UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

6. – Análisis forense de entornos móviles

Ciberseguridad en Dispositivos móviles
DISCA – ETS de Ingeniería informática (UPV)

Documento Original de incibe_

Objetivos

- Aprender a extraer información de dispositivos móviles
- Aprender a realizar un análisis de las pruebas informáticas a partir de evidencias
- Aprender a escribir un informe de las pruebas obtenidas

Índice

1. Introducción al análisis forense
2. Etapas de análisis forense
3. Métodos de adquisición de datos
4. Análisis de datos
5. Herramientas básicas
6. El informe forense

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.

Introducción al análisis forense

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.

Introducción al análisis forense

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 sensibles, etc.).
  - Revisar el cumplimiento de normativas y estándares de seguridad.
  - Asegurar que se cumplen los procedimientos para la destrucción de datos sensibles en un sistema.

Introducción al análisis forense

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 puedes 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.

Introducción al análisis forense

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.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE 298 (1999)
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE 77 (2015)
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Introducción al análisis forense

Consideraciones legales

- La Constitución española otorga a todos los ciudadanos una serie de derechos fundamentales y libertades públicas, reguladas por el título I de la Constitución, capítulo 2, sección 1. De entre ellos, cabe destacar:
  - Derecho a la seguridad jurídica y tutela judicial, la cual nos garantiza un proceso penal con garantías.
  - Derecho al secreto de las comunicaciones.
  - Derecho a la vida privada.
    - En este derecho se incluye el derecho a la intimidad, una vida privada, derecho al honor y la propia imagen.
    - Asimismo se incluye la limitación del uso de la informática para proteger la intimidad.
    - Derecho fundamental a la protección de datos.
      - En el año 2000 en la sentencia 292/2000, el Tribunal Constitucional crea el derecho fundamental a la protección de datos como un derecho diferente al de intimidad.

Introducción al análisis forense

Consideraciones legales

- Ley de Protección de Datos de Carácter Personal:
  - LOPD son las siglas abreviadas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
  - Esta Ley fundamentalmente tiene el objetivo de proteger a las personas físicas con respecto al tratamiento que se pueda realizar de sus datos propios por distintos sujetos, ya sean públicos o privados.
  - Dicha regulación pretende, fundamentalmente, establecer un control sobre quién tiene dichos datos, para qué los usa y a quién se los cede.
    - impone una serie de obligaciones a los responsables de dichos ficheros de datos:
      - como son las de recabar el consentimiento de los titulares de los datos para poder tratarlos,
      - comunicar a un registro especial la existencia de dicha base de datos y su finalidad,
      - así como mantener unas medidas de seguridad mínimas de la misma, en función del tipo de datos recogidos.
  - Antes de comenzar un análisis forense debe de obtenerse de forma explicita y por escrito el consentimiento del propietario del dispositivo/información o de la autoridad pertinente en la investigación

Introducción al análisis forense

Consideraciones legales

- Ley de Protección de Datos de Carácter Personal:
  - LOPD reconoce una serie de derechos al individuo sobre sus datos:
  - los de información, acceso, rectificación e, incluso, de cancelación de los mismos en determinados supuestos.
- Dentro del Reglamento de Desarrollo de la LOPD (RD 1720/2007), existen tres niveles de seguridad distintos:
  - Básico, medio y alto.
  - Para saber qué nivel debemos de aplicar, debemos referirnos al tipo de datos personales almacenados en el fichero, dispuesto en el artículo 81 del Reglamento.

Introducción al análisis forense

Consideraciones legales

- Nivel básico:
  - Aplicable a todos los sistemas con datos personales en general.
- Nivel medio:
  - Datos de comisión de infracciones administrativas o penales.
  - Datos de Hacienda pública.
  - Datos de servicios financieros.
  - Datos sobre solvencia patrimonial y crédito,
  - Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.
- Nivel alto:
  - Datos sobre ideología.
  - Datos sobre religión.
  - Datos sobre creencias.
  - Datos sobre origen racial.
  - Datos sobre salud o vida sexual.
  - Datos recabados para fines policiales.
  - Datos sobre violencia de género.

- Estas medidas de seguridad se aplican de forma acumulativa, así, el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad.

Introducción al análisis forense

Particularidades del entorno móvil II

- **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.
  - Siempre hay que verificar/contrastar cada evidencia en el contexto del caso, para poder detectar cualquier técnica anti-forense aplicada
  - Ejemplos de técnicas anti-forense:
    - DESTRUCCIÓN DE LA EVIDENCIA:
      - Este método busca tanto la eliminación de la evidencia como imposibilitar su recuperación. Para ello, se pueden llevar a cabo dos estrategias:
        - Destrucción a nivel físico: por ejemplo mediante la aplicación de campos magnéticos u otros métodos menos sutiles o poco convencionales.
        - Destrucción a nivel lógico: mediante la sobre escritura de datos o la eliminación de los mismos.
      - Para intentar recuperar información sobrescrita, dañada o eliminada se utilizan diferentes técnicas como el file carving o slack space.
      - Puede ser un proceso lento y costoso en lo que a recursos se refiere, y que su grado de eficacia no es del todo óptimo..

Introducción al análisis forense

Particularidades del entorno móvil II

- **Técnicas anti-forense:**
  - Ejemplos de técnicas anti-forense:
    - Ocultar de la evidencia:
      - Este método no busca manipular o destruir la evidencia sino hacerla lo menos accesible posible.
      - Para ello, se pueden utilizar técnicas como «covert channels» o esteganografía que permite la ocultación y el enmascaramiento de cierta información dentro de otra.
      - Para detectar este tipo de prácticas, se deben utilizar herramientas de estegoanálisis, que mediante complejos mecanismos estadísticos o mediante la búsqueda de anomalías con respecto a los formatos estándar, buscan información oculta.
      - Ambos métodos se pueden ser combinados y a la vez con métodos criptográficos con el fin de dificultar aún más la investigación.
        - El uso de herramientas de cifrado obstaculiza notablemente el trabajo de un investigador, el cual debe remitirse a métodos de criptoanálisis como meet in the middle, side-channel attacks o ataques por fuerza bruta para poder visualizar el contenido cifrado.

Introducción al análisis forense

Particularidades del entorno móvil II

- **Técnicas anti-forense:**
  - Ejemplos de técnicas anti-forense:
    - Ocultar de la evidencia:
      - Este método no busca manipular o destruir la evidencia sino hacerla lo menos accesible posible.
      - Para ello, se pueden utilizar técnicas como «covert channels» o esteganografía que permite la ocultación y el enmascaramiento de cierta información dentro de otra.
      - Para detectar este tipo de prácticas, se deben utilizar herramientas de estegoanálisis, que mediante complejos mecanismos estadísticos o mediante la búsqueda de anomalías con respecto a los formatos estándar, buscan información oculta.
      - Ambos métodos se pueden ser combinados y a la vez con métodos criptográficos con el fin de dificultar aún más la investigación.
        - El uso de herramientas de cifrado obstaculiza notablemente el trabajo de un investigador, el cual debe remitirse a métodos de criptoanálisis como meet in the middle, side-channel attacks o ataques por fuerza bruta para poder visualizar el contenido cifrado.
      - Utilización de Rootkits (encubridor)
        - Es un conjunto de herramientas que sirven para esconder los procesos y archivos.
        - Algunas herramientas como Procl o RootkitRevealer permiten realizar un listado de ficheros utilizando en primer lugar la API del sistema y posteriormente realizar otro listado mediante sus propios métodos implementados. Una vez finalizados ambos listados, los comparan y permiten visualizar la existencia de ficheros ocultos.

Introducción al análisis forense

Particularidades del entorno móvil II

- **Técnicas anti-forense:**
  - Ejemplos de técnicas anti-forense:
    - Eliminación de las fuentes de la evidencia
      - Esta técnica puede considerarse la más básica, ya que simplemente consiste en evitar dejar huellas para ocultar el rastro y así no ser detectado.
      - Una manera sencilla puede ser si se pretende evitar cualquier tipo de escritura en disco, por ejemplo desactivando los logs del sistema.
    - Falsificación de la evidencia
      - Este método consiste en la creación de evidencias falsas con el fin de dificultar el trabajo de los investigadores.
      - Algunos de los ejemplos de falsificación de evidencias más habituales son:
        - Lanzar ataques desde equipos comprometidos, como es el caso de las Botnets.
        - La utilización de redes comprometidas.
        - La utilización de cuentas comprometidas de usuarios.
        - La modificación de metadatos mediante utilidades como ExifTool.
        - La falsificación de mensajes de programas de mensajería instantánea, como es el caso de WhatsApp o la suplantación mediante el clonado de la tarjeta SIM.

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.

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

Etapas del análisis forense: Visión general

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.

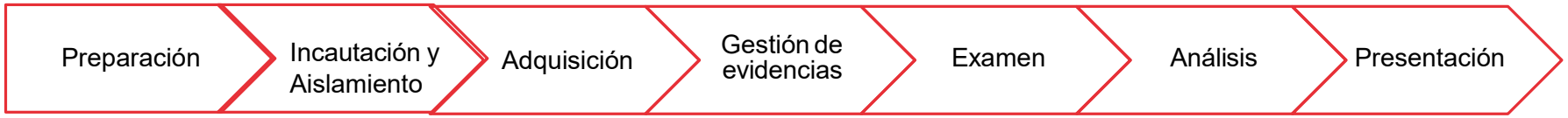
Etapas del análisis forense

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.
  - *Integrated Digital Forensic Process Model* de Michael Donovan Köhn, estudio que analiza modelos existentes ampliamente utilizados para definir un método que recoja lo más relevante de los métodos analizados.

Etapas del análisis forense

Esquema



Para la correcta consecución del proceso de análisis es crucial documentar todas las acciones realizadas a lo largo del análisis forense.

La documentación, cuanto más detalladas mejor, pueden incluir:

- Capturas de pantalla.
- Localización de evidencias encontradas.
- Notas manuscritas.
- Utilización de sistemas de anotación dentro de la propia aplicaciónforense.
- Herramientas utilizadas, detallando versiones, sistema sobre el que se utiliza,…

Etapas del análisis forense

Preparación

- Esta etapa se ejecuta de forma previa al proceso de análisis.
- En esta etapa se debe de preparar lo referente a formularios que tendrán que rellenarse en el momento inicial:
  - Autorización para la realización del análisis forense
  - Cadena de custodia
  - Identificar los elementos físicos que se van a analizar y las evidencias que se buscarán en cada uno de los elementos analizables.
    - Propietario de la información/dispositivo incautado
    - Modelo del dispositivo
    - Objetivo de la investigación:
      - Información proporcionada por el solicitante de la investigación
      - Información que busca el solicitante de la investigación
- Preparar el material informático necesario para recabar pruebas del incidente insitu si fuera necesario:
  - Estación de clonación (o computador para llevar acabo el copiado de pruebas)
  - Tarjetas SD
  - Discos externos

Etapas del análisis forense

Incautación y Aislamiento

- En el momento en el que el dispositivo es incautado, debe protegerse su integridad, de modo que nuestras acciones no conlleven ninguna modificación en el mismo
- Normalmente las evidencias se transportarán en bolsas antiestáticas/aislantes,
  - Diseñadas para proteger los componente electrónicos de daños producidos por electricidad estática
  - Aislar el dispositivo de señales externas insertándolo en una Jaula de Faraday
    - Prevenir que el contenido del dispositivo pueda ser modificado/borrado
    - Evitar que el dispositivo pueda ser accedido vía red (Wifi, 4G/5G), SMS, Bluetooth.
  - Los métodos de aislamiento indicados anteriormente no permiten el acceso al dispositivo, por ello también puede contemplarse el uso de tiendas/habitaciones Faraday (aisladas)

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).
- El **proceso de adquisición** se debe realizar teniendo en cuenta la volatilidad de las mismas.
- Es necesario recolectar primero las evidencias más volátiles.

Etapas del análisis forense

Orden de adquisición de evidencias

- 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**.
- 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 trazados
  - Generalmente se hace un resumen de los datos obtenidos mediante una función resumen (SHA-256)
  - Dependiendo de la finalidad de la investigación, el resultado puede ser firmado con la 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.

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 (Hex Dump)

- 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

Adquisición física (Chip-Off)

- La técnica de chip off permite extraer datos directamente de la memoria flash del dispositivo celular.
- Se quita físicamente el chip de memoria del teléfono y crean su imagen binaria.
- Este proceso es costoso y requiere un amplio conocimiento del hardware.
- Un manejo inadecuado puede causar daños físicos al chip y hace que los datos sean imposibles de recuperar.

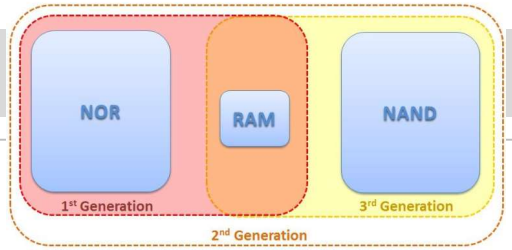
Tipos de adquisición de datos

Adquisición física (Micro Read)

- Este proceso implica la interpretación y visualización de datos en chips de memoria.
- Los investigadores usan un microscopio electrónico de alta potencia para analizar las puertas físicas en los chips y luego convierten el nivel de la puerta en 1 y 0 para descubrir el código ASCII resultante.
- Este proceso es costoso y requiere mucho tiempo. Además, requiere un amplio conocimiento de hardware y sistemas de archivos.

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

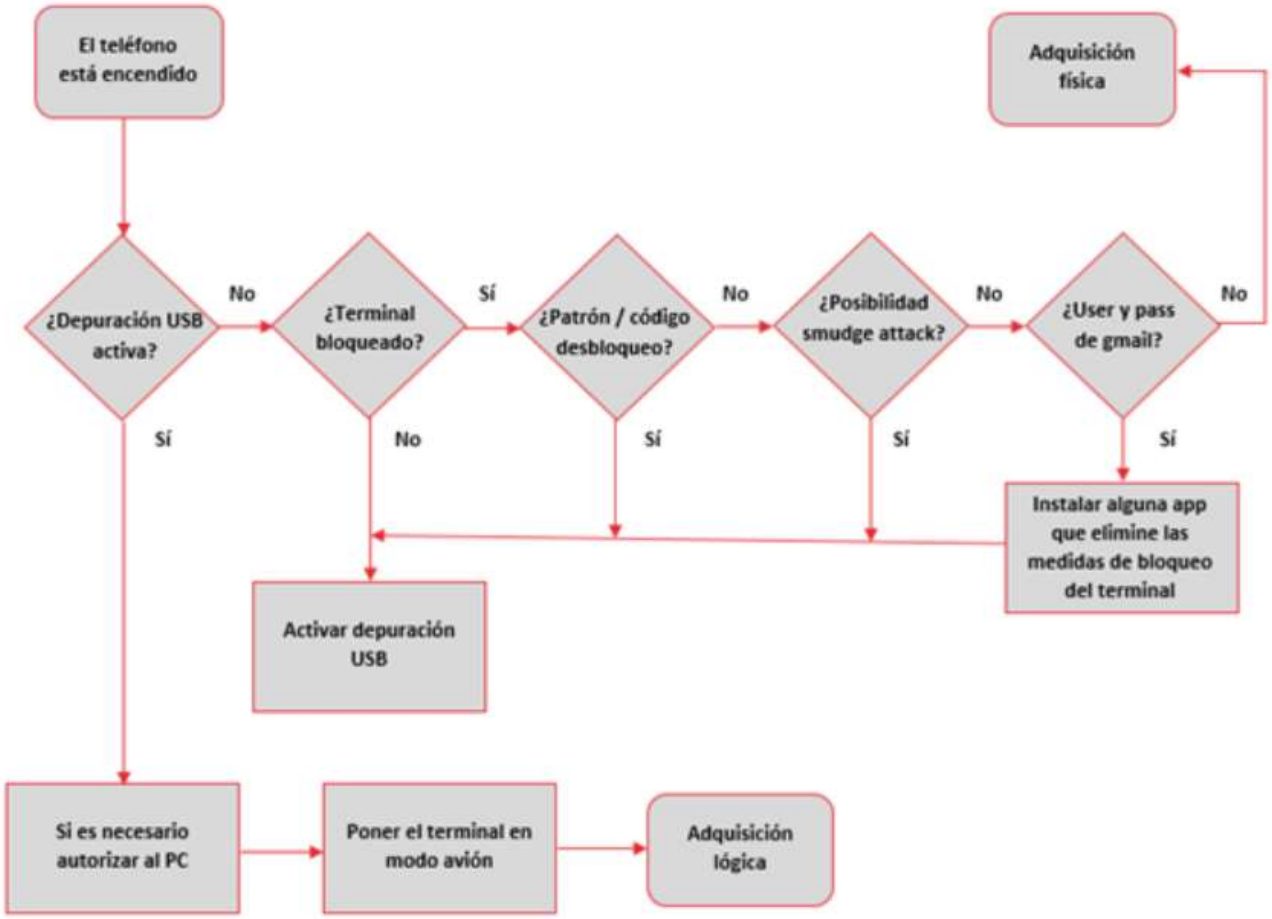
Introducción

- 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 bloqueé 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.

Maximizando la adquisición de datos

Introducción

- Pasos a seguir para maximizar la cantidad de datos posibles a obtener en un dispositivo . (Puede variar para cada plataforma).



Maximizando la adquisición de datos

Dispositivo desbloqueado

- Si el dispositivo incautado está 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 aísle 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 (computador).

Maximizando la adquisición de datos

Dispositivo bloqueado

- Si el dispositivo incautado está bloqueado, mediante uno de los tres tipos de mecanismos ofrecidos por Android: patrón, PIN, y contraseña, existen variadas formas de intentar desbloquearlo. Algunos de esos métodos son:
  - Si la depuración USB está habilitada:
    - Conectar el móvil a la estación forense (computador) mediante un cable USB y acceder a él mediante las ordenes *adb*. Si no estuviera habilitada la depuración USB no se podrá acceder con *adb*.
    - Podemos intentar dos métodos:
      - Eliminar el fichero *gesture.key*:
        - Eliminará el patrón de bloqueo en el móvil.
        - Únicamente funciona si el móvil esta rooteado.
        - Esta acción modificará implicará una modificación del estado del móvil permanentemente.
  - Actualizar el fichero *settings.db*
  - Utilizar herramientas como: Cellebrite, XRY, …
  - Si se conocen las credenciales Google del propietario se podría utilizar:
    - El servicio de “Encontrar mi móvil” proporcionado por el fabricante
    - Realizar varios intentos de acceso hasta que Android sugiera el servicio de “Olvidó Patrón/Contraseña” y seleccionar acceder como usuario Gmail.
      - Esto sólo funciona en Android 4,4 o anteriores
  - Determinar el patrón mediante la visualización de la huellas dactilares bajo una luz apropiada (Smudge attack)

Análisis de datos

Formatos de datos de interés

Formatos de interés

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.

Formatos de interés

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 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>

Formatos de interés

Ficheros SQLite

- Los ficheros SQLite están organizados en páginas de tamaño fijo que van siendo rellenadas 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 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.

Formatos de interés

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 datos

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 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 datos

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 datos

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 datos

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 archivos 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 Autopsy, y Scalpel 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 *grep*, *strings* o un editor hexadecimal.

Análisis de datos

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 datos

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 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.

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.
- En los siguientes links podemos encontrar listas de herramientas forenses:
  - https://en.wikipedia.org/wiki/List_of_digital_forensics_tools
  - https://geekflare.com/forensic-investigation-tools/
  - http://www.mitec.cz/
  - https://www.magnetforensics.com/resources/
- 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 (tiene una parte gratuita)
  - **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 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, sqlitedb, 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 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.

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 Kali 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

El 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.

El informe forense

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.

El informe forense

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.

El informe forense

Procesado de evidencias

- Se describen los pasos ejecutados para la extracción de información que no se encuentra de forma explicita 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.

El informe forense

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.