

◆◆◆ Etapas del análisis forense

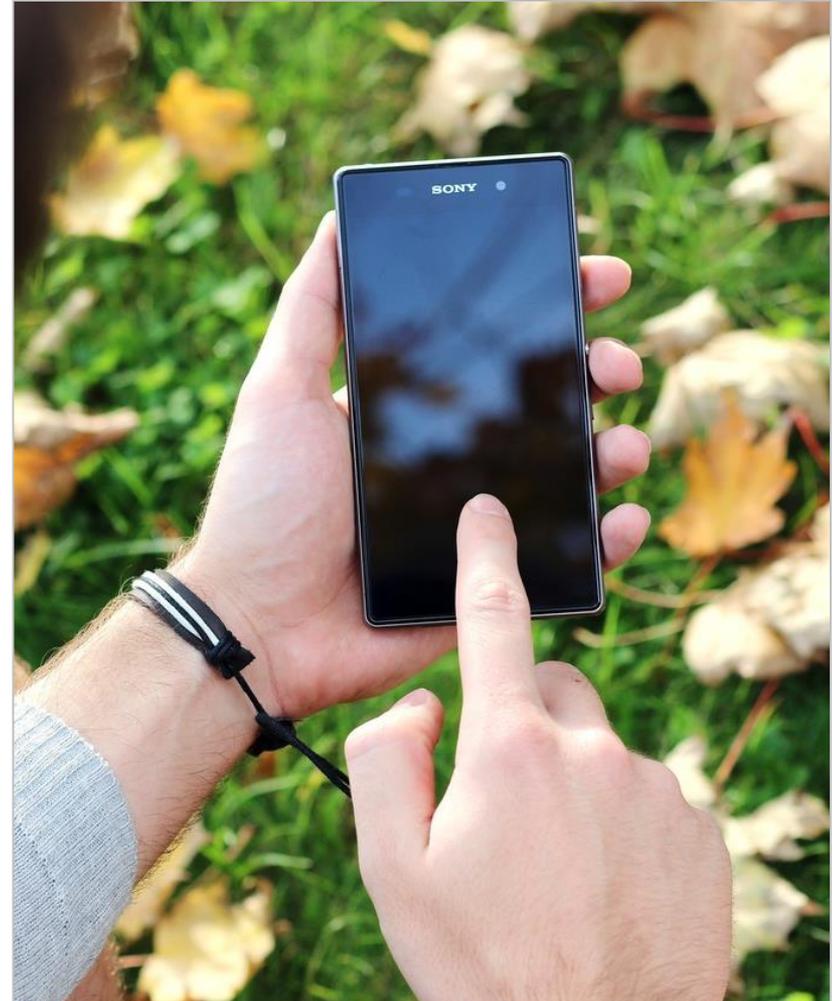
Preparación

- Esta etapa se ejecuta de forma previa al proceso de análisis.
- Consiste en identificar los elementos físicos que se van a analizar y las evidencias que se buscarán en cada uno de los elementos analizables.
- Dependen del objetivo del análisis forense:
 - El análisis de una intrusión a través de un dispositivo móvil requerirá, por ejemplo, el análisis del almacenamiento del dispositivo en busca de pruebas de acceso ilegítimo a los sistemas.
 - El análisis de un dispositivo para la comprobación de una coartada requerirá, por ejemplo, el análisis del almacenamiento del dispositivo para comprobar las localizaciones en las que ha estado el dueño del dispositivo.
- En ocasiones esta tarea se realiza de forma conjunta con la de adquisición de las propias evidencias debido a la necesidad de una respuesta rápida ante el incidente para evitar la eliminación de pruebas.
 - Por ejemplo, durante la incautación de un dispositivo móvil la primera tarea que se realiza es la preservación inicial de la evidencia mediante su inserción en una Jaula de Faraday, para aislarlo de señales externas.

◆◆◆ Etapas del análisis forense

Orden de adquisición de evidencias

- El **proceso de adquisición** se debe realizar teniendo en cuenta la volatilidad de las mismas.
- Es necesario recolectar primero las evidencias más volátiles.
- A continuación se describe un posible orden de adquisición según su volatilidad, aplicándose a dispositivos móviles los marcados en negrita ([RFC 3227](#)):
 - **Registros o cachés.**
 - Tablas de enrutamiento, **lista de procesos y memoria.**
 - Sistemas de ficheros temporales.
 - **Disco.**
 - Sistemas de monitorización remota.
 - Topología de red y configuración física.
 - **Medios físicos externos.**



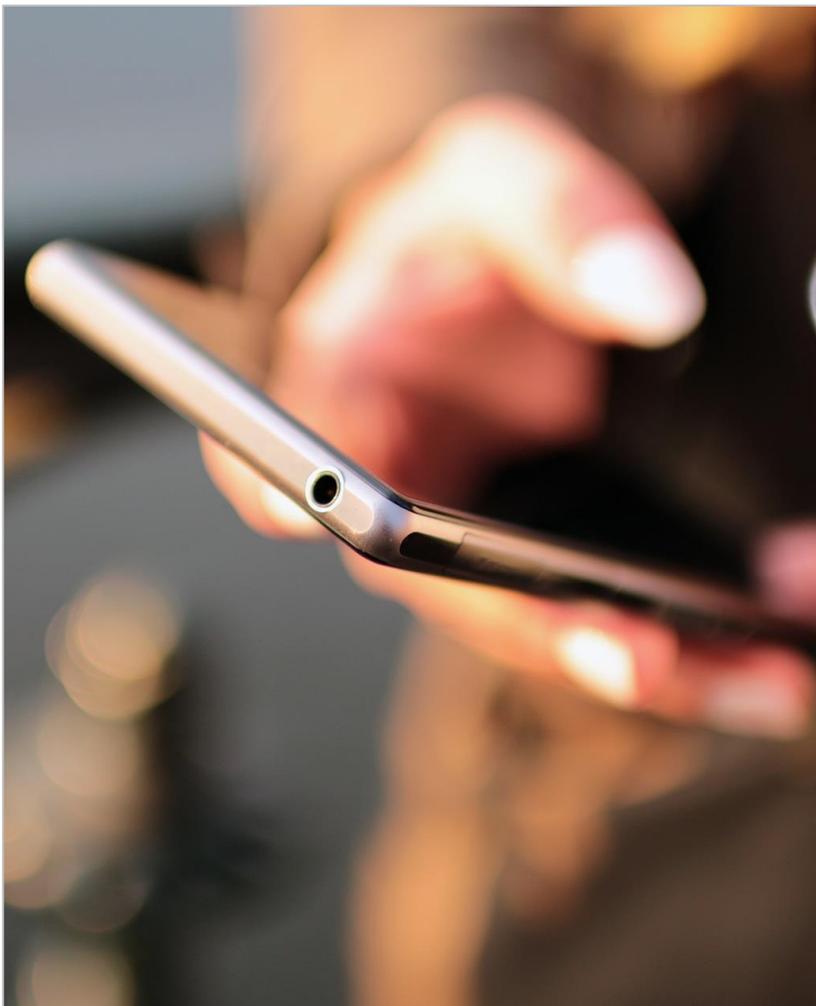
◆◆◇ Etapas del análisis forense

Adquisición I

- La **adquisición** consiste en obtener o capturar las evidencias enumeradas en la fase de preparación.
- Las evidencias se pueden caracterizar en dos grupos dependiendo de su tiempo de vida:
 - **Volatil:** Son aquellas evidencias que son creadas y destruidas durante la ejecución del sistema (memoria, paquetes de red, ficheros temporales, etc.). Pueden contener contraseñas de cifrado, procesos en ejecución que han sido borrados de disco u otros datos de interés.
 - **No volatil:** Son aquellas evidencias que se pueden obtener del dispositivo una vez ha sido apagado (principalmente dispositivos de almacenamiento).
- Siempre que sea posible se debe llevar a cabo un duplicado forense:
 - Consiste en realizar una copia bit a bit de la información de la fuente.
 - Una vez obtenida la copia, se obtiene su hash para poder validar que es una copia exacta.
 - Se puede comprimir para optimizar su almacenamiento.
 - Generalmente se realiza mediante la utilización de hardware específico.

◆◆◆ Etapas del análisis forense

Adquisición II



- Dependiendo del estado del dispositivo y el tipo de evidencia se requiere la utilización de diferentes técnicas y herramientas:
 - Si el dispositivo está encendido y desbloqueado, se pueden utilizar técnicas de monitorización de red o volcado de memoria para capturar evidencias en tiempo real.
 - Algunas de estas técnicas modifican levemente el sistema analizado. La validez de la prueba depende de la cantidad de cambios generados por la herramienta de adquisición.
 - Por ejemplo, el programa dd para el volcado de memoria se debe cargar en la memoria que se volcará para su ejecución.
 - Si el dispositivo está en reposo, la adquisición de información se puede realizar in situ o en el laboratorio tras la incautación del dispositivo.

◆◆◆ Etapas del análisis forense

Adquisición III

- Por cada evidencia recogida es fundamental:
 - Especificar las herramientas y procedimientos utilizados para su adquisición
 - Especificar la **evidencia** exacta que se ha recogido:
 - **Tráfico de red:** duración, hora de inicio, tipo de paquetes, datos obtenidos, etc.
 - **Disco duro:** porcentaje recuperado, método de recuperación, etc.
- Utilizar algún mecanismo para asegurar que los datos adquiridos no son modificados, y si lo son que los cambios puedan ser:
 - Generalmente se hace un resumen de los datos obtenidos mediante una función resumen (SHA-256)
 - Dependiendo de la finalidad de la investigación el resumen puede ser firmado con una clave privada del investigador



◆◆◇ Etapas del análisis forense

Cadena de custodia y gestión de evidencias

- La **gestión de evidencias** es un proceso fundamental para la validez de todo el proceso de análisis forense.
- Una buena gestión de evidencias asegura que la cadena de custodia sea respetada y que por lo tanto las evidencias no han sido comprometidas.
- La cadena de custodia es el conjunto de procedimientos encaminados a la recogida, el traslado y la custodia de las evidencias relativas a una investigación.
- La cadena de custodia tiene como objetivo garantizar la autenticidad, inalterabilidad e indemnidad de las evidencias.
- La cadena de custodia permite:
 - Trazar los elementos físico correspondientes a una evidencia en particular.
 - Identificar el origen del elemento físico utilizado como evidencia.
 - Asegurar que el acceso a una evidencia es controlado y registrado.
 - Documentar todos los procesos realizados para extraer las evidencias.
 - Demostrar que los procesos anteriores son reproducibles y replicables.

◆◆◇ Etapas del análisis forense

Examen

- El **examen** consiste en identificar las evidencias a partir de la información obtenida en la fase de adquisición.
- En el análisis de un disco:
 - Examinar las particiones y el sistema de archivos.
 - Ficheros existentes y ficheros borrados.
 - Espacio sin utilizar y bloques después de la marca de fin de fichero.
 - Obtener metadatos, categorizar ficheros y descartar los no relevantes.
- En el análisis de red:
 - Descartar paquetes que no sean relevantes.
- En el análisis de memoria:
 - Descartar procesos que no sean relevantes.
 - Extraer la información relevante de los procesos.

◆◆◇ Etapas del análisis forense

Análisis

- El **análisis** consiste en obtener conclusiones a partir de las evidencias obtenidas.
- Es la fase más compleja del proceso, y la que más libertad ofrece, por lo que suele variar en función del analista.
- En ocasiones, el análisis de las evidencias puede originar una nueva fase de examen y extracción para hacer visibles nuevas evidencias.
- Para ello se procede mediante un proceso iterativo:
 - **Construir una hipótesis** en base a la información existente sobre el caso.
 - **Probar la hipótesis** con las evidencias existentes. Hay que tener en cuenta también la posible existencia de contra-evidencias.
 - Ejemplo:
 - **Hipótesis:** El sujeto se encontraba en el lugar del crimen a una hora determinada.
 - **Evidencias:** El historial de localizaciones del dispositivo indica que estaba a 15 km.
 - **Técnicas antiforense:** El dispositivo ha sido manipulado y la fecha de última modificación del fichero del historial de localizaciones es inconsistente con la fecha de los eventos.

◆◆◆ Etapas del análisis forense

Presentación

- La **presentación** consiste en describir los diferentes sucesos probados y las evidencias que los corroboran.
- Generalmente consiste en la elaboración de un informe forense.
- El **informe forense** va a ser leído por personal que no es técnico (jueces, ejecutivos, etc.) por lo que debe ser claro y contener un lenguaje que se adapte al perfil adecuado.
- En caso de que sea escrito para un proceso judicial, es posible que sea necesaria su defensa ante el juez.





EI informe forense

◆◆◆ El informe forense

Estructura

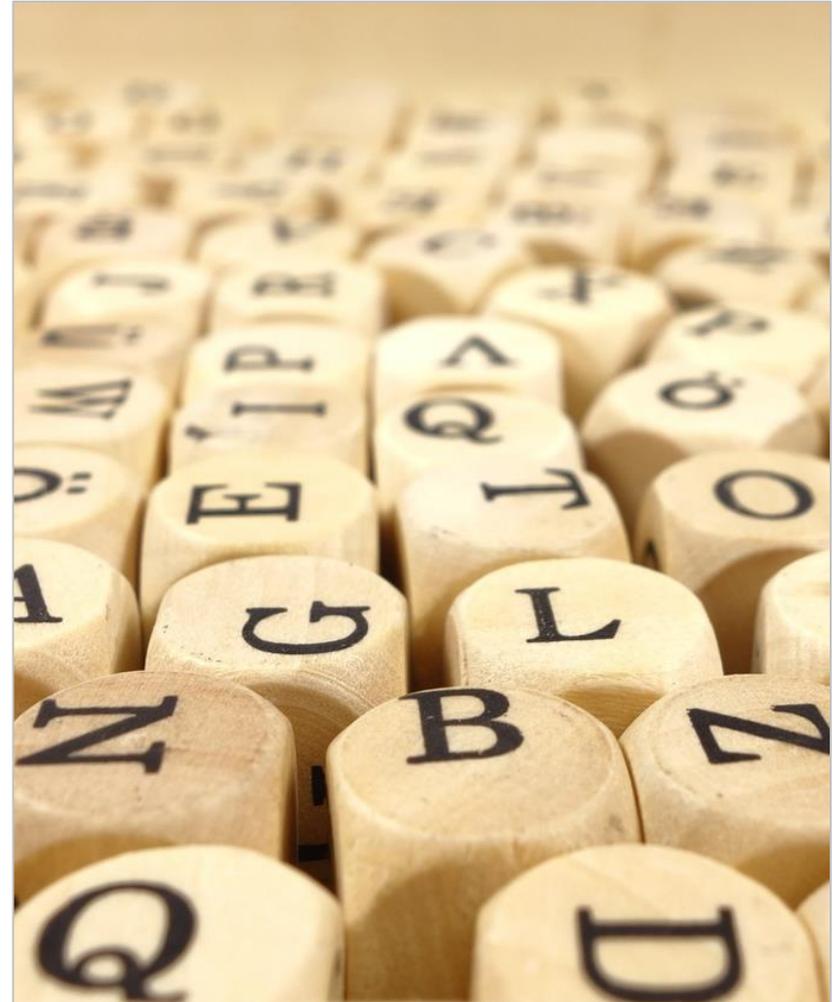
- En general un informe forense debe incluir las siguientes secciones:
 - Sumario o resumen del caso.
 - Herramientas utilizadas.
 - Adquisición de evidencias.
 - Procesado de evidencias.
 - análisis de evidencias.
 - Conclusiones.
- Dependiendo del objetivo y ámbito del mismo, puede ser necesario ajustar la estructura del informe forense.



◆◆◆ El informe forense

Resumen del caso

- Esta sección debe mencionar:
 - Las razones por las que se está llevando a cabo el análisis forense.
 - Como han llegado las pruebas al analista (cadena de custodia).
 - Quién ha solicitado el informe forense.
 - Las fechas más importantes en relación al informe.
 - Fecha de solicitud, recepción de evidencias y tiempo utilizado para la elaboración del informe.
- En algunos casos esta sección incluye también un resumen de los principales resultados del análisis . Hay que tener cuidado con la introducción de esta información para no predisponer al lector.



Herramientas utilizadas

- Debe describir todas las herramientas de terceros utilizadas para el análisis.
- Para cada una de las herramientas será necesario especificar:
 - Versión de la herramienta utilizada (incluyendo plataforma).
 - Fabricante.
 - Tarea para la que se ha utilizado.
- Si se ha desarrollado alguna herramienta específica para el análisis , se deberá mencionar en esta sección, pero también se deberá añadir un anexo en el que se demuestre la necesidad y validez de la herramienta.
- En algunas aproximaciones, esta sección puede ser dividida en subsecciones de cada una de las secciones siguientes del informe.

Adquisición de evidencias

- Debe detallar el proceso de interacción con las evidencias.
- Para ello se deben documentar los siguientes pasos de la forma más detallada posible:
 - **Momento** en el que el analista entra en contacto con las evidencias.
 - **Estado** en el que se reciben las evidencias (con fotos identificativas y describiendo los números de serie de los dispositivos si los tienen).
 - **Procesos ejecutados** para preservar cada una de las evidencias recibidas.
 - Deben incluir la configuración de los dispositivos o entornos en los que se preservarán las evidencias.
 - **Marcadores de integridad** de todas las copias y evidencias recolectadas.
 - Algunas herramientas utilizan MD5, pero es recomendable utilizar estándares superiores como SHA-256 ya que MD5 presenta colisiones o combinaciones de estándares.
- El contenido de esta sección debe probar que la integridad de las evidencias no se ha visto comprometida y que se ha respetado la cadena de custodia.

Procesado de evidencias

- Se describen los pasos ejecutados para la extracción de información que no se encuentra de forma explícita en la evidencia:
 - Bloques del sistema de ficheros eliminados.
 - Ficheros o datos después de las marcas de fin de fichero.
- Se deben documentar los siguientes pasos:
 - Proceso realizado para pasar de una imagen forense a una copia de trabajo. Es necesario asegurar que no se modifica la copia original y que la copia de trabajo es idéntica bit a bit al original.
 - Procesos ejecutados por cada elemento de evidencia extraído de la copia de trabajo.
 - Cada evidencia extraída debe poder trazarse de forma unívoca a los datos originales.

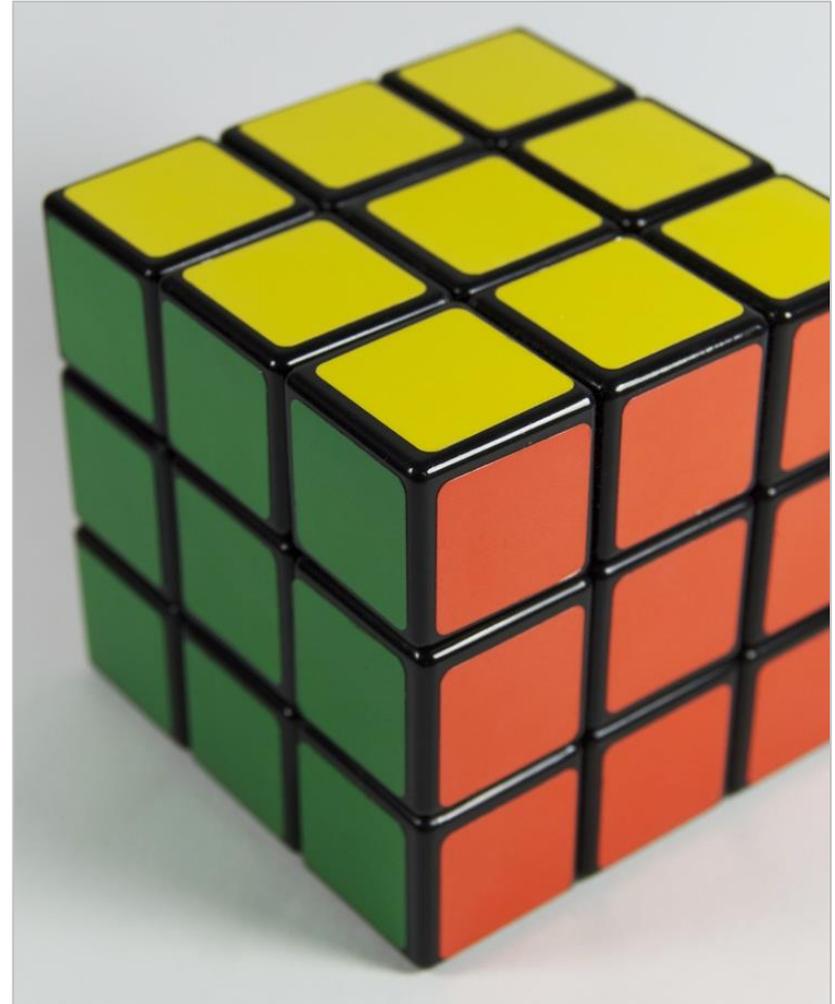
Análisis

- Esta sección del análisis forense se construye con las evidencias analizadas que son relevantes para el caso en concreto.
- Se presentan y razonan las evidencias que confirman o desmienten las diferentes hipótesis que se han analizado durante el proceso de análisis.
- Para cada una de las hipótesis que se han analizado:
 - Se declara la hipótesis inicial y la información previa que llevo a plantearla.
 - Se enumeran los artefactos y evidencias durante el análisis se han utilizado para verificar o desmentir la hipótesis.
 - Se ofrece una conclusión sobre si se ha verificado la hipótesis definida.
- Las hipótesis que no son corroboradas durante el análisis también deben incluirse en el informe si son relevantes de cara al caso.
- Es recomendable que todos los elementos (capturas de pantalla, *logs*, etc.) que sean necesarios para entender en el proceso de verificación de la hipótesis sean incluidos.

◆◆◆ El informe forense

Conclusiones

- Esta sección incluye las conclusiones a las que ha llegado el analista tras la realización de todas las tareas del análisis forense.
- El objetivo final de una análisis forense es describir los hechos de forma objetiva.
- Todas las conclusiones que se enumeren en esta sección deben estar soportadas por evidencias obtenidas y mostradas durante el informe.
- También es recomendable recordar al lector las razones por las que se ha realizado el informe forense.



A close-up, shallow depth-of-field photograph of a wooden workbench. In the foreground, a pair of silver compasses and a pencil with a black eraser tip lie on the wood. To the right, a blue cast-iron vise is mounted on the bench. In the background, a stack of papers or books is visible, slightly out of focus. A semi-transparent blue horizontal bar is overlaid across the middle of the image, containing the text 'Herramientas básicas' in white.

Herramientas básicas

◆◆◇ Herramientas básicas

Introducción

- Si bien el análisis forense depende en gran medida de la plataforma para la que se está realizando, existen un conjunto de herramientas básicas que podrán ayudar durante todo proceso de análisis forense.
- Durante esta sección se van a presentar las principales herramientas y programas de utilidad que se pueden necesitar durante las diferentes fases del análisis forense.
- Las suites forenses de nivel comercial, incluyen de forma general, varias de estas herramientas integradas en un único producto, facilitando así las tarea de análisis:
 - **EnCase Forensic** (Guidance Software) - <https://www.guidancesoftware.com>
 - **Oxygen Forensics** (Oxygen Forensics) - <http://www.oxygen-forensic.com/>
 - **Forensic ToolKit** (Access Data) - <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
 - **UFED** (Cellebrite) - <http://www.cellebrite.com/Mobile-Forensics/Applications>

◆◆◇ Herramientas básicas

Adquisición - dd

- `dd` es una herramienta de consola disponible en la mayoría de sistemas UNIX.
- `dd` puede escribir y leer de dispositivos directamente a través del driver de bajo nivel sin pasar por el sistema operativo.
- Esta característica hace que sea una herramienta de especial interés para el copiado en bruto de discos duros, memorias flash y RAM, pues copia bit a bit los datos ofrecidos por el driver de bajo nivel del dispositivo copiado.
 - En el caso de la memoria RAM debe cargarse en la misma para su ejecución por lo que es modificada (la huella de la utilidad en memoria es mínima).

- Para su ejecución basta con:

```
> dd if=/dev/disk of=myCD.iso bs=2048 conv=noerror, sync
```

Dispositivo
origen

Destino

Tam. bloque

Opciones
conversión

- `dd` está incluida en Santoku Linux, Android y dispositivos iOS con *jailbreak*.

◆◆◇ Herramientas básicas

Análisis – Visor hexadecimal

- Durante el análisis forense, en más de una ocasión será necesario analizar ficheros de datos en formato raw.
- La inspección de estos ficheros con editores de texto no es posible, pues muchos de los caracteres mostrados no serán imprimibles.
- Un editor hexadecimal muestra el contenido de un fichero con dos vistas:
 - Una muestra la conversión de los datos a hexadecimal.
 - Otra muestra los caracteres imprimibles si los tiene.
- De esta manera se pueden realizar búsquedas e incluso reemplazar el contenido de un fichero binario editando directamente sus caracteres imprimibles o valores en hexadecimal (según convenga).
- Editores hexadecimales existentes:
 - **iHex** (Mac OS X) – Disponible en la App Store.
 - **Bless** (Linux) - <http://home.gna.org/bless/downloads.html>
 - **HxD** (Windows) - <https://mh-nexus.de/en/hxd/>

◆◆◇ Herramientas básicas

Análisis – Editor SQLite

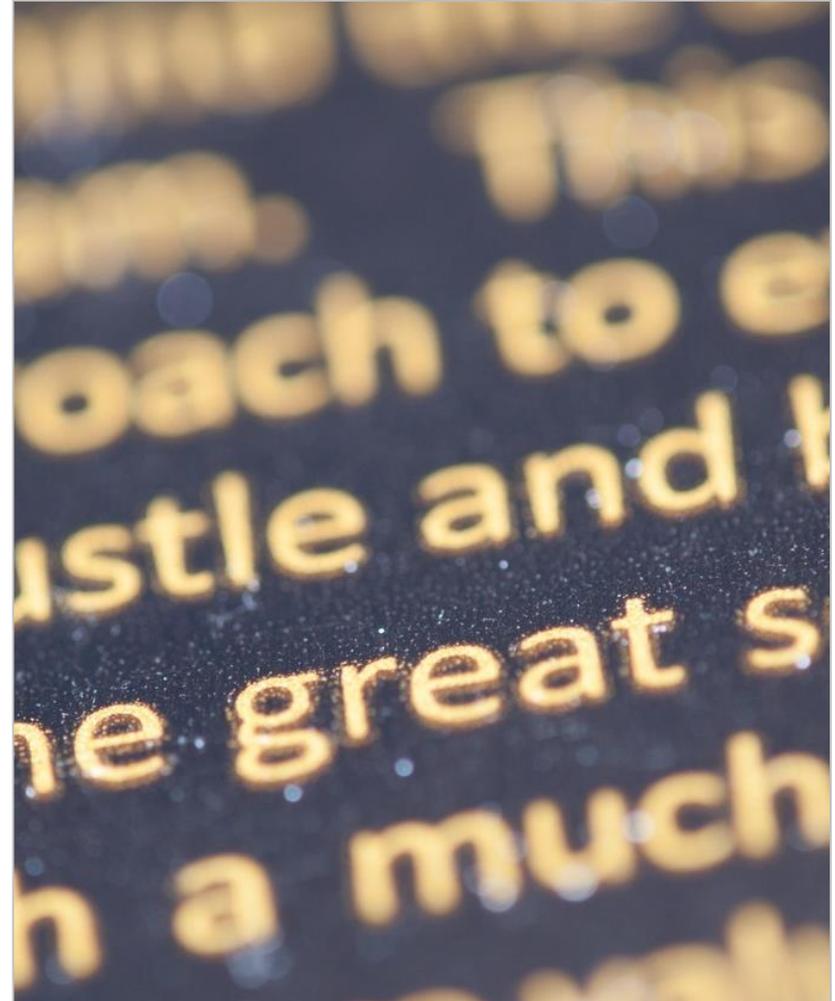
- SQLite es un motor muy popular de base de datos que se utiliza la mayoría de aplicaciones móviles para la persistencia de datos.
- Las bases de datos SQLite se almacenan en ficheros con extensión sqlite (aunque también utilizan otras extensiones como db, sqllitedb, sqlite3, etc.).
- Un visor SQLite permite inspeccionar el contenido de este tipo de ficheros.
- Existen multitud de editores SQLite para todas las plataformas:
 - **DB Browser**, es un proyecto de software libre disponible para todas las plataformas - <http://sqlitebrowser.org>
 - **Sqliteman** – Disponible en Santoku Linux.



◆◆◇ Herramientas básicas

Análisis – Editor de textos

- El editor de textos servirá para acceder a la información que sea almacenada en ficheros de texto durante el transcurso del análisis.
- Esta información puede incluir, entre otros:
 - Ficheros XML.
 - Ficheros de configuración.
 - Ficheros con texto utilizados por aplicaciones.
- Existen multitud de editores disponibles para cualquier plataforma actualmente:
 - **Atom** (multiplataforma) - <https://atom.io>
 - **Leafpad** – Disponible en Santoku Linux.



◆◆◇ Herramientas básicas

Análisis – Herramientas de consola

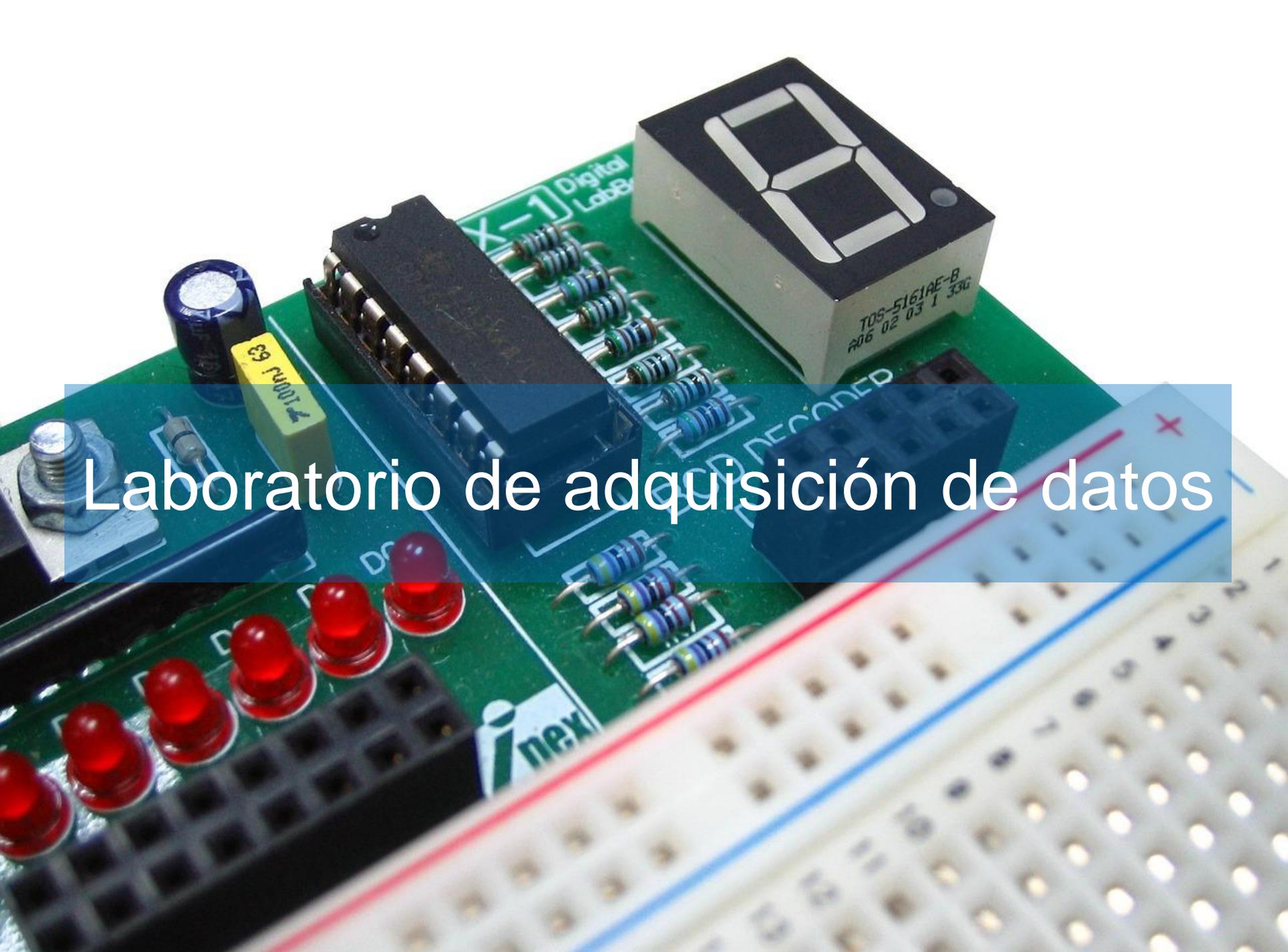
- Además de las herramientas anteriores, existen multitud de herramientas de consola que pueden ser útiles para el analista forense:
 - **Grep:** Herramienta para la búsqueda de expresiones regulares.
 - **Strings:** Identifica las cadenas de texto imprimible en un archivo binario.
 - **Exiftool:** Extrae los metadatos de una fotografía.
- Estas herramientas se encuentran instaladas en cualquier distribución de Linux (Santoku incluido).



◆◆◇ Herramientas básicas

Sleuth Kit y Autopsy

- The Sleuth Kit (TSK) es una colección de herramientas de consola y una librería que permiten el análisis de imágenes de disco y la recuperación de archivos de las mismas.
- Autopsy es un interfaz que utiliza Sleuth Kit para la gestión de casos mediante Autopsy. El analista puede crear un nuevo caso forense, cargar imágenes de adquisiciones, generar *hashes* MD5 de diferentes elementos de la imagen, navegar por la estructura de ficheros o por los bloques de la imagen, añadir notas sobre el análisis forense que está realizando, etc.
- Sleuth Kit y Autopsy están disponibles en Santoku Linux. Para abrirlo basta con ejecutar en consola (debido a la instalación, es necesario ejecutarlo en modo *root*).
 - > autopsy
- Existe una versión más reciente, pero sólo disponible para entornos Windows - <http://www.sleuthkit.org>



Laboratorio de adquisición de datos

Introducción

- Durante esta parte de la unidad se van a realizar una serie de laboratorios que tienen como objetivo mostrar las diferentes técnicas de extracción de información para dispositivos móviles.
- En concreto se realizarán las siguientes actividades:
 - Adquisición de una imagen forense de un dispositivo Android.
 - Adquisición de una imagen de una tarjeta SD.
 - Adquisición de una imagen forense de un dispositivo iOS.
 - Adquisición lógica de un dispositivo Android.
 - Adquisición de memoria de un dispositivo Android.
- En esta ocasión, los laboratorios serán descritos como un conjunto de pasos que puedes ir ejecutando a la vez que se van mostrando por pantalla.

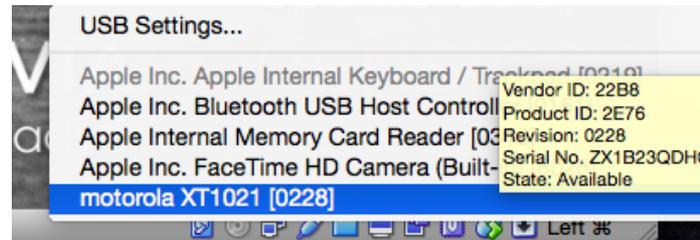


Imagen forense de un dispositivo Android

◆◆◇ Imagen forense de un dispositivo Android

Conexión del dispositivo

- Para la realización de este laboratorio es necesario disponer de un dispositivo *rootado*.
- La adquisición de la imagen del dispositivo se realizará mediante la conexión USB por lo que procedemos a conectarlo al equipo de análisis.
- Vamos a proceder a realizar la imagen desde Santoku, por lo que en VirtualBox, conectamos el dispositivo a la máquina virtual.



- En la opción de *Settings* activamos la opción de USB2.0 o 3.0, dependiendo de nuestro dispositivo. Para esto debemos descargar una extensión de VirtualBox.
 - <https://www.virtualbox.org/wiki/Downloads>

◆◆◇ Imagen forense de un dispositivo Android

Preparación de la adquisición

- Una vez conectado en Santoku abrimos una *shell* en el dispositivo y cambiamos al usuario *root*:

```
santoku@santoku-VirtualBox:~$ adb shell
shell@condor_umts:/ $ su
root@condor_umts:/ # █
```

- Dado que la única partición que puede modificarse por el usuario es aquella que está montada en *data*, utilizamos *mount* para averiguar el dispositivo que le corresponde:

```
root@condor_umts:/ # mount | grep data
/dev/block/platform/msm_sdcc.1/by-name/system /system ext4 ro,seclabel,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/userdata /data ext4 rw,seclabel,nosuid,nodev,noatime,nodiratime,disca
d,nobarrier,noauto_da_alloc,data=ordered 0 0
```

- Ahora, averiguamos el tamaño de bloque:

```
root@condor_umts:/ # df /data
Filesystem      Size      Used      Free      Blksize
/data           2.2G      1.2G      941.7M    4096
```

◆◆◇ Imagen forense de un dispositivo Android

Adquisición de la imagen

- La adquisición necesita de una tarjeta SD vacía en el dispositivo.
- Dependiendo de la versión de Android y el dispositivo la tarjeta se montará en un directorio.

```
root@condor_umts:/ # mount | grep sdcard
/dev/block/vold/179:65 /mnt/media_rw/sdcard1 vfat rw,dirsync,nosuid,nodev,n
mask=0007,dmask=0007,allow_utime=0020,codepage=cp437,icharset=iso8859-1,sh
ro 0 0
/dev/fuse /storage/sdcard1 fuse rw,nosuid,nodev,relatime,user_id=1023,group
_other 0 0
root@condor_umts:/ # █
```

- Para realizar la adquisición ejecutamos dd con los parámetros correspondientes.
> dd if=/dev/block/platform/msm_sdcc.1/by-name/userdata
of=/storage/sdcard1/user.img bs=4096
- Una vez se haya realizado la imagen desde la consola de la máquina de análisis.
> adb pull /storage/sdcard1/user.img
- Obteniendo la imagen de la partición del usuario.

◆◆ Video

Imagen forense de un dispositivo Android

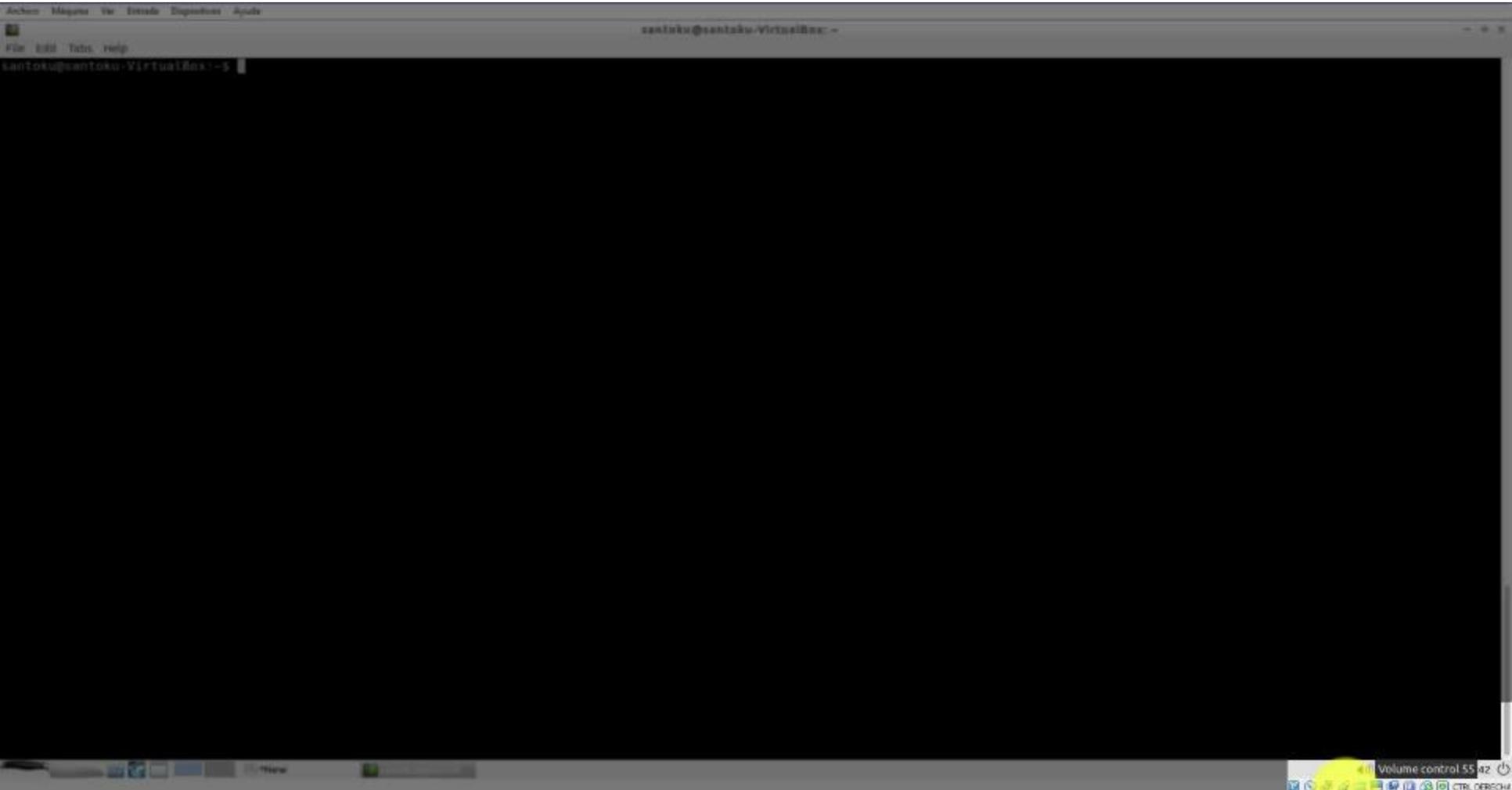


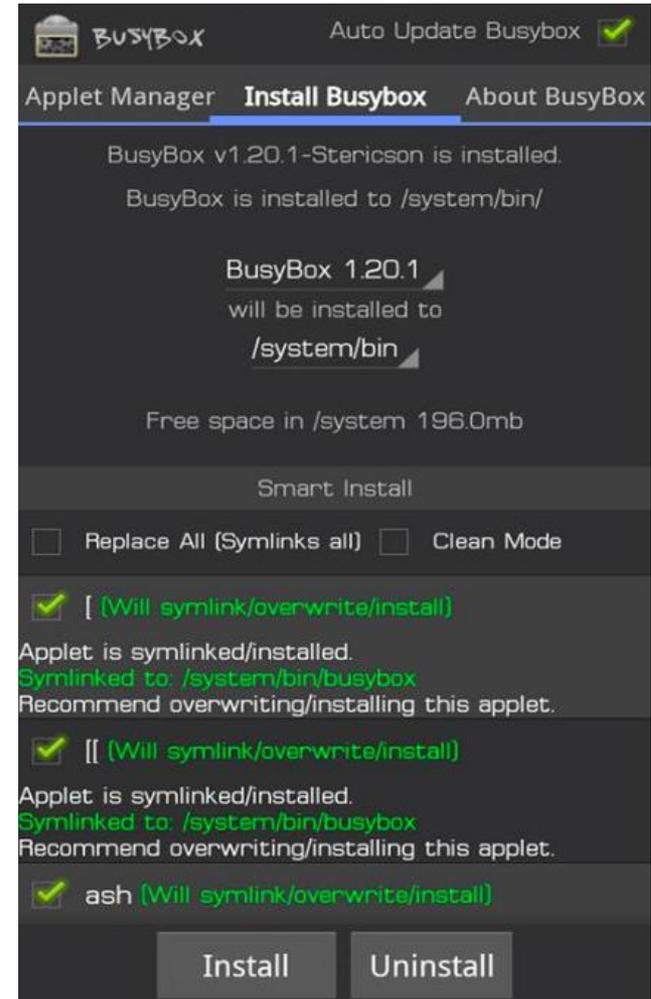


Imagen de una tarjeta SD

◆◆◆ Imagen de una tarjeta SD

Instalación de Busybox

- Para la adquisición de imágenes de tarjetas SD necesitamos otro dispositivo en el que almacenar la imagen capturada.
- Mediante la utilidad Busybox podemos redirigir los datos generados por dd, directamente a un puerto donde los reciba la máquina de análisis.
- Puedes instalar Busybox a través de Google Play:
 - <https://play.google.com/store/apps/details?id=stericson.busybox>
- Una vez instalado, lo ejecutamos y procedemos a la instalación sin aceptar los mensajes publicitarios.



◆◆◆ Imagen de una tarjeta SD

Obtención de la imagen

- Averiguamos el dispositivo correspondiente a la tarjeta de memoria:

```
root@condor umts:/ # mount | grep sdcard
/dev/block/vold/179:65 /mnt/media_rw/sdcard1 vfat rw,dirsync,nosuid,nodev,noexec,relatime,uid=1023,gid=1023,dm
mask=0007,dmask=0007,allow_utime=0020,codepage=cp437,iocharset=iso8859-1,showmount=info,ro 0 0
/dev/fuse /storage/sdcard1 fuse rw,nosuid,nodev,relatime,user_id=1023,group_id=1023,other 0 0
root@condor_umts:/ #
```

- Dado que no podemos guardar la imagen en la tarjeta SD la vamos a transmitir a la máquina de análisis a través de un socket. Para ello en una nueva terminal en la máquina de análisis escribimos:

```
santoku@santoku-VirtualBox:~$ adb forward tcp:8888 tcp:8888
```

- De esta manera nos aseguramos de que todo lo que le llega a adb por el puerto 8888 es transmitido a la máquina de análisis por el mismo puerto.

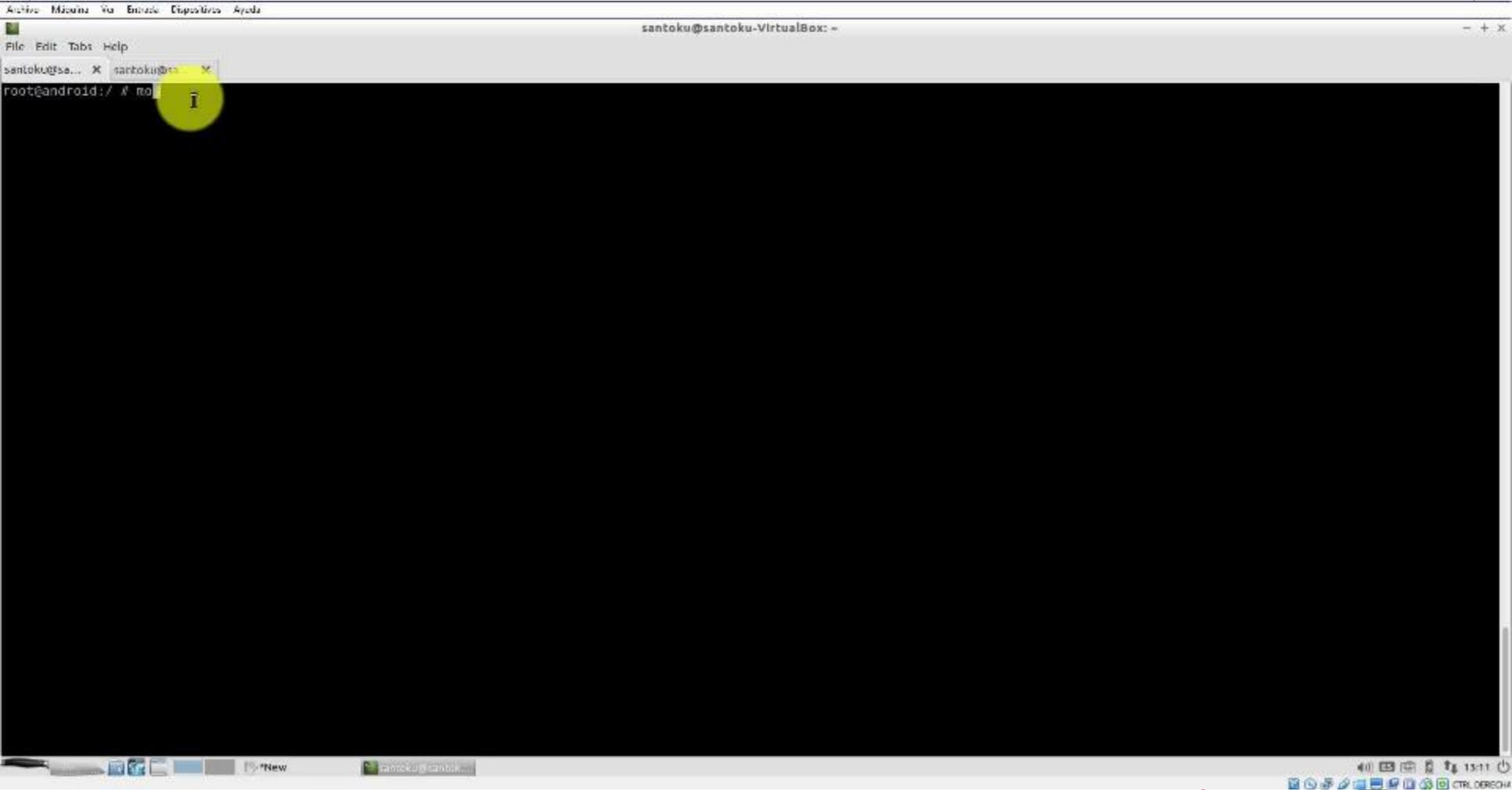
- Ejecutamos

```
> dd if=/dev/block/vold/179:65 | busybox nc -l -p 8888
```

- Y en la máquina de análisis empezamos a recibir la información mediante el siguiente comando:

```
santoku@santoku-VirtualBox:~$ nc 127.0.0.1 8888 > sd_image.dd
santoku@santoku-VirtualBox:~$
```

Imagen de una tarjeta SD



A close-up, side-profile view of a person with long dark hair holding a silver iPhone. The person is wearing a light-colored, possibly white, long-sleeved shirt. The background is a blurred indoor setting, likely a home office, with a laptop on a desk and a window with light coming through. The overall lighting is soft and somewhat dim, creating a focused atmosphere on the phone.

Imagen forense de un dispositivo iOS

◆◆◇ Imagen forense de un dispositivo iOS

Extracción de la imagen

- Al igual que en Android, la adquisición de una imagen del dispositivo requiere permisos de administrador, y por lo tanto *jailbreak*.
- En este caso, la adquisición de la imagen del dispositivo se realiza mediante una conexión SSH por lo que es necesario que el dispositivo se encuentre en la misma red WIFI que la máquina de análisis.
 - La instalación de este tipo de herramientas se explicó durante la unidad 3 del curso.
- Para realizar la extracción basta con ejecutar el siguiente comando

```
> ssh root@ip_iphone dd if=/dev/rdisk0 bs=1M | dd of=imagen-ios.img
```
- Una vez finalizado el comando obtendremos una imagen completa del dispositivo.
- Si el dispositivo utilizado es un iPhone 3GS o superior la imagen se encontrará cifrada, por lo que no será de utilidad. Es necesaria la utilización de una herramienta comercial.

Adquisición lógica de un dispositivo Android



◆◆◆ Adquisición lógica en Android

Instalación de AFLogical

- En este laboratorio vamos a utilizar la herramienta AFLogical para la adquisición lógica de evidencias.
- AFLogical es una aplicación de Android que contiene los permisos necesarios para extraer toda la información accesible mediante permisos de un sistema Android:
 - Historial de llamadas.
 - Contactos.
 - Mensajes SMS, MMS y sus adjuntos.
- Dado que se ejecuta a través de una aplicación normal, no requiere disponer de un teléfono *rooteado*.
- Para su instalación, desde una línea de comandos en Santoku:

```
> aflogical-ose
```
- Instalará la aplicación y la ejecutará.

◆◆◆ Adquisición lógica en Android

Ejecución de AFLogical

- Una vez ejecutada la aplicación, en el dispositivo deberemos marcar la información que queremos extraer en el dispositivo.
- Una vez obtenida la información en el dispositivo continuamos en la consola para transferir los datos a nuestro dispositivo.

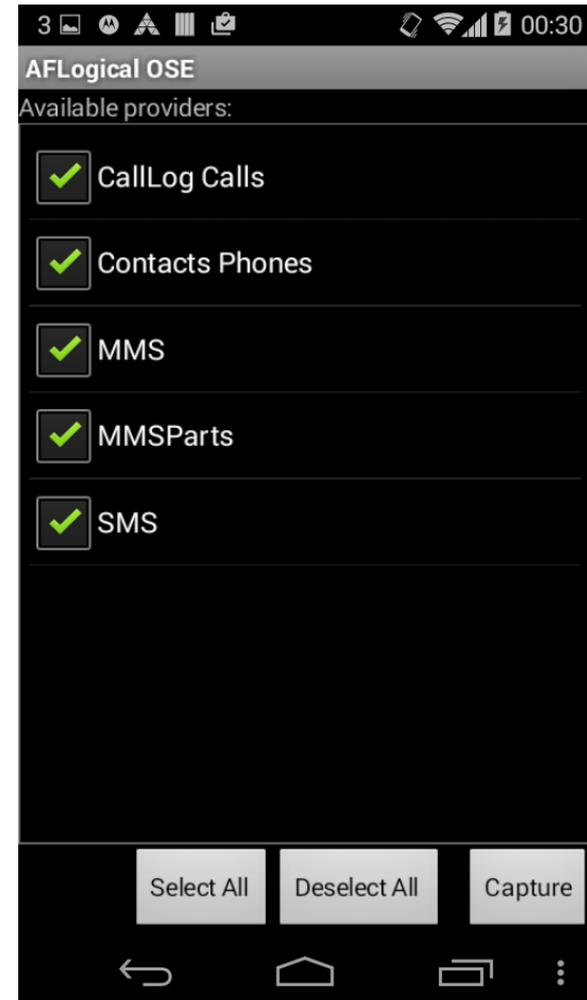
```
santoku@santoku-VirtualBox:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:

697 KB/s (28794 bytes in 0.040s)
  pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

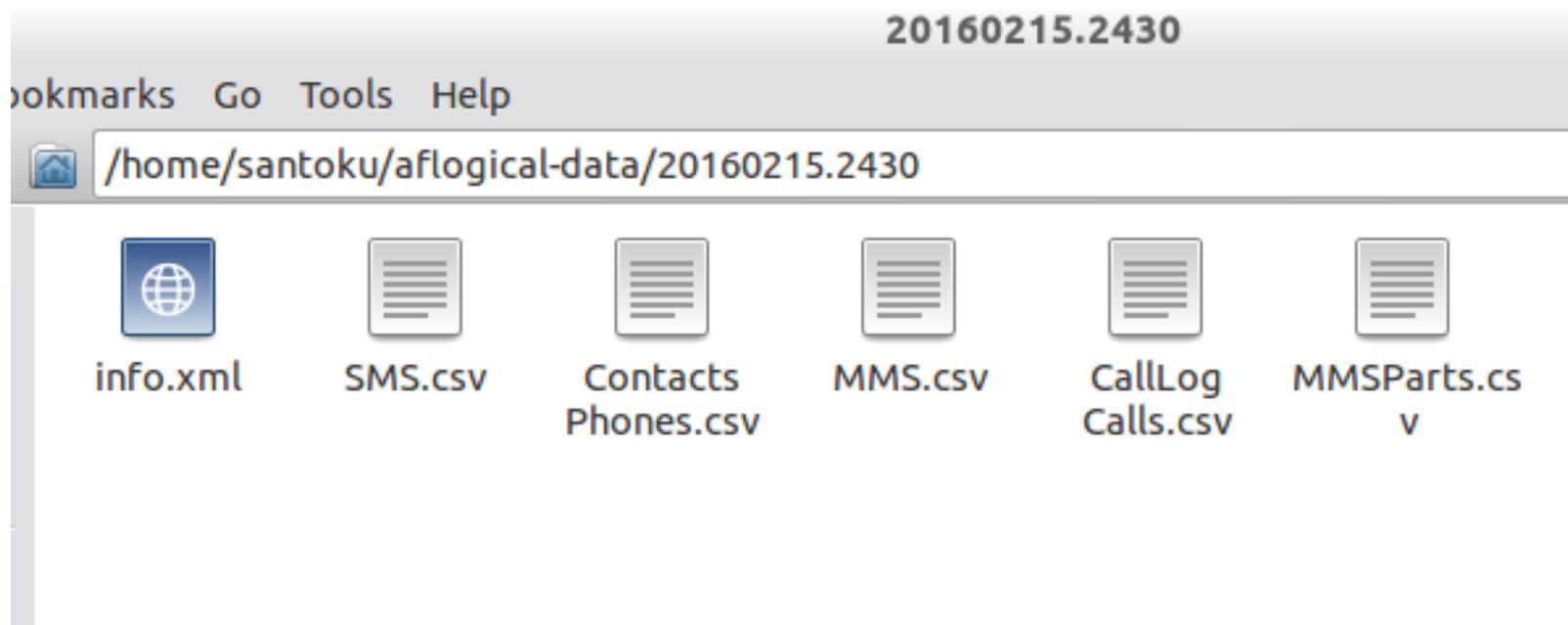
pull: building file list...
pull: /sdcard/forensics/20160215.2430/SMS.csv -> /home/santoku/aflogical-data/20
160215.2430/SMS.csv
pull: /sdcard/forensics/20160215.2430/MMS.csv -> /home/santoku/aflogical-data/20
160215.2430/MMS.csv
```



◆◆◆ Adquisición lógica en Android

Resultados

- Los resultados pueden ser inspeccionados utilizando el navegador de archivos de Santoku Linux.



A close-up, slightly angled view of an Android smartphone's home screen. The background is a dark, textured wallpaper featuring a stylized tree with glowing green and yellow leaves. Several app icons are visible: a red YouTube icon, a white circular icon with five dots, the multi-colored Chrome logo, a red-outlined Gmail icon, and a green speech bubble icon. At the bottom, a white square icon is visible on a blue gradient bar. A semi-transparent grey rectangular box is overlaid in the center, containing white text.

Adquisición de memoria de un dispositivo Android

◆◆◇ Adquisición de memoria en Android

Instalación y ejecución de LiME

- Al igual que en anteriores laboratorios, en esta ocasión será necesario contar con un dispositivo *rooteado*.
- En primer lugar debemos descargar y compilar LiME.
 - Guía de instalación: <https://github.com/504ensicsLabs/LiME/tree/master/doc>
- Una vez compilado, es necesario copiar el módulo al dispositivo del que se va a adquirir la memoria:

```
> adb push lime.ko /storage/sdcard1/lime.ko
```
- Modificamos los puertos para redirigir la salida de LiME:

```
> adb forward tcp:4444 tcp:4444
```
- Abrimos una *shell*:

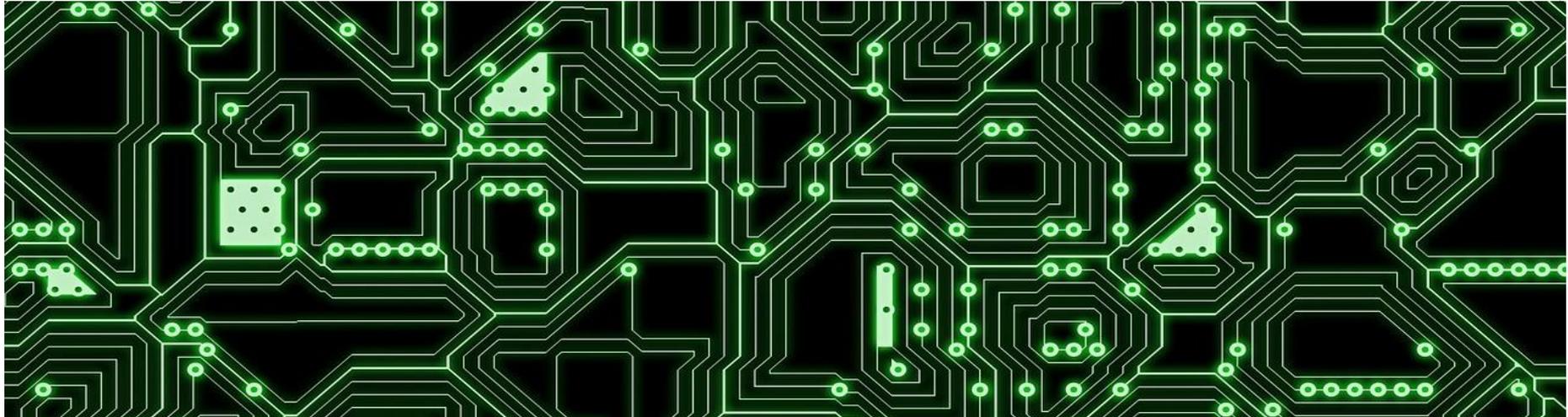
```
> adb shell
```
- Accedemos a *root* y ejecutamos el modulo de *kernel*:

```
> su
> insmod /sdcard/lime.ko "path=/storage/sdcard1/ram.lime
format=lime"
```

◆◆◆ Adquisición de memoria en Android

Transmisión de la imagen

- La imagen se crea en formato lime en la sdcard del sistema
- Para obtenerla en la máquina de análisis utilizamos adb
 - > `adb pull /storage/sdcard1/ram.lime`
- La imagen obtenida puede ser analizada con volatility. Requiere de su instalación en Santoku:
 - > `sudo apt-get install volatility`



A close-up, slightly blurred photograph of a laptop keyboard and screen. The screen shows a data analysis dashboard. At the top, there are tabs for 'Toutes les heures', 'Jour', 'Semaine', and 'Mois'. Below the tabs is a line graph with a dark blue line showing fluctuations over time. A legend below the graph identifies 'New Visitor' (dark blue square) and 'Returning Visitor' (light blue square). At the bottom of the screen, a pie chart is visible, with a green slice labeled '21.8%'. The text 'Análisis de datos' is overlaid in white on a semi-transparent blue rectangular background across the middle of the image.

Análisis de datos

Formatos de datos de interés

```
78 // ... strlen( realpath($_SERVER['DOCUMENT_ROOT']) ) . '?_CAPTCHA'
79 // ... rtrim(preg_replace('/\\\\\\\\/', '/', $image_src), '/');
80 $_SESSION['_CAPTCHA']['config'] = serialize($captcha_config);
81 return array(
82     'code' => $captcha_config['code'],
83     'image_src' => $image_src
84 );
85 }
86
87
88 ▼ if( !function_exists('hex2rgb') ) {
89 ▼ function hex2rgb($hex_str, $return_string = false) {
90     $hex_str = preg_replace("/^[^0-9A-Fa-f]+/", '', $hex_str); // Gets a proper hex string
91     $rgb_array = array();
92 ▼ if( strlen($hex_str) == 6 ) {
93         $color_val = hexdec($hex_str);
94         $rgb_array['r'] = 0xFF & ($color_val >> 0x10);
95         $rgb_array['g'] = 0xFF & ($color_val >> 0x8);
96         $rgb_array['b'] = 0xFF & $color_val;
97 ▼ } elseif( strlen($hex_str) == 3 ) {
98         $rgb_array['r'] = hexdec(str_repeat(substr($hex_str, 0, 1), 2));
99         $rgb_array['g'] = hexdec(str_repeat(substr($hex_str, 1, 1), 2));
00         $rgb_array['b'] = hexdec(str_repeat(substr($hex_str, 2, 1), 2));
01 ▼ } else {
02         return false;
03     }
04     return $return_string ? implode($separator, $rgb_array) : $rgb_array;
05 }
06
07 // Draw the image
08 ▼ if( isset($_GET['_CAPTCHA']) ) {
```

Introducción I

- Durante la etapa de análisis se revisan y estudian las evidencias adquiridas.
- Dada la ingente cantidad de información que almacenan los teléfonos móviles hoy en día, no se recomienda utilizar una estrategia en la que se extraiga toda la información posible del dispositivo sin orden y justificación.
- Dependiendo de los orígenes de las evidencias y el caso en concreto se deberán formular una serie de hipótesis.
- Mediante el análisis de los datos establecidos en la fase de examen y aquellos datos adicionales que puedan ser requeridos durante el análisis se intentará demostrar o refutar la hipótesis.
- Durante el resto de esta sección se describirán:
 - Los principales tipos de datos que se pueden encontrar en un dispositivo.
 - La forma de analizarlos dependiendo del tipo de evidencia adquirida.
 - Los principales tipos de datos de interés en las plataformas predominantes.

Introducción II

- Independientemente de la plataforma o sistema operativo, muchas aplicaciones utilizan los mismos formatos para el almacenamiento de información persistente.
- El conocimiento de la estructura y componentes de estos tipos de archivo puede servir, para identificar la existencia de información almacenada en un formato específico, incluso cuando el archivo ha sido borrado del sistema.
- En concreto, los tipos de archivo con más interés desde el punto de vista forense son:
 - Ficheros XML.
 - Ficheros de almacenamiento de bases de datos SQLite.
 - Fotografías y sus metadatos (EXIF).
 - Ficheros de texto planos y los *strings* contenidos en los mismos.

◆◆◇ Formatos de datos de interés

Ficheros XML

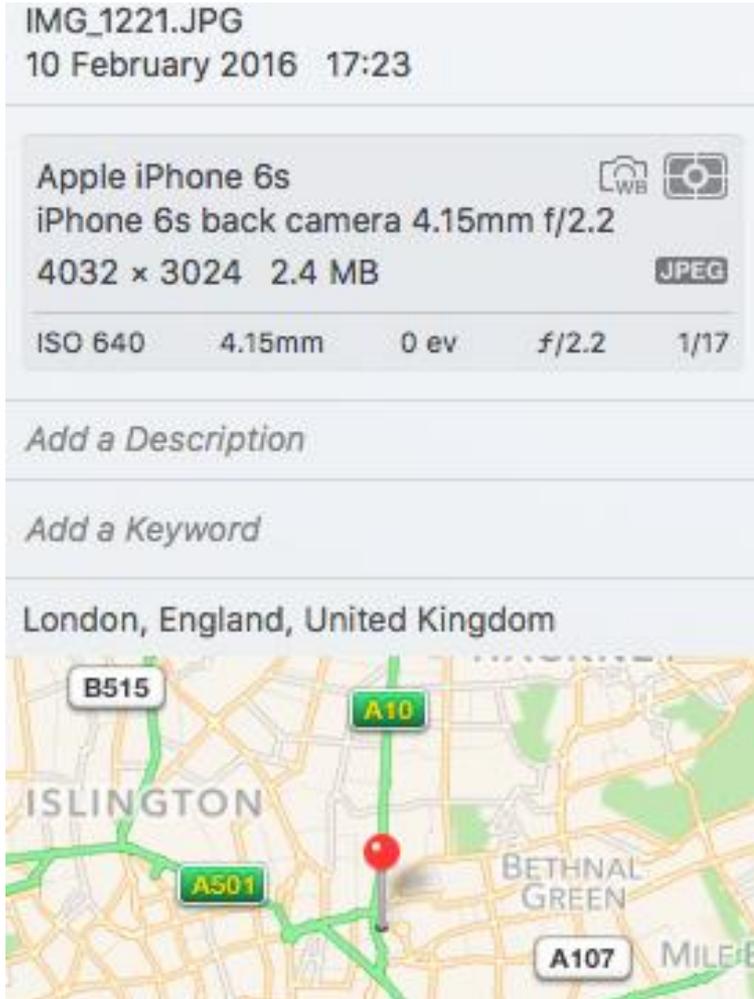
- Los ficheros XML (en inglés *eXtensible Markup Language*) son ficheros de texto que contienen información estructurada a través de lo que se denominan marcas.
- Se utilizan principalmente para el almacenamiento de preferencias.
- XML solo define la estructura del fichero, pero no su contenido:
 - Dependiendo de la plataforma el contenido de los ficheros será diferente.
 - Generalmente siempre empiezan con la siguiente línea.
 - `<?xml version="1.0" encoding="UTF-8"?>`
- Los ficheros XML generalmente tienen extensión `xml` pero también se pueden encontrar con otras extensiones (*plist* en iOS por ejemplo).
 - Los ficheros *plist* incluyen también una cabecera y tienen *tags* específicos:
 - `<plist version="1.0">`
 - `<key><dict><integer>`

Ficheros SQLite

- Los ficheros SQLite están organizados en páginas de tamaño fijo que van siendo rellenas desde abajo.
- Al igual que en un sistema de archivos, cuando el contenido de la página no se necesita, se marca como vacía pero no se borra (eficiencia). Algunos editores permiten inspeccionar este contenido:
 - Sqlite Viewer - <http://www.sqliteviewer.org>
- El almacenamiento se realiza en ficheros con diferente extensión, siendo sqlite y db las más utilizadas:
 - En algunos casos, los cambios realizados en una base de datos se almacenan en un fichero con el mismo nombre, pero con extensión añadida “-journal” o “-wal”.
 - Para poder reconstruir la información completa de la base de datos es necesario el acceso a ambos ficheros.
- Independientemente de su extensión, todas los ficheros SQLite empiezan con el *string* `SQLite format 3` para la versión 3 del formato. Puede ser utilizado para buscar ficheros sqlite borrados del sistema.

◆◆◇ Formatos de datos de interés

Fotografías - EXIF



- EXIF son las siglas en inglés de *Exchangeable image file format*.
- El formato EXIF permite añadir una serie de metadatos a las fotografías y vídeos capturados con cualquier tipo de cámara.
- En el caso de los teléfonos móviles, además del modelo de dispositivo y configuración de la cámara, los datos EXIF también pueden ofrecer información sobre la localización en la que fue tomada una imagen.
- Este tipo de información puede ser muy relevante para establecer líneas de tiempo y localizar el dispositivo en lugares que estén relacionados con los hechos que se están investigando.

Ficheros de texto

- Los ficheros de texto almacenan todo tipo de información en claro:
 - Textos de notas.
 - Configuración de aplicaciones, etc.
- Dado que los contenidos de los ficheros de texto se encuentran en claro en el dispositivo, es posible realizar búsquedas para encontrar datos.
- Esto permite obtener datos de ficheros existentes, pero también facilita la búsqueda de información en bloques borrados.
- En muchas ocasiones las claves y el tipo de palabra a buscar tendrá que ver con el caso específico que se esté investigando.
- Algunas claves que pueden ser interesantes incluyen:
 - Password, pass, pass= password=.
 - User, location.
 - Nombres de personas, lugares, etc.



Tipos de análisis dependiendo del tipo de evidencia adquirida

Análisis de archivos binarios ejecutables

- Dependiendo del tipo de caso es posible que sea necesario analizar los archivos ejecutables binarios de un dispositivo:
 - Una intrusión por *malware*.
 - Necesidad de extracción de datos de una aplicación específica.
- Específicamente, los siguientes elementos pueden ser de interés de cara a una investigación forense:
 - Credenciales almacenadas por la aplicación.
 - Datos de la aplicación como historial de conversaciones (Whatsapp), historial de compras, etc.
 - Interacción de la aplicación con las API del sistema.
- Una vez identificados los elementos de interés, utilizando las técnicas descritas en la Unidad 3, se procederá al análisis de los mismos.
- Para dar validez al análisis forense es necesario documentar y validar el proceso de extracción de información, si no ha sido documentado previamente por otros investigadores.

Análisis de sistema de ficheros

- Consiste en analizar los diferentes artefactos y datos de interés que se pueden encontrar en el sistema de ficheros de un dispositivo.
- La localización de los diferentes elementos dependerá de la plataforma, versión, dispositivo, etc. Tiene el beneficio de que generalmente es consistente entre todos los dispositivos de la misma plataforma y versión.
- El análisis del sistema de ficheros se realiza generalmente mediante el montaje de las imágenes adquiridas en modo de sólo lectura.
- De esta manera se puede navegar por la estructura de ficheros del sistema en busca de los datos o artefactos de interés.
- Dependiendo del sistema de adquisición de datos, una vez montado el disco, también se puede realizar un análisis del espacio no utilizado por el mismo.

Análisis de espacio borrado – *File carving*

- Generalmente, en los sistemas de ficheros tradicionales, borrar un archivo sólo marca como disponibles los bloques del disco en los que estaba almacenado el archivo.
- El contenido de los bloques permanece intacto hasta que son necesitados por el sistema de ficheros.
- Dependiendo del tipo de archivo, su tamaño y el estado de los bloques en los que estaba almacenado se podrá recuperar su contenido para el análisis.
- Para el análisis de espacio borrado hay que tener en cuenta los tipos de archivos que queremos recuperar.
- Dependiendo del tipo de archivo e información a recuperar podremos proceder de un modo u otro.

Análisis de espacio borrado – *File carving*

- La mayoría de ficheros de interés tienen un inicio de cabecera específico (MAGIC NUMBER):
 - SQLite Format 3 (en notación ASCII) para ficheros sqlite.
 - %PDF (en notación ASCII) para ficheros pdf.
 - \211PNG\r\n (en notación ASCII para archivos png).
 - FFD8 (en hexadecimal) para archivos jpeg.
- A su vez, el tamaño del archivo es descrito en la cabecera del mismo:
 - Si el archivo es menor que el tamaño del bloque no hará falta buscar.
 - Si el archivo es mayor, primero se buscará en los bloques contiguos y después en otros bloques del disco si no ha habido éxito (con diferentes heurísticas).
- Afortunadamente, existen herramientas como Scalpel (disponible en Santoku) que realizan esta tarea de forma automática.
- En algunas ocasiones, no siempre es necesario recuperar el archivo completo. Por ejemplo, para recuperar una contraseña se pueden realizar búsquedas de cadenas como *password*, *pass*, etc. Este tipo de búsqueda se puede realizar con el programa de consola *strings* (disponible en Santoku) o un editor hexadecimal.

Análisis de memoria

- Consiste en analizar un volcado de la memoria:
 - El volcado puede ser de la memoria completa del dispositivo.
 - O de un proceso únicamente.
- Se puede realizar de dos maneras:
 - En bruto: Analiza la memoria como un *stream* de bytes. Permite buscar *strings* y otros datos, pero el análisis de variables, de código, etc. es más complejo
 - Organizado: Utiliza un mapa de memoria para interpretar los diferentes valores y estructura del fichero de imagen capturado. Permite distinguir las partes de código y datos de la memoria. Al igual que en el sistema de ficheros, la organización de la memoria del dispositivo depende del terminal y versión del sistema operativo utilizado.
- Si, por las restricciones del dispositivo, se realiza la extracción a la tarjeta SD, hay que asegurarse de que la tarjeta SD haya sido copiada. Esta norma viola el orden de adquisición de volátil a menos volátil, pero en algunos casos es necesario.

Análisis de *backup*

- Consiste en analizar las copias de seguridad que se hayan hecho de un dispositivo:
 - A través de un equipo al que haya sido conectado.
 - A través de los servicios de copia de seguridad en la nube.
- La estructura y localización de los ficheros almacenados en la copia de seguridad es diferente a la estructura física del dispositivo.
- Para comprobar la precisión de los datos almacenados en la copia de seguridad se puede utilizar un dispositivo para volcar la copia.
- En el caso de que la copia de seguridad haya sido cifrada, será necesario averiguar la contraseña de la copia de seguridad:
 - Phone Password Breaker, permite extraer la contraseña utilizada mediante ataques de fuerza bruta - <https://www.elcomsoft.com/eppb.html>
 - Este tipo de herramientas no son capaces de extraer las copias de seguridad cifradas de dispositivos BlackBerry 10. Para ellos, se necesitan las credenciales de BlackBerry Link.

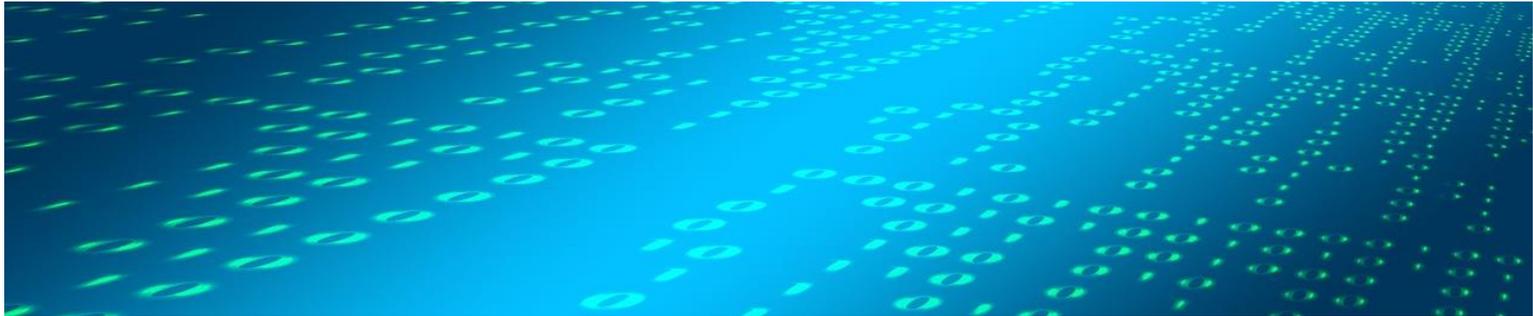
Próximo contenido

Análisis en las diferentes plataformas



A continuación se van a revisar los diferentes archivos, etc. de utilidad para cada plataforma móvil. Dependiendo de la plataforma, se verá el análisis de memoria, backup o sistema de archivos.

Además, para cualquiera de las plataformas estudiadas, se podrán aplicar las técnicas de búsqueda en bloques sin asignar como se ha mencionado en esta sección.





Análisis en Android

Generalidades

- En general, la información analizada en un dispositivo Android se va a encontrar en forma de:
 - **Ficheros SharedPreferences:** Ficheros XML que almacenan pares clave-valor.
 - **Bases de datos Sqlite con diferentes extensiones:** Los *ContentProviders* del sistema son generalmente almacenados en ficheros sqlite.
 - **Ficheros de texto en claro.**
 - **Ficheros binarios:** Imágenes.
- Los ficheros se pueden almacenar en:
 - Almacenamiento interno del dispositivo (protegidos del acceso de otras aplicaciones si no está *rooteado*).
 - Almacenamiento externo del dispositivo (accesible sin problemas por el resto de aplicaciones).

Sistema de ficheros

- El sistema de ficheros de Android está dividido en varias particiones:
 - **boot loader**: Partición de sólo lectura. El primer código que se ejecuta al encender el teléfono. Carga el kernel de Android.
 - **boot**: Incluye el *kernel* de Android.
 - **splash**: Guarda la imagen que se muestra al iniciar el dispositivo.
 - **userdata**: Almacena todos los datos del usuario (aplicaciones, fotografías, etc.).
 - **System**: Incluye las librerías, las aplicaciones del sistema y el *framework* de Android.
 - **cache**: almacena los ficheros utilizados temporalmente por las diferentes aplicaciones (incluyendo la máquina virtual de Dalvik).
- Todos los procesos tienen el acceso a ciertos directorios restringidos (incluido el proceso de adb).

◆◆◆ Análisis en Android

Directorios de interés – Aplicaciones del sistema

- Las aplicaciones del sistema en Android se localizan en ***/system/app***
- Esta partición es de sólo lectura. Sólo almacena los ficheros APK y ficheros *odex* (código de la aplicación preparado para su ejecución en la máquina virtual).
- Los datos generados por las aplicaciones son guardados en ***/data/data/***

```
root@condor_umts:/data/data # ls -las
total 552
drwxr-x--x u0_a3    u0_a3          1970-02-26 01:42 com.android.backupconfirm
drwxr-x--x bluetooth bluetooth      1970-02-26 01:44 com.android.bluetooth
drwxr-x--x u0_a49   u0_a49          1970-02-26 01:43 com.android.browser.provider
drwxr-x--x u0_a50   u0_a50          1970-02-26 01:43 com.android.calculator2
drwxr-x--x u0_a6    u0_a6          1970-02-26 01:44 com.android.calendar
drwxr-x--x u0_a51   u0_a51          1970-02-26 01:44 com.android.cellbroadcastreceiver
drwxr-x--x u0_a52   u0_a52          1970-02-26 01:43 com.android.certinstaller
drwxr-x--x u0_a53   u0_a53          2016-02-13 18:02 com.android.chrome
drwxr-x--x u0_a9    u0_a9          1970-02-26 01:42 com.android.contacts
drwxr-x--x u0_a12   u0_a12          2016-02-13 15:43 com.android.defcontainer
drwxr-x--x u0_a14   u0_a14          1970-02-26 01:44 com.android.deskclock
drwxr-x--x u0_a16   u0_a16          1970-02-26 01:44 com.android.dialer
drwxr-x--x u0_a55   u0_a55          1970-02-26 01:43 com.android.documentsui
drwxr-x--x u0_a47   u0_a47          1970-02-26 01:43 com.android.dreams.basic
drwxr-x--x u0_a79   u0_a79          1970-02-26 01:43 com.android.dreams.phototable
drwxr-x--x u0_a18   u0_a18          1970-02-26 01:44 com.android.email
drwxr-x--x u0_a57   u0_a57          1970-02-26 01:44 com.android.exchange
drwxr-x--x u0_a19   u0_a19          2016-02-13 16:16 com.android.externalstorage
drwxr-x--x u0_a65   u0_a65          1970-02-26 01:43 com.android.htmlviewer
```

```
root@condor_umts:/ # cd /system/app/
3c_main.apk
3c_main.odex
AonIntLT.apk
AonIntLT.odex
BasicDreams.apk
BasicDreams.odex
Bluetooth.apk
Bluetooth.odex
BluetoothExt.apk
BluetoothExt.odex
Books.apk
BrowserProviderProxy.apk
Bug2GoStub.apk
Calculator.apk
Calculator.odex
CellBroadcastReceiver.apk
CellBroadcastReceiver.odex
CertInstaller.apk
CertInstaller.odex
Chrome.apk
```

Directorios de interés – Aplicaciones de terceros

- Los archivos **APK** se encuentran en `/data/app`

```
[root@condor_umts:/data/app # ls -las
total 105028
-rw-r--r-- system system 32940855 2016-02-13 20:35 com.facebook.katana-1.apk
-rw-r--r-- system system 46874450 2016-02-13 20:39 com.snapchat.android-1.apk
-rw-r--r-- system system 27726782 2016-02-13 20:37 com.spotify.music-1.apk
```

- Las **sandbox** están localizadas en `/data/data/`

```
drwxr-x--x u0_a74 u0_a74 1970-02-26 01:43 com.motorola.motosignature.app
drwxr-x--x u0_a84 u0_a84 1970-02-26 01:43 com.motorola.pgmsystem2
drwxr-x--x radio radio 1970-02-26 01:43 com.motorola.programmenu
drwxr-x--x u0_a38 u0_a38 1970-02-26 01:45 com.motorola.setup
drwxr-x--x u0_a41 u0_a41 2016-02-13 17:48 com.motorola.so
drwxr-x--x u0_a45 u0_a45 1970-02-26 01:44 com.motorola.wappushi
drwxr-x--x system system 1970-02-26 01:44 com.qualcomm.atfwd
drwxr-x--x u0_a67 u0_a67 1970-02-26 01:43 com.qualcomm.interfacepermissions
drwxr-x--x system system 1970-02-26 01:43 com.qualcomm.location
drwxr-x--x u0_a85 u0_a85 1970-02-26 01:43 com.qualcomm.qcom_qmi
drwxr-x--x radio radio 1970-02-26 01:44 com.qualcomm.qcrilmsgtunnel
drwxr-x--x system system 1970-02-26 01:44 com.qualcomm.qualcommsettings
drwxr-x--x system system 1970-02-26 01:44 com.qualcomm.services.location
drwxr-x--x u0_a89 u0_a89 2016-02-13 15:43 com.qualcomm.timeservice
drwxr-x--x u0_a86 u0_a86 1970-02-26 01:43 com.quickoffice.android
drwxr-x--x u0_a95 u0_a95 2016-02-13 20:37 com.spotify.music
drwxr-x--x u0_a93 u0_a93 2016-02-13 18:02 eu.chainfire.supersu
drwxrwx--- media media 1970-02-26 01:42 media
drwxr-x--x bluetooth bluetooth 1970-02-26 01:43 org.codeaurora.bluetooth
```

- Se puede comprobar como cada aplicación es asociada a un usuario específico.

Estructura de la *sandbox* de una aplicación

- El directorio de cada aplicación de Android está estructurado en las siguientes carpetas (no todas estarán presentes en todas las aplicaciones):
 - **files**: almacena los ficheros que la aplicación pueda generar y necesitar durante su ejecución. Puede servir de almacenamiento para fotos u otros elementos utilizados por la aplicación.
 - **lib**: almacena enlaces a los directorios en los que se encuentran las librerías compiladas específicamente para la plataforma que necesita la aplicación.
 - **shared_prefs**: Almacena los ficheros de *SharedPreferences* creados por la aplicación.
 - **databases**: Almacena los ficheros sqlite (*providers*) que utiliza la aplicación.
 - **cache**: Ficheros temporales utilizados por la aplicación.

```
[root@condor_umts:/data/data/com.spotify.music # ls
app_MixpanelAPI.Images.DecideChecker
app_MixpanelAPI.Images.ViewCrawler
cacert.pem
cache
code_cache
databases
files
lib
shared_prefs
```

Datos de interés – Fotografías

- El directorio de almacenamiento de las fotografías en Android depende en gran medida del fabricante y el tipo de ROM exacta:
 - */storage/emulated/DCIM*, si el dispositivo no tiene una tarjeta SD.
 - */storage/sdcardX/DCIM*, si el dispositivo tiene una tarjeta SD.
- Dependiendo del uso del teléfono es posible que haya fotografías en ambas localizaciones.
- En el interior de la carpeta DCIM, las fotos generadas con la cámara del dispositivo se guardan en la carpeta Camera.

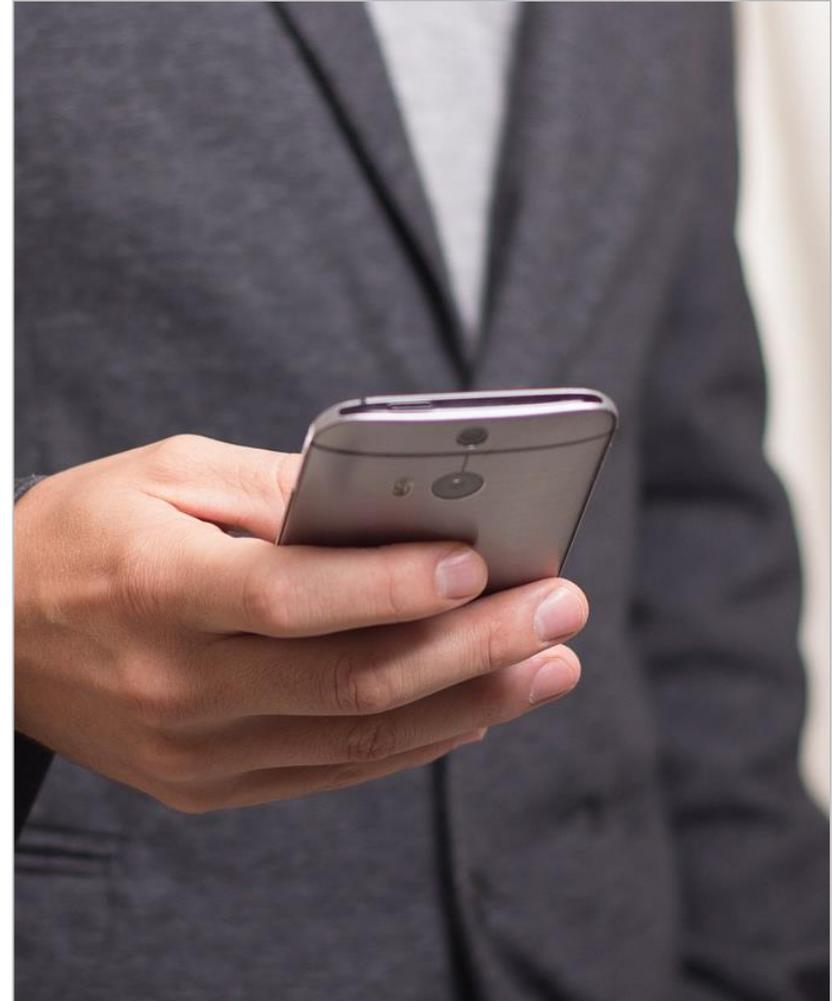
```
[root@condor_umts:/storage/emulated/0/DCIM # ls
Camera
[root@condor_umts:/storage/emulated/0/DCIM # cd Camera
[root@condor_umts:/storage/emulated/0/DCIM/Camera # ls
IMG_20160213_201017879.jpg
IMG_20160213_201022555.jpg
root@condor_umts:/storage/emulated/0/DCIM/Camera # █
```

- Independientemente del dispositivo de almacenamiento, las fotografías pueden ser accedidas desde el propio equipo del analista a través de la conexión USB (o la imagen de la tarjeta SD).

◆◆◇ Análisis en Android

Datos de interés – Caché del teclado

- Android guarda en un **Content Provider** las palabras seleccionadas por el usuario como parte del sistema predictivo del teclado:
/data/data/com.android.providers.userdictionary/database/user_dict.db
- Las palabras introducidas en campos de contraseñas no se guardan en este diccionario.
- No contiene marcas de tiempo.



Datos de interés – Contraseñas y configuraciones

- En caso de que se haya configurado el código de bloqueo se encuentra en:
 - */data/system/gesture.key*, si se trata de un patrón de bloqueo:
 - Cada punto del patrón es asignado un número (empezando por el 0 en el punto más alto del lado izquierdo).
 - Se hace un resumen de la concatenación del valor en byte del patrón (ej: 01254).
 - Dado el "pequeño" número de combinaciones posibles se puede obtener fácilmente a través de la generación de todas las combinaciones en SHA1.
 - <http://forensics.spreitzenbarth.de/2012/02/28/cracking-the-pattern-lock-on-android/>
 - */data/system/password.key*, si se trata de un código numérico:
 - Almacena el resumen del código numérico resumido junto con una semilla en SHA y MD5 (ambos concatenados).
 - El lugar de almacenamiento de la semilla depende de la versión de Android:
 - */data/data/com.android.providers.settings/databases/settings.db*
 - */data/system/locksettings.db*
 - En ambos ficheros se guarda en *lockscreen.password_salt*.
 - Una vez obtenida la semilla y el hash final, se puede realizar un ataque de diccionario para obtener el PIN o *password* original.
 - <http://forensics.spreitzenbarth.de/2015/08/12/breaking-the-screenlock-a-short-update/>

Redes wifi conectadas

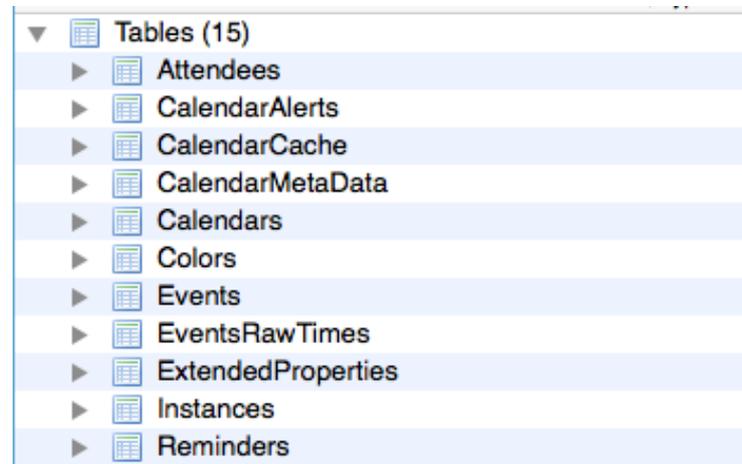
- Los datos de las redes wifi a las que ha tenido acceso el dispositivo se encuentran en ***/data/misc/wifi***
- El fichero `wpa_supplicant.conf` almacena la información relativa a la configuración de los puntos de acceso WiFi.
- Además de la lista de últimas redes wifi a las que se ha conectado el dispositivo, también se pueden encontrar las contraseñas de acceso a las mismas. Entre estos datos se pueden encontrar claves de acceso a entornos corporativos.

```
root@condor_umts:/data/misc/wifi # cat wpa
wpa_supplicant.conf wpa_supplicant/
t wpa_supplicant.conf
mot_wpa_conf_version=3
ctrl_interface=/data/misc/wifi/sockets
disable_scan_offload=1
driver_param=use_p2p_group_interface=1
update_config=1
device_name=condor_retgb
manufacturer=motorola
model_name=XT1021
model_number=XT1021
serial_number=ZX1B23QDHQ
device_type=10-0050F204-5
config_methods=physical_display virtual_push_button
p2p_disabled=1
p2p_no_group_iface=1
country=US

network={
  ssid="SK 3BA"
  psk="
  key_mgmt=WPA-PSK
  priority=1
}
```

Datos de interés – Calendario

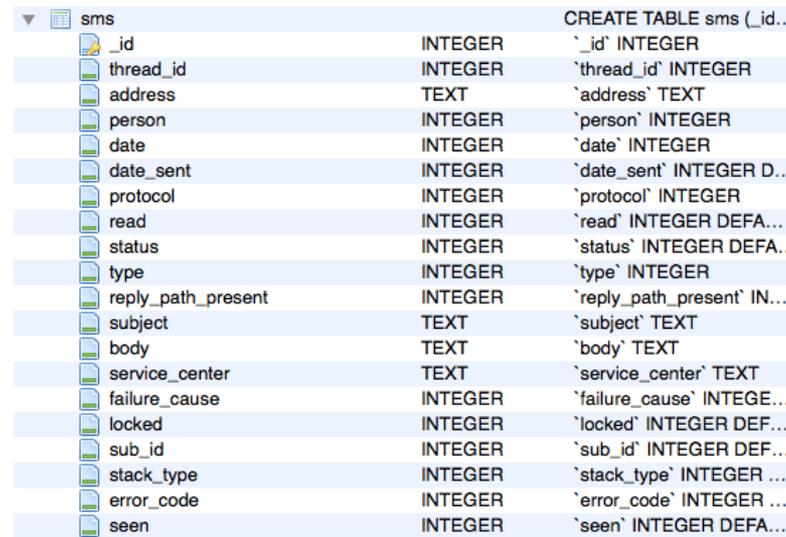
- La agenda de eventos del sistema se almacenan en un *Content Provider* localizado en: `/data/data/com.android.providers.calendar/databases/calendar.db`
- Esta base de datos incluye información sobre eventos, sus asistentes, recordatorios y alertas.



- La información de esta tabla puede ser de especial interés pues, en general, contiene el calendario que el usuario tiene sincronizado con su cuenta de Google.

Datos de interés – Mensajes de texto

- Los mensajes de texto se almacenan en un Content Provider localizado en:
 - `/data/data/com.android.providers.telephony/databases/mmssms.db`
- Los mensajes de texto se almacenan dentro de la tabla SMS.



Column Name	Column Type	Column Definition
_id	INTEGER	`_id` INTEGER
thread_id	INTEGER	`thread_id` INTEGER
address	TEXT	`address` TEXT
person	INTEGER	`person` INTEGER
date	INTEGER	`date` INTEGER
date_sent	INTEGER	`date_sent` INTEGER D..
protocol	INTEGER	`protocol` INTEGER
read	INTEGER	`read` INTEGER DEFA...
status	INTEGER	`status` INTEGER DEFA..
type	INTEGER	`type` INTEGER
reply_path_present	INTEGER	`reply_path_present` IN...
subject	TEXT	`subject` TEXT
body	TEXT	`body` TEXT
service_center	TEXT	`service_center` TEXT
failure_cause	INTEGER	`failure_cause` INTEGE...
locked	INTEGER	`locked` INTEGER DEF...
sub_id	INTEGER	`sub_id` INTEGER DEF...
stack_type	INTEGER	`stack_type` INTEGER ...
error_code	INTEGER	`error_code` INTEGER ...
seen	INTEGER	`seen` INTEGER DEFA...

- El *provider* también ofrece otras tablas para acceder a los mensajes por hilos (*threads*).
- Las URI de los MMS se encuentran en la tabla *attachments*.

Datos de interés – Navegador

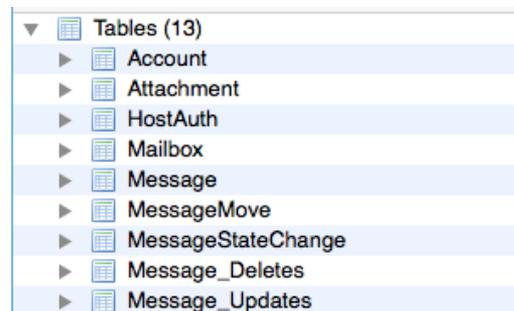
- En Android el navegador por defecto depende del fabricante y versión del sistema operativo:
 - */data/data/com.android.chrome* para Chrome:
 - Los datos de interés se almacenan la carpeta *app_chrome/Default/*
 - Ficheros de interés en la misma carpeta :
 - *Login Data*: Fichero Sqlite con credenciales de acceso a páginas web.
 - *Cookies*: Fichero Sqlite con las cookies de los sitios visitados.
 - *Bookmarks*: Fichero Json con los favoritos guardados en el navegador.
 - *History*: Fichero Sqlite con el historial de páginas visitadas.
 - *Web Data*: Fichero Sqlite con información de auto-relleno de formularios.
 - */data/data/com.android.browser* para navegadores por defecto que no sean Chrome:
 - La base de datos de contraseñas guardadas se almacena en:
/data/data/com.android.browser/databases/webview.db

Datos de interés – Contactos y llamadas

- Los contactos y llamadas del dispositivo se almacenan en el **ContentProvider** localizado en:
/data/data/com.android.providers.contacts/
- Dependiendo del fabricante y operadora, la localización puede variar.
- La base de datos que almacena esta información se encuentra en **databases/contacts2.db**
 - Los contactos se almacenan en las tablas *contacts*, *raw_contacts* y *deleted_contacts*.
 - Las llamadas recientes se almacenan en la tabla **call**.
- Además, la carpeta **photos** almacena todas las fotos asociadas a contactos en el teléfono.
- La lista de llamadas *recientes* del dispositivo se encuentra en el mismo archivo **databases/contacts2.db**, en la tabla **call**.

Datos de interés – Correo electrónico

- Al igual que en el caso del navegador, dependerá del tipo de cuenta que tenga configurada el usuario.
- Para las cuentas de Gmail, una base de datos por cuenta:
 - `/data/data/com.google.android.gm/databases/mailstore.[CUENTA].db`
 - Incluye tablas como:
 - `conversations`
 - `attachments`
 - `messages`
- Las demás cuentas de correo se pueden localizar en el *Content Provider*.
 - `/data/data/com.android.email/databases/EmailProvider.db`



◆◆◆ Análisis en Android

Datos de interés – Datos geográficos

- Los datos geográficos en Android se almacenan principalmente en la aplicación de Google Maps.
- Su carpeta se encuentra en `/data/data/com.google.android.apps.maps`
- Dentro de la carpeta hay varios datos de interés:
 - La carpeta cache almacena imágenes con partes de los mapas y Street View vistos previamente.
 - En el fichero `databases/gmm_myplaces.db` se almacenan los lugares que el usuario ha marcado como favoritos en la aplicación.





Análisis en iOS

Generalidades

- En general, la información analizada en un dispositivo iOS se va a encontrar en forma de:
 - Ficheros *plist*.
 - Ficheros XML que almacenan pares clave-valor.
 - Las preferencias de las aplicaciones almacenadas mediante *NSUserDefaults* se almacenan con este formato.
 - Bases de datos Sqlite con diferentes exten
 - Ficheros de texto en claro.
 - Ficheros binarios: imágenes.
 - Ficheros de texto plano.



Sistema de ficheros

- El sistema de ficheros de iOS (HFS+) ofrece la fecha de última modificación, acceso, cambio y creación. Estas fechas se ofrecen en segundos transcurridos desde el 1 de enero de 2001.
- El sistema está dividido en dos particiones:
 - **Partición del *firmware***: Sólo lectura a excepción de los procesos de actualización. Almacena los ficheros del sistema y aplicaciones del sistema operativo.
 - **Partición del usuario**: Almacena las aplicaciones y datos que se generan durante el uso del teléfono.
- A partir del iPhone 3GS, todos los dispositivos iOS incluyen por defecto un motor AES que cifra los datos almacenados en la memoria flash, por lo que la lectura física del dispositivo no es de utilidad a no ser que se posea la clave de cifrado.

Directorios de interés – Aplicaciones del sistema

- Todos los datos de las aplicaciones instaladas por defecto son guardados en: */private/var/mobile/Library*

▶ Accounts	-- 02/06/2014, 19:46
▶ AddressBook	-- 02/06/2014, 19:47
▶ adi	-- 31/01/2016, 21:59
▶ AggregateDictionary	-- 28/12/2015, 19:50
▶ ApplePushService	-- 02/06/2014, 19:47
▶ Application Support	-- 28/12/2015, 19:49
▶ ApplicationSync	-- Today, 00:27
▶ Assets	-- 01/02/2016, 03:22
▶ BackBoard	-- Today, 22:37
▶ BulletinBoard	-- 01/02/2016, 01:41
▶ Caches	-- Today, 22:32
▶ Calendar	-- 28/12/2015, 19:49
▶ Carrier Bundle.bundle	-- 28/12/2015, 19:51
▶ CarrierDefault.bundle	-- 02/06/2014, 19:46
▶ com.apple.itunesstored	-- Today, 00:27
▶ com.apple.nsnetworkd	-- 04/02/2016, 20:39
▶ ConfigurationProfiles	-- Today, 00:13
▶ ConfigurationProfilesAp...essibilityParameters.plist	181 B 02/06/2014, 19:46
▶ Cookies	-- Today, 00:13
▶ Cydia	-- 28/12/2015, 20:18
▶ DataAccess	-- 13/01/2016, 21:08
▶ Duet	-- 28/12/2015, 19:50
▶ FairPlay	-- 28/12/2015, 19:50
▶ IdentityServices	-- 02/06/2014, 19:47
▶ Keyboard	-- 04/02/2016, 20:40
▶ Logs	-- Today, 00:01
▶ Mail	-- 01/02/2016, 01:42

Directorios de interés – Aplicaciones de terceros

- Las aplicaciones de terceros se almacenan en: `/private/var/mobile/Applications`

▶  1B79EF4A-4F35-4A80-9E47-487743AC1CD3	-- 02/06/2014, 19:47
▶  6CD73469-98F1-4FB9-BE24-6FE273E4567E	-- 02/06/2014, 19:47
▶  303D7F2A-BB68-4640-91EB-2676F1739F42	-- 02/06/2014, 19:47
▶  592AD005-2D16-4968-9406-2AC5015A3FFF	-- Today, 00:15
▶  631FFD33-5D49-4E18-86F9-09C4E632F2DE	-- 08/02/2016, 13:29
▶  864EB949-E1AD-4039-8C17-158D16150EAF	-- 02/06/2014, 19:46
▶  1322E7DE-C499-4185-B986-8E83E7440AFC	-- 31/01/2016, 22:05
▶  64653523-6D05-4D5E-89B4-71417F51B82A	-- 02/06/2014, 19:47
▶  A5FEC033-54E7-4CBF-8A11-E066F8AC6B05	-- 08/02/2016, 13:29
▶  A35FBD93-B22E-42E5-8996-6138D66CD711	-- 02/06/2014, 19:47
▶  AB3718E2-B24B-4841-A3DD-9FC01DFBF56F	-- 02/06/2014, 19:46
▶  AE326639-4687-476B-B0E1-C2FF684E2D99	-- 31/01/2016, 21:53
▶  AFE689B8-1EB8-4718-AB91-6AF6772024A9	-- 02/06/2014, 19:46
▶  CCB0CA51-5230-4FFF-A12E-C4BCF06BFF0A	-- 02/06/2014, 19:46
▶  F212F15B-AB35-438F-A884-3C20FB206C27	-- 31/01/2016, 23:25

- Cada aplicación es identificada con un UUID de 32 caracteres (el mismo para la misma aplicación en diferentes dispositivos).

Estructura de la *sandbox* de una aplicación

- Cada aplicación contiene como mínimo los siguientes directorios:
 - **Documents**: Almacena los archivos creados y utilizados por la aplicación.
 - **Library**: Almacena ficheros de configuración creados mediante API de iOS y ficheros de caché.
 - **tmp**: Ficheros temporales que se crean durante la ejecución de una aplicación.

▼	1B79EF4A-4F35-4A80-9E47-487743AC1CD3	-- 02/06/2014, 19:47
▶	Documents	-- 02/06/2014, 19:47
▶	Library	-- 02/06/2014, 19:47
▶	tmp	-- 02/06/2014, 19:47
▶	Web.app	-- 02/06/2014, 19:47
▼	6CD73469-98F1-4FB9-BE24-6FE273E4567E	-- 02/06/2014, 19:47
▶	Documents	-- 02/06/2014, 19:47
▶	Library	-- 02/06/2014, 19:47
▶	StoreKitUIService.app	-- 02/06/2014, 19:47
▶	tmp	-- 02/06/2014, 19:47

- Como se comprobó durante el análisis de seguridad de una aplicación, es posible que se guarden datos sensibles (credenciales, etc.) en estas carpetas.

Datos de interés – Fotografías

- Las fotos del dispositivo se encuentran almacenadas en el directorio: *private/var/mobile/media/DCIM*

▼ 100APPLE	-- Today, 22:56
IMG_0001.PNG	57.1 KB 31/01/2016, 20:52
IMG_0002.JPG	1.5 MB Today, 22:55
IMG_0003.JPG	1.8 MB Today, 22:56

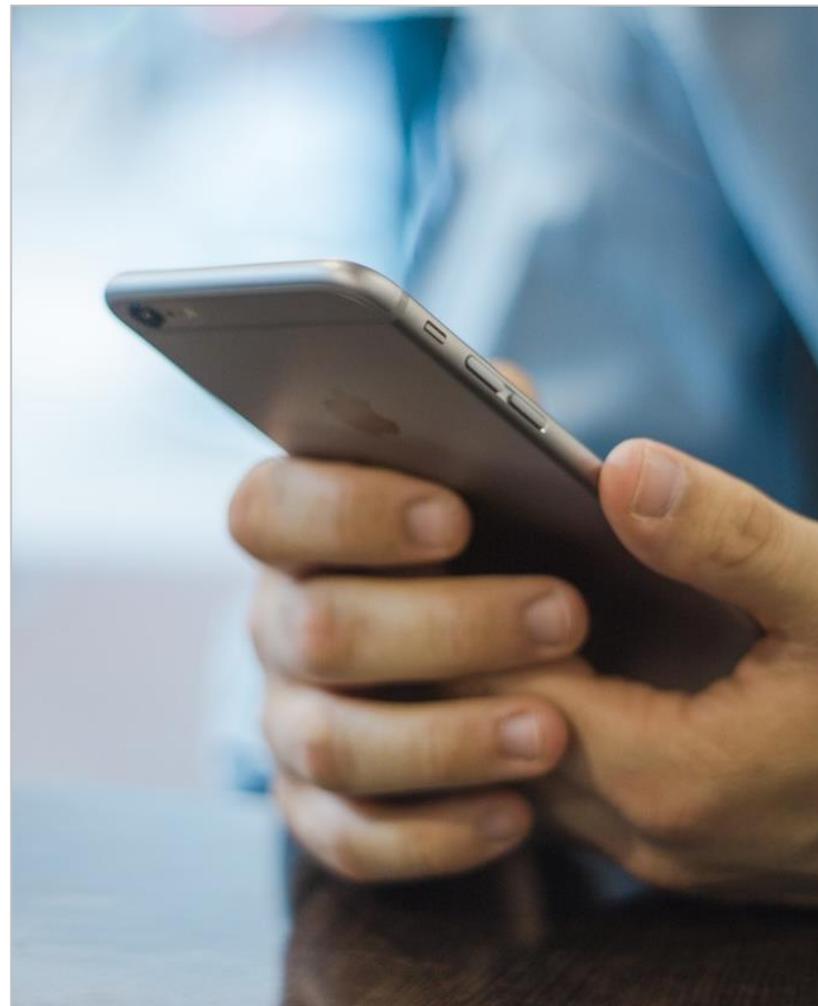
- Dentro de ese directorio, la carpeta 100Apple almacena las fotos tomadas con el propio dispositivo.
- Las fotografías tomadas son nombradas con números consecutivos. Si falta un número de la secuencia, se habrá borrado del teléfono.
- Las capturas de pantalla se encuentran en la misma carpeta pero en formato PNG.
- Los datos EXIF de las fotos pueden ser muy importantes de cara al análisis.

IMG_0001.PNG	57.1 KB 31/01/2016, 20:52
IMG_0002.JPG	1.5 MB Today, 22:55
IMG_0003.JPG	1.8 MB Today, 22:56
IMG_0004.PNG	1.0 MB Today, 23:00

◆◆◇ Análisis en iOS

Datos de interés – Caché del teclado

- iOS guarda un fichero con palabras escritas por el usuario durante el uso normal del dispositivo
/private/var/mobile/Library/Keyboard/dynamic-text.dat
- Recoge palabras tecleadas en cualquier aplicación que reciba input del teclado.
- Las palabras introducidas en campos de contraseñas no se guardan en este diccionario.
- No contiene marcas de tiempo.
- El fichero *UserDictionary.sqlite* almacena las correcciones del usuario hechas al diccionario del sistema.

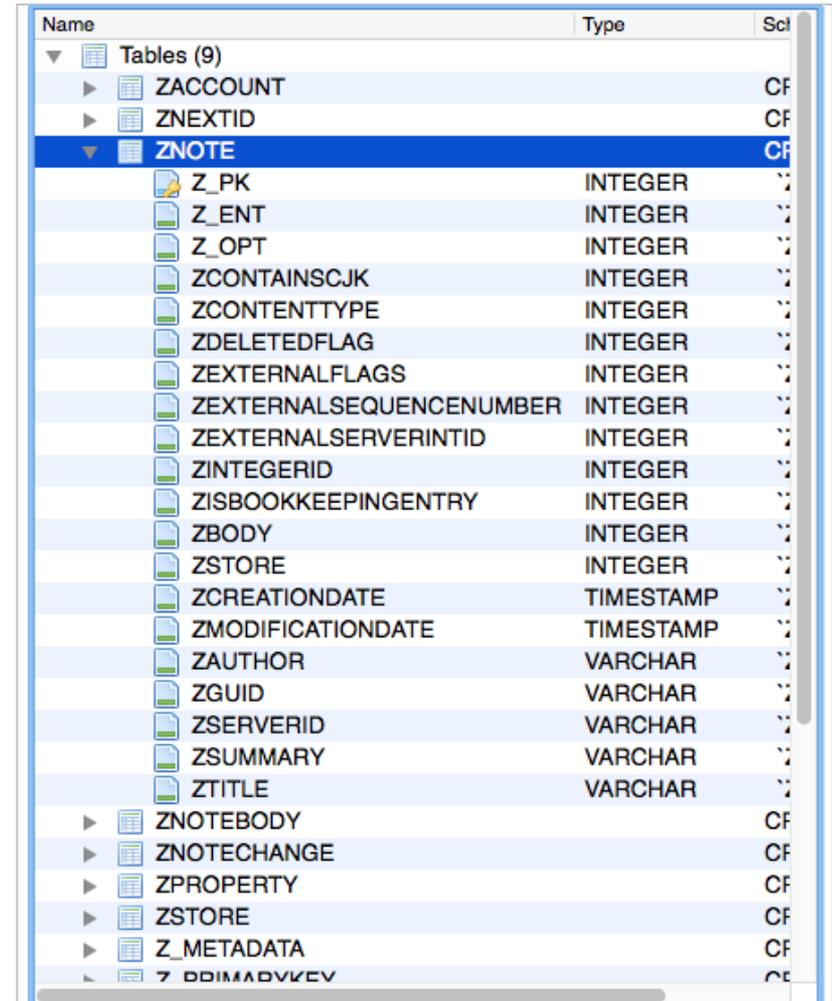


Datos de interés – Keychain

- Las aplicaciones de iOS pueden utilizar el servicio de Keychain para almacenar contraseñas en el dispositivo.
- Dentro de este fichero se pueden encontrar diferentes tablas genp, cert, inet, keys que contienen información sobre contraseñas que han sido utilizadas alguna vez por el dispositivo.
- En muchos casos, la información almacenada en este fichero se encuentra cifrada por lo que es necesaria la utilización de herramientas forenses como iPhone Password Breaker de Elcomsoft para descifrar los archivos.

Datos de interés – Notas

- Los datos existentes en la aplicación de notas (y otras similares en el sistema) pueden ser de gran utilidad durante el análisis forense.
- Los datos de la aplicación de notas se encuentran en:
 - `/private/var/mobile/Library/Notes/notes.sqlite`
- Las tablas del fichero sqlite contienen información como fecha de creación y última modificación de la nota.
- Desde la versión 9.3 de iOS las notas pueden cifrarse utilizando el Keychain y el código de bloqueo del usuario.



Name	Type	Sql
Tables (9)		
▶ ZACCOUNT		CF
▶ ZNEXTID		CF
▼ ZNOTE		CF
Z_PK	INTEGER	PK
Z_ENT	INTEGER	
Z_OPT	INTEGER	
ZCONTAINSCJK	INTEGER	
ZCONTENTTYPE	INTEGER	
ZDELETEDFLAG	INTEGER	
ZEXTERNALFLAGS	INTEGER	
ZEXTERNALSEQUENCENUMBER	INTEGER	
ZEXTERNALSERVERINTID	INTEGER	
ZINTEGERID	INTEGER	
ZISBOOKKEEPINGENTRY	INTEGER	
ZBODY	INTEGER	
ZSTORE	INTEGER	
ZCREATIONDATE	TIMESTAMP	
ZMODIFICATIONDATE	TIMESTAMP	
ZAUTHOR	VARCHAR	
ZGUID	VARCHAR	
ZSERVERID	VARCHAR	
ZSUMMARY	VARCHAR	
ZTITLE	VARCHAR	
▶ ZNOTEBODY		CF
▶ ZNOTECHANGE		CF
▶ ZPROPERTY		CF
▶ ZSTORE		CF
▶ Z_METADATA		CF
7 DDIMADVKEV		CF

Datos de interés – Mensajes de texto

- A diferencia de los correos electrónicos y otros medios de mensajería corporativos, los SMS sólo están accesibles en el dispositivo.
- En iOS, la base de datos de mensaje se encuentra en:
 - `/private/var/mobile/Library/SMS/sms.db`
- Las tablas más relevantes de este fichero:
 - `messages` Contiene los mensajes enviados y recibidos.
 - `msg_pieces` Contiene los elementos enviados junto a los mensajes (vídeos y fotografías).
- Los mensajes de iMessage se guardan en la misma base de datos. Los adjuntos se guardan en la carpeta *Attachments* del directorio SMS.

◆◆◆ Análisis en iOS

Datos de interés – Cookies

- Se almacenan en un fichero binario en:
 - `/private/var/mobile/Library/Cookies/Cookies.binarycookies`
- Compuesto de una cabecera y *cookies* separadas en páginas.

Campo	Tamaño	Descripción
Cabecera	4 bytes	“COOK”
N. Páginas	4 bytes	En <i>Little Endian</i>
Tamaño de la página	4 bytes	En <i>Little Endian</i>
Página	Variable	<i>Cookies</i>
Cola	8 bytes	<i>Checksum</i> del contenido del fichero

- Necesita un programa especializado o un visor hexadecimal.

◆◆◆ Análisis en iOS

Datos de interés – Búsquedas y favoritos

- Se almacenan en la carpeta:
/private/var/mobile/Library/Safari
- El fichero de favoritos es una base de datos SQLite: *Bookmarks.db*
- Las búsquedas recientes se almacenan en un fichero *plist*:
SearchEngines.plist



Datos de interés – Contactos y llamadas

- Los contactos del teléfono se almacenan en:
 - */private/var/mobile/Library/AddressBook*
- Dos tablas son de especial interés:
 - *ABPerson*: Almacena nombres y detalles personales del contacto.
 - *ABMultiValue*: Almacena los teléfonos y direcciones de correo y otras cuentas de la persona. Está relacionada directamente mediante una Foreign Key con los valores de *ABPerson*.
- El historial de llamadas se almacena en:
 - */private/var/Library/CallHistory/call_history.db*
- Incluye el número de teléfono, la fecha y duración de la llamada y la referencia al contacto.
- También indica si la llamada es entrante o saliente.

Datos de interés – Datos geográficos

- En iOS el demonio de localización del sistema almacena la información relativa a la localización en la carpeta:
 - `/private/var/root/Library/Caches/locationd`
- Dependiendo de la versión de iOS el contenido y ficheros utilizados en esta carpeta varían de nombre:
 - `consolidated.db`
 - `Cache_encryptedA.db`
- Estos ficheros almacenan información geográfica de varios aspectos del dispositivo incluyendo la localización de los últimos puntos wifi a los que se ha conectado, localización de celdas y últimas localizaciones solicitadas por las aplicaciones del dispositivo.

Otros datos de interés

- El directorio *Preferences* almacena varios ficheros de información de interés:
 - *com.apple.accountsettings.plist*: Información de las cuentas de correo.
 - *com.apple.AppStore.plist*: Última búsqueda de aplicaciones en la AppStore.
 - *com.apple.facetime.plist*: Información sobre el uso de Facetime.
- Los buzones de voz se encuentran en el fichero */mobile/Library/Voicemail/voicemail.db*



Otros datos de interés – Copias de seguridad

- Cada copia de seguridad realizada por iTunes se guarda en una carpeta con el UDID del dispositivo.
- Las copias diferenciales se guardan en carpetas con el mismo UDID y la fecha.
- Las carpetas de seguridad de iTunes incluyen los siguientes ficheros de interés:
 - *Status.plist*: Fecha e información sobre del *backup* realizado.
 - *Manifest.plist*: incluye información de las aplicaciones de terceros instaladas y datos de configuración de las aplicaciones del sistema.
 - *Info.plist*: información del dispositivo como el IMEI, serial de la SIM, etc.

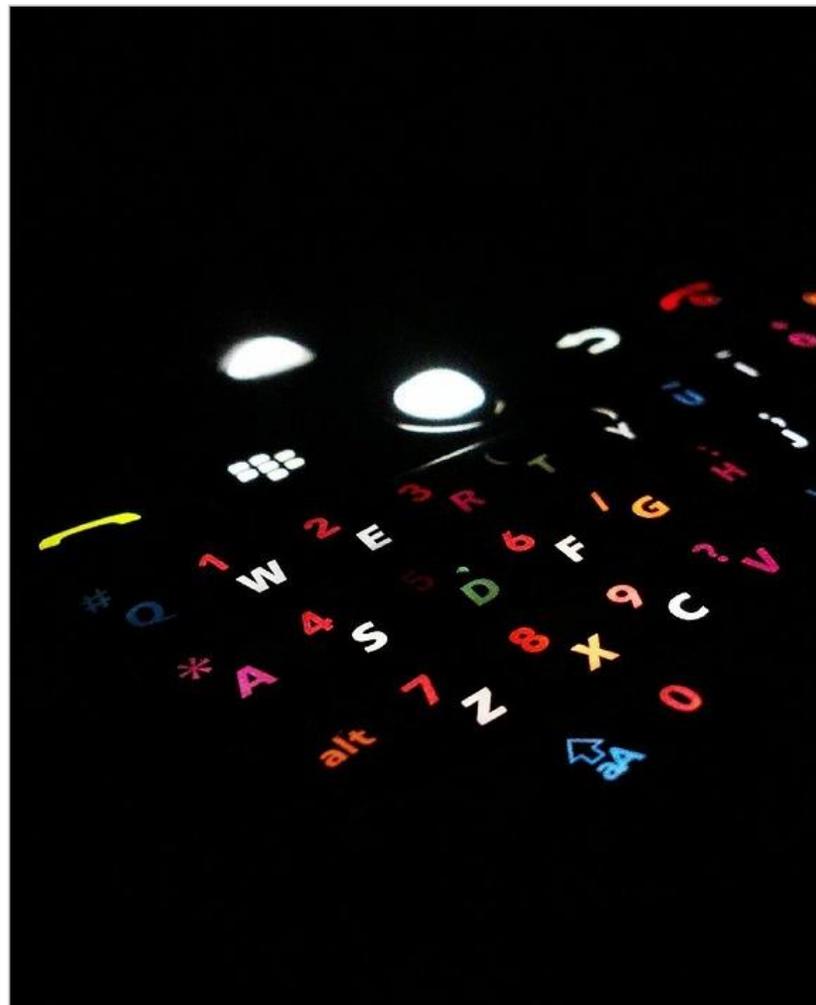


Análisis de BlackBerry

◆◆◆ Análisis en BlackBerry

Generalidades

- En general, la información analizada en un dispositivo BlackBerry 10 se va a encontrar en forma de:
 - Bases de datos Sqlite con extensiones .db y .dat.
 - Ficheros XML.
 - Ficheros .ini.
 - Ficheros binarios (.bin): Imágenes.
 - Ficheros de texto plano y otros ficheros de configuración (.conf).



◆◆◆ Análisis en BlackBerry

Ficheros

- En general, y debido a las restricciones de seguridad existentes en BlackBerry 10, el análisis se realiza siempre sobre una copia de seguridad del dispositivo
- La copia de seguridad de un dispositivo BlackBerry 10 contiene tres archivos tipo tar:
 - **App:** Contiene las aplicaciones instaladas en el dispositivo.
 - **Media:** Contiene los datos que se han generado durante el uso del dispositivo (incluyendo los datos generados por las aplicaciones).
 - **Settings:** Incluye los datos de configuración del dispositivo, aplicaciones y las cuentas.



Directorios de interés – Aplicaciones

- Todas las aplicaciones del sistema se encuentran almacenadas en la carpeta `app`.
- Las aplicaciones pueden tener dos tipos de nombre:
 - `com.[nombre app].gYABG[caracteres alfanuméricos]`
 - `sys.[nombre app].gYABG[caracteres alfanuméricos]`
- El prefijo `com` se utiliza para aplicaciones de terceros y el prefijo `sys` para aplicaciones del sistema.
- Al final del nombre se añaden un conjunto de caracteres alfanuméricos aleatorios.
- Los datos de ciertas aplicaciones del sistema como el calendario, contactos, etc. se encuentran localizados en:
 - `/settings/accounts/1000/sysdata/pim`
 - Siendo `pim` un acrónimo de *Personal Information Manager*.

Datos de interés – Fotografías

- Las fotografías capturadas por la cámara del dispositivo se almacenan en `/media/camera` si no hay tarjeta SD insertada. En caso de haber tarjeta, las fotos pasan a la carpeta `/sdcard/camera` de la tarjeta. Los vídeos se almacenan de la misma manera, pero en la carpeta `videos`.
- Las fotografías almacenadas por otras aplicaciones se almacenan en la carpeta correspondiente dentro de la carpeta `media`.
- Las capturas de pantalla siempre se almacenan en el dispositivo en la carpeta `/media/camera` en formato PNG y sin información EXIF.

◆◆◇ Análisis en BlackBerry

Datos de interés

- El calendario del dispositivo se almacena en:
 - */settings/accounts/1000/sysdata/pim/db/1-pm.db*
 - Los eventos se guardan en la tabla CalendarEvent. Las marcas de tiempo se almacenan en GMT.
- Los contactos del dispositivo se almacenan en:
 - */settings/accounts/1000/sysdata/pim/db/2-pm.db*
- El historial de llamadas se almacena en:
 - */settings/accounts/1000/sysdata/pim/db/8-pm.db*
 - El historial se guarda en las tabla Call y CallDetail. Las marcas de tiempo se almacenan en GMT.
- Los recordatorios del dispositivo se almacenan en:
 - */settings/accounts/1000/sysdata/pim/db/18-pm.db*

Datos de interés – Mensajes de texto

- Los mensajes se almacenan en:
 - */settings/var/db/text_messagingsettings/messages.db*
- El contenido de los mensajes se puede encontrar en la tabla Attachements.
- Para saber si un mensaje es saliente o entrante hay que inspeccionar el campo inbound de la tabla Messages. El valor 0 indica enviado y el valor 1 indica recibido.
- La base de datos de BlackBerry Messenger se encuentra en:
 - */app/sys.bbm.gYABgLOJBR2Vz7FzS.kdgJchuag/appdata/data/master.db*
- Esta base de datos también registra las llamadas de voz y vídeo realizadas a través de BMM (sólo se registra el evento).

◆◆◇ Análisis en BlackBerry

Datos de interés – BlackBerry Hub

- El BlackBerry Hub centraliza la información de llamadas, mensajes en el buzón de voz, correos, sms, feeds de redes sociales, eventos de calendarios y notificaciones.
- Si bien la información existente en el hub puede ser accedida a través de otros medios, su utilización en el análisis es importante, pues ofrece una línea de tiempo de todos los eventos sucedidos en el dispositivo.
- Su base de datos se encuentra en:
/sys.pim.messages.gYABgJ8jn83Ok_NEWYpIPYozt5w/appdata/data/unfied.db
- En esta base de datos hay una entrada por evento que incluye:
 - El tipo de aplicación o evento que se generó (aplicación, calendario, notificación, etc.).
 - El texto que se muestra en el hub.
 - La fecha del evento en segundos desde el 1 de enero de 1970.

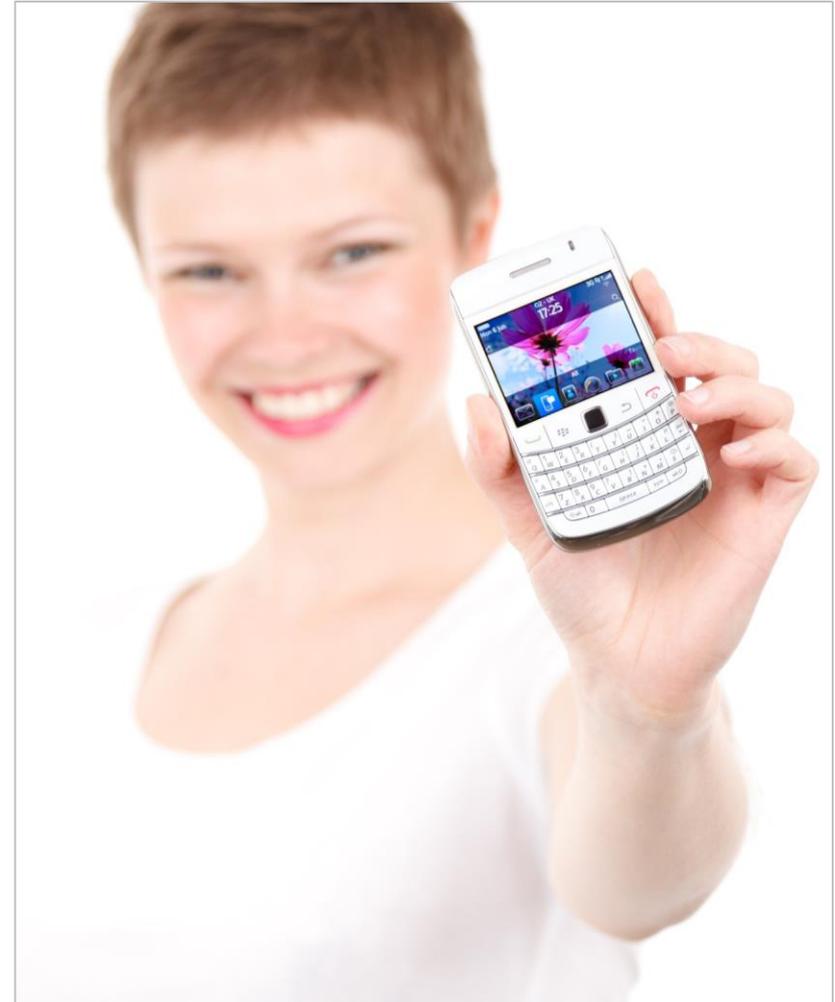
Datos de interés – Historial y favoritos

- Los ficheros de importancia relativos al navegador se almacenan en:
 - `/app/sys.browser.gYABgJYFHAzbeFMPCCPYWBtHAm0/appdata/data/chrome/databases/local-0`
- El fichero Databases.db apunta a los ficheros (varían dependiendo del modelo) que contienen el historial y los favoritos del navegador.
- En cada uno de esos ficheros hay dos tablas de interés:
 - *history*: incluye una entrada por cada página que esté en el historial de navegación. Las URL son dadas con identificadores.
 - *urls*: mapea las URL a los identificadores mencionados en la anterior tabla. Incluye un campo con la última fecha en la que se visitó la URL.

◆◆◆ Análisis en BlackBerry

Datos de interés – Caché de navegación y cookies

- Otros datos de importancia en relación al uso del navegador se pueden encontrar en:
 - `/app/sys.browser.gYABgJYFHAzbeFM PCCpYWBtHAm0/appdata/data/webviews`
- El fichero `cookieCollection.db` almacena las cookies de navegación.
- La carpeta `cache` almacena archivos temporales de Internet.
- La carpeta `databases` almacena las bases de datos específicas de cada sitio que ha requerido utilizar almacenamiento a través de HTML 5.



Análisis de Windows Phone



◆◆◇ Análisis en Windows Phone

Generalidades

- El poco tiempo del sistema operativo Windows 10 Mobile en el mercado y su poca cuota de mercado hacen que este sistema operativo no esté lo suficientemente documentado aún dentro del ámbito de la informática forense.
- En cualquier caso, su estructura guarda múltiples similitudes con la estructura general de los sistemas Windows, y más en particular con el sistema Windows 10 para escritorio:
 - Esto incluye el uso de un registro para el almacenamiento de configuraciones e información del sistema.
 - El uso de particiones NFTS.
 - La estructura de directorios del sistema.
- A continuación se pasan a enumerar los artefactos y datos de interés documentados hasta la fecha para sistemas Windows Phone 8.

◆◆◇ Análisis en Windows Phone

Datos de interés – Fotografías

- Las fotografías y vídeos grabados por la cámara se encuentran almacenados en el directorio:
 - *Users\Public\Pictures\CameraRoll*
- El formato de las fotografías es:
 - *WP_YYYYMMDD_###.jpg*
 - Siendo
 - WP el acrónimo de Windows Phone.
 - YYYYMMDD el año (Y), mes (M) y día (D) en el que fue tomada la foto.
 - ### es un número secuencial que se autoincrementa.
- En el caso de que el teléfono tenga una tarjeta SD instalada, las fotografías también podrán encontrarse, en el mismo formato, en la tarjeta SD.
- Las fotografías guardadas desde otras fuentes se encuentran almacenadas en:
 - *Users\Public\Pictures\SavedPictures*

◆◆◇ Análisis en Windows Phone

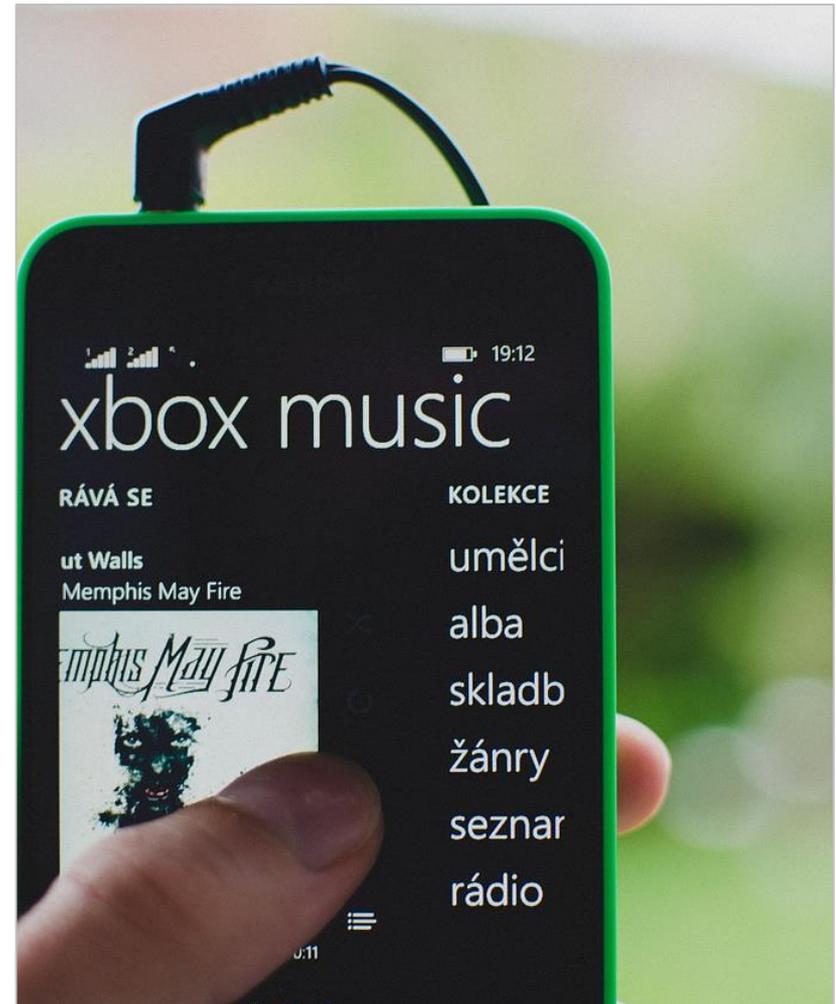
Datos de interés – Historial de llamadas y mensajes

- El historial de llamadas se encuentra almacenado en un fichero sin extensión:
 - *Users\WPCOMMSERVICES\APPDATA\Local\UserData\phone*
 - Todas las entradas de llamadas existentes en ese fichero terminan con el *String* *B1776703-738E-437D-B891- 44555CEB6669*.
- Los mensajes SMS se localizan en:
 - *Users\WPCOMMSERVICES\APPDATA\Local\Unistore\store.vol*
- Los adjuntos a los mensajes MMS se pueden localizar en:
 - *SharedData\Comms\Unistore\Data*
 - Este directorio almacena imágenes, texto y otros archivos multimedia con extensión *.dat* (la codificación de la información respeta el formato original, solo se modifica la extensión).

◆◆◆ Análisis en Windows Phone

Datos de interés – Navegación web

- El historial del navegador y las *cookies* se almacenan en:
 - `Users\DefApps\APPDATA\INERNETE XPLORER\NetCache\`
- A su vez el historial que aún no ha sido consolidado en el archivo anterior se almacena en:
 - `Users\DefApps\APPDATA\Local\Microsoft\Windows\WebCache\01.dat`
- Los favoritos del sistema se almacenan en:
 - `SharedData\InternetExplorer\Favorites`



◆◆◇ Análisis en Windows Phone

Datos de interés – Notas

- Las notas del sistema se almacenan dentro de la aplicación One Note, incluida en la suite Office.
- El directorio de instalación de la aplicación y sus consiguientes datos se puede encontrar en:
 - *Users\DefApps\APPDATA\OFFICE\Temp\OneNote*
- Adicionalmente, la caché de aplicaciones también puede almacenar información introducida que aún no ha sido almacenada en la parte persistente de la aplicación:
 - *Users\DefApps\APPDATA\OFFICE\Temp\OneNote\OneNoteRuntimeCache\OneNoteRuntimeCache_Files*

◆◆◇ Análisis en Windows Phone

Datos de interés – Caché del teclado

- La caché del teclado y los elementos para el relleno automático de formularios se encuentran almacenados en la carpeta:
 - *SharedData\Input\nutral*
- En el interior de esta carpeta se pueden encontrar dos archivos:
 - **ihds.dat**: Almacena las palabras utilizadas por el usuario a través del teclado en cualquiera de las aplicaciones del teléfono.
 - **livehds.dat**: Almacena datos introducidos previamente en formularios para su auto-relleno posterior.



Laboratorio de análisis



Introducción al laboratorio

Análisis de una imagen de un dispositivo Android

- Durante este laboratorio se va a completar el análisis forense de una imagen Android.
- El ejercicio de laboratorio se basará en una simulación en la que deberás asumir el papel de investigador forense en un caso ficticio.
- **El objetivo final del análisis es redactar un informe forense que será discutido en el foro correspondiente.**
- La realización del laboratorio está dividida en tareas:
 - Al final de cada tarea, dispondrás de la solución a la misma para que puedas seguir con el ejercicio aún si tienes dificultades.
 - **Para mejorar tus opciones de aprendizaje, intenta realizar la tarea al completo antes de revisar su solución .**
- Es posible que durante tu análisis se encuentren más evidencias de las que se enumeran en las soluciones ofrecidas.



Dada la cantidad de evidencias que generan los dispositivos móviles esto es completamente normal. Las restricciones de tiempo y espacio del curso nos obligan a mostrarte sólo algunas de ellas en la solución. Te animamos a utilizar el foro para compartir aquellas que no están documentadas en esta solución

Preparación de Autopsy

- Durante la realización del laboratorio, utilizaremos Santoku Linux, por lo tanto te recomendamos que descargues todo el material necesario para la realización del mismo desde la propia máquina virtual de Santoku.
- Entre las herramientas que utilizaremos se encuentran:
 - Autopsy
 - Sqliteman
 - exiftool
- En el caso de Autopsy, existe un pequeño bug en la versión de Santoku que debemos subsanar antes de comenzar la práctica. Para ello sólo debes escribir en la consola lo siguiente:
 - > `sudo ln -s /usr/bin/icat /usr/bin/icat-sleuthkit`
 - > `sudo ln -s /usr/bin/ils /usr/bin/ils-sleuthkit`
 - Esto permite a sleuthkit utilizar *icat* e *ils* para el mostrado de información de los ficheros.

A close-up photograph of a person's hands writing on a document. The person is wearing a light blue button-down shirt. They are holding a dark blue pen with a silver clip and are in the process of writing on a white sheet of paper. The background is blurred, showing more of the person's shirt and the desk. A semi-transparent dark grey rectangular box is overlaid on the center of the image, containing the text "Presentación del caso" in white. The overall lighting is soft and professional.

Presentación del caso

◆◆◇ Presentación del caso

Escenario

- Debido a un soplo de un confidente a la policía, se conoce que unos delincuentes de habla hispana pueden estar preparando una serie de robos en la ciudad de Londres.
- Tras un primer robo en una de las joyerías más famosas de la ciudad, uno de los delincuentes de forma descuidada deja su cara descubierta y es captado por las videocámaras existentes en la ciudad. En el robo participan cuatro delincuentes.
- El seguimiento del sospechoso a través de las cámaras existentes por la ciudad permite a la policía identificarle en una casa, aparentando ser residencia actual.
- Tras una redada en el domicilio del presunto delincuente, se recupera un dispositivo Android que el sospechoso estaba utilizando en el momento de la redada.

◆◆◇ Presentación del caso

Estado del dispositivo

- El dispositivo incautado no tenía configurado ningún sistema de bloqueo y además estaba *rootead*o.
- El dispositivo no tenía insertada ninguna tarjeta SD.
- Aprovechando el estado actual del dispositivo, justo después de la incautación, un experto de la policía llevo a cabo las siguientes tareas:
 - Formatear una tarjeta SD de 8GB para la adquisición de datos forenses.
 - Conectar desde un equipo de análisis forense, a través de un cable USB al dispositivo incautado.
 - Utilizar `adb` y el comando `dd` para volcar el contenido físico de la partición de disco que ha sido montada en `/data` (partición de datos de usuario) a la tarjeta SD.
 - Extraer la imagen capturada desde la tarjeta SD al equipo del analista mediante el comando `adb pull`.
 - El hash MD5 de la imagen obtenida es `235fdf8cdba7584ac5c8a10fc9e11c56`.

◆◆◆ Presentación del caso

Enunciado

- La imagen obtenida ha sido enviada a nuestro laboratorio de análisis forense para el análisis.
- Se nos pide un informe forense de la imagen encontrada, que incluya:
 - Localizaciones de posibles futuros objetivos del grupo criminal.
 - Nombres o cualquier otro elemento identificativo de posibles cómplices del sospechoso.
 - Información adicional (nombres de cuentas, etc.) que, tras la obtención de la correspondiente orden judicial, pueda ofrecer más información sobre el sospechoso y sus actividades.



A close-up photograph of a microscope's objective lenses. The lenses are metallic and have various markings, including '10x/0.25', '20x/0.40', and '40x/0.65'. A semi-transparent grey box is overlaid on the center of the image, containing the text 'Creación del caso' in white. The background is dark and out of focus.

Creación del caso

◆◆◇ Creación del caso

Carga en Autopsy

- Durante la resolución de este ejercicio vamos a utilizar como herramienta principal Autopsy.
- Para lanzar Autopsy, en una consola de Santoku Linux escribimos (necesita ejecutarse como administrador en esta instalación).

```
> sudo autopsy
```

```
santoku@santoku-VirtualBox:~$ sudo autopsy
=====
                          Autopsy Forensic Browser
                          http://www.sleuthkit.org/autopsy/
                          ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: Mon Feb 15 13:23:09 2016
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

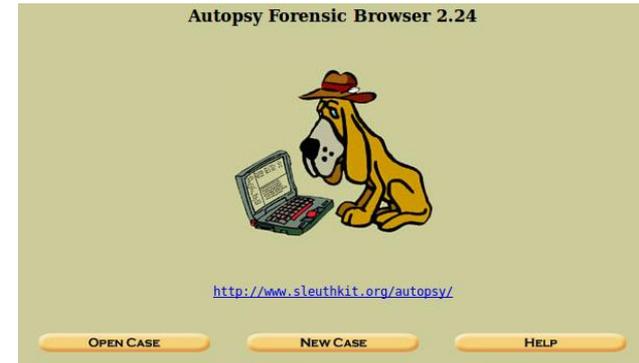
Keep this process running and use <ctrl-c> to exit
```

- Y abrimos el navegador y escribimos la dirección indicada.

◆◆◆ Creación del caso

Abriendo un nuevo caso

- En la ventana del navegador presionamos "New Case".
- Y rellenamos los datos del caso.



1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.

b.

c.

d.

e.

f.

g.

h.

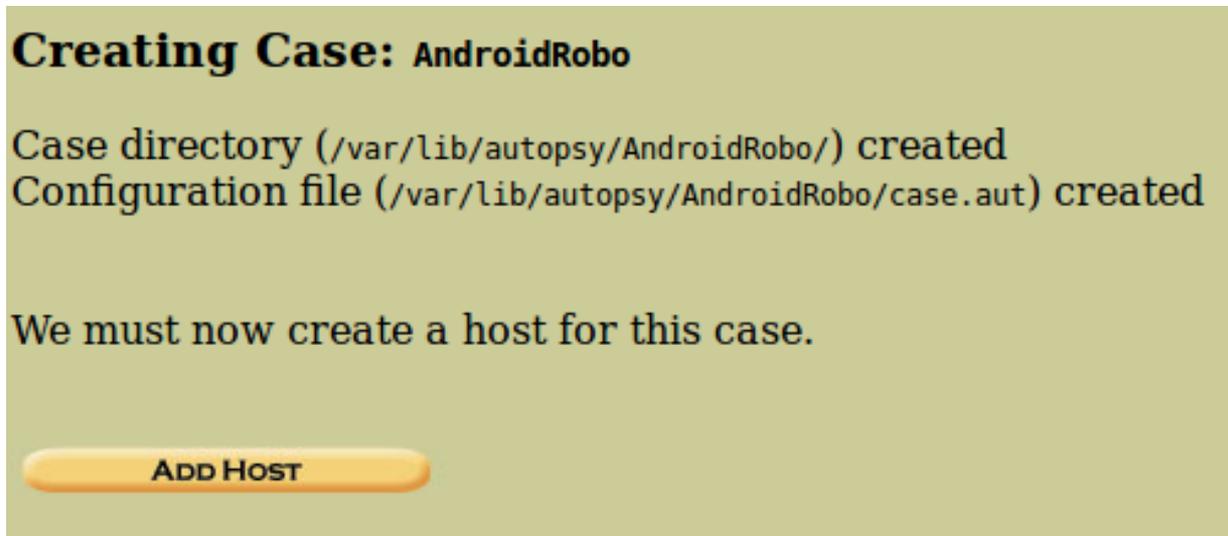
i.

j.

◆◆◆ Creación del caso

Añadiendo dispositivos

- Llegaremos a una ventana en la que se nos informa de los directorios de configuración y del caso.
- En este caso solo vamos a analizar un dispositivo así que presionamos “Add Host”.



Detalles del dispositivo

- Añadimos los detalles del dispositivo:

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST CANCEL HELP

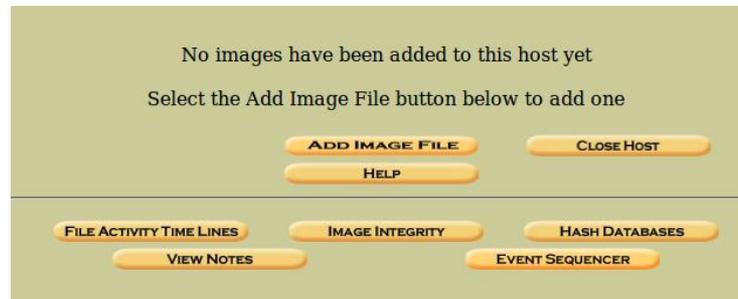
◆◆◆ Creación del caso

Añadiendo la imagen

- Seleccionamos “Add Image”:



- Y “Add Image File”:



◆◆◆ Creación del caso

Añadiendo la imagen

- Escribimos la localización del fichero en nuestro sistema de archivos.
- Como se especifico durante la descripción del caso, la imagen se trata de una partición del disco por lo que seleccionamos la opción correspondiente.
- Para no copiar o mover todo el fichero seleccionamos Symlink.

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

Disk Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink Copy Move

NEXT

CANCEL **HELP**

◆◆◇ Creación del caso

Integridad de la imagen

- Como analistas forenses, debemos asegurarnos de que la imagen se corresponde exactamente con la que se obtuvo del volcado del teléfono.
- Para ello disponemos del hash MD5, por lo que procedemos a verificar su integridad antes de incorporarla al análisis.

235fdf8cdba7584ac5c8a10fc9e11c56

Local Name: images/data.img
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- Ignore the hash value for this image.
- Calculate the hash value for this image.
- Add the following MD5 hash value for this image:

Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ext4)
Mount Point: File System Type:

◆◆◆ Creación del caso

Comprobación de la integridad

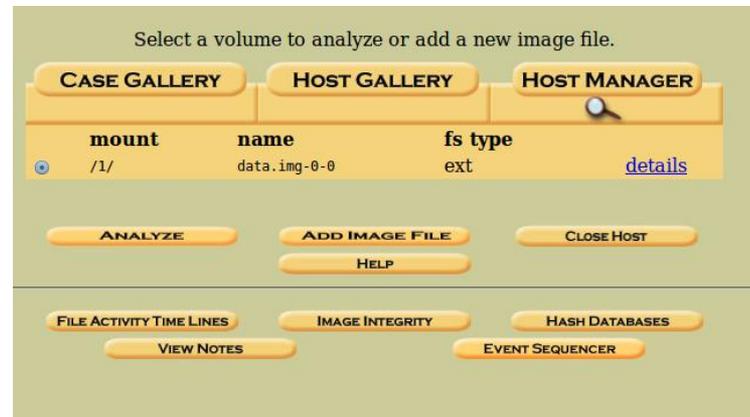
- Una vez comprobada la integridad de la imagen deberíamos obtener un resultado como el mostrado a continuación.

```
Calculating MD5 (this could take a while)
Current MD5: 235FDF8CDBA7584AC5C8A10FC9E11C56
Integrity Check Passed
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Volume image (0 to 0 - ext - /1/) added with ID vol1
```

OK

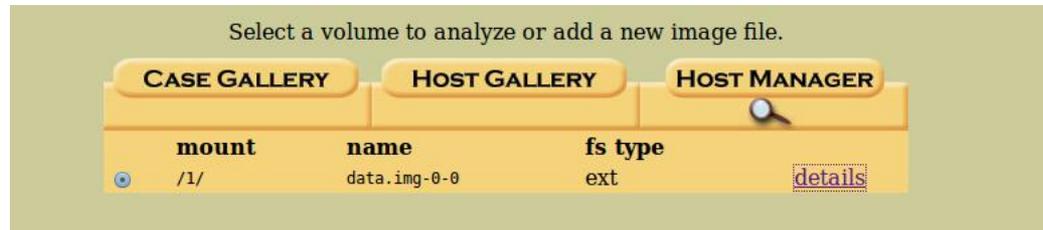
- Teniendo como resultado la imagen cargada dentro del caso.



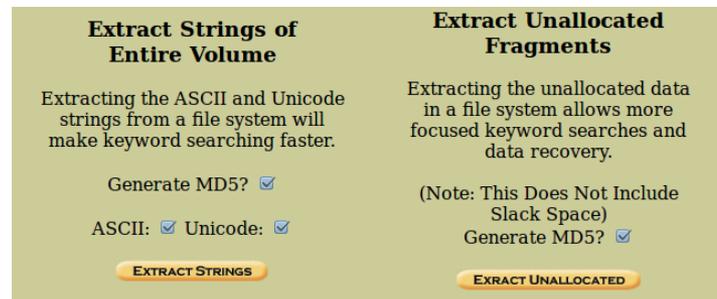
◆◆◆ Creación del caso

Análisis inicial

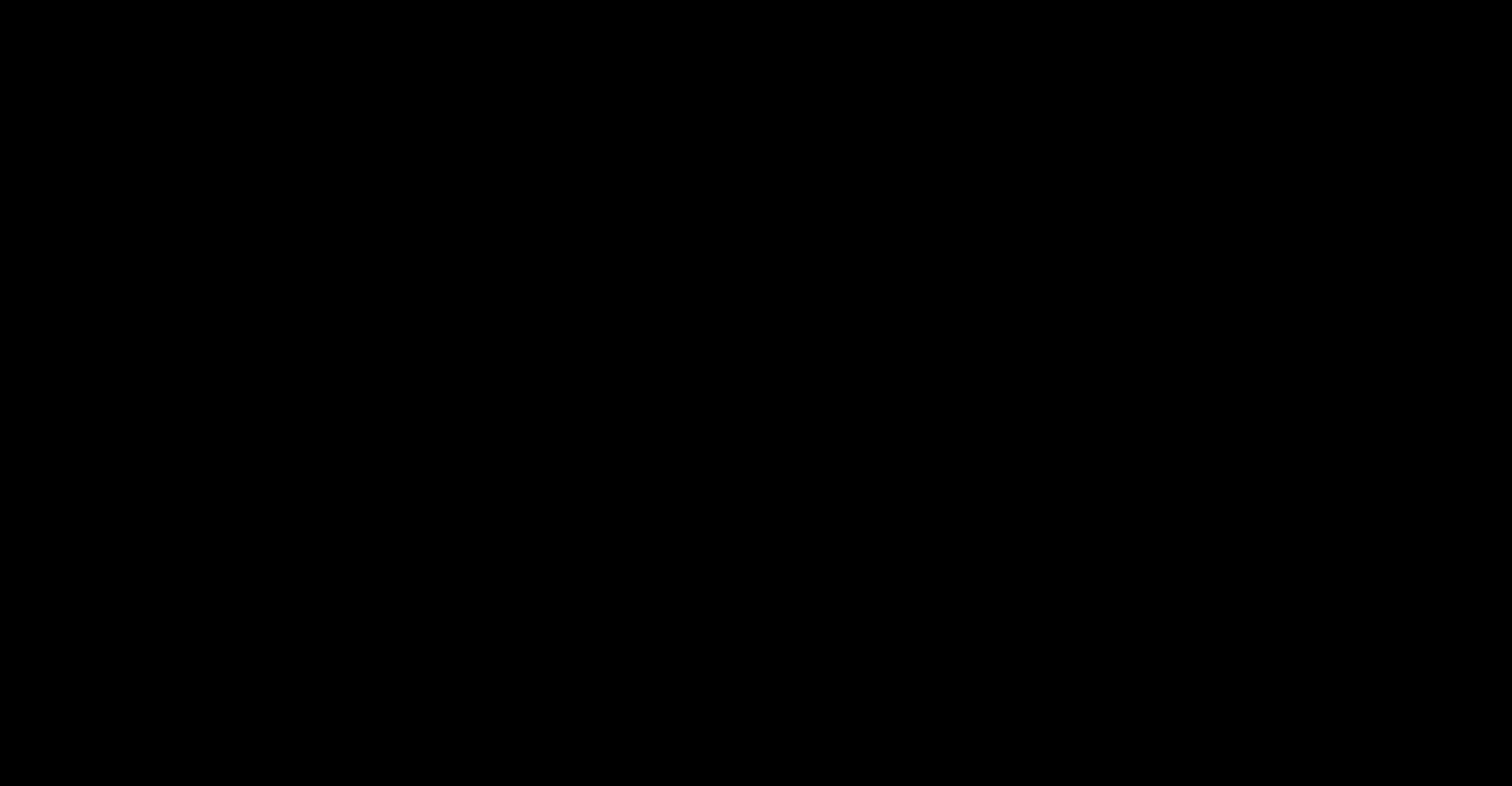
- Para facilitar la extracción de evidencias futuras, procedemos a:
 - Analizar el espacio del dispositivo.
 - Generar un índice de strings para la realización de búsquedas de forma eficiente.
- Para ello, en la ventana del caso abrimos los detalles de la imagen.



- Y seleccionamos "Extract Strings" y "Extract Unallocated".
 - Una vez extraído el espacio borrado, puedes extraer también los strings del mismo.



Análisis inicial Autopsy



A person is seen from behind, sitting at a wooden table and typing on a silver laptop. The laptop screen is black. To the left of the laptop is a smartphone. In front of the laptop is a notebook with a pen on it. To the right of the laptop is a white coffee cup on a saucer. The person is wearing a dark blue long-sleeved shirt and a watch on their left wrist. The background is blurred, showing an outdoor setting with trees.

Extracción de Información

◆◆◇ Extracción de información

Determinando los elementos iniciales a examinar

- Una vez cargada la imagen en Autopsy, el primer paso de la investigación será decidir que información contenida en la imagen será de interés para el caso en cuestión. Para ello deberás tener en cuenta el objetivo con el que se ha encargado el informe forense en el enunciado.

Tarea

Elabora una lista con los elementos de información de interés para el caso en cuestión.

Resultado esperado

Deberás obtener una lista con la información que pudiese contener el dispositivo que permita razonar sobre los posibles futuros objetivos, los cómplices del sospechoso o información adicional para continuar las investigaciones.

◆◆◇ Extracción de información

Determinando los elementos iniciales a examinar

- El informe que se nos ha pedido tiene como objetivo recabar información sobre tres elementos en particular:
 - Posible **localización** de nuevos objetivos.
 - Las **conexiones personales** del sospechoso con otros cómplices.
 - La información adicional sobre su **presencia online**.
- En lo relativo a la localización de nuevos objetivos serán de interés:
 - Información de aplicaciones de localización. Los pares de coordenadas almacenados en las diferentes aplicaciones nos pueden ofrecer datos de interés.
 - Puntos WiFi a los que se ha conectado el dispositivo. Si las conexiones WiFi han sido a redes públicas, podremos ubicar el dispositivo en un entorno determinado.
 - Mensajes que incluyan información sobre localizaciones. La información que haya podido intercambiar con otras personas sobre las localizaciones puede ser de interés también para el análisis.

Determinando los elementos iniciales a examinar

- En lo relativo a las conexiones personales, serán de interés:
 - Agenda del teléfono, indica las personas con la que el sospechoso tiene contacto frecuente.
 - Historial de llamadas, indica las personas con la que el sospechoso ha tenido contacto recientemente.
 - Mensajes recibidos a través de SMS y otras aplicaciones de mensajería/correo, ofrece información sobre las relaciones personales con cada una de esas personas.
- En lo relativo a la presencia online del sospechoso:
 - Nombres de usuario (y credenciales si es posible) del sospechoso en otros servicios online. Nos permitirá acceder a información adicional para determinar el grado de participación del sospechoso en los hechos.
- Dado que ciertos elementos de información pueden ser generados por diferentes aplicaciones, deberemos también elaborar un inventario de las aplicaciones instaladas en el dispositivo.

◆◆◇ Extracción de información

Lista de elementos a examinar

- Lista de aplicaciones instalada con especial detalle para aquellas aplicaciones que tengan relación con:
 - Localización.
 - Mensajería.
 - Servicios en la red (redes sociales, etc.).
- Localizaciones incluidas en aplicaciones de localización.
- Redes WiFi a las que se ha conectado el dispositivo.
- Agenda del teléfono.
- Historial de llamadas.
- Contenido y destinatarios de los mensajes de las diferentes aplicaciones de mensajería existentes en el dispositivo.
- Listado de credenciales de acceso a redes sociales de aplicaciones instaladas en el dispositivo a tal efecto.
- Fotografías que incluyan información relevante sobre alguno de los elementos anteriores.

◆◆◇ Extracción de información

Extracción de elementos de información

- Una vez listados todos los elementos a extraer durante el análisis, procedemos su extracción.
- Cada una de las siguientes tareas está enfocada a la obtención uno de los elementos mencionados en la tabla anterior.
- Para proceder a la fase de análisis deberás haber extraído la información relativa a cada uno de ellos.
- Es posible que durante la fase de análisis necesites realizar la extracción de nuevos elementos de información. Esta tarea es normal dentro de los procesos de análisis forense.
- De cara a la elaboración del informe forense, deberás tomar notas sobre todos los pasos y procesos que realizas durante estas tareas.



◆◆◇ Extracción de información

Extracción del listado de aplicaciones

- El primer paso a realizar para acotar el resto de tareas es identificar las aplicaciones que se encuentran instaladas en el dispositivo.

Tarea

Elabora una lista las aplicaciones instaladas en el dispositivo, haciendo énfasis en las aplicaciones que puedan incluir información de localización, mensajes o acceso a redes sociales

Resultado esperado

El listado de aplicaciones especificando el tipo de información que se puede extraer de cada una de ellas

◆◆◇ Extracción de información

Extracción del listado de aplicaciones

- Las aplicaciones instaladas en un dispositivo Android se encuentran en: */data/data*
- La imagen obtenida en el caso es de la partición data, por lo que sólo tendremos que inspeccionar el contenido de la carpeta data para averiguar las aplicaciones instaladas.
- En Autopsy navegamos a data y comprobamos la lista de aplicaciones.
- De entre las multitud de aplicaciones existentes se observan algunas interesantes como las mostradas a continuación:

d / d	com.quickoffice.android/	18:48:08 (GMT) 2016-02-14 18:07:42 (GMT)	28:48:17 (GMT) 1970-02-25 23:43:16 (GMT)	18:48:08 (GMT) 2016-02-14 18:07:42 (GMT)	4096	10086	10086	72241
d / d	com.skype.raider/	2016-02-14 14:42:01 (GMT)	2016-02-13 18:40:40 (GMT)	2016-02-14 14:42:01 (GMT)	4096	10097	10097	73230
d / d	com.snapchat.android/	2016-02-14 14:42:00 (GMT)	2016-02-13 18:39:40 (GMT)	2016-02-14 14:42:00 (GMT)	4096	10096	10096	73355
d / d	com.spotify.music/	2016-02-14 14:42:00 (GMT)	2016-02-13 18:37:53 (GMT)	2016-02-14 14:42:00 (GMT)	4096	10095	10095	73419
d / d	com.whatsapp/	2016-02-14 14:42:02 (GMT)	2016-02-13 18:41:44 (GMT)	2016-02-14 14:42:02 (GMT)	4096	10099	10099	73421

◆◆◇ Extracción de información

Extracción del listado de aplicaciones

- En el listado de aplicaciones, comprobamos que hay una que ha sido borrada del dispositivo.

Tarea personal: Investiga la utilidad de esa aplicación. Si lo crees conveniente del análisis de la aplicación al informe.

		15:48:30 (GMT)	23:43:01 (GMT)	15:48:30 (GMT)				
d / d	com.motorola.wappushsi/	1970-02-25 23:44:42 (GMT)	1970-02-25 23:43:04 (GMT)	1970-02-25 23:44:42 (GMT)	4096	10045	10045	72133
✓ d / r	com.pinellascodeworks.securewipe	2016-02-14 14:50:04 (GMT)	2016-02-14 14:50:04 (GMT)	2016-02-14 14:50:04 (GMT)	20480	10021	10021	73691 (realloc)
d / d	com.qualcomm.atfwd/	1970-02-25 23:44:46 (GMT)	1970-02-25 23:43:18 (GMT)	1970-02-25 23:44:46 (GMT)	4096	1000	1000	72261
d / d	com.qualcomm.interfacepermissions/	1970-02-25 23:43:10 (GMT)	1970-02-25 23:43:10 (GMT)	1970-02-25 23:43:10 (GMT)	4096	10067	10067	72195

- Se puede comprobar que el listado de aplicaciones es muy grande:
 - Hay que tener en cuenta que en esta carpeta se almacenan todas las aplicaciones, incluidas las que vienen por defecto en el sistema.
 - En el informe se deberían listar todas, pero especificar los que está relacionadas directamente con el caso.

Extracción del listado de aplicaciones

- Lista de aplicaciones de interés I:
 - com.quickoffice.android - QuickOffice
 - Puede almacenar documentos de interés.
 - com.skype.raider - Skype
 - Puede almacenar contactos, fotografías mensajes y localizaciones.
 - com.snapchat.android – Snapchat
 - Puede almacenar contactos, fotografías mensajes y localizaciones.
 - com.whatsapp
 - Puede almacenar contactos, fotografías mensajes y localizaciones.
 - com.instagram.android
 - Puede almacenar contactos, fotografías mensajes y localizaciones.
 - com.google.android.gm
 - Puede almacenar correos electrónicos de interés.
 - com.android.browser
 - Almacena los datos de navegación.

Extracción del listado de aplicaciones

- Lista de aplicaciones de interés II:
 - com.google.android.apps.maps
 - Puede almacenar localizaciones.
 - com.facebook.katana
 - Puede almacenar contactos, fotografías mensajes y localizaciones.
 - com.android.email
 - Puede almacenar correos electrónicos de interés.
 - com.android.chrome
 - Almacena los datos de navegación.
- Además, dentro del dispositivo se pueden encontrar los siguientes *providers* de interés forense (mencionados anteriormente):
 - com.android.providers.calendar
 - com.android.providers.telephony
 - com.android.providers.contacts

◆◆◇ Extracción de información

Extracción de datos de interés

- Una vez recuperada la lista de aplicaciones de interés del dispositivo, pasamos a analizarlas en busca de datos que puedan ser relevantes para la investigación.
- Una vez extraídos los datos relevantes de cada aplicación, pasaremos a realizar las tareas de análisis.
- Es conveniente documentar y etiquetar correctamente la información extraída durante este proceso para facilitar las posteriores tareas de análisis.
- En la mayoría de los casos, la validez de la información extraída durante este proceso ha sido corroborada por la comunidad. Como en los datos que se han observado durante el estudio de los diferentes elementos analizables.
- En el caso de que hubiese que extraer información de aplicaciones o servicios no documentados sería necesario validar que la información extraída corresponde con la existente en los dispositivos. Este tipo de validación queda fuera del alcance de este laboratorio.

◆◆◆ Extracción de información

Historial de llamadas y contactos

Tarea

Localiza y extrae la información relativa al historial de llamadas, contactos del teléfono.

Resultado esperado

El fichero que identifica las últimas llamadas realizadas desde el dispositivo.

◆◆◆ Extracción de información

Historial de llamadas y contactos

- Tanto el historial de llamadas como los contactos del dispositivo se encuentra en:
 - `/data/com.android.providers.contacts/databases/contacts2.db`
- Procedemos a extraer el fichero (su correspondiente *journal* está vacío).
 - Tomamos notas de todo el proceso para su documentación de cara al informe.

	23:44:29 (GMT)	23:42:5
./	2016-02-14 18:07:55 (GMT)	1970-02 23:44:1
contacts2.db	2016-02-14 15:02:18 (GMT)	1970-02 23:44:1
contacts2.db- journal	2016-02-14 15:02:18 (GMT)	1970-02 23:44:1
contacts2.db- mj0F6E4D94B	2016-02-14 18:07:55 (GMT)	2016-02 18:07:5
profile.db	2016-02-13 21:07:29 (GMT)	1970-02 23:44:1
profile.db-journal	2016-02-13 21:07:29 (GMT)	1970-02 23:44:1

...ta.com.android.providers.contacts.databases.contacts2.db
which is: unknown
from: http://localhost:9999

What should Firefox do with this file?

Open with Leafpad (default)

Save File

Do this automatically for files like this from now on.

Cancel OK

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)

◆◆◆ Extracción de información

Mensajes de texto

Tarea

Localiza y extrae la información relativa a los mensajes de texto existentes en el dispositivo.

Resultado esperado

El fichero que identifica los mensajes de texto existentes en el dispositivo.

◆◆◆ Extracción de información

Mensajes de texto

- Los mensajes de texto del dispositivo se encuentran en:
 - `/data/com.android.providers.telephony/databases/mmssms.db`
- Procedemos a extraer el fichero (y su correspondiente *journal*).
 - Tomamos notas de todo el proceso para su documentación de cara al informe.

The screenshot shows a file analysis tool interface with a table of files and a Firefox dialog box. The table lists files such as `mmssms.db` and `mmssms.db-journal`, which are circled in red. The dialog box shows the file `...a.com.android.providers.telephony.databases.mmssms.db` and offers options to open it with Leafpad or save it. The 'Save File' option is selected, and the 'OK' button is circled in red. At the bottom of the tool, the 'Export' button is also circled in red.

File Name	Timestamp 1	Timestamp 2	Timestamp 3	Size	Permissions
<code>./</code>	1970-02-25 23:44:28 (GMT)	1970-02-25 23:44:19 (G			
<code>dlut.db</code>	1970-02-25 23:44:20 (GMT)	1970-02-25 23:44:19 (G			
<code>dlut.db-journal</code>	1970-02-25 23:44:20 (GMT)	1970-02-25 23:44:19 (G			
<code>mmssms.db</code>	2016-02-14 15:25:12 (GMT)	1970-02-25 23:44:28 (G			
<code>mmssms.db-journal</code>	2016-02-14 15:25:12 (GMT)	1970-02-25 23:44:28 (G			
<code>telephony.db</code>	2016-02-14 14:43:59 (GMT)	1970-02-25 23:44:20 (G			
<code>telephony.db-journal</code>	2016-02-14 14:43:59 (GMT)	1970-02-25 23:44:20 (GMT)	2016-02-14 18:02:20 (GMT)	8720	1001 T

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)
File Type: SQLite 3.x database, user version 58

◆◆◇ Extracción de información

Redes wifi

Tarea

Localiza y extrae la información relativa a las redes wifi a las que se ha conectado el dispositivo.

Resultado esperado

El fichero que identifica las redes wifi a las que se ha conectado el dispositivo.

◆◆◆ Extracción de información

Redes wifi

- La información de las redes wifi a las que se ha conectado el dispositivo se puede encontrar en:
 - `/misc/wifi/wpa_supplicant.conf`
- En este caso podemos ver la información contenida en el mismo antes de la extracción incluso.
- Extraemos el fichero.
 - Tomamos notas de todo el proceso para su documentación de cara al informe.

The screenshot shows a file explorer window with a list of files and a Firefox dialog box. The file list includes:

File Name	Modification Date	Size
p2p_supplicant.conf	2016-02-14 14:42:06 (GMT)	2016-02-14 14:42:06
sockets/	2016-02-14 14:42:06 (GMT)	1970-02-25 23:42:44
softap.conf	1970-02-25 23:44:16 (GMT)	1970-02-25 23:44:16
WCNSS_qcom_wlan_cal.bin	2009-01-02 11:00:04 (GMT)	1970-02-25 23:42:51
wpa_supplicant.conf	2016-02-14 14:42:06 (GMT)	1970-02-25 23:44:17
wpa_supplicant/	1970-02-25 23:42:44 (GMT)	1970-02-25 23:42:44

The `wpa_supplicant.conf` file name is circled in red. The Firefox dialog box shows the file `vol1-1.misc.wifi.wpa_supplicant.conf` with the following information:

- which is: unknown
- from: `http://localhost:9999`

The dialog asks "What should Firefox do with this file?" and has the following options:

- Open with: Leafpad (default)
- Save File
- Do this automatically for files like this from now on.

The "Cancel" and "OK" buttons are circled in red. At the bottom of the dialog, the text "ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note" is visible, with "Export" circled in red. The file type is listed as "File Type: data".

◆◆◆ Extracción de información

Localizaciones en la aplicación de mapas

Tarea

Localiza y extrae la información relativa a las localizaciones existentes en la aplicación de mapas.

Resultado esperado

El fichero que identifica las localizaciones existentes en la aplicación de mapas.

◆◆◆ Extracción de información

Localizaciones en la aplicación de mapas

- Accedemos a la carpeta de la aplicación de mapas para buscar información relacionada con las localizaciones:
 - `/data/com.google.android.apps.maps/`
- En la carpeta `cache/http` localizamos dos imágenes.

52a6786d8aab81daefa5bd8117265422_0	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:21 (GMT)	5591	10059	10059	80306
52a6786d8aab81daefa5bd8117265422_1	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:21 (GMT)	23084	10059	10059	80307
52a6786d8aab81daefa5bd8117265422_1.tmp	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:21 (GMT)	23084	10059	10059	80307 (realloc)
cdbcca21c9097e1d4198f169434eef5a_0	2016-02-14 15:00:19 (GMT)	2016-02-14 15:00:19 (GMT)	2016-02-14 15:00:21 (GMT)	5621	10059	10059	80037
cdbcca21c9097e1d4198f169434eef5a_1	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:19 (GMT)	2016-02-14 15:00:21 (GMT)	22569	10059	10059	80300

- Además de extraerlas, podemos añadir notas en las mismas para facilitar la creación del informe.

Enter a note for `/1/data/com.google.android.apps.maps/cache/http/52a6786d8aab81daefa5bd8117265422_1 (80307)`:

A note works like a bookmark and allows you to later find this data more easily.

Imagen de interés

Add a Standard Note

Add a Sequencer Event:

A sequencer event will be sorted based on the time so that event reconstruction will be easier

M-Time (Sun Feb 14 16:00:21 2016)
 A-Time (Sun Feb 14 16:00:20 2016)
 C-Time (Sun Feb 14 16:00:21 2016)

OK

◆◆◆ Extracción de información

Localizaciones en la aplicación de mapas

- Además de extraerlas, podemos añadir notas en las mismas para facilitar la creación del informe.
 - Además de un texto de información, podemos añadir las fechas que queremos añadir a la nota para la creación de una línea de tiempo de eventos.

Enter a note for /1/data/com.google.android.apps.maps/cache/http/52a6786d8aab81daefa5bd8117265422.1 (80307):

A note works like a bookmark and allows you to later find this data more easily.

Imagen de interés

Add a Standard Note

Add a Sequencer Event:

A sequencer event will be sorted based on the time so that event reconstruction will be easier

M-Time (Sun Feb 14 16:00:21 2016)
 A-Time (Sun Feb 14 16:00:20 2016)
 C-Time (Sun Feb 14 16:00:21 2016)

OK

◆◆◆ Extracción de información

Localizaciones en la aplicación de mapas

- En `files/share_history.xml` podemos encontrar un listado con las aplicaciones con las que se han compartido ubicaciones:
 - Gmail
 - Snapchat
- Más adelante comprobaremos las ubicaciones compartidas.
- En la carpeta `databases` encontramos las bases de datos que pueden ser de nuestro interés.

Las guardamos y anotamos.

[gmm_myplaces.db](#)

[gmm_myplaces.db-journal](#)

[gmm_storage.db](#)

[gmm_storage.db-journal](#)

Fotografías

Tarea

Localiza y extrae las fotografías existentes en la imagen del dispositivo

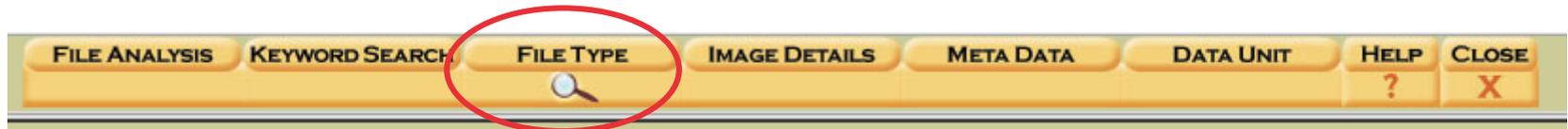
Resultado esperado

Los ficheros de fotografías existentes en la imagen del dispositivo

◆◆◇ Extracción de información

Fotografías

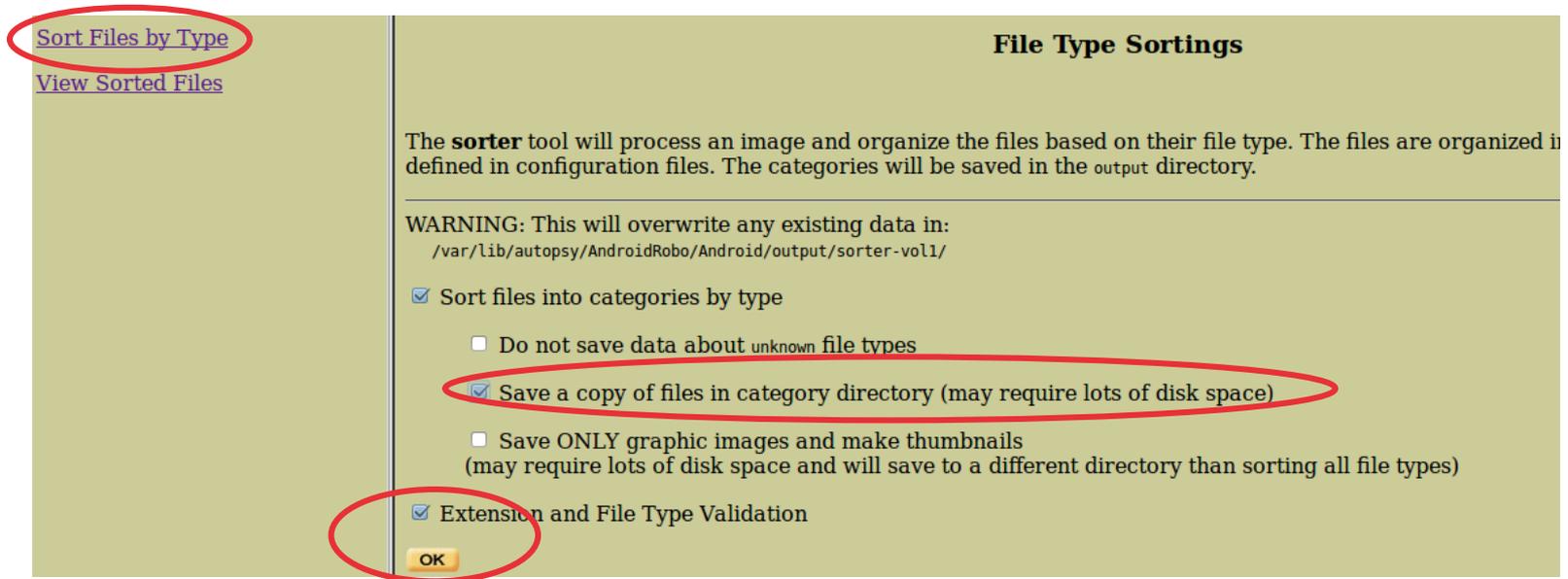
- En primer lugar, accedemos al directorio donde se guardarán por defecto las fotografías para inspeccionar su contenido:
 - */media*
- Comprobamos que hay imágenes de interés en:
 - */media/0/WhatsApp/Media/WhatsApp Images/*
 - */media/0/DCIM/Camera/*
 - */media/0/Pictures/Screenshots/*
- Autopsy nos permite también buscar todas las imágenes existentes en la imagen de forma automática.
- En File Type.



◆◆◆ Extracción de información

Fotografías

- Seleccionamos la opción “Sort Files by Type” y marcando las opciones mostradas en la captura Autopsy extraerá todos los tipos de archivos relevantes.



- Una vez generada la lista de ficheros se puede navegar a ella accediendo a la URL mostrada en la opción de “View Sorted Files”.

◆◆◆ Extracción de información

Fotografías

Files (3801)

Files Skipped (1002)

- Non-Files (1002)
- Reallocated Name Files (786)
- 'ignore' category (0)

Extensions

- [Extension Mismatches](#) (156)

Categories (2013)

- [archive](#) (28)
- [audio](#) (2)
- [compress](#) (2)
- [crypto](#) (0)
- [data](#) (625)
- [disk](#) (0)
- [documents](#) (306)
- [exec](#) (183)
- [images](#) (117) ([thumbnails](#))
- [system](#) (0)
- [text](#) (172)
- [unknown](#) (578)
- [video](#) (0)

- [Page 1](#)
- [Page 2](#)

Image Thumbnails - Page 2

A	B	C
		
h1a81hurcs00h4507433862891678094.jpg.nomedia details	h1a81hurcs00h4825957787411738656.jpg.nomedia details	h1a81hurcs00h735044565813f details
		
5eb76d7c56a5083a548abb5329640b6d.1 details	0385b01fb8b771a0a59e0be73faa3966.0 details	f9bd7bc259559a8a20c72eac5a details
		
Screenshot_2016-02-13-17-41-37.png	Screenshot_2016-02-14-15-32-48.png	IMG_20160213_201017879.jpg

Correos electrónicos

Tarea

Localiza y extrae los correos electrónicos existentes en la imagen del dispositivo.

Resultado esperado

La base de datos de correos electrónicos existentes en la imagen del dispositivo.

◆◆◆ Extracción de información

Correos electrónicos

- Existen dos aplicaciones de correo en el dispositivo:
 - `/data/com.android.email/`
 - `/data/com.google.android.gm/`
- Comprobamos el contenido de las bases de datos y comprobamos que en lo que refiere a la primera aplicación, no hay ningún contenido adicional de interés salvo el código de creación de las tablas, por lo que añadimos las notas correspondientes para la posterior elaboración del informe.

r / r	EmailProvider.db	2016-02-14 14:42:40 (GMT)	1970-02-25 23:44:32 (GMT)	2016-02-14 14:42:40 (GMT)	131072
r / r	EmailProvider.db-journal	2016-02-14 14:42:40 (GMT)	1970-02-25 23:44:32 (GMT)	2016-02-14 14:42:40 (GMT)	0
✓ r / r	EmailProvider.db- mj8722619EE	2016-02-14 15:01:24 (GMT)	2016-02-14 15:01:24 (GMT)	2016-02-14 15:01:24 (GMT)	36824
r / r	EmailProviderBackup.db	1970-02-25 23:44:33 (GMT)	1970-02-25 23:44:32 (GMT)	2016-02-14 14:42:39 (GMT)	131072
r / r	EmailProviderBackup.db-	1970-02-25	1970-02-25	2016-02-14	8720

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * A
File Type: SQLite 3.x database, user version 124

ASCII String Contents Of File: /1/data/com.android.email/databases/EmailProvider.db

```
SQLite format 3
;triggermessage_count_message_insertMessageCREATE TRIGGER message_count_message_insert after insert on Message begin update Mailbox s
Utriggerunread_message_readMessageCREATE TRIGGER unread_message_read before update of flagRead on Message when OLD.flagRead!=NEW.flag
ytriggerunread_message_moveMessageCREATE TRIGGER unread_message_move before update of mailboxKey on Message when OLD.flagRead=0 begin
Striggerunread_message_deleteMessageCREATE TRIGGER unread_message_delete before delete on Message when OLD.flagRead=0 begin update Ma:
Striggerunread_message_insertMessageCREATE TRIGGER unread_message_insert before insert on Message when NEW.flagRead=0 begin update Ma:
qtriggermessage_deleteMessageCREATE TRIGGER message_delete before delete on Message begin delete from Attachment where messageKey=ol
indexmessage_syncServerIdMessage
CREATE INDEX message_syncServerId on Message (syncServerId)
```

◆◆◇ Extracción de información

Correos electrónicos

- En el caso de la aplicación de Gmail existen ficheros de base de datos que hacen referencia a una cuenta de Gmail, los anotamos como importantes y los descargamos.

internal.johntoppysmith@gmail.com.db	14:20
internal.johntoppysmith@gmail.com.db-journal	14:20
mailstore.johntoppysmith@gmail.com.db	15:00
mailstore.johntoppysmith@gmail.com.db-shm	15:00
mailstore.johntoppysmith@gmail.com.db-wal	15:00

◆◆◆ Extracción de información

Datos de navegación web

Tarea

Localiza y extrae los datos de navegación web existentes en la imagen del dispositivo.

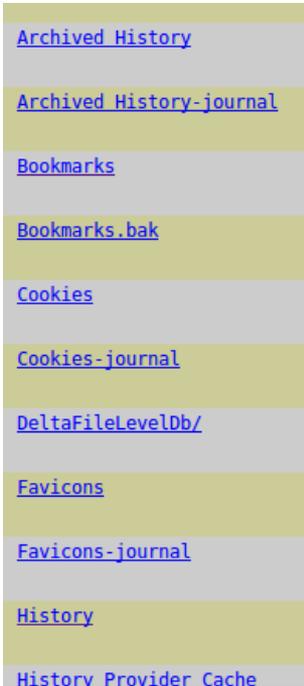
Resultado esperado

La base de datos de correos electrónicos existentes en la imagen del dispositivo.

◆◆◇ Extracción de información

Correos electrónicos

- La imagen analizada solo tiene instalado un navegador en:
 - */data/com.google.chrome/*
- Inspeccionamos el contenido y anotamos para su posterior análisis todos los ficheros existentes en la carpeta interna:
 - *app_chrome/Default*



A vertical list of files and folders, each on a separate line. The text is blue and appears to be a screenshot of a file explorer or terminal output. The items are: Archived History, Archived History-journal, Bookmarks, Bookmarks.bak, Cookies, Cookies-journal, DeltaFileLevelDb/, Favicons, Favicons-journal, History, and History Provider Cache.

- [Archived History](#)
- [Archived History-journal](#)
- [Bookmarks](#)
- [Bookmarks.bak](#)
- [Cookies](#)
- [Cookies-journal](#)
- [DeltaFileLevelDb/](#)
- [Favicons](#)
- [Favicons-journal](#)
- [History](#)
- [History Provider Cache](#)

◆◆◇ Extracción de información

Información relativa a las redes sociales

Tarea

Localiza y extrae la información que pueda ser de interés y esté relacionada con las aplicaciones de redes sociales en el dispositivo.

Resultado esperado

Los ficheros de bases de datos, fotografías y otros ficheros existentes en las cachés de las aplicaciones relacionadas con redes sociales.

◆◆◇ Extracción de información

Información relativa a las redes sociales

- Para realizar esta tarea debemos inspeccionar los contenidos de todas las aplicaciones que están relacionadas con redes sociales.
- Procedemos a entrar en cada una de las aplicaciones y anotamos los ficheros relevantes de cada una de las mismas.
- Las aplicaciones que analizamos son:
 - com.quickoffice.android - QuickOffice
 - com.skype.raider - Skype
 - com.snapchat.android – Snapchat
 - com.whatsapp
 - com.instagram.android
 - com.facebook.katana
- Durante la etapa de análisis se analizarán los contenidos de las mismas en busca de pruebas.

A photograph of a wooden desk with a silver laptop, a pair of glasses, and a white mouse. The word "Análisis" is overlaid in white text on a semi-transparent grey rectangle. In the background, a white chair is visible against a light blue wall.

Análisis

Tareas de análisis

- Durante esta parte del laboratorio vamos a inspeccionar los contenidos marcados en las anteriores tareas y añadir anotaciones con respecto a la información contenida en los mismos.
- El objetivo de esta tarea es la obtención de la información que necesitamos para la correcta elaboración del informe.
- Para ello partimos de la siguiente hipótesis:
 - El dispositivo ha sido utilizado para que los miembros de una banda criminal intercambien algún tipo de información sobre sus objetivos.
- Y los datos que necesitamos para que las investigaciones puedan continuar son:
 - Información sobre los posibles cómplices en la ejecución de los hechos.
 - Localizaciones de los posibles futuros objetivos.
 - Información sobre las cuentas existentes en el propio dispositivo para la posterior adquisición de las mismas a través de la correspondiente orden judicial.

Información sobre los cómplices

Tarea

Analiza los datos obtenidos para establecer una lista de contactos frecuentes en el dispositivo y el tipo de información que han intercambiado.

Resultado esperado

Una parte del informe forense que especifique los contactos de interés encontrados en el dispositivo así como los mensajes que han sido intercambiados.

Información sobre los cómplices

- Analizando la tabla call de la base de datos de llamadas contacts2.db

	_id	number	presentation	date	duration	type	new	name	num
1	1	444	1	1455393591600	119	2	1	{null}	
2	2	07484157148	1	1455401147692	0	2	1	{null}	
3	3	07454127148	1	1455401158993	0	2	1	{null}	
4	4	+448444827777	1	1455465631810	1	2	1	{null}	

- Además, navegando a la tabla de contactos observamos lo siguiente:
 - Se ha ejecutado la sentencia `Select display_name, sync1 from raw_contacts` para reducir el número de columnas.

display_name	
J	https://www.google.com/m8/feeds/contacts/joh
J	447401089370@s.whatsapp.net
j.thebest@gmail.com	https://www.google.com/m8/feeds/contacts/joh

Información sobre los cómplices

- La inspección de la base de datos de mensajes (mmssms.db) nos ofrece la siguiente información.
 - Se ha ejecutado la sentencia `Select address, person, body from sms` para simplificar la salida obtenida y facilitar su lectura.

	address	person	
			You can also tap on this link to verify your phone: v.whatsapp.com/492!
8	Snapchat	{null}	Snapchat Code: 727829. Happy Snapping!
9	7401 089370	{null}	Movil nuevo. Aun no me hago con el. La app de Snapchat esta muy bien
10	+447401089370	1	Hola John! Móvil nuevo :) aunque aún no me hago con el. Snapchat esta
11	7401 089370	{null}	Siii
12	+447401089370	1	También estoy llegando. No tengo tarifa de datos ya

Información sobre los cómplices y otros teléfonos

- Tras la información analizada de las bases de datos de SMS, contactos y teléfonos podemos concluir que se han realizado llamadas a 4 números diferentes, información que completaremos a partir de las redes sociales:
 - El 444 parece ser un número de información de la operadora.
 - Se han realizado dos llamadas telefónicas a teléfonos móviles muy similares pero ninguna de ellas ha sido respondida.
 - La búsqueda en Internet no proporciona información de utilidad.
 - Se han enviado varios mensajes sospechosos a un contacto con el número de teléfono 7401089370.
 - Se ha realizado una llamada al teléfono +448444827777.
 - Una búsqueda en Internet muestra que el teléfono pertenece al servicio de Palacios Históricos de Reino Unido.
 - Existe un contacto de correo con la dirección j.thebest@gmail.com
 - Se han recibido mensajes de texto para el alta en servicios como Snapchat y WhatsApp.

◆◆◇ Extracción de información

Información sobre las localizaciones

Tarea

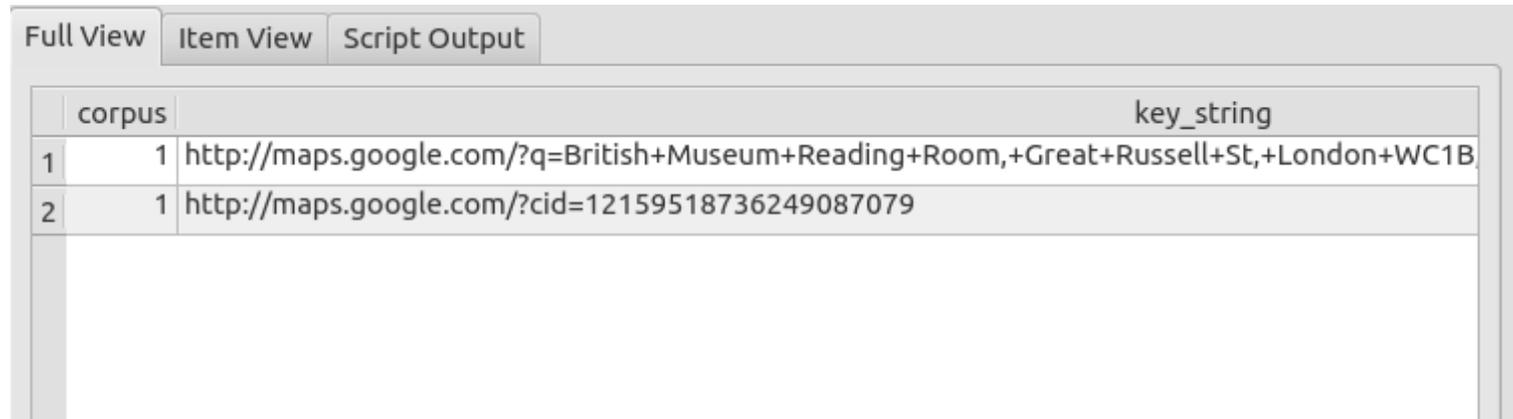
Analiza la información sobre las localizaciones en las que haya podido estar el dispositivo

Resultado esperado

Una parte del informe que especifique las localizaciones encontradas y su interés en relación con el caso en estudio.

Información sobre las localizaciones

- Analizando la base de datos ggm_myplaces.db observamos que existen dos entradas en la tabla sync_item con URL pertenecientes a mapas de Google.

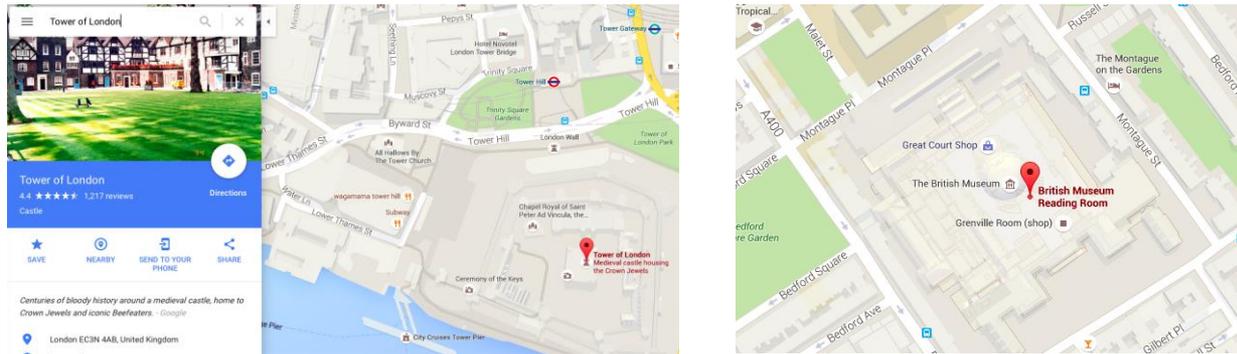


The screenshot shows a database viewer interface with three tabs: 'Full View', 'Item View', and 'Script Output'. The 'Full View' tab is active, displaying a table with two columns: 'corpus' and 'key_string'. The table contains two rows of data.

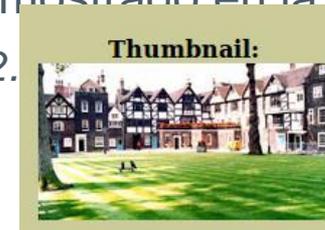
	corpus	key_string
1	1	http://maps.google.com/?q=British+Museum+Reading+Room,+Great+Russell+St,+London+WC1B
2	1	http://maps.google.com/?cid=12159518736249087079

Información sobre las localizaciones

- Comprobamos el resultado que devuelven las URL y comprobamos que apuntan a dos localizaciones específicas de la ciudad de Londres.



- El teléfono de contacto de La Torre de Londres coincide con el encontrado en el historial de llamadas.
- Además, si analizamos uno de los ficheros encontrados en la caché de la aplicación vemos que la imagen coincide con el mostrado en la figura:
 - `cache/http/52a6786d8aab81daefa5bd8117265422.`



Información sobre las localizaciones

- Analizamos ahora el contenido del fichero de redes WiFi y comprobamos que tiene datos de una conexión (con contraseña incluida), pero el nombre del punto de acceso no ofrece ninguna información sobre su localización más allá del país de origen (Gran Bretaña).

```
-----8-----  
p2p_disabled=1  
p2p_no_group_iface=1  
country=GB  
  
network={  
    ssid="SKY565BA"  
    psk="EABATUTD"  
    key_mgmt=WPA-PSK  
    priority=1  
}  
000003000000e0000
```

- Anotamos todos los descubrimientos realizados en esta tarea para la posterior realización del informe.

Información sobre las localizaciones

- Las fotografías tomadas por la cámara no muestran las coordenadas GPS entre su información EXIF.

```
santoku@santoku-VirtualBox:~/Downloads$ exiftool /var/lib/autopsy/AndroidRobo/Android/output/sorter-voll/images/data.img-104106.jpg
ExifTool Version Number      : 9.46
File Name                    : data.img-104106.jpg
Directory                    : /var/lib/autopsy/AndroidRobo/Android/output/sorter-voll/images
File Size                    : 809 kB
File Modification Date/Time  : 2016:02:16 23:13:28+01:00
File Access Date/Time       : 2016:02:16 23:15:36+01:00
File Inode Change Date/Time  : 2016:02:16 23:13:28+01:00
File Permissions             : rw-r--r--
File Type                    : JPEG
MIME Type                    : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Make                        : Motorola
Camera Model Name            : XT1021
X Resolution                  : 72
```

- Pero su contenido muestra que han sido tomadas en un museo con importantes piezas de arte.
 - Dada la información de localización obtenida anteriormente, se trata con toda seguridad del Museo Británico.
- Anotamos todos los descubrimientos realizados en esta tarea para la posterior realización del informe.



Información sobre las cuentas existentes

Tarea

Analiza los datos en cada una de las aplicaciones de interés encontradas en el dispositivo para establecer una lista de contactos frecuentes y el tipo de información que ha enviado mediante la utilización de las mismas.

Resultado esperado

Una parte del informe forense que especifique la información de interés encontrada en cada una de las aplicaciones analizadas y si tiene alguna relación con datos anteriormente analizados.

Información sobre las cuentas existentes

- Durante esta tarea vamos a analizar la información existente en el resto de aplicaciones instaladas en el dispositivo.
- Tal y como se mencionó anteriormente durante la unidad, el análisis de estas aplicaciones debe ser validado con dispositivos de control:
 - Por cada una de las aplicaciones, se deberán generar evidencias en el dispositivo de control y se deberá verificar que las evidencias generadas corresponden de verdad con los hechos que se pueden observar de forma directa en el teléfono.
 - Este ejercicio asume que la validación del significado de los datos ya ha sido realizada con anterioridad.
 - Si el alumno lo desea, puede realizar la validación por si mismo.
- En esta sección del análisis mostramos sólo una parte de los posibles resultados a obtener.

Queda como tarea adicional para el alumno la revisión del posible conjunto de evidencias adicionales.

Información sobre las cuentas existentes - Spotify

- Tras un primer análisis , se comprueba que las siguientes aplicaciones no han sido utilizadas y por lo tanto no incluyen información de interés:
 - Facebook
 - Instagram
 - Skype
- Tras el análisis de la aplicación de Spotify se localiza un fichero que contiene el usuario y el token de autenticación de la cuenta.
 - *data/com.spotify.music/files/settings/prefs*

```
autologin.canonical_username="johntoppysmith"  
autologin.username="johntoppysmith"  
autologin.saved_credentials="{\"johntoppysmith\":[\"johntoppysmith\", \"ajpHPT8ErZCWmrR3x0NUPmbfsSKbL+krHEWhyqKJqrjlbqDUobsfu065eWVKXEIn\"]}"  
language="en_GB"  
autologin.blob="ajpHPT8ErZCWmrR3x0NUPmbfsSKbL+krHEWhyqKJqrjlbqDUobsfu065eWVKXEIn"  
core.clock_delta=-1
```

Información sobre las cuentas existentes - Gmail

- El análisis de los correos de Gmail se puede comprobar en el fichero:
 - *databases/mailstore.johntoppysmith@gmail.com.db*
- Su contenido muestra una serie de mensajes al contacto j.thebest@gmail.com compartiendo la ubicación del museo y después mencionando unas joyas. Se ha realizado la siguiente consulta para facilitar la lectura del resultado:
 - *Select toAddresses, snippet from messages*

4	John Smith <johntoppysmith@gmail.com>	Hi John tips to get the most out of Gmail bring your
5	"johntoppysmith" <johntoppysmith@gmail.com>	Hey johntoppysmith! Before you start Snapping, it's a
6	"" <j.thebest@gmail.com>	British Museum Reading Room Great Russell St Lond
7	"" <j.thebest@gmail.com>	Ya he llegado
8	"" <j.thebest@gmail.com>	Despues iremos a ver las joyas

- Dadas las evidencias encontradas hasta la fecha es posible que tengan que ver con La Torre de Londres.

Información sobre las cuentas existentes - WhatsApp

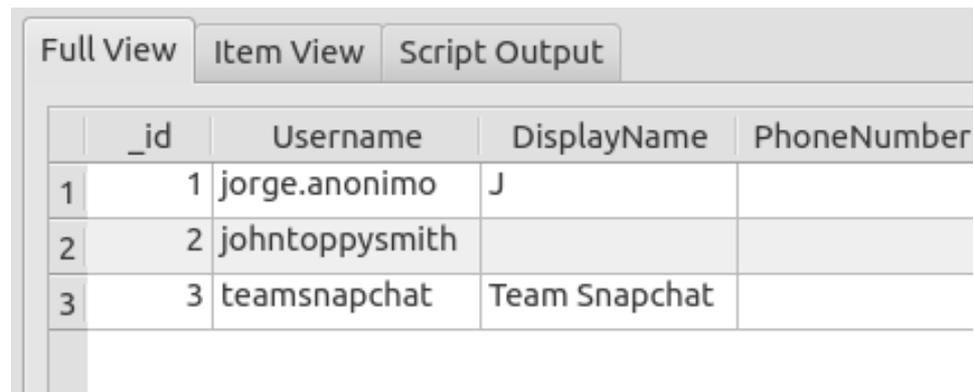
- Se analizan las bases de datos de la aplicación WhatsApp. Los chats de la aplicación se encuentran en el fichero: */databases/msgstore.db*
- Analizando el contenido se pueden observar la siguientes entradas. Se ha realizado la siguiente consulta para facilitar su lectura:
 - *Select key_remote_jid, data, latitude, longitude from messages*

	key_remote_jid	data	latitude	longitude
1	-1	{null}	0	0
2	447401089370@s.whatsapp.net	Hola!	0	0
3	447401089370@s.whatsapp.net	{null}	51.52393464	-0.07597850985
4	447401089370@s.whatsapp.net	Voy de camino	0	0
5	447401089370@s.whatsapp.net	{null}	0	0
6	447401089370@s.whatsapp.net	{null}	51.5211384	-0.1149357
7	447401089370@s.whatsapp.net	Genial!	0	0

- Se comprueba que hay una comunicación mediante con mensajes de chat con el mismo teléfono con el que se intercambiaron SMS.
- Se han compartido dos localizaciones. Tras la búsqueda de las coordenadas se comprueba:
 - La primera corresponde a la dirección 10 Redchurch St, Londres E2 7DD.
 - La segunda corresponde a la dirección A401, Londres WC1X 8NX.

Información sobre las cuentas existentes - Snapchat

- De la aplicación de Snapchat podemos analizar el fichero de base de datos principal:
 - *databases/tcspahn.db*
- Y extraemos que también se ha entrado en contacto con el contacto J mediante la aplicación de Snapchat.



	_id	Username	DisplayName	PhoneNumber
1	1	jorge.anonimo	J	
2	2	johntoppysmith		
3	3	teamsnapchat	Team Snapchat	

- No se ha podido acceder a los ficheros borrados por Snapchat
 - Esto es posible que se deba a la utilización de la aplicación `com.pinellascodeworks.secureswipe` que permite el borrado seguro de los bloques no utilizados en la memoria interna.



Informe

Introducción

- Como último paso para la realización del laboratorio deberás realizar un informe con las evidencias encontradas y las conclusiones a las que has llegado tras la realización del análisis.
 - Para la realización del informe puedes ayudarte de todas las notas e información que has recopilado durante el análisis , incluyendo la que se ha mostrado durante las soluciones guiadas a cada uno de los pasos.
 - En las siguientes páginas, podrás ver una descripción de la estructura general que se espera del informe.
-  La estructura aquí mencionada es muy similar a la mencionada en esta misma unidad, pero te ofrecemos pistas y guías sobre el caso específico para guiarte durante el proceso.
- Una vez lo hayas completado, te recomendamos que lo subas al apartado correspondiente del foro, donde podrás también leer y comparar con los informes que han realizado tus compañeros

Resumen del caso

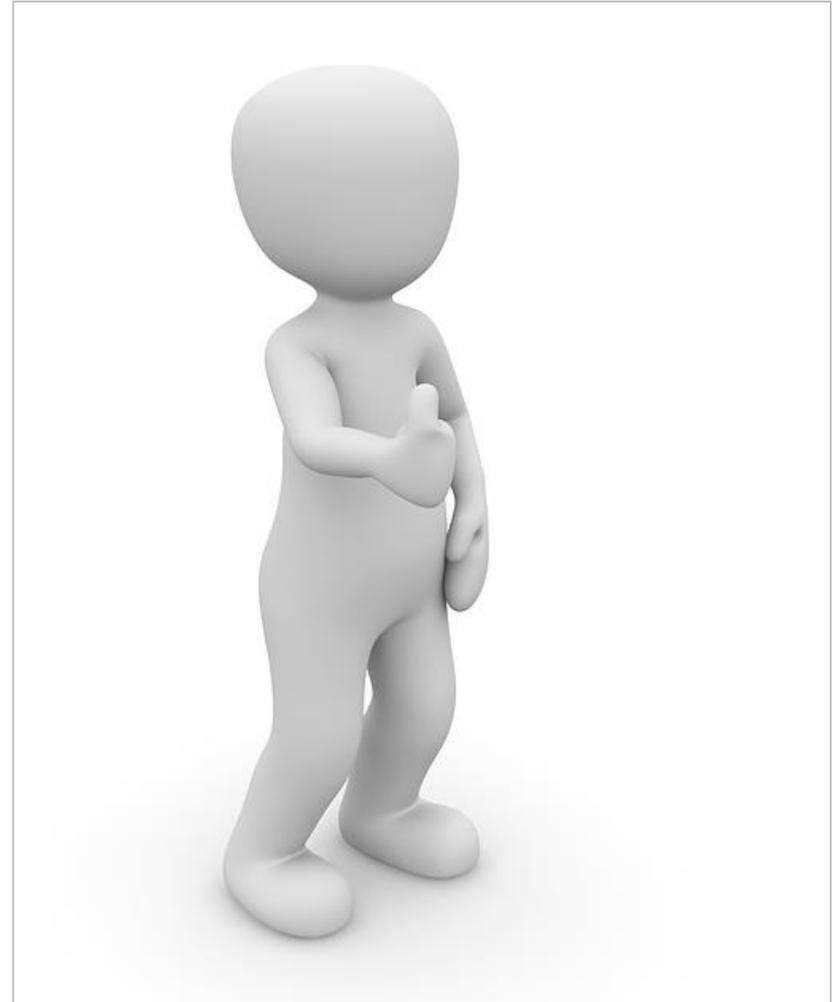
- En esta sección deberás describir:
 - Una portada que incluya tu identificador de usuario en el foro.
 - Los antecedentes concretos que conozcas del caso. Enunciado del mismo descrito con tus propias palabras.
 - Estado de las evidencias que te fueron entregadas. El tamaño y descripción del archivo de evidencias recibido con los datos que puedan permitir la comprobación de su integridad por terceros.
 - Las limitaciones del análisis que estás realizando dado el estado y conjunto de evidencias recibidas. Ten en cuenta que no tienes acceso al dispositivo real y que solo estás analizando una de las particiones del dispositivo.
 - Lo que se te pide corroborar o comprobar como analista forense.
- Dado el caso simulado del informe, no será necesario que incluyas:
 - Quién ha solicitado el informe forense.
 - Las fechas más importantes en relación al informe.
 - Datos personales del analista.

Herramientas utilizadas

- Deberás describir todas las herramientas utilizadas.
- Además de las mostradas durante la resolución del ejercicio:
 - Autopsy.
 - Sqliteman.
 - Firefox.
 - Exiftool.
- Deberás añadir todas las herramientas adicionales que hayas utilizado. Por cada una de ellas recuerda especificar:
 - Versión de la herramienta utilizada (incluyendo plataforma).
 - Fabricante.
 - Tarea para la que se ha utilizado.
- Si has utilizado alguna herramienta reciente o poco conocida deberás incluir un test de validación de la misma.

Adquisición de evidencias

- Deberás incluir el proceso que has llevado para añadir la imagen obtenida a Autopsy.
- Para esta simulación esta sección del informe no será muy relevante, ya que el proceso será muy similar para todos los alumnos.

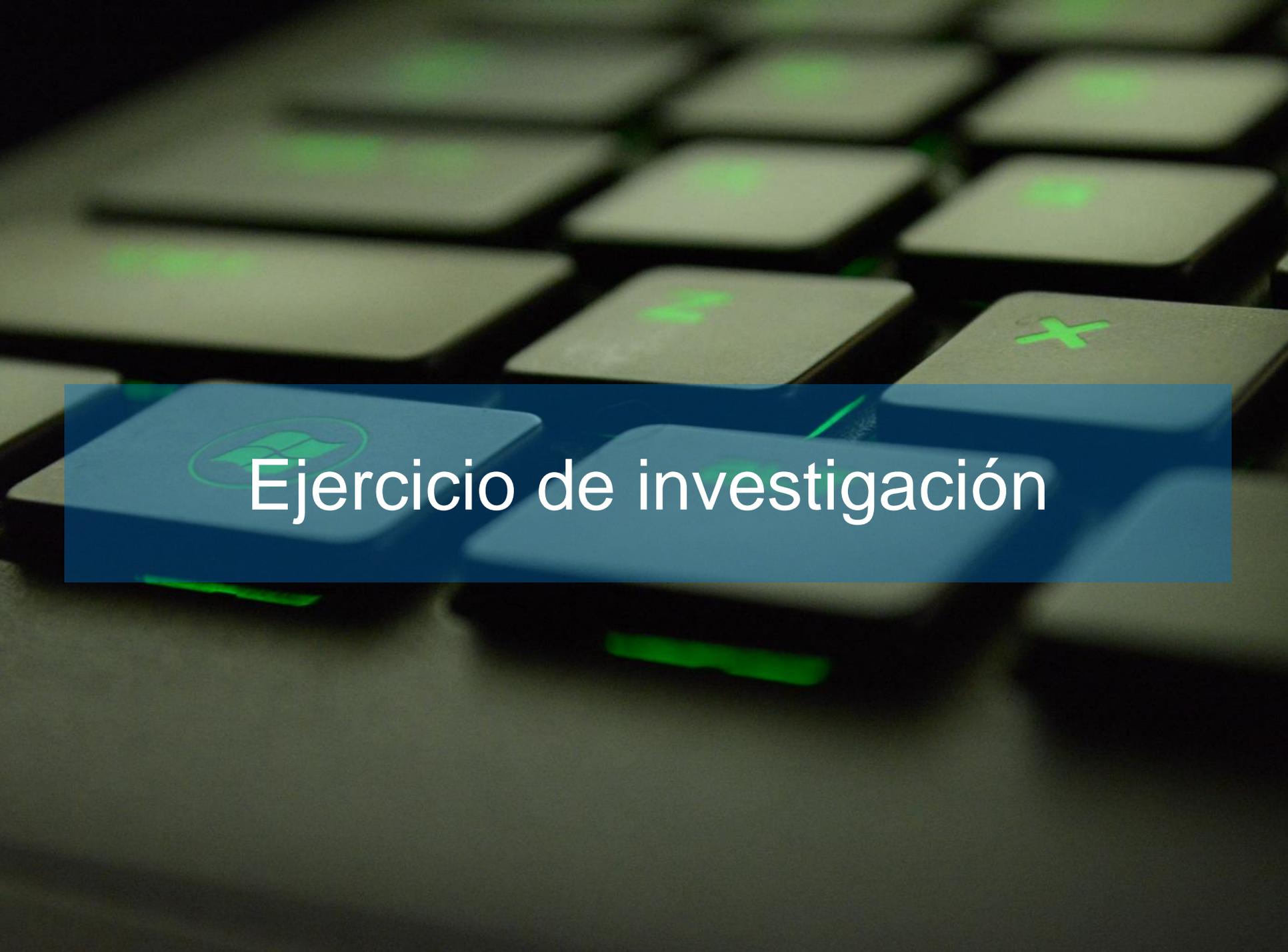


Procesado de evidencias

- En esta sección deberás escribir como has extraído los diferentes ficheros de evidencias que utilizarás para demostrar tus razonamientos durante la fase de análisis.
- Si has realizado alguna operación para la recuperación de archivos en el espacio borrado deberás describir el proceso llevado a cabo.
- Además, por cada elemento de información extraído de la imagen deberás obtener su resumen MD5 y añadirlo al informe forense:
 - Cada evidencia extraída debe poder trazarse de forma unívoca a los datos originales.
 - Además, de esta manera también podrás comprobar que tus compañeros han analizado exactamente las mismas evidencias.

Análisis y conclusiones

- En esta sección deberás razonar, basándote en la información extraída en la sección anterior, los diferentes hechos que se demuestran con la información existente en la imagen analizada.
- En este caso, el conjunto de razonamientos e hipótesis vienen dirigidos por el personal que nos ha encargado el caso, por lo que nuestro trabajo en ese sentido está limitado.
- Cada una de las conclusiones que extraigas del análisis deberá estar justificada por alguna evidencia que se haya identificado durante el proceso de extracción y análisis.
- Es posible que dadas las evidencias existentes, no puedas realizar ciertas afirmaciones con rotundidad, por lo tanto debes limitar tus afirmaciones a lo que indican las evidencias.



Ejercicio de investigación

◆◆◇ Ejercicio de Investigación

Descripción

- Durante este ejercicio deberás realizar una labor de investigación y volcar en el foro de la asignatura los resultados obtenidos para el debate con el resto de alumnos.
- Durante la unidad, hemos estudiado y visto las limitaciones que suponen algunas de las tecnologías de seguridad incluidas en los dispositivos móviles para el análisis forense.
- En este ejercicio deberás investigar una de las tecnologías que se presentan a continuación:
 - Cifrado de disco.
 - Cifrado de copias de seguridad.
 - Bloqueo con código del terminal.
 - Borrado remoto.

◆◆◆ Ejercicio de Investigación

Descripción

- Para la tecnología que selecciones, deberás especificar:
 - Plataformas que la implementan.
 - ¿Desde qué versión?
 - Impacto en los resultados del análisis forense (por plataforma).
 - ¿Cuánto puede llegar a dificultar el análisis?
 - Recomendaciones para reducir su impacto durante el proceso de análisis.
 - ¿Se puede evitar de alguna manera durante la incautación o cualquier otro momento del análisis?
 - Herramientas (comerciales o no) que permiten mitigarla durante el proceso de análisis forense.

A hand holding a pen is positioned over an open notebook. In the foreground, a black calculator is placed on the notebook's pages. The notebook contains mathematical problems, including arithmetic series and word problems. A semi-transparent blue banner is overlaid across the center of the image, containing the text 'Test de evaluación'.

Test de evaluación

26. $1 + 5 + 9 + \dots + 401$
28. $(-30) + (-35) + (-20) + \dots + 79$
30. $2 + 13 + 24 + \dots + 79$
32. the first 30 terms of the series

34. $\sum_{n=1}^{10} (2n - 4)$
the arithmetic series $7 + 11 + 15 + 19 + \dots$
the arithmetic series $1 + 1.25 + 1.5 + 1.75 + \dots$

39. $2 + 9 + 16 + \dots + 65$
41. $80 + 76 + 72 + \dots + 40$
the seventeenth hexagonal number, which is equal to S_{17} for the

Nation in a country experiencing runaway inflation, the cost of a tomato on January 1 of a non-leap year a tomato during the year?
the first five terms of the sequence graphed at
\$0 for the first parking offense. The fine
subsequent offense.
driver would pay for ten offenses.

Gracias por su atención





Métodos de adquisición de datos



Tipos de adquisición de datos

◆◆◆ Tipos de adquisición de datos

Introducción I

- Una vez enumeradas las evidencias que se van a adquirir hay que obtener los datos de los dispositivos que van a ser objeto del informe forense.
- El método utilizado para adquirir los datos del dispositivo variará dependiendo de:
 - La plataforma de la que se van a adquirir los datos (Android, iOS, Windows Phone, BlackBerry, etc.).
 - La versión específica del hardware, software y configuración del dispositivo (versión del dispositivos, configuración de desbloqueo activa, etc.).
 - El estado en el que se encontró el dispositivo (apagado o encendido, bloqueado o sin bloquear, etc.).
 - El tipo de datos a adquirir y su volatilidad (capturar datos en almacenamiento persistente o en memoria).
- Dependiendo de la variables anteriores se pueden realizar tres tipos principales de adquisición: manual, lógica y física.

◆◆◆ Tipos de adquisición de datos

Adquisición manual

- Se interacciona con el propio dispositivo para acceder a los datos del mismo. La adquisición de los datos, se realiza mediante capturas de pantalla o fotografías a la pantalla del dispositivo.
- Este tipo de adquisición cuenta con varias ventajas:
 - + No requiere de herramientas adicionales.
 - + Permite extraer la información en un contexto sencillo de entender para lectores no especializados.
- Pero también con ciertas desventajas:
 - Sólo se puede acceder a datos visibles en la pantalla.
 - Puede modificar el estado del dispositivo.
 - El tiempo de procesado de los datos es más prolongado.

◆◆◆ Tipos de adquisición de datos

Adquisición lógica

- Consiste en copiar los archivos y directorios del sistema de archivos del dispositivo.
- Para ello se utilizan:
 - Las propias API de acceso al sistema de ficheros del dispositivo objeto de análisis . El sistema operativo del dispositivo copiará a otro dispositivo los ficheros y directorio solicitados.
 - Las API de el sistema operativo de la herramienta de adquisición, la unidad se conecta al dispositivo a analizar. Los datos del sistema analizado seguirán siendo leídos por el *firmware* del dispositivo analizado.
- Sus puntos positivos son:
 - + Es fácil de conseguir y, generalmente, no requiere hardware especializado.
 - + En algunos casos se puede realizar desde otro dispositivo (testadas), por lo que las API del dispositivo analizado no son utilizadas.
- Mientras que los negativos:
 - No copia archivos borrados o información que haya sido ocultada en el sistema de archivos.
 - Depende de los permisos de acceso a los diferentes archivos del sistema.

◆◆◇ Tipos de adquisición de datos

Adquisición física

- Consiste en el copiado físico bit a bit del dispositivo físico de almacenamiento.
- Requiere de acceso completo al dispositivo de almacenamiento.
- En el dispositivo móvil, de forma general el sistema de almacenamiento se encuentra soldado al resto de los componentes del teléfono y no es accesible de forma física.
- Además, dadas las medidas de seguridad incluidas en los sistemas operativos móviles, en muchas ocasiones, es necesario ejecutar *exploits* sobre el sistema para realizar el copiado a bajo nivel.
- Sus ventajas son:
 - + Permite acceder a todos los bloques del soporte físico copiado, incluyendo los archivos borrados y bloques que no están marcados como utilizados.
- Y sus inconvenientes:
 - Es generalmente, el proceso más complejo de todos, y no siempre es posible de realizar.

◆◆◆ Tipos de adquisición de datos

Tipos de almacenamiento

- La adquisición física depende de los tipos de almacenamiento con los que consta el dispositivo móvil:
 - La memoria NAND es el tipo de memoria flash más utilizada para el almacenamiento en los dispositivos móviles. Se puede leer y escribir en bloques.
 - Es utilizada de forma genérica para el almacenamiento del sistema operativo, la partición de datos del sistema y otras memorias extraíbles.
 - La memoria NOR es otro tipo de memoria flash optimizada para la ejecución de código. Permite la lectura y ejecución de bytes de forma independiente.
 - En los últimos años, su utilización se está viendo reducida a favor de las memorias NAND, para usos más genéricos.
 - Las tarjetas de memoria utilizan memorias NAND. Generalmente están formateadas en FAT32.
 - Los dispositivos iOS no permiten la utilización de tarjetas SD. Los dispositivos con Windows Phone, Android y BlackBerry sí, dependiendo del modelo.

◆◆◇ Tipos de adquisición de datos

Modificación del dispositivo adquirido

- En un entorno ideal, la adquisición de datos del dispositivo no debería modificar el estado físico del dispositivo.
- Desgraciadamente esto no siempre es posible.
- Dependiendo de su estado, el tipo de adquisición y las herramientas utilizadas, el estado del dispositivo se verá afectado:
 - Fecha y hora de acceso a ficheros.
 - Borrado o creación de nuevos ficheros.
 - Modificación de la memoria del dispositivo para la carga de aplicaciones de volcado.
- Para que la validez del análisis no se vea afectada, es necesario documentar todos los tipos de adquisición realizadas y las consecuencias que tiene cada una de ellas sobre el dispositivo analizado:
 - La adquisición manual creará ficheros de captura de pantalla.
 - La adquisición lógica puede modificar la fecha de acceso a los ficheros.



Maximizando la adquisición de
datos

◆◆◇ Maximizando la adquisición de datos

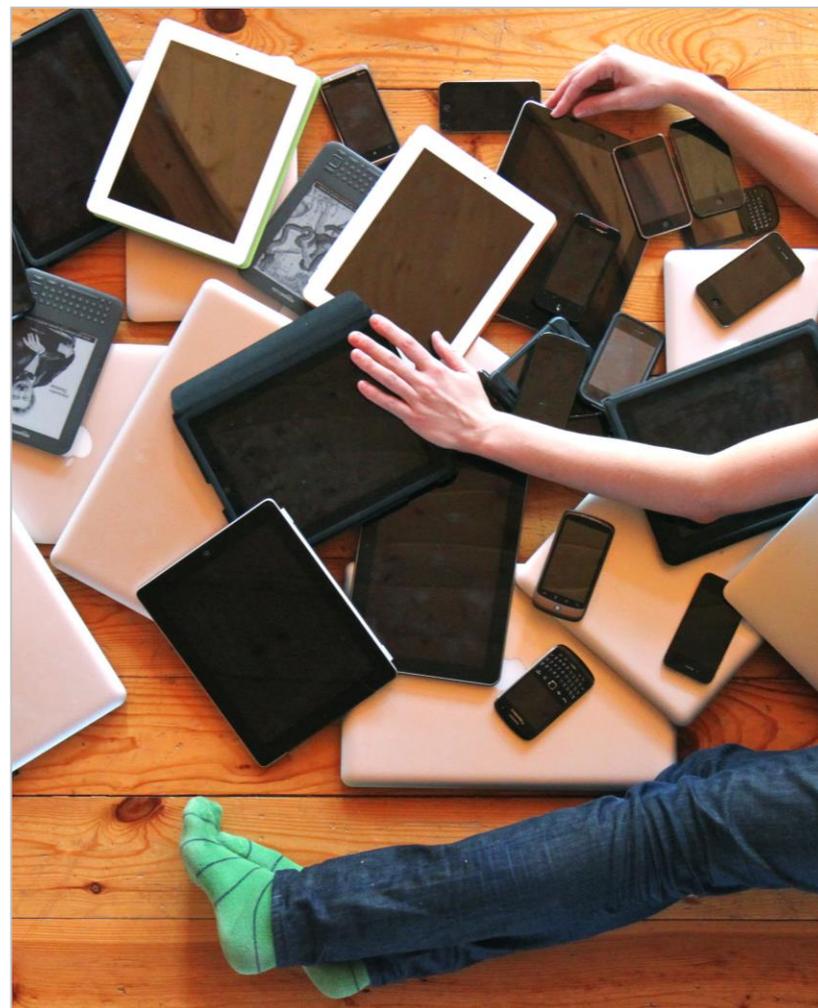
Introducción

- La cantidad de datos accesibles en un dispositivo móvil dependen en gran medida en el estado en el que se encuentra:
 - **Desbloqueado:** Se puede acceder al dispositivo hasta que se bloquee por inactividad.
 - **Bloqueado** por código u otro sistema de autenticación: Es necesario introducir un código de acceso (o huella dactilar o similar) para acceder al dispositivo.
 - **Apagado:** Para poder acceder al dispositivo hay que pasar por el proceso de encendido.
- Para maximizar la cantidad de datos posibles a obtener en un dispositivo es fundamental seguir un conjunto de pasos iniciales. Si bien los pasos concretos variarán para cada plataforma, este conjunto de procedimientos se puede realizar con cualquier terminal, independientemente del sistema operativo o fabricante.

◆◆◆ Maximizando la adquisición de datos

Dispositivo desbloqueado

- Si el dispositivo ha sido incautado desbloqueado, los pasos a realizar serán los siguientes:
 - Aislar el dispositivo de la red, poner en modo avión y extraer la tarjeta SIM. Es recomendable introducirlo en un recipiente que aisle el campo electromagnético (Jaula de Faraday).
 - Activar todas las opciones posibles para permitir el acceso físico al dispositivo:
 - Eliminar el código de bloqueo (si se puede).
 - Activar la depuración a través de USB.
 - Desactivar el bloqueo por inactividad (siempre activo).
 - Obtener todos los medios extraíbles, tarjeta SD, SIM o copias de seguridad en dispositivos asociados (ordenadores).



◆◆◆ Maximizando la adquisición de datos

Dispositivo bloqueado

- Si el dispositivo está bloqueado solo podremos:
 - Aislar el dispositivo de la red, extraer la tarjeta SIM o introducirlo en una caja de Faraday.
 - Comprobar si el dispositivo tiene activada la depuración a través de USB. En el caso de que la conexión USB esté activa es posible que podamos cargar *bootloaders* para modificar el sistema de arranque del dispositivo y permitir así el acceso físico al mismo.
 - Si el dispositivo no tiene activada la depuración USB, ejecutar un ataque para la extracción del código de bloqueo (*smudge attack* o *fuerza bruta*).
 - Obtener todos los medios extraíbles: tarjeta SD, SIM o copias de seguridad en dispositivos asociados (ordenadores).
 - Si el dispositivo se encuentra apagado podemos proceder directamente a extraer todos los medios extraíbles y encender el teléfono.

A group of green Android robots standing in a line, with a semi-transparent text box overlaid in the center. The robots are rendered in a 3D style with soft shadows and highlights, set against a light gray background. The text box is a horizontal rectangle with a semi-transparent green fill, containing the text "Adquisición de datos en Android" in white, sans-serif font.

Adquisición de datos en Android

◆◆◆ Adquisición de datos en Android

Adquisición manual

- Solo es realizable si el teléfono se encuentra desbloqueado.
- Listar todas las aplicaciones existentes y realizar capturas de pantalla de los elementos que se consideren pertinentes.
- Es posible que para el acceso a los datos de algunas aplicaciones sea necesario conectar el dispositivo a Internet. Esto se debe realizar sólo como último recurso, ya que el dispositivo puede ser bloqueado remotamente.
- Además de las aplicaciones, es importante acceder a los ajustes y capturar la información de cada una de las cuentas existentes en el dispositivo.
- El método utilizado para la realización de capturas de pantalla puede diferir dependiendo de la versión del sistema. En general se puede realizar manteniendo pulsado el botón de bajar el volumen y el botón de inicio hasta que se realiza la captura de pantalla.

◆◆◆ Adquisición de datos en Android

Adquisición lógica

- Se puede realizar mediante adb con el siguiente comando

```
> adb backup -apk -shared -system -all -f file.backup
```

Incluir APK de aplicaciones de terceros

Incluir almacenamiento extraíble

Incluir aplicaciones del sistema

Incluir todas las aplicaciones

Fichero de salida

- Las aplicaciones que no permitan el *backup* no se copiarán.
- Una vez obtenida la copia de seguridad se puede extraer utilizando:
 - Android Backup Extractor - <https://sourceforge.net/projects/adbextractor/>
- Y el comando:

```
> java -jar abe.jar unpack file.backup file.tar
```
- También se puede realizar a través de apps (solo se podrá acceder a información del teléfono accesible mediante permisos):
 - AFLogical - Disponible en Santoku Linux.

◆◆◆ Adquisición de datos en Android

Adquisición física

- Sólo se puede realizar si se tiene acceso de administrador al dispositivo o mediante acceso físico y una conexión al interfaz JTAG del chip de memoria.
- Si el dispositivo está *rootado*, se puede realizar con `dd`.
- En primer lugar se busca la ruta a toda la memoria flash:
 - > `cat /proc/partitions`
 - La primera entrada (`mmcblk0` generalmente) corresponde a la totalidad de la memoria flash.
- Averiguamos el tamaño de bloque del sistema:
 - > `df /data`
- Y con lo obtenido bajo la columna `Blksize` ejecutamos `dd`:
 - > `dd if=/dev/block/mmcblk0 of=/sdcard/blk0.img bs=4096`
 - `conv=notrunc,noerror,sync`
- Si la imagen del disco se guarda en la tarjeta SD, hay que asegurarse de que la tarjeta introducida ha sido borrada convenientemente (todo 0s).

◆◆◇ Adquisición de datos en Android

Adquisición física - Memoria

- La implementación de `dd` para Android no está convenientemente preparada para leer la memoria RAM del dispositivo.
- La memoria del dispositivo se puede adquirir utilizando la herramienta Linux Memory Extractor (LiME) que se encarga de:
 - Averiguar las direcciones físicas de los rangos de direcciones de la RAM inspeccionando el *kernel*.
 - Transformar las direcciones físicas en virtuales.
 - Copiar el contenido de las direcciones virtuales a un *socket* de red o a la tarjeta SD para su extracción.
- LiMe es una extensión del *kernel* que se debe cargar a través de `adb` (se verá el proceso durante un laboratorio).
- La adquisición de Memoria RAM de procesos separados también es posible en dispositivos marcados como producción (o el emulador), a través del Android Device Monitor.



Adquisición de datos en iOS

◆◆◆ Adquisición de datos en iOS

Adquisición manual

- Solo es realizable si el teléfono se encuentra desbloqueado.
- Para desactivar el código de bloqueo es necesario conocer el existente, por lo que se recomienda desactivar el bloqueo automático.
- Listar todas las aplicaciones existentes y realizar capturas de pantalla de los elementos que se consideren pertinentes.
- Es posible que para el acceso a los datos de algunas aplicaciones sea necesario conectar el dispositivo a Internet. Esto se debe realizar sólo como último recurso, ya que el dispositivo puede ser bloqueado remotamente.
- En los ajustes de privacidad es posible acceder a los datos de diagnóstico enviados a los desarrolladores de aplicaciones.

◆◆◆ Adquisición de datos en iOS

Adquisición lógica I

- Se puede realizar sólo si el teléfono está desbloqueado o no tiene código.
- En iOS9 seleccionar “Confiar en este ordenador”.
- Mediante iTunes:
 - Se conecta el dispositivo a iTunes y se realiza la copia de seguridad.
 - Si la copia de seguridad está cifrada se deberá realizar un ataque de fuerza bruta para descifrarla:
 - Existen utilidades de pago para esta tarea (<https://www.elcomsoft.com/eppb.html>).
- Mediante idevicebackup (idevicebackup2):
 - Disponible en Santoku en dos versiones, dependiendo de la versión de iOS:
 - > idevicebackup backup directorio
 - Si el dispositivo tiene *jailbreak*, se puede instalar el servidor SSH o la aplicación de terminal para abrir una conexión SSH a otro equipo.
- Mediante iCloud, son necesarias las credenciales de la cuenta Apple enlazada con el dispositivo.

Adquisición lógica II

- Mediante las aplicaciones del tipo iFunBox o iPhone Explorer:
 - El soporte depende de la versión del sistema operativo.
 - Dependiendo de la versión de iOS permiten el acceso a la *sandbox* de cada aplicación.
 - Si el dispositivo tiene *jailbreak* se puede acceder a todo el sistema de archivos.
- La información extraída por estos métodos no incluye:
 - Correos electrónicos.
 - Historial de localización.
 - Caché de las aplicaciones.
 - Ficheros ejecutables.



◆◆◆ Adquisición de datos en iOS

Adquisición física

- Si el dispositivo tiene *jailbreak*, se puede realizar de forma similar a la realizada en Android:
 - Desde la máquina del analista ejecutamos:
> `ssh root@ip dd if=/dev/rdisk0 bs=1M | dd of=ios-root.img`
 - Ejecuta dd en el iPhone a través de SSH y redirige la salida del comando a la imagen en la máquina del analista (con el comando dd de nuevo).
 - A partir del iPhone 3GS esta herramienta tiene poca utilidad ya que la memoria flash del dispositivo se encuentra cifrada.
- Mediante aplicaciones comerciales:
 - Lantern de Katana Forensics - <https://katanaforensics.com>
 - Mobile Phone Examiner de Access Data - <http://accessdata.com>
 - Encase.
 - FTK.
 - Este tipo de herramientas son capaces de extraer la clave de cifrado y descifrar la imagen resultante.



Adquisición de datos en Windows Phone

◆◆◆ Adquisición de datos en Windows Phone

Adquisición manual

- Solo es realizable si el teléfono se encuentra desbloqueado.
- Para desactivar el código de bloqueo es necesario conocer el existente, por lo que se recomienda desactivar únicamente desactivar el bloqueo automático.
- Listar todas las aplicaciones existentes y realizar capturas de pantalla de los elementos que se consideren pertinentes.
- Es posible que para el acceso a los datos de algunas aplicaciones sea necesario conectar el dispositivo a Internet. Esto se debe realizar sólo como último recurso, ya que el dispositivo puede ser bloqueado remotamente.
- Además de las aplicaciones, también se puede acceder, a través de los ajustes del teléfono a las últimas wifi conectadas y otros datos importantes de configuración del teléfono.

◆◆◆ Adquisición de datos en Windows Phone

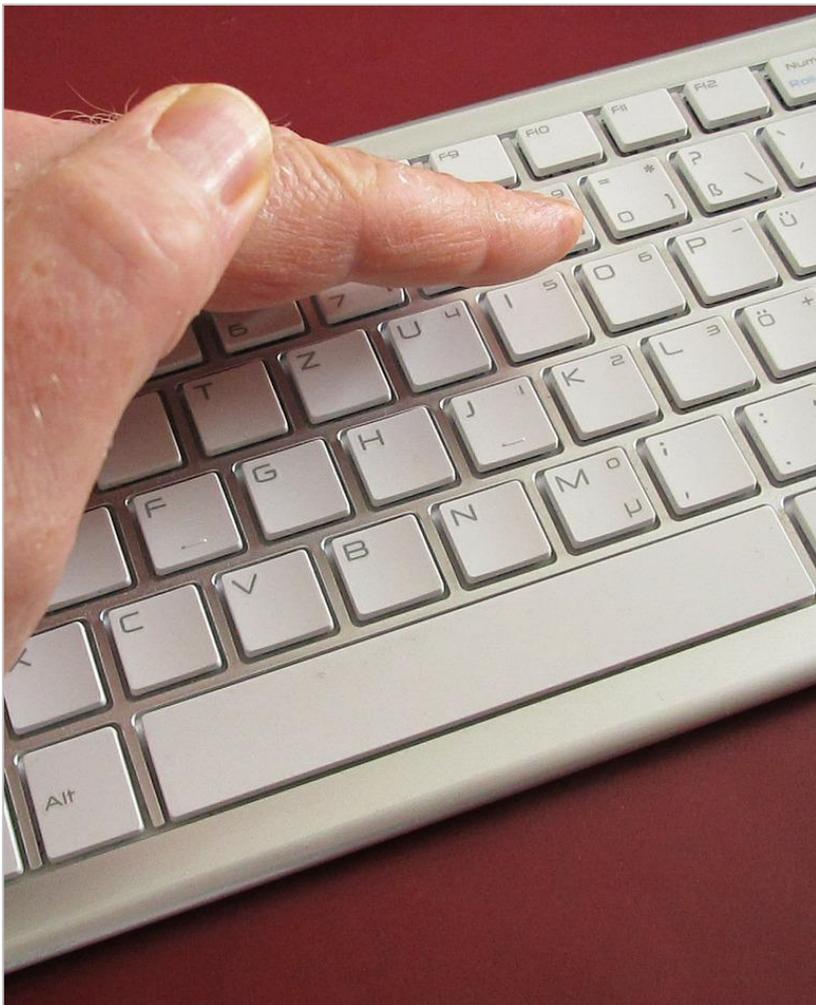
Adquisición lógica



- Antes de Windows Phone 7.5 se puede realizar mediante la aplicación Windows Phone Device Manager.
- A partir de Windows Phone 8.0 el almacenamiento del dispositivo no es accesible a través de la conexión USB.
- Sólo es posible la adquisición a través de la utilidad de copia de seguridad en la nube accesible utilizando las credenciales de la cuenta asociada al dispositivo.

◆◆◆ Adquisición de datos en Windows Phone

Adquisición física



- No existen aplicaciones forenses que soporten la extracción física de dispositivos Windows Phone.
- La única opción posible es la adquisición a través del interfaz JTAG de la memoria flash. Si el dispositivo está cifrado (uso empresarial) esta tarea no es de mucha utilidad.



Adquisición de datos en BlackBerry

◆◆◆ Adquisición de datos en BlackBerry

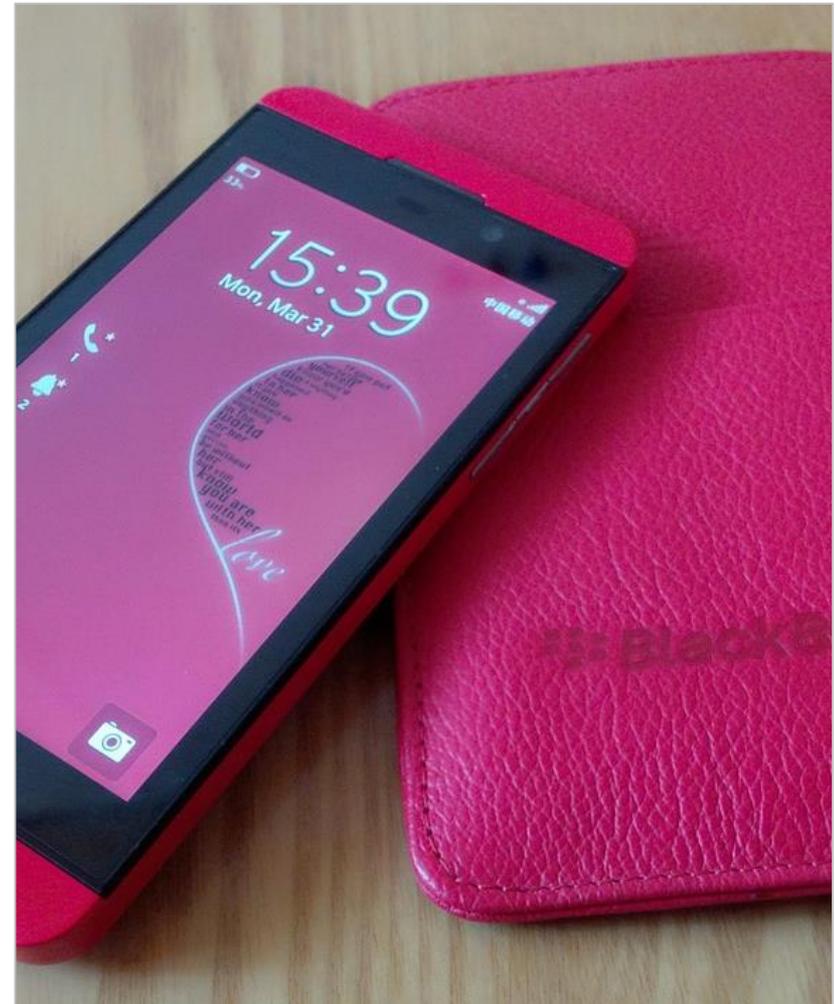
Adquisición manual

- Solo es realizable si el teléfono se encuentra desbloqueado.
- Para desactivar el código de bloqueo es necesario conocer el existente, por lo que se recomienda desactivar únicamente desactivar el bloqueo automático.
- Listar todas las aplicaciones existentes y realizar capturas de pantalla de los elementos que se consideren pertinentes.
- Es posible que para el acceso a los datos de algunas aplicaciones sea necesario conectar el dispositivo a Internet. Esto se debe realizar sólo como último recurso, ya que el dispositivo puede ser bloqueado remotamente.
- Además de las aplicaciones, también se puede acceder, a través de los ajustes del teléfono a las últimas wifi conectadas y otros datos importantes de configuración del teléfono.

◆◆◆ Adquisición de datos en BlackBerry

Adquisición lógica

- Además del dispositivo, la tarjeta SD se puede encontrar cifrada también (si el modelo tiene ranura SD).
- El único método disponible es la utilización de las credenciales de acceso a la cuenta de BlackBerry Link del dispositivo asociado. Desde la cuenta se puede descargar la copia de seguridad del dispositivo para su análisis con las herramientas forenses adecuadas.



◆◆◆ Adquisición de datos en BlackBerry

Adquisición física

- El almacenamiento en los dispositivos BlackBerry se encuentra cifrado por lo que la extracción física del dispositivo no es de utilidad de cara al análisis forense.

