

# Análisis Forense en Dispositivos Android

Tema 3. Análisis Forense Informático

## Introducción

No cabe duda de que los dispositivos móviles se han convertido en parte de nuestras vidas y han revolucionado la forma en que realizamos la mayoría de nuestras actividades. Como resultado, un dispositivo móvil es ahora un enorme repositorio que contiene información sensible y personal sobre su propietario. Esto, a su vez, ha provocado el auge del análisis forense de dispositivos móviles, una rama del análisis forense digital que se ocupa de recuperar datos de un dispositivo móvil.

En este capítulo, trataremos los siguientes temas:

- La necesidad de la criminalística móvil.
- La comprensión del análisis forense de dispositivos móviles Android.
- Desafíos de la investigación forense de móviles.
- El proceso de extracción de pruebas en el móvil.
- Enfoques prácticos del análisis forense de móviles.
- Posibles pruebas almacenadas en los teléfonos móviles.
- Examen y análisis.
- Reglas de las pruebas.
- Buenas prácticas forenses.

## La necesidad del análisis forense en dispositivos móviles

Según los informes de Statista ([statista.com](https://www.statista.com)), el número de usuarios de teléfonos móviles en el mundo supera los 5.000 millones en 2020. El mundo es testigo de la migración de la tecnología de los usuarios de los ordenadores de sobremesa a los teléfonos móviles. La mayor parte del crecimiento del mercado móvil puede atribuirse la continua demanda de teléfonos inteligentes.

Según un informe de Ericsson, el tráfico mundial de datos móviles alcanza los 71 exabytes mensuales en 2022, frente a los 8,8 exabytes de 2017, lo que supone una tasa de crecimiento anual compuesta del 42%.

Los teléfonos inteligentes de hoy, como el iPhone de Apple y la serie Galaxy de Samsung, son formas compactas de ordenadores con alto rendimiento, enorme almacenamiento y mayor funcionalidad.

Los teléfonos móviles son el dispositivo electrónico más personal al que accede un usuario. Se utilizan para realizar tareas de comunicación sencillas, como llamar y enviar mensajes de texto, al tiempo que ofrecen de Internet, el correo electrónico, la toma de fotos y vídeos, la creación y el almacenamiento de documentos, identificar ubicaciones con servicios GPS y gestionar tareas empresariales. A medida que se incorporan nuevas funciones y aplicaciones a los teléfonos móviles, la cantidad de información almacenada en los dispositivos crece continuamente. Los teléfonos móviles se han convertido en portadores de datos portátiles, que registran todos sus movimientos.

Con la creciente prevalencia de los teléfonos móviles en la vida cotidiana de las personas y en la delincuencia, los datos de los teléfonos se han convertido en una fuente inestimable de pruebas para las investigaciones relacionadas con casos penales, civiles e incluso de alto perfil. Es raro realizar una investigación forense digital que no incluya un teléfono. Los registros de llamadas de los dispositivos móviles y los datos del GPS se utilizaron para ayudar a resolver el intento de atentado en Times Square, Nueva York, en 2010. En el siguiente enlace se incluye más información de este caso:

<https://www.forensicon.com/forensics-blotter/cell-phone-email-forensics-investigation-cracks-nyc-times-square-car-bombing-case/>

La ciencia que hay detrás de la recuperación de pruebas digitales de los teléfonos móviles se llama análisis forense de los dispositivos móviles. Las pruebas digitales se definen como la información y los datos almacenados, recibidos o transmitidos por un dispositivo electrónico que se utiliza para las investigaciones. Las pruebas digitales abarcan todos y cada uno de los datos digitales que pueden ser usados como evidencia en un caso.

## Entendiendo el análisis forense en dispositivos móviles

La ciencia forense digital es una rama de la ciencia forense que se centra en la recuperación e investigación de los datos en bruto que residen en dispositivos electrónicos o digitales. El objetivo del proceso es extraer y recuperar cualquier información de un dispositivo digital sin alterar los datos presentes en el dispositivo. A lo

largo de los años, la ciencia forense digital ha crecido junto con el rápido crecimiento de ordenadores y otros dispositivos digitales. Hay varias ramas de la ciencia forense digital según el tipo de dispositivo digital de que se trate, como la informática forense, la informática forense de redes y el análisis forense de móviles.

El análisis forense de móviles es una rama del análisis forense digital que se ocupa de la obtención y recuperación de pruebas de los dispositivos móviles. El término "forense" se utiliza ampliamente en la comunidad forense digital para calificar y justificar el uso de una tecnología o metodología forense. Uno de los principios fundamentales que rigen el examen forense es que las pruebas originales no deben ser alteradas de ninguna manera. Esto es extremadamente difícil con los dispositivos móviles. Algunas herramientas forenses requieren un vector de comunicación con el dispositivo móvil, por lo que la protección contra escritura estándar no funcionará durante la adquisición forense.

Otros métodos de adquisición forense pueden implicar la separación de un chip o la instalación de una aplicación en el dispositivo móvil antes de extraer los datos para el examen forense. En los casos en los que el examen o la adquisición de datos no es posible sin cambiar la configuración del dispositivo, el procedimiento y los cambios deben ser cuidadosamente probados y documentados para referencia posterior. Seguir una metodología y unas directrices adecuadas es crucial para examinar los dispositivos móviles, ya que así se obtienen los datos más valiosos. Al igual que en la recogida de pruebas, no seguir el procedimiento adecuado durante el examen puede provocar la pérdida o el daño de pruebas o hacerlas inadmisibles en el tribunal.

El proceso forense móvil se divide en tres categorías principales: incautación, adquisición y examen/análisis. Los examinadores forenses se enfrentan a algunos retos al incautar el dispositivo como fuente de pruebas. En la escena del crimen, si el dispositivo móvil se encuentra apagado, usted, como examinador, debe colocar el dispositivo en una bolsa de Faraday para evitar cambios en caso de que el dispositivo se encienda automáticamente. Las bolsas de Faraday están diseñadas específicamente para aislar un teléfono de la red. Si el teléfono se encuentra encendido, apagarlo conlleva muchas preocupaciones. Si el teléfono está bloqueado con un PIN o una contraseña, o está cifrado, será necesario saltarse el o determinar el PIN para acceder al dispositivo. Los teléfonos móviles son dispositivos conectados en red y pueden enviar y recibir datos a través de diferentes

fuentes, como los sistemas de telecomunicación, puntos de acceso Wi-Fi y Bluetooth. Por lo tanto, si el teléfono está en estado de funcionamiento, un delincuente podría borrar de forma segura los datos almacenados en el teléfono ejecutando un comando de borrado remoto. Cuando un teléfono se enciende, debe colocarse en una bolsa de Faraday. Si es posible, antes de colocar un dispositivo móvil en una bolsa de Faraday, debe desconectarlo de la red para proteger las pruebas, activando el modo de vuelo y desactivando todas las conexiones de red (Wi-Fi, GPS, puntos de acceso, etc.). Esto también preservará la batería, que se agotará mientras esté en una bolsa de Faraday, y protegerá contra las fugas en la bolsa de Faraday. Una vez que el dispositivo móvil se haya incautado, el examinador puede necesitar varias herramientas forenses para adquirir y analizar los datos almacenados en el teléfono.

La adquisición forense de dispositivos móviles puede realizarse mediante múltiples métodos, que se definiremos más adelante. Cada uno de estos métodos afecta a la cantidad de análisis necesarios. Si un método falla, debe intentarse otro. Pueden ser necesarios varios intentos y herramientas para obtener la máxima cantidad de datos del dispositivo móvil. Los teléfonos móviles son sistemas dinámicos que nos plantean muchos retos a la hora de extraer y analizar las pruebas digitales. El rápido aumento del número de diferentes tipos de teléfonos móviles de diferentes fabricantes hace que sea difícil desarrollar un único proceso o herramienta para examinar todos los tipos de dispositivos. Los teléfonos móviles evolucionan continuamente a medida que tecnologías existentes y se introducen otras nuevas. Además, cada móvil está diseñado con una variedad de sistemas operativos integrados. Por lo tanto, se requieren conocimientos y habilidades especiales de los expertos forenses para adquirir y analizar los dispositivos.

## Desafíos en la investigación forense de móviles

Uno de los mayores retos forenses cuando se trata de la plataforma móvil es el hecho de que los datos pueden ser accedidos, almacenados y sincronizados a través de múltiples dispositivos. Como los datos son volátiles y pueden transformarse o borrarse rápidamente de forma remota, se requiere un mayor esfuerzo para la preservación de estos datos. El análisis forense de los móviles es diferente del análisis forense de los ordenadores y presenta desafíos únicos para los examinadores forenses.

Las fuerzas del orden y los examinadores forenses suelen tener dificultades para obtener pruebas digitales de los dispositivos móviles. Algunos de los motivos son los siguientes:

- **Diferencias de hardware:** el mercado está inundado de diferentes modelos de teléfonos móviles de diferentes fabricantes. Los examinadores forenses pueden encontrarse con diferentes tipos de modelos de móviles que difieren en tamaño, hardware, características y sistema operativo. Además, con un ciclo de desarrollo de productos corto, los nuevos modelos surgen nuevos modelos con mucha frecuencia. Como el panorama de los móviles cambia cada día, es fundamental que usted se adapte a todos los retos y se mantenga actualizado en las técnicas forenses de dispositivos móviles en varios dispositivos.
- **Sistemas operativos móviles:** a diferencia de los ordenadores personales, en los que Windows ha dominado el mercado durante años, los dispositivos móviles utilizan ampliamente más sistemas operativos, como iOS de Apple, Android de Google, BlackBerry OS de RIM el sistema operativo Windows Phone de Microsoft, el webOS de HP y muchos otros. Incluso dentro de estos sistemas operativos, hay varias versiones, lo que hace que su tarea sea aún más difícil.
- **Características de seguridad de la plataforma móvil:** las plataformas móviles modernas contienen características de seguridad para proteger los datos y la privacidad del usuario. Estas características actúan como un obstáculo durante la adquisición y el examen forense. Por ejemplo, los dispositivos móviles modernos vienen con mecanismos de cifrado por defecto, desde la capa de hardware hasta la capa de software. Es posible que haya que romper estos mecanismos de cifrado para extraer datos de los dispositivos. La disputa sobre el cifrado entre el FBI y Apple fue un momento decisivo en este sentido, en el que la de Apple impidió al FBI entrar en un iPhone incautado a un atacante en el caso de San Bernardino.
- **Impedir la modificación de los datos:** una de las reglas fundamentales en la ciencia forense es asegurarse de que los datos del dispositivo no se modifican. En otras palabras, cualquier intento de extraer datos del dispositivo no debe alterar los datos presentes en ese dispositivo. Pero esto no es posible en la práctica con los móviles, porque el simple hecho de encender un dispositivo puede cambiar los datos de ese dispositivo. Incluso si un dispositivo parece estar en un estado

apagado, los procesos en segundo plano pueden seguir ejecutándose. Por ejemplo, en la mayoría de los móviles, el despertador del reloj de alarma sigue funcionando incluso cuando el teléfono está apagado. Una transición repentina de un estado a otro puede provocar la pérdida o modificación de datos.

- Técnicas antforenses: las técnicas antforenses, como la ocultación de datos, la falsificación de datos y el borrado seguro, dificultan las investigaciones sobre las evidencias digitales.
- Recuperación del código de acceso: si el dispositivo está protegido con una contraseña, el examinador forense tiene que acceder al dispositivo sin dañar los datos que contiene el dispositivo. Aunque existen técnicas para eludir el bloqueo de pantalla, es posible que no siempre funcionen en todas las versiones del sistema operativo.
- Falta de recursos: como se ha mencionado anteriormente, con el creciente número de teléfonos móviles, también aumenta la cantidad de herramientas que necesita un examinador forense. Los accesorios de adquisición forense, como cables USB, baterías y cargadores para diferentes teléfonos móviles, tienen que mantenerse para poder adquirir esos dispositivos.
- Naturaleza dinámica de las pruebas: las pruebas digitales pueden ser fácilmente alteradas, intencionadamente o no. Por ejemplo, navegar por una aplicación en un teléfono puede alterar los datos almacenados por esa aplicación en el dispositivo.
- Restablecimiento accidental: los teléfonos móviles ofrecen funciones para restablecer todo. Reiniciar un dispositivo accidentalmente mientras lo examina puede provocar la pérdida de datos.
- Alteración del dispositivo: las posibles formas de alterar los dispositivos pueden ir desde mover datos de aplicaciones o cambiar el nombre de los archivos hasta modificar el sistema operativo del fabricante. En este caso, debe tenerse en cuenta la experiencia del sospechoso.
- Blindaje de las comunicaciones: los dispositivos móviles se comunican a través de redes celulares, redes Wi-Fi, bluetooth e infrarrojos. Como la comunicación de los dispositivos podría alterar los datos del dispositivo, debe eliminarse la posibilidad de que siga habiendo comunicación después de incautar el dispositivo.

- Falta de disponibilidad de herramientas: existe una amplia gama de dispositivos móviles. Es necesario utilizar una combinación de herramientas, ya que una sola puede no ser compatible con todos los dispositivos o realizar todas las funciones necesarias. Por lo tanto, elegir la herramienta adecuada para un teléfono concreto puede ser difícil.
- Programas maliciosos: el dispositivo podría contener malware o software malicioso, como un virus o un troyano. Estos programas pueden intentar propagarse a otros dispositivos a través de una interfaz de red.
- Cuestiones legales: los dispositivos móviles pueden estar implicados en delitos que traspasan las fronteras geográficas. Para hacer frente a estas cuestiones multijurisdiccionales, el examinador forense debe conocer la naturaleza del delito y las leyes de la región en la que se comete. Por eso, en la mayoría de las ocasiones debe tenerse en cuenta la ayuda con un abogado especialista en cuestiones tecnológicas.

## El proceso de extracción de pruebas o evidencias digitales del teléfono móvil

La extracción de pruebas y el examen forense de los distintos dispositivos móviles pueden diferir en función de diversos factores. Sin embargo, seguir un proceso de examen coherente ayudará a garantizar que las pruebas obtenidas de cada teléfono estén bien documentadas y que los resultados sean fiables.

No existe un proceso estándar bien establecido para la investigación forense de móviles. Sin embargo, el siguiente diagrama proporciona una visión general de las consideraciones del proceso para la extracción de pruebas de los dispositivos móviles. Todos los métodos utilizados para extraer datos de dispositivos móviles deben ser probados, validados y bien documentados:



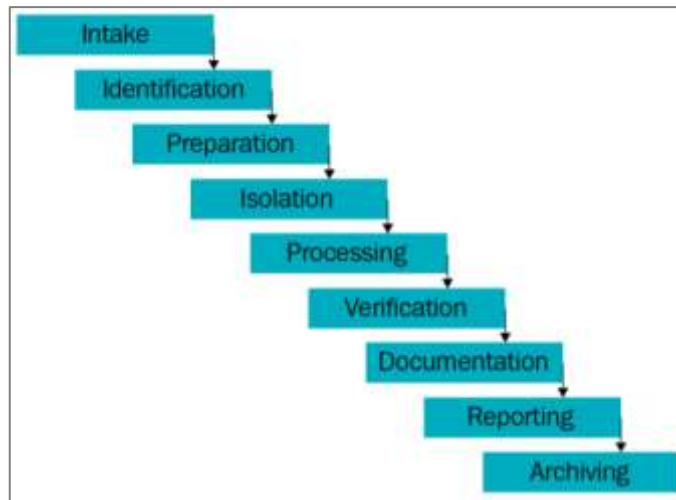


Figura 1. Proceso de extracción de pruebas del teléfono móvil.

Un gran recurso para el manejo y procesamiento de dispositivos móviles se puede encontrar en el siguiente enlace: <https://www.sans.org/posters/?focus-area=digital-forensics>

Como se muestra en el diagrama anterior, el análisis forense de un dispositivo móvil incluye varias fases, desde la fase de obtención de pruebas hasta la fase de archivo.

### Fase de adquisición de pruebas

La fase de admisión de pruebas es la fase inicial e implica un papeleo que recoge información sobre la propiedad y el tipo de incidente en el que estuvo implicado el dispositivo móvil, y el tipo de datos que busca el solicitante. El desarrollo de objetivos específicos para cada examen es la parte fundamental de esta fase. Sirve para aclarar sus objetivos. Antes de que comience el proceso de incautación física, debe conocer las leyes federales, estatales y locales relativas a los derechos del individuo. Si no se siguen los procedimientos adecuados, la investigación puede ser considerada ilegal en un tribunal de justicia. El procedimiento y la legalidad pueden variar en función de si se trata de un agente del gobierno o de un particular. Por ejemplo, en Estados Unidos, los derechos de la cuarta enmienda impiden cualquier registro o incautación por parte de un agente del gobierno sin tener una orden de registro adecuada. La orden de registro debe autorizar claramente la incautación del dispositivo móvil, así como el tipo de datos que deben

recogerse. Tras una incautación exitosa, se debe tener cuidado para asegurar que se establezca una cadena de custodia del dispositivo, y también de los datos recogidos.

Según el NIST (<https://csrc.nist.gov/>), la cadena de custodia se refiere a un proceso que rastrea el movimiento de la evidencia a través de su recolección, su recogida, salvaguardia y ciclo de vida de análisis, documentando a cada persona que ha manipulado las pruebas, la fecha y la hora en que se han recogido o transferido y el propósito de la transferencia.

Además, mientras se incauta el dispositivo, se debe tener cuidado de no modificar ningún dato presente en el dispositivo. Al mismo tiempo, no debe perderse ninguna oportunidad de ayudar a la investigación. Por ejemplo, en el momento de incautar el dispositivo, si éste está desbloqueado, se debe intentar desactivar el código de acceso.

### La fase de identificación

El examinador forense debe identificar los siguientes detalles en cada examen de un dispositivo móvil:

- La autoridad legal.
- Los datos que deben extraerse.
- La marca, el modelo y los datos de identificación del dispositivo.
- Los medios de almacenamiento de datos.
- Otras fuentes de pruebas potenciales

En las siguientes secciones hablaremos de cada una de ellas.

### La autoridad legal

Es importante que el analista forense determine y documente qué autoridad legal en forma de permisos para la realización de la adquisición de evidencias digitales y el examen del dispositivo, así como las limitaciones impuestas antes de realizar el examen del dispositivo. Por ejemplo, si la investigación sobre el dispositivo se está llevando a cabo sobre la base de una orden judicial, la búsqueda debe limitarse únicamente a las áreas

que se definen en la orden. En resumen, antes de la incautación del dispositivo, hay que responder a las siguientes preguntas:

- Si no existe una orden de registro, ¿ha consentido el propietario del dispositivo el registro?
- Si existe una orden de registro, ¿está el dispositivo incluido en la orden original?
- Si el dispositivo está incluido en la orden, ¿se definen también los datos que se pueden recoger?
- Si se trata de una investigación corporativa, ¿el dispositivo es propiedad de un individuo o de su empleador?
- ¿Permite la política de la empresa la recogida de los datos y el posterior análisis?

#### Datos que hay que extraer

En función de los datos solicitados, se determinará el grado de profundidad del examen del dispositivo móvil. El objetivo del examen marca una diferencia significativa a la hora de seleccionar las herramientas y técnicas para examinar el teléfono y aumenta la eficacia del proceso de examen.

#### La marca, el modelo y los datos de identificación del dispositivo

Como parte del examen, la identificación de la marca y el modelo del teléfono ayuda a determinar qué herramientas pueden funcionar con el teléfono. Cuando esté disponible, se recomienda capturar los siguientes detalles del dispositivo incautado:

- El fabricante del dispositivo.
- El número de modelo del dispositivo.
- El número de serie del dispositivo móvil.
- El color del dispositivo.
- El fondo de pantalla visible en la pantalla del dispositivo o el fondo de pantalla de bloqueo.
- La presencia de cualquier componente de hardware (como la cámara frontal, la toma de auriculares, etc.).

- Una descripción de cualquier detalle específico del dispositivo (arañazos, pantalla rota, etc.)

A continuación, veamos los medios de almacenamiento de datos.

### Medios de almacenamiento de datos

Muchos teléfonos móviles ofrecen la posibilidad de ampliar la memoria con dispositivos de almacenamiento extraíbles. En los casos en los que se encuentre este tipo de medios extraíbles en un teléfono móvil que se someta para su examen, la tarjeta de almacenamiento debe extraerse y procesarse con las técnicas forenses tradicional. También es conveniente adquirir la tarjeta mientras está en el dispositivo móvil para garantizar que los datos almacenados tanto en la memoria del teléfono como en la tarjeta están vinculados para facilitar el análisis.

### Otras fuentes de pruebas potenciales

Los teléfonos móviles son una buena fuente de huellas dactilares y otras pruebas biológicas. Estas pruebas deben recogerse antes de examinar el teléfono móvil para evitar problemas de contaminación, a menos que el método de recogida dañe el dispositivo. Los examinadores deben utilizar guantes para manipular las pruebas.

### La fase de preparación

Una vez identificado el modelo de teléfono móvil, la fase de preparación implica la investigación sobre el teléfono móvil que se va a examinar y los métodos e instrumentos y las herramientas adecuadas para su adquisición y examen. Por lo general, esto se hace en función del modelo de dispositivo, el sistema operativo subyacente, su versión, etc. Además, las herramientas que deben utilizarse durante el examen se determinarán en función del dispositivo en cuestión, así como en el alcance y los objetivos del examen.

## La fase de aislamiento

Los teléfonos móviles, por su diseño, están pensados para comunicarse a través de redes de telefonía móvil, bluetooth, infrarrojos y redes inalámbricas (Wi-Fi). Cuando un teléfono está conectado a una red, se añaden nuevos datos al teléfono a través de llamadas entrantes, mensajes y datos de aplicaciones, lo que modifica las pruebas del teléfono.

La destrucción completa de los datos también es posible mediante el acceso o el borrado remoto a distancia. Por este motivo, es importante aislar el dispositivo de las fuentes de comunicación importante antes de la adquisición y el examen del dispositivo. El aislamiento de la red se puede hacer colocando el teléfono en un paño de blindaje de radiofrecuencias y poniendo el teléfono en modo avión o vuelo. El modo avión desactiva los canales de comunicación del dispositivo, como la radio, el Wi-Fi y el Bluetooth. Sin embargo, si el dispositivo tiene la pantalla bloqueada, esto no es posible. Además, dado que el Wi-Fi está ahora disponible en los aviones, algunos dispositivos tienen acceso al Wi-Fi en modo avión.

Una solución alternativa es el aislamiento del teléfono mediante el uso de bolsas de Faraday, que bloquean las señales de radio hacia o desde el teléfono. Las bolsas de Faraday contienen materiales que bloquean los campos eléctricos estáticos externos (incluidas las ondas de radio). Así, las bolsas de Faraday protegen los dispositivos móviles incautados de las interferencias externas para evitar el borrado y el rastreo. Para trabajar más cómodamente con dispositivos incautados, también existen tiendas y salas Faraday.

## La fase de procesamiento

Una vez que el teléfono ha sido aislado de las redes de comunicación, el procesamiento real del teléfono móvil comienza. Uno de los retos a los que se enfrentará en esta fase es identificar qué herramientas utilizar, ya que en ello influyen diversos factores como el precio, la facilidad de uso, aplicabilidad, etc. El software forense para móviles es muy caro y, a diferencia de la informática forense, a veces hay que utilizar varias herramientas para acceder a los datos. Mientras se realiza la selección de una herramienta, asegúrese de que tiene funciones incorporadas para mantener la integridad forense.

Mantener la integridad forense requiere una herramienta que empaquete los datos recogidos en un formato que probablemente no pueda ser modificado o alterado fácilmente. El teléfono debe adquirirse utilizando un método probado que sea repetible y que sea lo más sólido posible desde el punto de vista forense. La adquisición física es el método preferido, ya que extrae los datos en bruto de la memoria y el dispositivo suele estar apagado durante el proceso de adquisición.

En la mayoría de los dispositivos, el menor número de cambios se produce durante la adquisición física. Si la adquisición física no es posible o falla, se debe intentar adquirir el sistema de archivos del dispositivo móvil. Siempre debe realizarse una adquisición, ya que puede contener sólo los datos analizados y proporcionar punteros para examinar la imagen de la memoria.

### La fase de verificación

Después de procesar el teléfono, hay que verificar la exactitud de los datos extraídos del para asegurarse de que los datos no han sido modificados. La verificación de los datos extraídos puede realizarse de varias maneras:

- Comparando los datos extraídos con los datos del teléfono: comprobar si los datos extraídos del dispositivo coinciden con los datos mostrados por el dispositivo, si es el caso. Los datos extraídos pueden compararse con los del propio dispositivo o con un informe lógico, lo que se prefiera. Recuerde que la manipulación del dispositivo original puede realizar cambios en la única prueba: el propio dispositivo.
- Utilizar varias herramientas y comparar los resultados: para garantizar la precisión, utilice múltiples herramientas para extraer los datos y comparar los resultados.
- Uso de valores hash: todos los archivos de imágenes deben ser sometidos a hash después de la adquisición para garantizar que los datos permanecen inalterados. Si se admite la extracción del sistema de archivos, puede extraer el sistema de archivos y luego calcular los hash de los archivos extraídos. Más tarde, cualquier hash de archivo extraído individualmente se calcula y se compara con el valor original para verificar su integridad. Cualquier discrepancia en los valores hash

debe ser explicable (por ejemplo, el dispositivo se encendió y se adquirió de nuevo, por lo que los valores hash son diferentes).

### La fase de documentación e información

El examinador forense debe documentar, durante todo el proceso de examen todo lo relacionado con lo que se hizo durante la adquisición y el examen. Una vez que completa la investigación, los resultados deben pasar por algún tipo de revisión por pares para garantizar

que los datos están comprobados y la investigación está completa. Sus notas y documentación pueden incluir información como la siguiente:

- La fecha y hora de inicio del examen.
- El estado físico del teléfono.
- Fotos del teléfono y de los componentes individuales.
- El estado del teléfono cuando se recibió: encendido o apagado.
- Marca y modelo del teléfono.
- Herramientas utilizadas para la adquisición.
- Herramientas utilizadas para el examen.
- Datos encontrados durante el examen.
- Notas de la revisión por pares

A lo largo de la investigación, es importante asegurarse de que la información extraída y documentada de un dispositivo móvil pueda presentarse con claridad a cualquier otro examinador o a un tribunal. La documentación es una de las habilidades más importantes.

La creación de un informe forense de datos extraídos de un dispositivo móvil durante la adquisición y el análisis es importante. Esto puede incluir datos tanto en papel como en formato electrónico. Sus hallazgos deben estar documentados y presentados de manera que las pruebas hablen por sí solas ante el tribunal.

Las conclusiones deben ser claras, concisas y repetibles. El análisis de líneas de tiempo y de enlaces, características que ofrecen muchas herramientas forenses comerciales,

ayudarán a informar y explicar los hallazgos en varios dispositivos móviles. Estas herramientas permiten relacionar los métodos de comunicación de múltiples dispositivos.

### La fase de archivo

La conservación de los datos extraídos de un teléfono móvil es una parte importante del proceso. También es importante que los datos se conserven en un formato utilizable para el proceso judicial en curso, para futuras referencias, en caso de que el archivo de pruebas actual se corrompa, y para los requisitos de mantenimiento de registros. Los casos judiciales pueden prolongarse durante muchos años antes de que se dicte una sentencia definitiva, y la mayoría de las jurisdicciones exigen que los datos se conserven durante largos periodos de tiempo a efectos de apelación. A medida que el campo y los métodos avanzan, surgen nuevos métodos para la adquisición de datos a partir de una imagen física sin procesar, y entonces se pueden volver a consultar los datos sacando una copia de los archivos.

## Enfoques forenses prácticos para móviles

Al igual que en cualquier investigación forense, existen varios enfoques que pueden utilizarse para la adquisición y examen/análisis de datos de teléfonos móviles.

El tipo de dispositivo móvil, el sistema operativo y la configuración de seguridad suelen dictar el procedimiento que debe seguirse en un proceso forense.

Cada investigación es distinta con sus propias circunstancias, por lo que no es posible diseñar un único enfoque procedimental definitivo para todos los casos. En los siguientes apartados se describen los enfoques generales que se siguen en la extracción de datos de los dispositivos móviles.

### Comprendiendo los sistemas operativos de los dispositivos móviles

Uno de los principales factores en la adquisición de datos y el examen/análisis de un teléfono móvil es el sistema operativo. Desde los teléfonos móviles de gama baja hasta los smartphones, los sistemas operativos han recorrido un largo camino con un montón



de características. Los sistemas operativos para móviles afectan directamente a la forma de acceder al dispositivo móvil. Por ejemplo, Android ofrece acceso a nivel de terminal mientras que iOS no da esa opción.

Un conocimiento exhaustivo de la plataforma móvil ayuda al examinador forense a tomar decisiones forenses sólidas y a llevar a cabo una investigación concluyente. Aunque existe una gran cantidad de familias de dispositivos móviles inteligentes, con la desaparición de Blackberry, actualmente dos sistemas operativos principales dominan el mercado de los dispositivos móviles, Google Android y Apple iOS (seguidos por Windows Phone en un lejano tercer lugar).

Puede encontrar más información en el siguiente enlace:

<https://www.idc.com/promo/smartphone-market-share/os>

### *Android*

Android es un sistema operativo basado en Linux, y es una plataforma de código abierto de Google para teléfonos móviles. Android es el sistema operativo para teléfonos inteligentes más utilizado del mundo.

Las fuentes muestran que iOS de Apple ocupa el segundo lugar (<https://www.idc.com/promo/smartphonemarket-share/os>).

Android fue desarrollado por Google como una opción abierta y gratuita para fabricantes de hardware y operadores telefónicos. Esto hace que Android sea el software preferido por empresas que necesitan un sistema operativo ligero, personalizable y de bajo coste para sus dispositivos inteligentes sin tener que desarrollar un nuevo sistema operativo desde cero.

La naturaleza abierta de Android ha animado a los desarrolladores a crear un gran número de aplicaciones y subirlas a Google Play. Posteriormente, los usuarios finales pueden descargar las aplicaciones desde Android Market, lo que convierte a Android en un potente sistema operativo. Se estima que Google Play Store tiene 3,3 millones de aplicaciones.

## *iOS*

iOS, conocido como el sistema operativo del iPhone, es un sistema operativo móvil desarrollado y distribuido exclusivamente por Apple Inc. iOS se está convirtiendo en un sistema operativo universal para todos los dispositivos móviles de Apple, como el iPad, el iPod Touch y el iPhone.

Se basa en un sistema operativo de tipo Unix. iOS gestiona el hardware del dispositivo. Las tecnologías necesarias para implementar aplicaciones nativas también son proporcionadas por iOS. También incluye varias aplicaciones del sistema, como Mail y Safari, que proporcionan servicios estándar del sistema al usuario.

Las aplicaciones nativas de iOS se distribuyen a través de la App Store, que está estrechamente controlada por Apple.

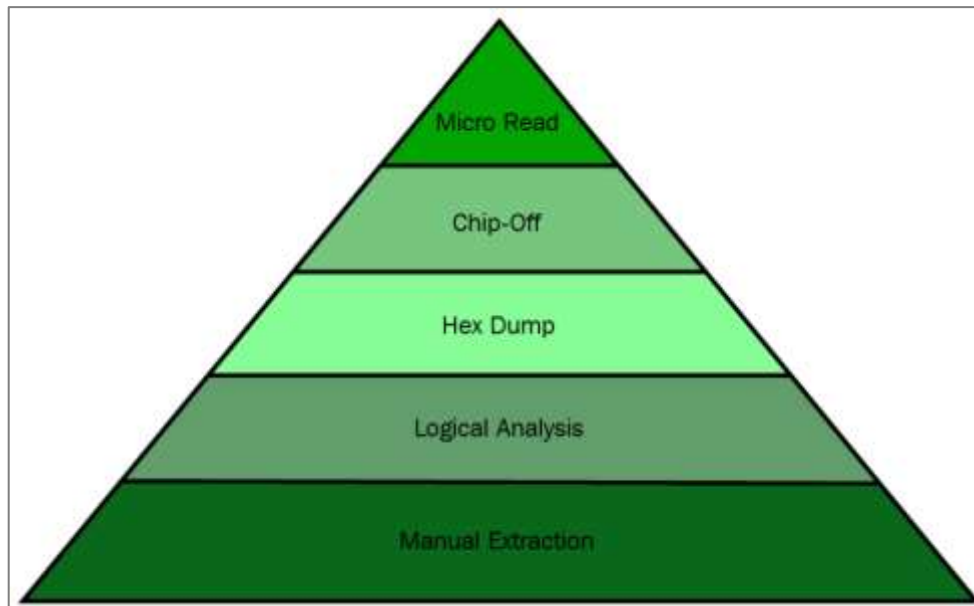
## *Windows Phone*

Windows Phone es un sistema operativo móvil propio desarrollado por Microsoft para smartphones y ordenadores de bolsillo. Es el sucesor de Windows Mobile y está dirigido principalmente al mercado de consumo más que al empresarial. El sistema operativo Windows Phone es similar al sistema operativo de escritorio de Windows, pero está optimizado para dispositivos con una pequeña cantidad de almacenamiento.

## *Sistema de nivelación de herramientas forenses para móviles*

La adquisición y el análisis forense de teléfonos móviles implica un esfuerzo manual y el uso de herramientas automatizadas. Hay una gran variedad de herramientas disponibles para realizar análisis forense de dispositivos móviles. Todas las herramientas tienen sus pros y sus contras, y es fundamental entender que ninguna herramienta es suficiente para todos los fines. Por lo tanto, es importante comprender los distintos tipos de herramientas forenses para móviles es importante para los examinadores forenses.

A la hora de identificar las herramientas adecuadas para la adquisición y el análisis forense de de teléfonos móviles, un sistema de clasificación de herramientas forenses para dispositivos móviles desarrollado por Sam Brothers (que se muestra en el siguiente diagrama) es muy útil para los examinadores.



*Figura 2. Pirámide de nivelación de herramientas de telefonía móvil (Sam Brothers, 2009).*

El objetivo del sistema de clasificación de herramientas forenses para dispositivos móviles es permitir a un examinador clasificar las herramientas forenses en función de la metodología de examen de la herramienta.

Cuando se pasa de la base de la pirámide a la cima, los métodos y las herramientas utilizadas para el análisis suelen ser más técnicas y sofisticadas y requieren más tiempo de análisis.

Existen ventajas y desventajas de las diferentes técnicas utilizadas en cada capa. El examinador forense debe ser consciente de estas cuestiones antes de aplicar una determinada técnica. Las pruebas pueden destruirse por completo si no se utiliza correctamente el método o la herramienta no se utiliza correctamente.

Este riesgo aumenta a medida que se asciende en la pirámide. Por lo tanto, se requiere una formación adecuada para obtener la mayor tasa de éxito en la extracción de datos de los dispositivos móviles.

### *Extracción manual*

El método de extracción manual consiste simplemente en desplazarse por los datos del dispositivo y ver los datos en el teléfono directamente mediante el uso del teclado del dispositivo o pantalla táctil del dispositivo.

A continuación, se documenta fotográficamente la información descubierta. El proceso de extracción de proceso de extracción es rápido y fácil de usar, y funcionará en casi todos los teléfonos. Este método es propenso a errores humanos, como la omisión de ciertos datos debido a la falta de familiaridad con la interfaz. A este nivel, no es posible recuperar la información borrada y obtener todos los datos presentes en el dispositivo.

Existen algunas herramientas, como Project-A-Phone, que se han desarrollado para ayudar a un examinador a documentar fácilmente una extracción manual. Sin embargo, esto también podría dar lugar a la modificación de los datos. Por ejemplo, ver un SMS no leído lo marcará como leído.

### *Análisis lógico*

El análisis lógico consiste en conectar el dispositivo móvil al hardware forense o a una estación de trabajo mediante un cable USB, un cable RJ-45, infrarrojos o Bluetooth. Una vez conectado, el ordenador inicia un comando y lo envía al dispositivo, que luego es interpretado por el procesador del dispositivo. A continuación, los datos solicitados se reciben de la memoria del dispositivo y se envían a la estación de trabajo forense. Posteriormente, se pueden revisar los datos.

La mayoría de las herramientas forenses disponibles actualmente trabajan en este nivel del sistema de clasificación.

El proceso de extracción es rápido y fácil de usar y requiere poca formación por su parte. Por otro lado, el proceso puede escribir datos en el móvil y podría alterar la integridad de las pruebas. Además, los datos borrados no suelen ser accesibles con este procedimiento.

### *Volcado hexadecimal*

Un volcado hexadecimal, también denominado extracción física, se consigue conectando un dispositivo a una estación de trabajo forense e introduciendo un código sin firmar o un

cargador de arranque en el teléfono y se le indica al teléfono que vuelque la memoria del teléfono al ordenador. Dado que la imagen en bruto resultante está en formato binario, se requieren conocimientos técnicos para analizarla.

El proceso es barato, proporciona más datos al examinador y permite la recuperación de archivos borrados del espacio no asignado en la mayoría de los dispositivos.

### *Chip-off*

Chip-off se refiere a la adquisición de datos directamente desde el chip de memoria presente en el dispositivo. En este nivel, el chip se extrae físicamente del dispositivo y se utiliza un lector de chips o un segundo teléfono para extraer los datos almacenados en él. Este método es técnicamente más complejo y delicado, ya que en los móviles se utiliza una gran variedad de tipos de chip. El proceso es caro y requiere conocimientos de hardware, ya que implica la desoldadura y el calentamiento del chip de memoria y de la placa donde se encuentra el chip soldado.

Se necesita formación para realizar con éxito la extracción del chip. Los procedimientos inadecuados pueden dañar el chip de memoria y hacer que todos los datos sean insalvables. Cuando seaposible, se recomienda que se intenten los otros niveles de extracción antes del chipoff, ya que este método es de naturaleza destructiva. Además, la información que sale de memoria está en un formato crudo y tiene que ser analizada, decodificada e interpretada. El método de chip-off se prefiere en situaciones en las que es importante preservar el estado de la memoria exactamente como existe en el dispositivo. También es la única opción cuando un dispositivo está dañado pero el chip de memoria está intacto.

El chip de un dispositivo suele leerse mediante el método del Grupo de Acción Conjunta de Pruebas (JTAG). El JTAG consiste en conectarse a los puertos de acceso de prueba (TAP) de un dispositivo y forzar al procesador a transferir los datos brutos almacenados en el chip de memoria. El método JTAG se generalmente se utiliza con dispositivos que están operativos pero que son inaccesibles mediante herramientas estándar. Ambas de estas técnicas también funcionan incluso cuando el dispositivo está bloqueado en la pantalla.

### *Microlectura*

El proceso de microlectura consiste en ver e interpretar manualmente los datos vistos en el chip de memoria. El examinador utiliza un microscopio electrónico y analiza las puertas físicas del chip y luego traduce el estado de las puertas a 0s y 1s para determinar los caracteres ASCII resultantes. Todo el proceso es largo y costoso, y requiere amplios conocimientos y formación sobre la memoria y los archivos.

Debido a los extremos tecnicismos implicados en la microlectura, sólo se intenta en casos de alto perfil equivalentes a una crisis de seguridad nacional, después de todos los demás niveles de extracción.

El proceso se realiza raramente y no está bien documentado en este momento.

Además, actualmente no hay herramientas comerciales disponibles para realizar una microlectura.

### *Métodos de adquisición de datos*

La adquisición de datos es el proceso de obtención de imágenes o de extracción de información de un dispositivo digital y otros medios adjuntos. La adquisición de datos de un teléfono móvil no es tan sencilla como la adquisición forense de un disco duro estándar. Los siguientes puntos desglosan los tres tipos de métodos de adquisición forense para teléfonos móviles: físico, lógico y manual.

Estos métodos pueden coincidir en parte con un par de niveles que se analizan en el sistema de nivelación de herramientas forenses para móviles.

La cantidad y el tipo de datos que pueden recogerse variará en función del tipo de método de adquisición que se utilice.

### *Adquisición física*

La adquisición física de un dispositivo móvil no es más que una copia bit a bit del almacenamiento físico. Con el acceso directo a la memoria flash, la información puede ser adquirida del dispositivo a través de la extracción física. La memoria flash es una memoria

no volátil y se utiliza principalmente en tarjetas de memoria y unidades flash USB como almacenamiento de estado sólido. El proceso crea una copia bit a bit copia de un sistema de archivos completo, similar al enfoque adoptado en las investigaciones informáticas forenses.

La adquisición física es capaz de adquirir todos los datos presentes en un dispositivo, incluyendo los datos borrados, y el acceso al espacio no asignado en la mayoría de los dispositivos.

#### *Adquisición lógica*

La adquisición lógica consiste en extraer objetos de almacenamiento lógicos, como archivos y directorios que residen en un sistema de archivos. La adquisición lógica de los teléfonos móviles se realiza utilizando la interfaz de programación de aplicaciones del fabricante del dispositivo para sincronizar el contenido del teléfono con un ordenador. Muchas herramientas forenses pueden realizar una adquisición lógica. Es mucho más fácil para una herramienta forense organizar y presentar los datos extraídos a través de la adquisición lógica.

Sin embargo, el analista forense debe entender cómo se produce la adquisición y si el móvil fue modificado de alguna manera durante el proceso.

Según el teléfono y las herramientas forenses utilizadas, se adquieren todos o algunos de los datos. Una adquisición lógica es fácil de realizar y sólo recupera los archivos de un teléfono móvil y no recupera los datos contenidos en espacio no asignado.

#### *Adquisición manual*

Con los teléfonos móviles, la adquisición física suele ser la mejor opción, y la adquisición lógica es la segunda mejor opción. La extracción manual debe ser la última opción al realizar en el proceso de adquisición forense de la información presente en un teléfono móvil. Tanto la adquisición lógica como la manual pueden utilizarse para validar los hallazgos en los datos físicos. Durante la adquisición manual, el examinador utiliza la interfaz de usuario para investigar el contenido de la memoria del teléfono.

El dispositivo se utiliza normalmente mediante el teclado o la pantalla táctil y la navegación por el menú, y el examinador toma imágenes del contenido de cada pantalla. La extracción manual introduce un mayor grado de riesgo en forma de error humano, y existe la posibilidad de que se borren pruebas. La adquisición manual es fácil de realizar y sólo adquiere los datos que aparecen en un teléfono móvil.

A continuación, veamos la cantidad de información que puede extraerse de los teléfonos móviles.

## Posibles pruebas almacenadas en los teléfonos móviles

La gama de información que puede obtenerse de los teléfonos móviles se detalla en este apartado. Los datos de un teléfono móvil pueden encontrarse en varios lugares: la tarjeta SIM, la tarjeta de almacenamiento externo y la memoria del teléfono, por ejemplo.

Además, el proveedor de servicios también almacena información relacionada con las comunicaciones. En este apartado nos centraremos principalmente en los datos adquiridos de la memoria del teléfono.

Las herramientas de extracción de datos de dispositivos móviles recuperan datos de la memoria de un teléfono. Aunque los datos recuperados durante la adquisición forense dependen del modelo de móvil, los siguientes datos son comunes a todos los modelos y resultan útiles como prueba.

Hay que tener en cuenta que la mayoría de los siguientes elementos contienen marcas de tiempo:

- Libreta de direcciones: contiene nombres de contactos, números de teléfono, direcciones de correo electrónico, etc.
- Historial de llamadas: contiene las llamadas marcadas, recibidas y perdidas y la duración de las mismas.
- SMS: contiene los mensajes de texto enviados y recibidos.
- MMS: contiene archivos multimedia como fotos y vídeos enviados y recibidos.
- Correo electrónico: contiene los mensajes de correo electrónico enviados, redactados y recibidos.



- Historial del navegador web: contiene el historial de sitios web que se han visitado.
- Fotos: contiene las imágenes capturadas con la cámara del teléfono móvil, las descargadas de Internet y las transferidas desde otros dispositivos.
- Vídeos: contiene los vídeos capturados con la cámara del móvil, los descargados de Internet, y los transferidos desde otros dispositivos.
- Música: contiene los archivos de música descargados de Internet y los transferidos desde otros dispositivos.
- Documentos: contiene los documentos creados con las aplicaciones del dispositivo, los descargados de Internet y los transferidos desde otros dispositivos.
- Calendario: contiene las entradas del calendario y las citas.
- Comunicación de red: contiene las localizaciones GPS.
- Mapas: contiene los lugares visitados por el usuario, las direcciones buscadas y los mapas y descargado mapas.
- Datos de redes sociales: Contiene los datos almacenados por las aplicaciones, como Facebook, Twitter, LinkedIn, Google+ y WhatsApp.
- Datos eliminados: Contiene información eliminada del teléfono.

A continuación, echaremos un vistazo rápido al último paso de la investigación: el examen y el análisis.

## Examen y análisis

Este es el último paso de la investigación, y tiene como objetivo descubrir los datos que están presentes en el dispositivo. El examen se realiza aplicando métodos científicos y bien probados para establecer resultados concluyentes.

La fase de análisis se centra en separar los datos relevantes del resto y en buscar datos que sean valiosos para el caso subyacente.

El examen comienza con una copia de las pruebas adquiridas mediante algunas de las técnicas descritas anteriormente. El examen y el análisis utilizando herramientas de

terceros se realiza generalmente importando el volcado de memoria del dispositivo en una herramienta forense para móviles que recuperará automáticamente los resultados. La comprensión del caso es también crucial para realizar un análisis específico de los datos. Por ejemplo, un caso de pornografía infantil puede requerir centrarse en todas las imágenes presentes en el dispositivo en lugar de en lugar de mirar otros artefactos.

Es importante tener un buen conocimiento de cómo funcionan las herramientas forenses que se utilizan para realizar el examen. Un buen uso de las funciones y opciones disponibles en una herramienta acelerará drásticamente el proceso de examen. A veces, debido a fallos de programación en el software, una herramienta puede no ser capaz de reconocer o convertir los bits en un formato comprensible por usted. Por lo tanto, es crucial que tenga las habilidades necesarias para identificar tales situaciones y utilizar herramientas o software alternativos para construir los resultados. En algunos casos, un individuo puede manipular a propósito la información del dispositivo o puede borrar/ocultar algunos datos cruciales.

Los analistas forenses deben comprender las limitaciones de sus herramientas y, en ocasiones compensarlas para conseguir los mejores resultados posibles.

## Reglas de las evidencias o pruebas

Los tribunales confían cada vez más en la información de los teléfonos móviles como prueba vital. Para que las pruebas prevalezcan en los tribunales es necesario conocer bien las normas de las pruebas.

El análisis forense de los móviles es una disciplina relativamente nueva, y las leyes que dictan la validez de las pruebas no son muy conocidas, y además difieren de un país a otro. Sin embargo, hay cinco reglas generales de evidencia que se aplican a la ciencia forense digital y que deben seguirse para que las pruebas sean útiles. Ignorar estas reglas hace que las pruebas sean inadmisibles, y su caso podría ser desestimado.

Estas cinco reglas son: admisible, auténtica, completa, fiable y creíble.

- Admisible: esta es la regla más básica y una medida de la validez e importancia de las pruebas. Las pruebas deben conservarse y reunirse de forma que puedan ser

utilizadas en un tribunal o en cualquier otro lugar. Se pueden cometer muchos errores que pueden hacer que un juez considere inadmisibles una prueba. Por ejemplo, las pruebas obtenidas con métodos ilegales suelen ser consideradas inadmisibles.

- Auténtica: las pruebas deben estar vinculadas al incidente de forma relevante para demostrar algo. El examinador forense debe ser responsable del origen de las pruebas.
- Completa: cuando se presentan las pruebas, deben ser claras y completas y deben reflejar toda la historia. No basta con recoger pruebas que sólo muestren una perspectiva de un incidente. Presentar pruebas incompletas es más peligroso que no presentar ninguna prueba, ya que podría dar lugar a un juicio diferente.
- Fiable: las pruebas recogidas en el dispositivo deben ser fiables. Esto depende de las herramientas y la metodología utilizadas. Las técnicas utilizadas y las pruebas recogidas no deben poner en duda la autenticidad de las pruebas. Si se han utilizado algunas técnicas que no se pueden reproducir, la prueba no se considera a menos que los que consideren las pruebas, como el juez y el jurado, tengan que hacerlo.
- Creíble: un examinador forense debe ser capaz de explicar, con claridad y concisión, qué procesos utilizó y cómo se preservó la integridad de las pruebas. Las pruebas que presente deben ser claras, fáciles de entender y creíbles para el jurado.

## Buenas prácticas forenses

Las buenas prácticas forenses se aplican a la recogida y conservación de pruebas. La falta de prácticas forenses adecuadas puede incluso hacer que las pruebas recogidas sean inútiles ante un tribunal de justicia. La modificación de las pruebas ya sea intencionada o accidental, puede afectar a un caso.

Por lo tanto, comprender las mejores prácticas es fundamental para los examinadores forenses.

## Asegurar las pruebas

Con las funciones avanzadas de los teléfonos inteligentes, como Find My iPhone y los borrados remotos, asegurar un teléfono móvil de manera que no pueda ser borrado a distancia es de gran importancia. Además, cuando el teléfono está encendido y tiene servicio, recibe constantemente nuevos datos.

Para asegurar las pruebas, utilice el equipo y las técnicas adecuadas para aislar el teléfono de todas las redes. Con el aislamiento, se impide que el teléfono reciba nuevos datos que podría provocar el borrado de los datos activos.

Dependiendo del caso, puede ser necesario utilizar otras técnicas forenses como la comparación de huellas dactilares, para establecer una conexión entre el dispositivo y su propietario. Si el dispositivo no se manipula de forma segura, las pruebas físicas pueden ser manipuladas involuntariamente y quedar inutilizadas.

También es importante recoger todos los periféricos, soportes asociados, cables, adaptadores de corriente y otros accesorios que estén presentes en el lugar de los hechos. En el lugar de la investigación, si el dispositivo se encuentra conectado a un ordenador personal, si se tira de él directamente se detendrá la transferencia de datos.

En su lugar, se recomienda capturar la memoria del ordenador personal antes de extraer el dispositivo, ya que ésta contiene detalles significativos en muchos casos.

## Preservar las pruebas

A medida que se recogen las pruebas, deben conservarse en un estado aceptable para los tribunales. Trabajar directamente en las copias originales de las pruebas podría alterarlas. Así que, tan pronto como recuperes una imagen de disco o archivos, cree una copia maestra de sólo lectura y duplíquela.

Para que las pruebas para que sean admisibles, debe haber un método científico para validar que las pruebas presentadas son exactamente la misma que el original recogido. Esto puede lograrse creando un valor hash de la imagen obtenida.

Una función hash se utiliza para garantizar la integridad de una adquisición mediante el cálculo de un valor criptográficamente fuerte y no reversible de la imagen/datos.

Después de duplicar la imagen de disco o los archivos en bruto, calcule y verifique los valores hash del original y la copia para garantizar que se mantiene la integridad de las pruebas.

Cualquier cambio en los valores hash deben documentarse y explicarse.

Todo el procesamiento o examen posterior debe realizarse con copias de las pruebas.

Cualquier uso del dispositivo podría alterar la información almacenada en el terminal. Por lo tanto, sólo hay que realizar las tareas que sean absolutamente necesarias.

### Documentar las pruebas y los cambios

Siempre que sea posible, debe crearse un registro de todos los datos visibles. Se recomienda

fotografiar el dispositivo móvil junto con cualquier otro medio encontrado, como cables, periféricos, etc. Esto será útil si más adelante surgen preguntas sobre el entorno. No toques ni pongas las manos sobre el dispositivo móvil cuando lo fotografíes.

Asegúrese de documentar todos los métodos y herramientas utilizados para recoger y extraer las pruebas. Detalla tus notas para que otro examinador pueda reproducirlas. Su trabajo debe ser reproducible. Si no lo es, un juez puede declararlo inadmisibles. Es importante documentar el todo el proceso de recuperación, incluidos todos los cambios realizados durante la adquisición y examen. Por ejemplo, si la herramienta forense utilizada para la extracción de datos troceó la imagen del disco de disco para almacenarla, esto debe documentarse. Todos los cambios realizados en el dispositivo móvil, incluidos los ciclos de alimentación y la sincronización, deben documentarse en las notas del caso.

### Informes

El informe es el proceso de preparación de un resumen detallado de todos los pasos dados y las conclusiones alcanzadas en el marco de un examen. El informe debe incluir detalles sobre todas las acciones importantes realizadas por usted, los resultados de la adquisición y cualquier inferencia de los resultados. La mayoría de las herramientas

forenses incorporan funciones de elaboración de informes que autogeneran los informes al mismo tiempo que ofrecen la posibilidad de personalizarlos.

En general, un informe puede contener los siguientes detalles:

- Datos del organismo informante.
- Identificador del caso.
- Investigador forense.
- Identidad del remitente.
- Fecha de recepción de las pruebas.
- Datos del dispositivo incautado para su examen, incluidos el número de serie, la marca y el modelo.
- Detalles del equipo y las herramientas utilizadas en el examen.
- Descripción de las medidas adoptadas durante el examen.
- Documentación de la cadena de custodia.
- Detalles de los hallazgos o problemas identificados.
- Pruebas recuperadas durante el examen, desde mensajes de chat.
- el historial del navegador, los registros de llamadas, los mensajes borrados, etc..
- Cualquier imagen capturada durante el examen.
- Información sobre el examen y el análisis.
- Conclusión del informe.

## Análisis Forense en Dispositivos Android

Esta sección cubrirá todo lo que necesitas saber sobre el análisis forense en dispositivos Android.

Empezaremos por entender la plataforma Android y su sistema de archivos y luego cubriremos los temas de configuración, adquisición/extracción y recuperación. También veremos el malware de Android y cómo realizar ingeniería inversa en aplicaciones Android utilizando herramientas de código abierto.

## Comprendiendo Android

En este capítulo, nos centraremos en la plataforma Android y en cómo realizar análisis forenses en dispositivos Android. Tener un buen conocimiento del ecosistema Android, las restricciones de seguridad, los sistemas de archivos y otras características puede ser útil durante una investigación forense.

El conocimiento de estos fundamentos ayudará a un experto forense a tomar decisiones informadas durante la investigación.

En este punto trataremos los siguientes temas:

- La evolución de Android.
- La arquitectura de Android.
- La seguridad de Android.
- La jerarquía de archivos de Android.
- El sistema de archivos de Android.

## La evolución de Android

Android es un sistema operativo móvil basado en Linux desarrollado para dispositivos móviles con pantalla táctil. Está desarrollado por un consorcio de empresas conocido como Open Handset Alliance (OHA), cuyo principal contribuyente y comercializador es Google.

El sistema operativo Android ha evolucionado considerablemente desde su fecha de lanzamiento.

Android se lanzó oficialmente al público en 2008, con la versión 1.0. Con el lanzamiento de Android 1.5 Cupcake en 2009, nació la tradición de nombrar las versiones de Android con nombres de de dulces. Los nombres de las versiones también se lanzaron en orden alfabético durante los siguientes 10 años. Sin embargo, en 2019, Google anunció que ponía fin a la nomenclatura basada en la confitería, y que utilizaban el orden numérico para las futuras versiones. En los primeros años, las versiones de Android se actualizaban más de dos veces al año, pero en los últimos años, las actualizaciones de versiones se realizan una vez al año. La última gran actualización de Android es Android 11, la undécima gran versión del sistema operativo Android, anunciada por Google el 19 de febrero de 2020. A continuación se presenta un resumen de la historia de las versiones de Android:

Version	Version name	Release year
Android 1.0	Apple Pie	2008
Android 1.1	Banana Bread	2009
Android 1.5	Cupcake	2009
Android 1.6	Donut	2009
Android 2.0	Eclair	2009
Android 2.2	Froyo	2010
Android 2.3	Gingerbread	2010
Android 3.0	Honeycomb	2011
Android 4.0	Ice Cream Sandwich	2011
Android 4.1	Jelly Bean	2012
Android 4.4	KitKat	2013
Android 5.0	Lollipop	2014
Android 6.0	Marshmallow	2015
Android 7.0	Nougat	2016
Android 8.0	Oreo	2017
Android 9.0	Pie	2018
Android 10.0	Q	2019
Android 11	R	2020

Esta evolución también ha tenido un impacto dramático en las consideraciones de seguridad de Android y cómo se aplican las técnicas forenses. Por ejemplo, las versiones iniciales de Android no contaban con un mecanismo de cifrado de disco completo (FDE)



para almacenar los datos en un formato cifrado dentro del dispositivo. Como resultado, la extracción de datos del dispositivo era mucho más fácil para un investigador forense de lo que es actualmente.

Con cada actualización de la versión de Android, más y más funciones de seguridad, como los permisos de las aplicaciones, el entorno de ejecución de confianza (TEE) y el y el kernel seguro, se han añadido para mejorar la seguridad de la plataforma en general, pero complican el proceso de extracción de datos.

## La arquitectura de Android

Para comprender eficazmente los conceptos forenses cuando se trata de Android, debe tener una comprensión básica de la arquitectura de Android. Al igual que un ordenador, cualquier sistema informático que interactúa con el usuario y realiza tareas complicadas requiere un sistema operativo para manejar las tareas de manera eficaz. Este sistema operativo (ya sea un sistema operativo de escritorio o un sistema operativo para teléfonos móviles) se encarga de gestionar los recursos del sistema, para proporcionar una manera de que las aplicaciones hablen con el hardware o componentes físicos para realizar determinadas tareas.

Android es actualmente el sistema operativo móvil más popular diseñado para alimentar dispositivos móviles. Puedes encontrar más información sobre esto en <https://developer.android.com/about/android.html>.

Android, como sistema operativo de código abierto, libera su código bajo la licencia Apache una de las muchas licencias de código abierto. En la práctica, esto significa que cualquiera (especialmente los fabricantes de dispositivos) puede acceder a él, modificarlo libremente y utilizar el software según los requisitos de cualquier dispositivo. Esta es una de las principales razones de su amplia aceptación.

Entre los principales fabricantes que utilizan Android se encuentran Samsung, HTC, Sony y LG.

Como cualquier otra plataforma, Android consiste en una pila de capas que se ejecutan una sobre otra. Para entender el ecosistema Android, es esencial tener una comprensión básica de qué son estas capas y qué hacen.

El siguiente diagrama resume las distintas capas que intervienen en la pila del software de Android:



Figura 3. Arquitectura Android.

Cada una de estas capas realiza varias operaciones que soportan funciones específicas del sistema operativo. Cada capa proporciona servicios a las capas que están por encima de ella.

La capa del kernel de Linux

La capa de abstracción de hardware

Bibliotecas

Dalvik Virtual Machine (DVM)

ART

La capa del marco de la API de Java

La capa de aplicaciones del sistema

Es la capa superior en la que el usuario puede interactuar directamente con el dispositivo.

Hay dos tipos de aplicaciones: las preinstaladas y las instaladas por el usuario.

Las aplicaciones preinstaladas -como el marcador, el navegador web y los contactos- vienen con el dispositivo. Las aplicaciones instaladas por el usuario pueden descargarse de diferentes lugares, como Google Play Store, Amazon Marketplace, etc. Todo lo que ves en tu teléfono (contactos, correo, cámara, etc.) es una aplicación.

## Configuración previa para realizar análisis forense de Android y Técnicas de extracción de datos previas

### Instalación de Genymotion

En el siguiente apartado se explica la instalación de una de las herramientas más utilizadas dentro de los simuladores de dispositivos Android para realizar pruebas sobre ellos o pruebas sobre apps para dispositivos Android.

El enlace de descarga de la herramienta es el siguiente: <https://www.genymotion.com/>

Se recomienda descargar la opción de Genymotions sin VirtualBox. Para ello será necesario tener instalado el sistema de virtualización previamente a la instalación de Genymotions.

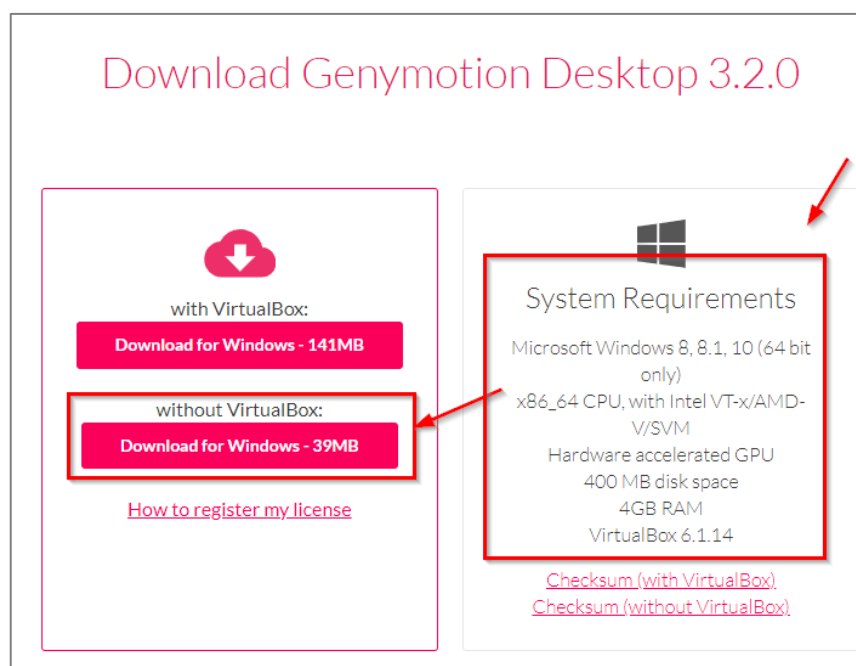


Figura 4. Descarga de la opción de Genymotions sin VirtualBox.

Como las pruebas se realizarán desde un ordenador personal, se recomienda descargar la versión de escritorio.

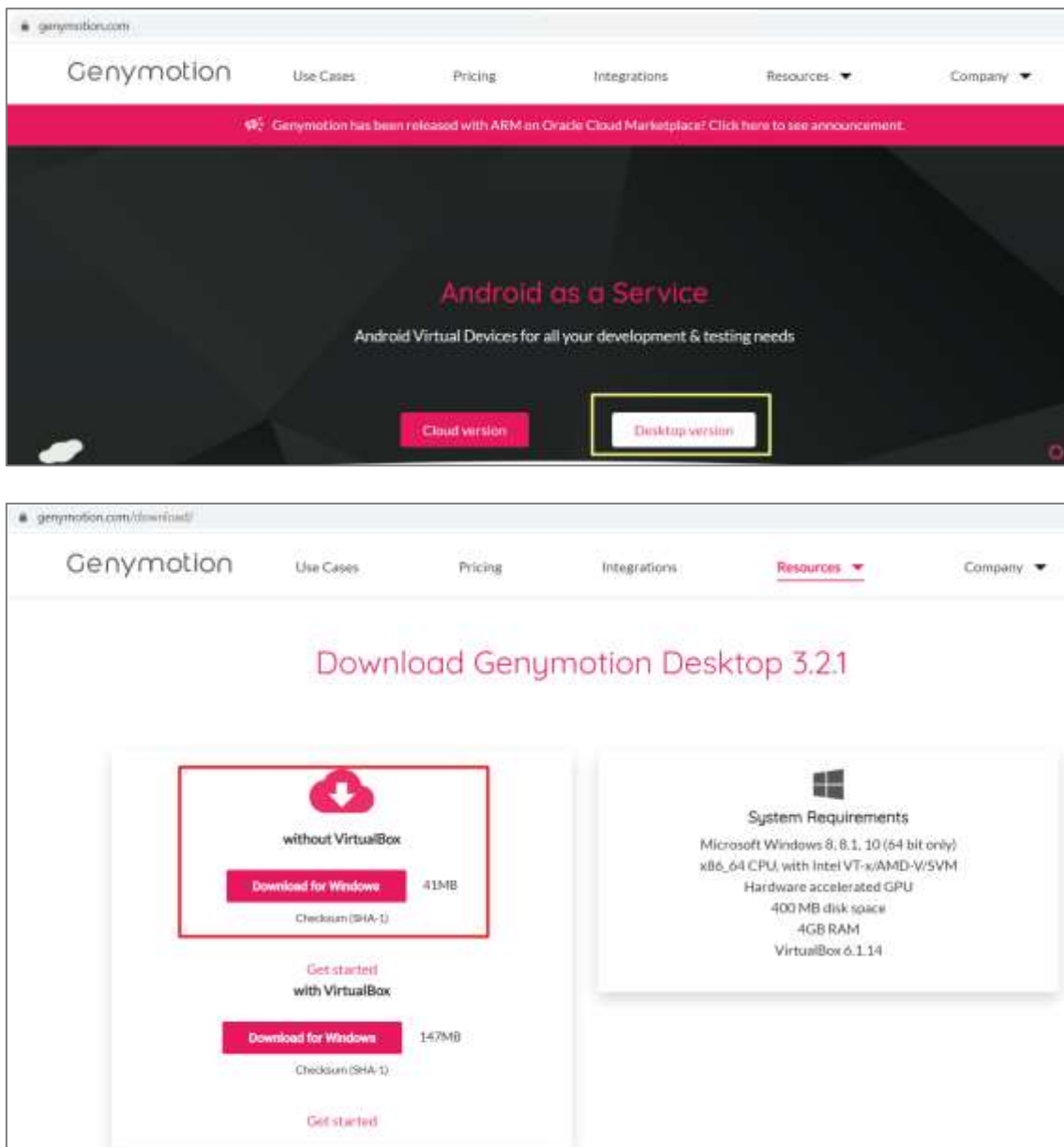


Figura 5. Página de descarga de Genymotions versión escritorio.

Durante el proceso de instalación de la herramienta, preguntará el idioma que se quiere utilizar para su uso.

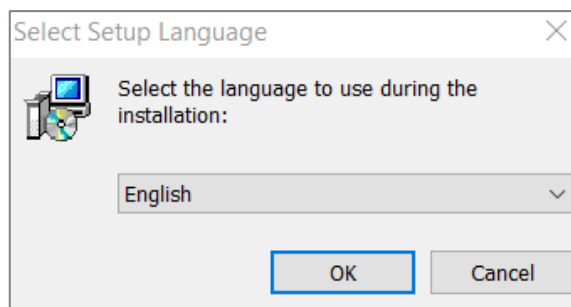


Figura 6. Selección del idioma para trabajar con Genymotion.

Seleccionado el idioma, el siguiente paso será escoger el directorio de instalación de la herramienta.

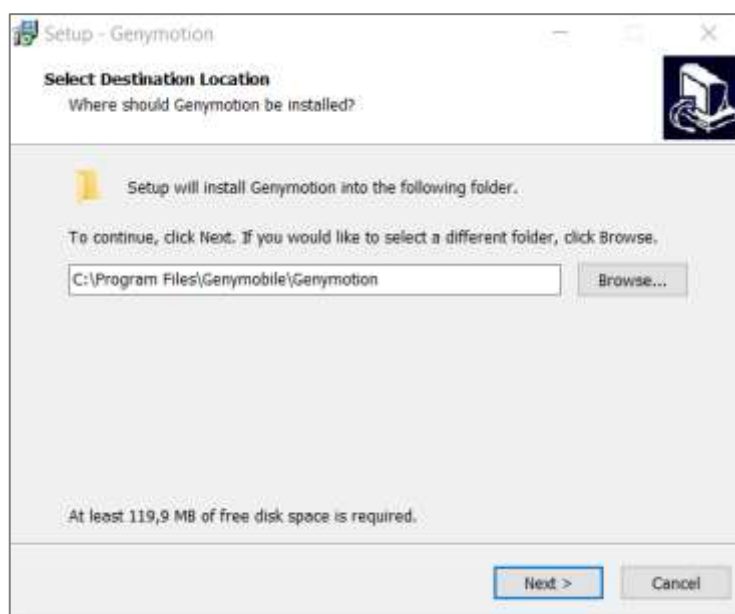


Figura 7. Selección del directorio de instalación de Genymotion.

Seleccionado el lugar de la instalación, el siguiente paso será escoger la carpeta de instalación del programa, por defecto seleccionamos la carpeta “Genymotion”.

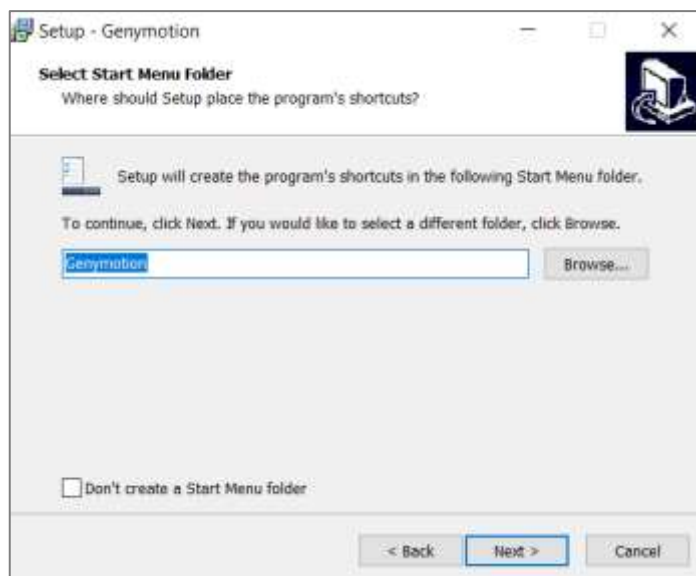


Figura 8. Carpeta de instalación para Genymotions.

El siguiente paso de la instalación será la creación de un icono en el escritorio del

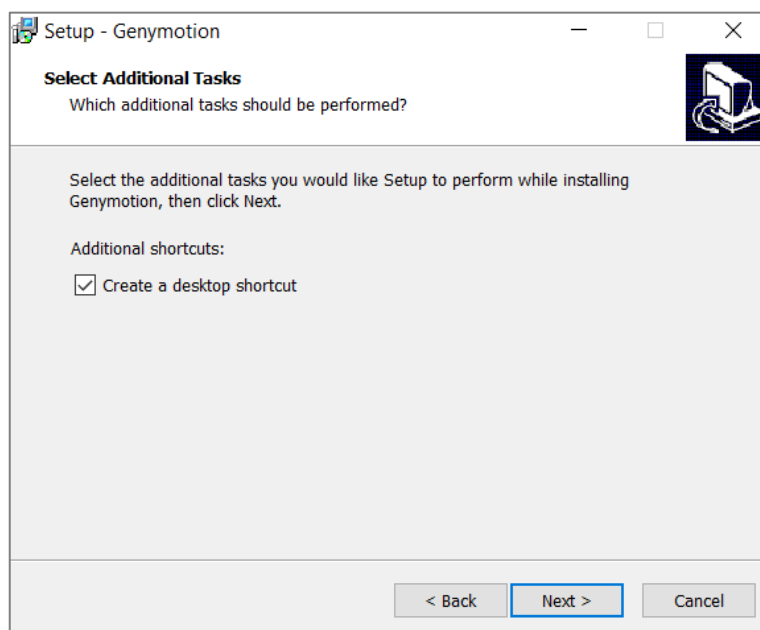


Figura 9. Opción para seleccionar la instalación del icono de Genymotion en el escritorio.

Tras seleccionar la instalación del icono en el escritorio, comenzará el proceso de instalación de Genymotion.

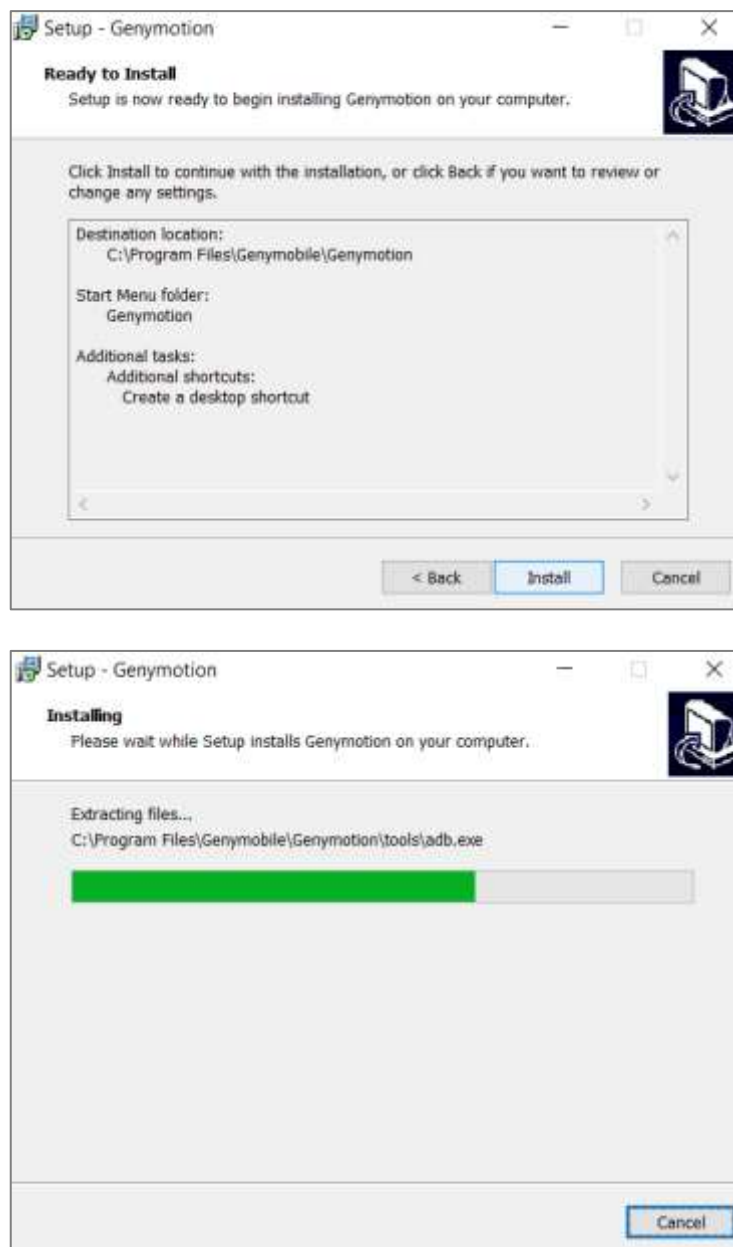


Figura 10. Proceso de instalación de Genymotion.

Una vez terminada la instalación de Genymotion, se dará la posibilidad de lanzar la herramienta justo después de la finalización de la instalación.



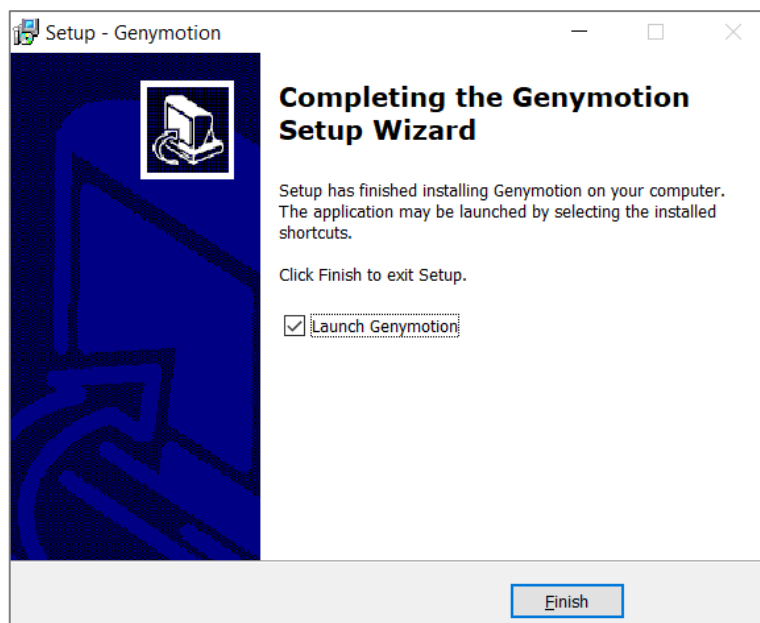


Figura 11. Inicio de Genymotion tras su instalación.

## Ejecución de Genymotions

Aunque se trabaje con una cuenta que no tenga privilegios administrativos, se recomienda ejecutar Genymotion dentro de un contexto con permisos administrativos.

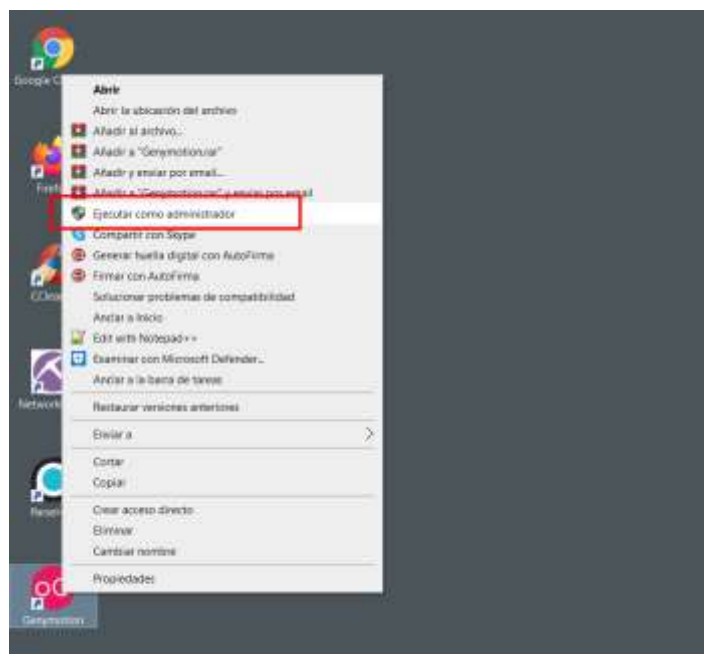


Figura 12. Ejecución de Genymotion en un contexto con privilegios administrativos.

Tras la ejecución de Genymotion en un contexto con privilegios administrativos, el siguiente paso será la creación de un dispositivo virtual.

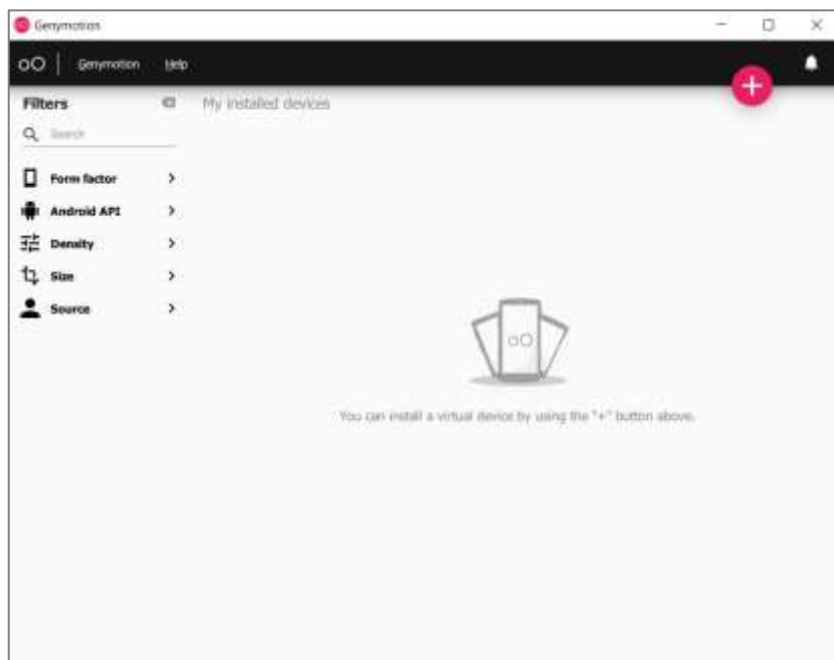
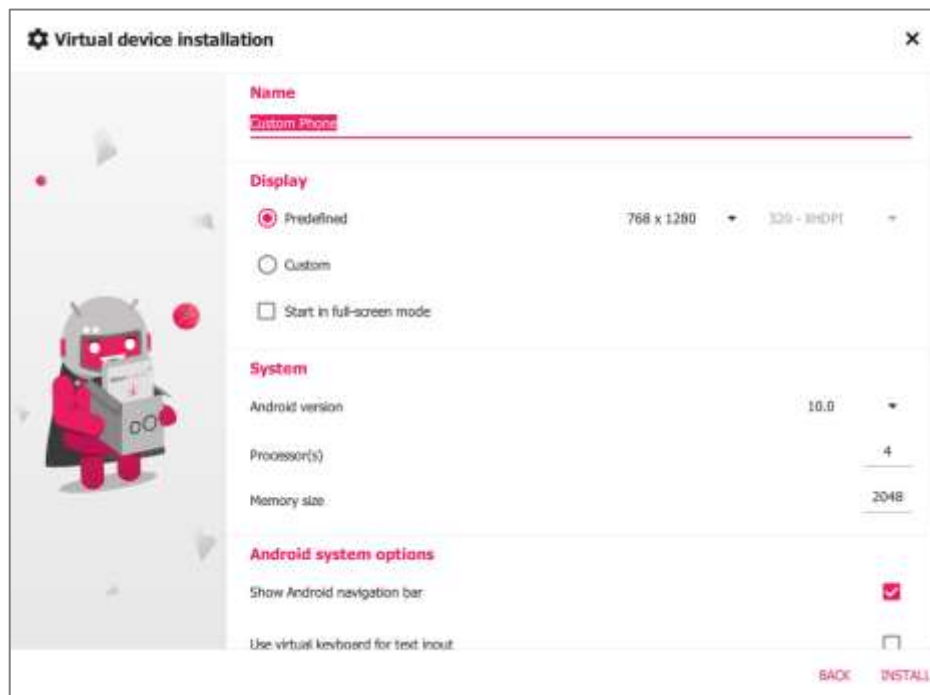
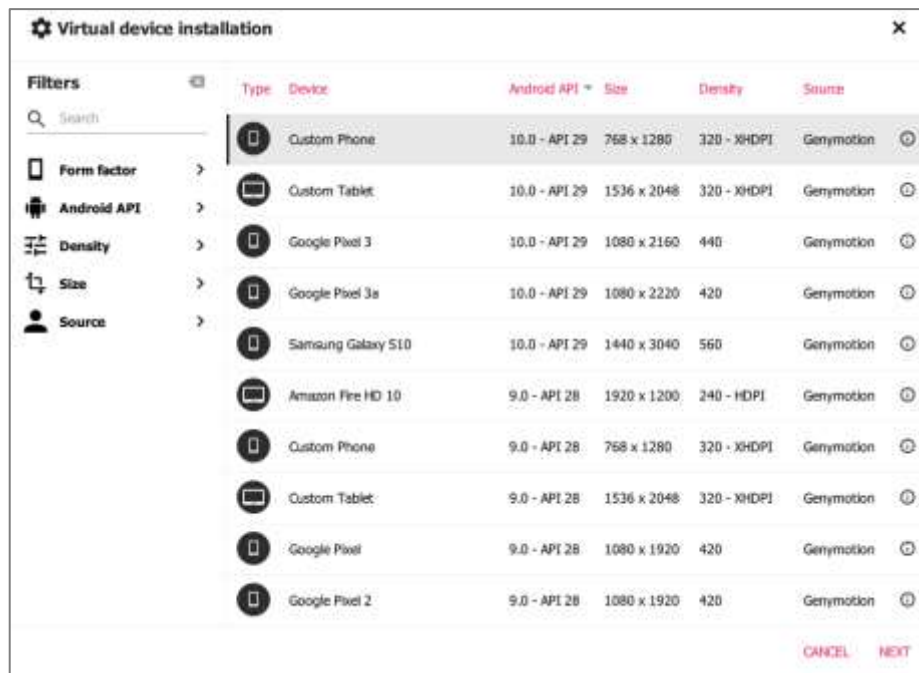


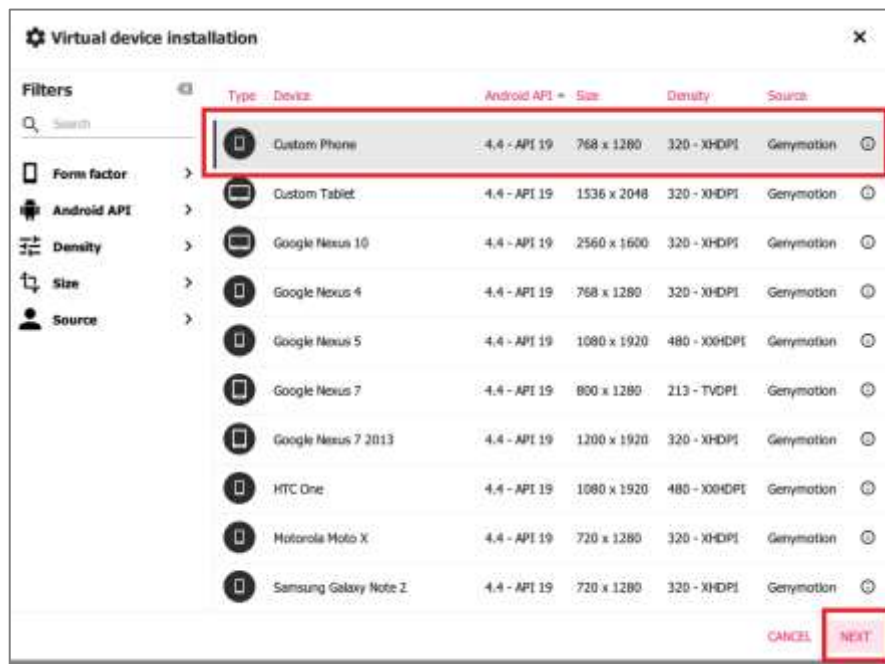
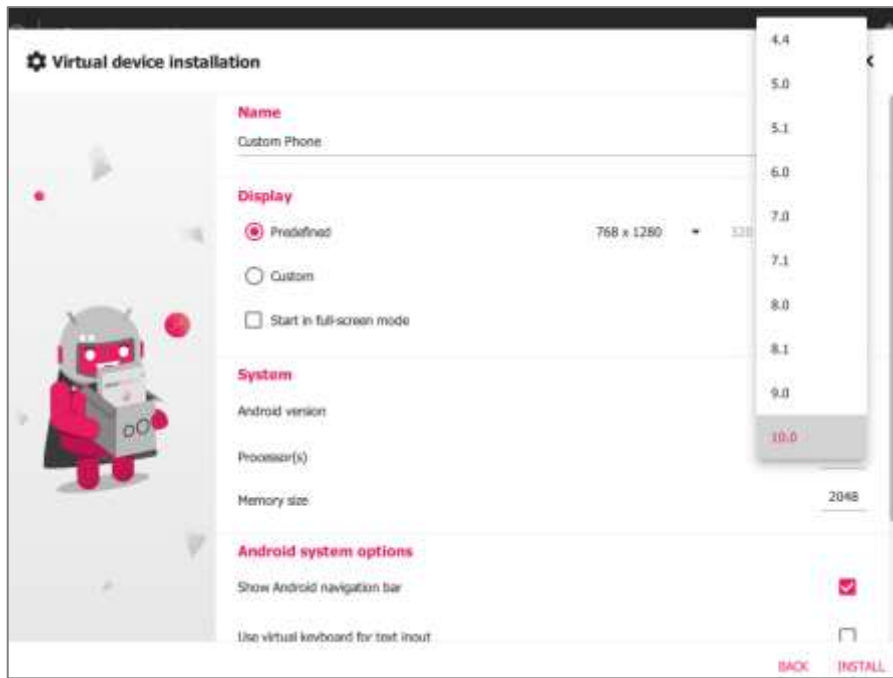
Figura 13. Pantalla para la creación de un dispositivo virtual.

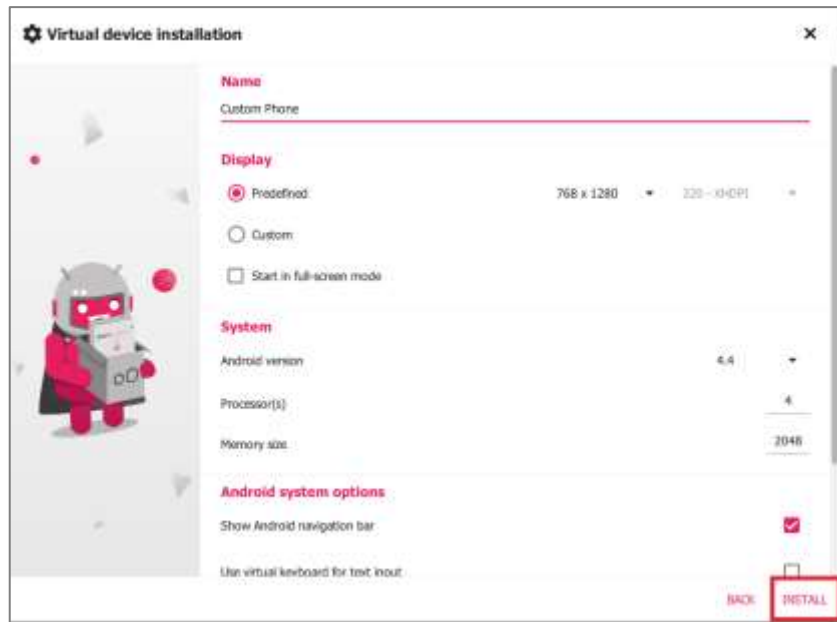
Para la creación de un dispositivo virtual Android, presionamos en le botón “+” de la parte superior derecha.

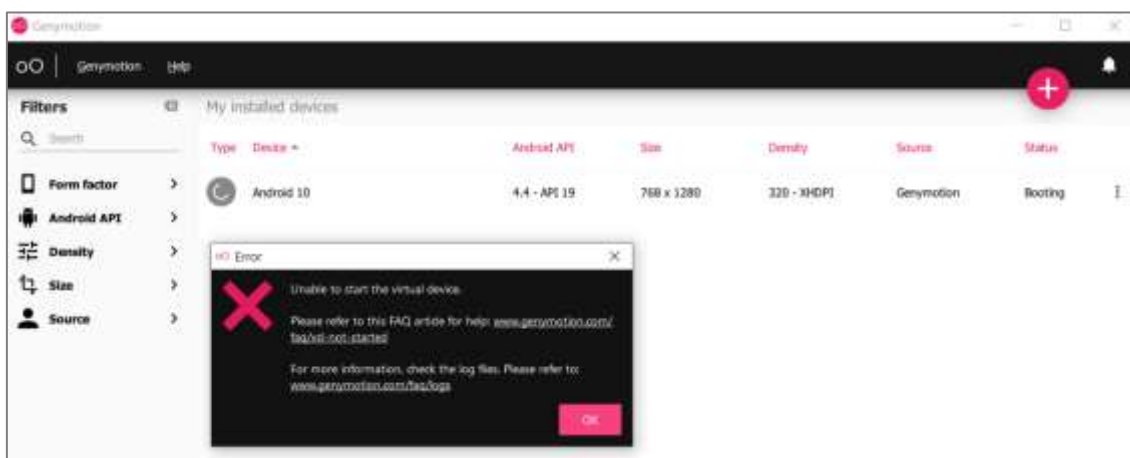
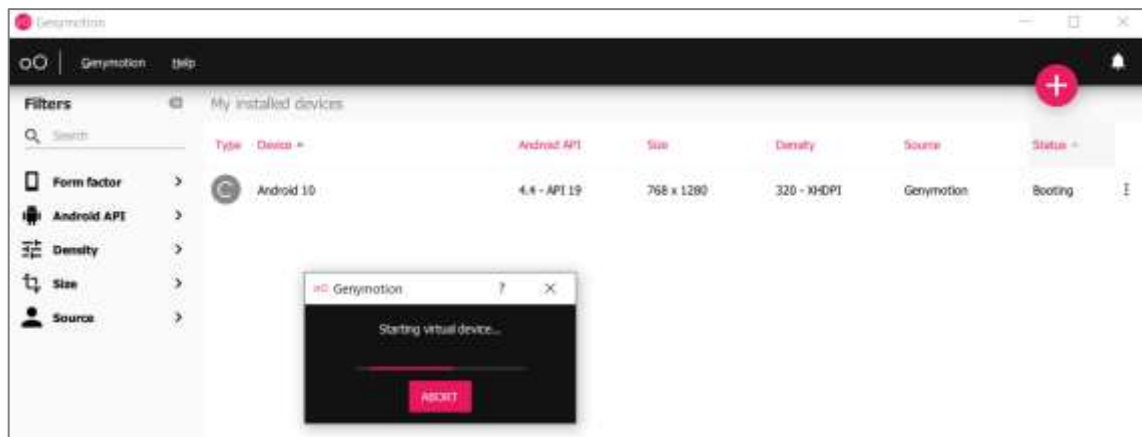


Figura 14. Botón para la creación de un dispositivo virtual Android.

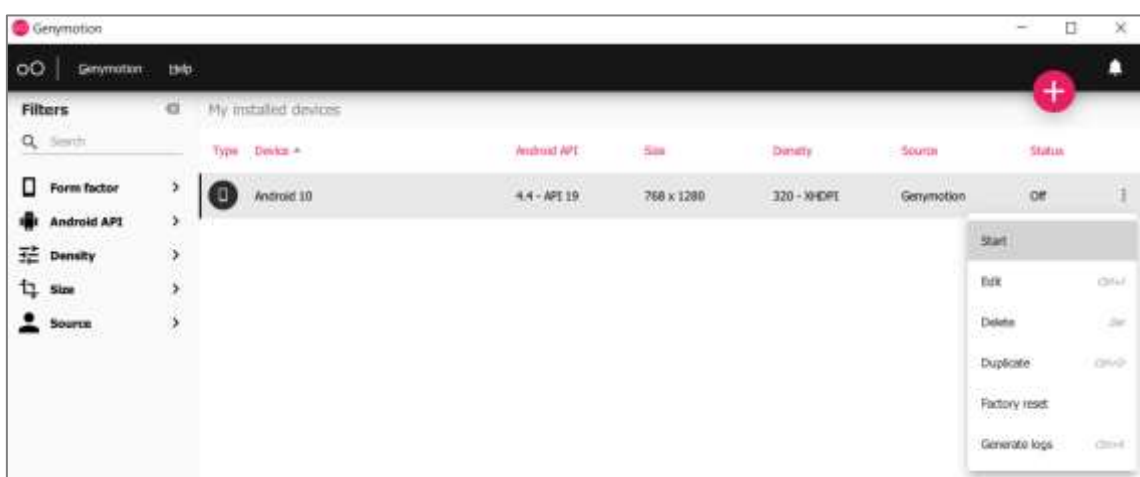


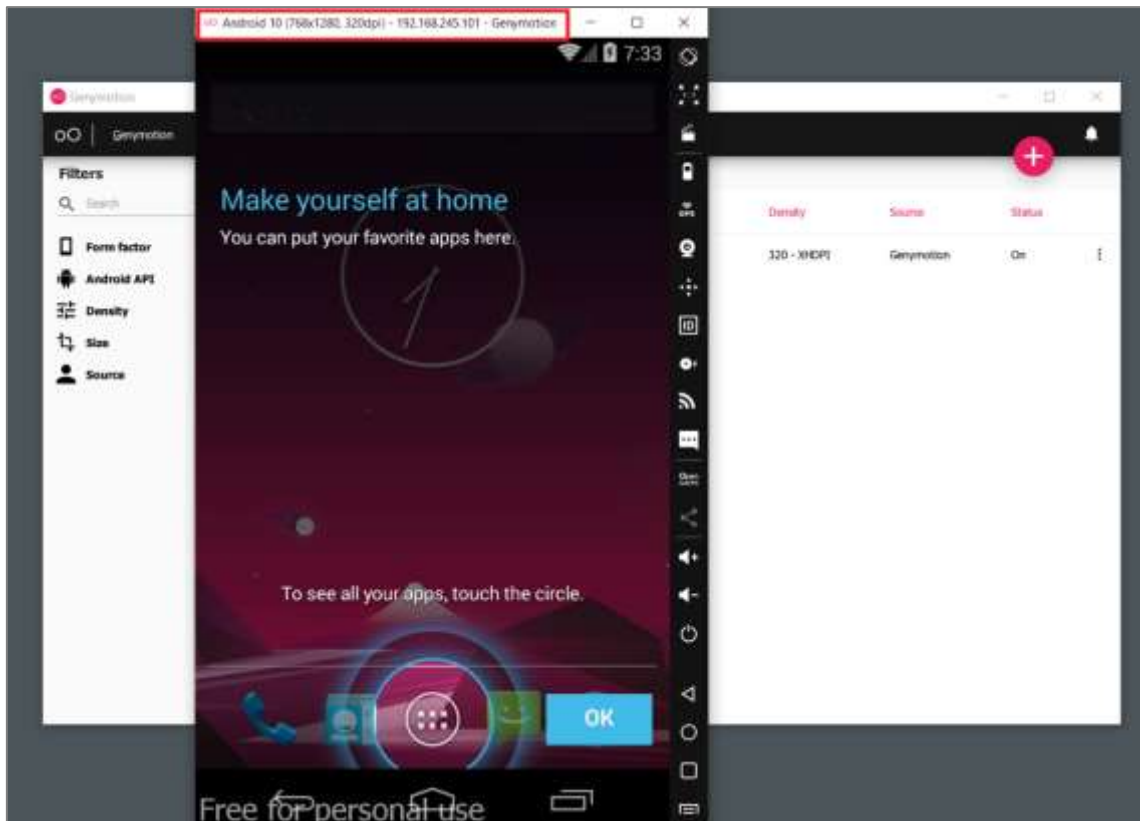






Reiniciamos el ordenador Genymotions bajo un contexto con privilegios administrativos.





```
C:\Users\Internet>ping 192.168.245.101

Haciendo ping a 192.168.245.101 con 32 bytes de datos:
Respuesta desde 192.168.245.101: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.245.101: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.245.101: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.245.101: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.245.101:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

## Conectar un dispositivo Android a una estación de trabajo

La adquisición forense de un dispositivo Android mediante herramientas de código abierto requiere que se conecte el dispositivo a una estación de trabajo forense. La adquisición forense de cualquier dispositivo debe realizarse en una estación de trabajo forense estéril. Esto significa que la estación de trabajo se utiliza estrictamente forense y no para uso personal.

Tenga en cuenta que cada vez que un dispositivo se conecta a un ordenador, se pueden hacer cambios en el dispositivo. Es muy importante tener el control total de todas las interacciones con el dispositivo Android en todo momento.

Para conectar correctamente el dispositivo, deberá seguir los siguientes pasos a una estación de trabajo. Tenga en cuenta que la protección contra escritura puede impedir la adquisición satisfactoria ya que puede ser necesario enviar comandos al dispositivo para obtener información.

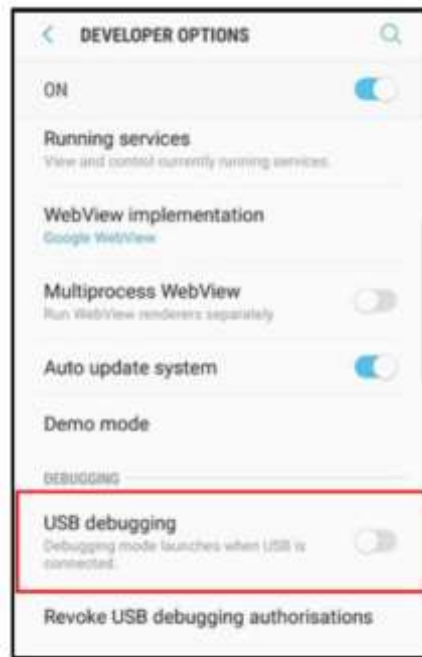
### El puente de depuración de Android

Considerado como uno de los componentes más cruciales en el análisis forense de Android, el *Android Debug Bridge* (ADB) es una herramienta de línea de comandos que le permite comunicarse con el dispositivo Android y controlarlo.

### Depuración USB

La función principal de esta opción es permitir la comunicación entre el dispositivo Android y la estación de trabajo en la que está instalado el SDK de Android. En un teléfono Samsung puede acceder a esta opción en Ajustes | Opciones de desarrollador, como se muestra en la siguiente captura de pantalla:





*Figura 15. La opción de depuración USB en un dispositivo Samsung S8.*

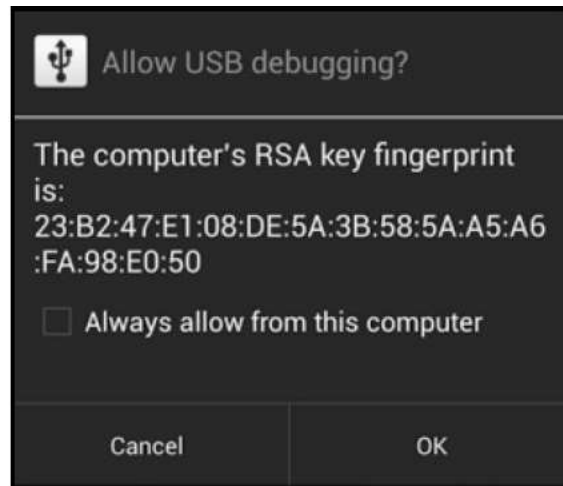
Otros teléfonos Android pueden tener entornos y características de configuración diferentes. Usted puede tener que forzar la opción de Opciones de Desarrollador accediendo al modo de compilación.

Sin embargo, a partir de Android 4.2, el menú de Opciones de Desarrollador está oculto para asegurar que los usuarios no lo habiliten por accidente. Para activarlo, vaya a Ajustes | Acerca del teléfono y luego pulse siete veces el campo Número de compilación. Después de esto, las Opciones de Desarrollador estarán disponibles en el menú de Ajustes.



Antes de Android 4.2.2, habilitar esta opción era el único requisito para comunicarse con el dispositivo a través de ADB; sin embargo, a partir de Android 4.2.2, Google ha introducido la opción de depuración USB segura. Esta característica sólo permite a los hosts que estén explícitamente autorizados por el usuario para conectarse al dispositivo mediante ADB.

Por lo tanto, cuando se conecta el dispositivo a una nueva estación de trabajo a través de USB con el fin de acceder a ADB, primero debe desbloquear el dispositivo y autorizar el acceso pulsando OK en la ventana de confirmación como se muestra en la siguiente captura de pantalla. Si la opción Permitir siempre desde este ordenador está marcada, el dispositivo no pedirá autorización en el futuro:



*Figura 16. Depuración USB segura.*

Cuando se selecciona la opción de depuración USB, el dispositivo ejecutará el demonio adb (adbd) en segundo plano y buscará continuamente una conexión USB. El demonio normalmente ejecutará bajo una cuenta de usuario shell sin privilegios y, por lo tanto, no proporcionará acceso a los datos completos; sin embargo, en los teléfonos rooteados, adbd se ejecutará bajo la cuenta de root y, por lo tanto, proporcionará acceso a todos los datos. No se recomienda hacer root a un dispositivo para obtener un acceso completo a menos que todos los demás métodos forenses fallen. En caso de que elija hacer root a un dispositivo, los métodos deben estar bien documentados y probados antes de intentarlo con pruebas reales.

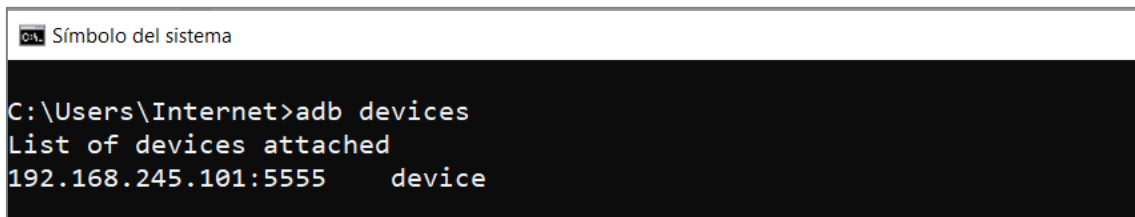
En la estación de trabajo donde está instalado el SDK de Android, adb se ejecutará como un proceso en segundo plano de fondo. Además, en la misma estación de trabajo, un programa cliente, que puede ser invocado desde una shell emitiendo el comando adb. Cuando el cliente adb se inicia, primero comprueba si ya se está ejecutando un demonio adb. Si la respuesta es negativa, inicia un nuevo proceso para iniciar el demonio adb. El programa cliente adb se comunica con el adbd local a través del puerto 5037.

### Acceso al dispositivo mediante adb

Una vez que la configuración del entorno esté completa y el dispositivo Android esté en modo de depuración USB, conecte el dispositivo Android a la estación de trabajo forense con un cable USB y comience a utilizar adb.

### Detección de dispositivos conectados

El siguiente comando adb proporciona una lista de todos los dispositivos conectados a la estación de trabajo forense. Esto también mostrará el emulador si se está ejecutando en el momento de emitir el comando. Recuerde también que, si los controladores necesarios no están instalados, se mostrará un mensaje en blanco. Si se encuentra con esta situación, descargue los controladores necesarios del fabricante e instálelos:



```
C:\Users\Internet>adb devices
List of devices attached
192.168.245.101:5555    device
```

*Figura 17. Dispositivos Android conectados.*

Ahora tenemos una lista de dispositivos conectados a la estación de trabajo.

### Eliminación del servidor ADB local

El siguiente comando mata el servicio local de adb:

```
C:\android-sdk\platform-tools>adb.exe kill-server
```

Después de matar el servicio local de adb, ejecute el comando adb devices. Verá que el servidor se vuelve a iniciar, como se muestra en la siguiente imagen:

```
C:\Users\Internet>adb kill-server

C:\Users\Internet>adb devices
List of devices attached

C:\Users\Internet>adb devices
List of devices attached

C:\Users\Internet>adb devices
List of devices attached
192.168.245.101:5555    device
```

*Figura 18. Eliminación del proceso de escucha y rearranque del proceso de escucha adbd.*

Ahora accederemos al shell ADB en el dispositivo Android

#### Accediendo al shell adb

El comando ADB shell le permite acceder al shell de un dispositivo Android e interactuar con el dispositivo. El siguiente es el comando para acceder al shell adb y ejecutar un comando ls básico para ver el contenido del directorio actual:

```
C:\Users\Internet>adb shell
```

```
C:\Users\Internet>adb shell
root@vbox86p:/ # ls
acct
cache
config
d
data
default.prop
dev
etc
file_contexts
fstab.vbox86
```

*Figura 19. Ejecución de comandos con adb.*

El emulador de Android puede ser utilizado para ejecutar y entender los comandos adb antes de utilizarlos en el dispositivo.

## Uso de ADB para eludir el bloqueo de pantalla

Debido al aumento de la concienciación de los usuarios y a la facilidad de su funcionalidad, se ha producido un aumento exponencial en el uso de las opciones de código de acceso para bloquear los dispositivos Android.

Esto significa que eludir el bloqueo de pantalla del dispositivo durante una investigación forense es cada vez más importante.

La aplicabilidad de las técnicas de anulación del bloqueo de pantalla analizadas hasta ahora se basa en la situación. Tenga en cuenta que algunos de estos métodos pueden hacer que hagamos cambios en el dispositivo. Asegúrese de probar y validar todos los pasos indicados en dispositivos Android y evidenciarlos en un informe.

Es muy importante tener la autorización para realizar los cambios necesarios en el dispositivo, documentar todos los pasos realizados, y ser capaz de describir los pasos realizados si se requiere un testimonio en la sala de justicia.

Actualmente, hay tres tipos de mecanismos de bloqueo de pantalla que ofrece Android. Aunque hay algunos dispositivos que tienen opciones de bloqueo por voz, bloqueo facial y bloqueo por huella dactilar, nos limitaremos a las tres opciones siguientes, ya que son las más utilizadas en todos los dispositivos Android:

- Bloqueo por patrón: el usuario establece un patrón o diseño en el teléfono y el mismo patrón debe ser dibujado para desbloquear el dispositivo. Android fue el primer teléfono inteligente en introducir el bloqueo por patrón.
- Código PIN: Esta es la opción de bloqueo más común y se encuentra en muchos teléfonos móviles. El código PIN es un número de al menos cuatro dígitos numéricos que hay que introducir para desbloquear el dispositivo.
- Código de acceso: se trata de un código de acceso alfanumérico. A diferencia del PIN, que tiene al menos cuatro dígitos numéricos, el código de acceso alfanumérico incluye letras.

## Usar ADB para saltarse el bloqueo de pantalla

Si la depuración USB parece estar habilitada en el dispositivo Android, es conveniente aprovecharse de la misma mediante la conexión con adb utilizando una conexión USB.

Debe conectar el dispositivo a la estación de trabajo forense y ejecutar el comando `adb devices`. Si el dispositivo aparece, implica que la depuración USB está habilitada.



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19043.1165]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Internet>adb devices
List of devices attached
192.168.245.105:5555 device
```

Figura 20. Dispositivo móvil conectado a la estación de trabajo con la depuración USB habilitada.

Si el dispositivo está bloqueado, debe intentar saltarse el bloqueo de pantalla. Los siguientes dos métodos pueden permitirle eludir el bloqueo de pantalla cuando la depuración USB está habilitada.

#### Borrado del archivo `gesture.key`

La eliminación del archivo `gesture.key` eliminará el bloqueo de patrones en el dispositivo. Sin embargo, es importante tener en cuenta que esto cambiará permanentemente el dispositivo, ya que el bloqueo de patrones desaparecerá. Esto debe tenerse en cuenta si se realizan operaciones encubiertas.

A continuación, se muestra cómo se realiza el proceso:

1. Conecte el dispositivo a la estación de trabajo forense (una máquina Windows, en nuestro ejemplo) mediante un cable USB.
2. Abra el símbolo del sistema y ejecute las siguientes instrucciones: `adb.exe shell, cd /data/system rm gesture.key`
3. Reinicie el dispositivo. Si el patrón de bloqueo sigue apareciendo, simplemente dibuje cualquier diseño al azar y el dispositivo debería desbloquearse sin problemas.

Este método funciona cuando el dispositivo está arraigado. Este método puede no ser exitoso en dispositivos no rooteados. El rooteo de un dispositivo Android no debe ser realizar sin la debida autorización, ya que el dispositivo se altera.

### Extracción lógica de datos

Las técnicas de extracción de datos lógicos extraen los datos presentes en el dispositivo interactuando con el sistema operativo y accediendo al sistema de archivos. Estas técnicas son importantes porque proporcionan datos valiosos, funcionan en la mayoría de los dispositivos y son fáciles de usar. Una vez más, el concepto de rooting entra en escena al extraer los datos.

Las técnicas lógicas no requieren acceso de root para la extracción de datos. Sin embargo, tener acceso en modo root en un dispositivo le permite acceder a todos los archivos presentes en un dispositivo. Esto significa que algunos datos pueden ser extraídos en un dispositivo no rooteado mientras que el acceso root abrirá el dispositivo y proporcionará acceso a todos los archivos presentes en el dispositivo. Por lo tanto, tener acceso root a un dispositivo influiría en gran medida en la cantidad y el tipo de datos que podrían extraerse mediante técnicas lógicas.

### Extracción de datos utilizando ADB

Como se ha visto anteriormente, adb es una herramienta de línea de comandos que le ayuda a comunicarse con un dispositivo para recuperar información. Usando adb, puede extraer datos de todos los archivos del dispositivo o sólo los archivos relevantes en los que esté interesado. Esta es la técnica más utilizada como parte de la extracción lógica.

Para acceder a un dispositivo Android a través de adb, la opción de depuración USB debe estar activada.



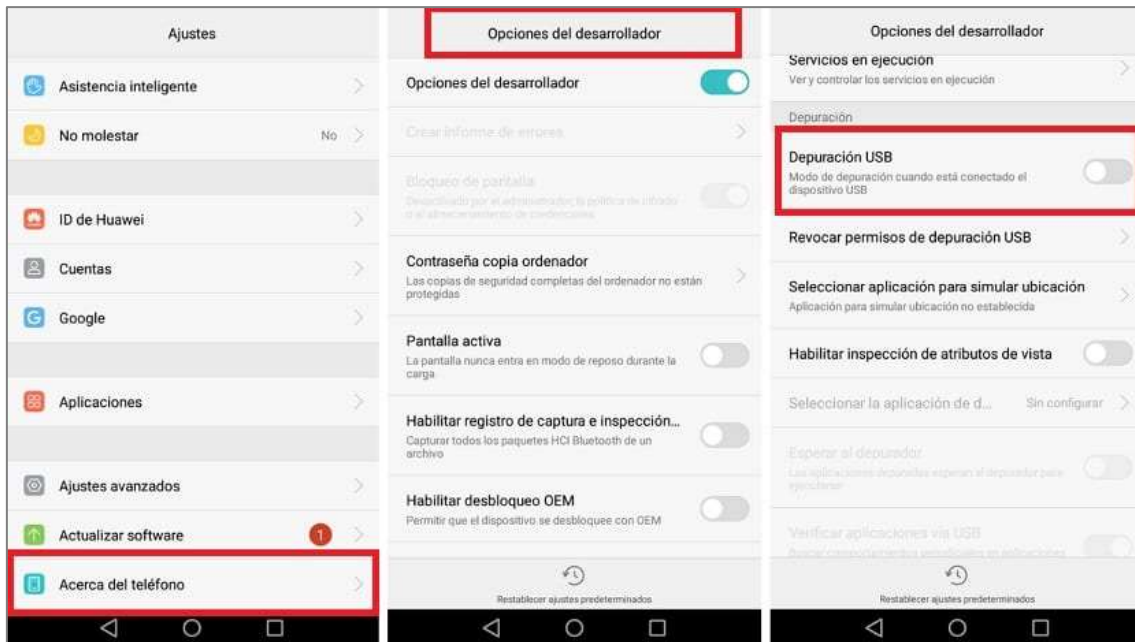


Figura 21. Opción de configuración de depuración USB.

A partir de Android 4.2.2, debido a la depuración USB segura, el host que se conecta al dispositivo debe también estar autorizado.

Como examinador forense, es importante que sepa cómo se almacenan los datos en el dispositivo Android y entender dónde se almacena la información importante y sensible para que los datos puedan ser extraídos en consecuencia. Los datos de las aplicaciones suelen contener una gran cantidad de datos del usuario que pueden ser relevantes para la investigación. Todos los archivos pertenecientes a las aplicaciones de interés pueden almacenarse en una de las siguientes ubicaciones:

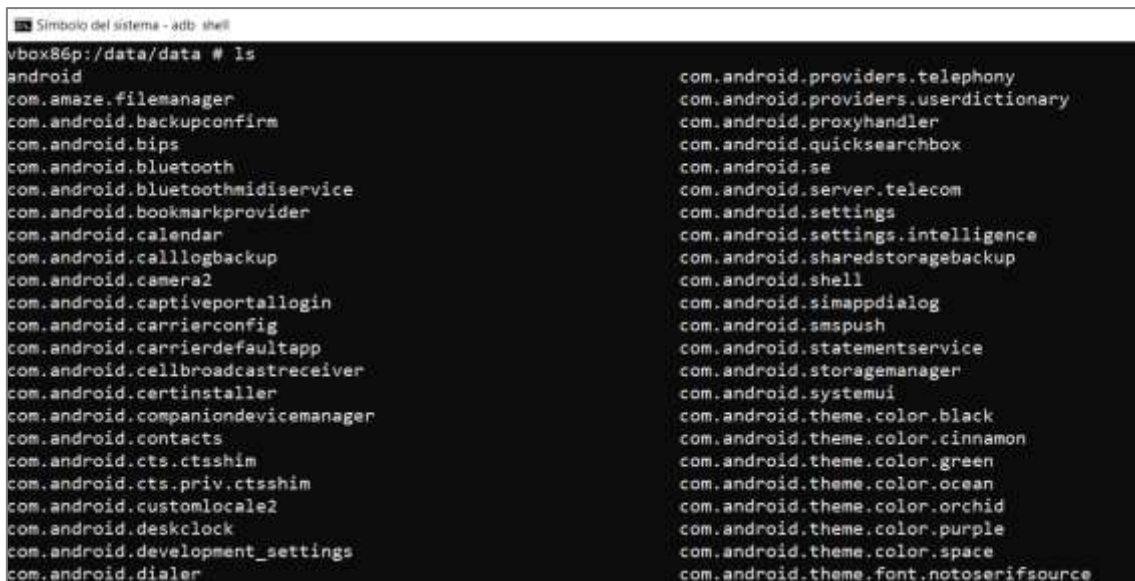
- Preferencias compartidas: esto almacena los datos en pares clave-valor en un formato XML ligero. Los archivos de preferencias compartidas se almacenan en la carpeta `shared_prefs` directorio `/data` de la aplicación.
- Almacenamiento interno: almacena datos que son privados y están presentes en la memoria interna del dispositivo. Los archivos guardados en el almacenamiento interno son privados y no pueden ser acceder por otras aplicaciones.
- Almacenamiento externo: almacena datos que son públicos en la memoria externa del dispositivo, que no suele aplicar mecanismos de seguridad. Estos datos están disponibles en el directorio `/sdcard`.

- Base de datos SQLite: estos datos están disponibles en el directorio `/data/data/PackageName/`

Las bases de datos suele almacenarse con la extensión de archivo `.db`. Los datos presentes en un archivo SQLite pueden verse utilizando el navegador SQLite (<https://sourceforge.net/projects/sqlitebrowser/>) o ejecutando los comandos comandos SQLite necesarios en los respectivos archivos.

Cada aplicación Android almacena datos en el dispositivo utilizando una o más de las opciones de almacenamiento de datos anteriores. Así, la aplicación Contactos almacenaría toda la información sobre los detalles de los contactos en la carpeta `/data/data` bajo su nombre de paquete.

Tenga en cuenta que `/data/data` es una parte del almacenamiento interno de su dispositivo, donde se instalan todas las aplicaciones en circunstancias normales. Algunos datos de las aplicaciones residirán en la tarjeta SD y en la partición `/data/data`.



```

vbox86p:/data/data # ls
android
com.amaze.filemanager
com.android.backupconfirm
com.android.bips
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.bookmarkprovider
com.android.calendar
com.android.calllogbackup
com.android.camera2
com.android.captiveportallogin
com.android.carrierconfig
com.android.carrierdefaultapp
com.android.cellbroadcastreceiver
com.android.certinstaller
com.android.companiondevicemanager
com.android.contacts
com.android.cts.ctsshim
com.android.cts.priv.ctsshim
com.android.customlocale2
com.android.deskclock
com.android.development_settings
com.android.dialer
com.android.providers.telephony
com.android.providers.userdictionary
com.android.proxyhandler
com.android.quicksearchbox
com.android.se
com.android.server.telecom
com.android.settings
com.android.settings.intelligence
com.android.sharedstoragebackup
com.android.shell
com.android.simappdialog
com.android.smspush
com.android.statementservice
com.android.storagemanager
com.android.systemui
com.android.theme.color.black
com.android.theme.color.cinnamon
com.android.theme.color.green
com.android.theme.color.ocean
com.android.theme.color.orchid
com.android.theme.color.purple
com.android.theme.color.space
com.android.theme.font.notoserifsource

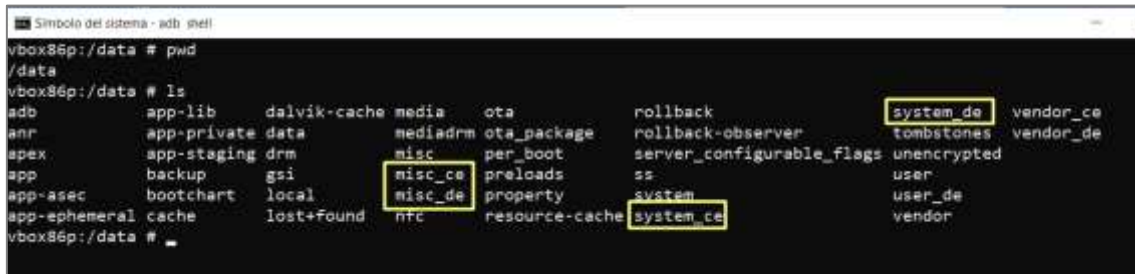
```

Figura 22. Apps dentro de la carpeta `/data`.

Usando `adb`, podemos extraer los datos presentes en esta partición para su posterior análisis utilizando el comando `adb pull`.

Una vez más, es importante tener en cuenta que este directorio sólo es accesible en un teléfono rooteado.

En Android 7.0 (Nougat), se ha introducido un nuevo tipo de almacenamiento llamado almacenamiento cifrado del dispositivo para permitir que las apps guarden ciertos tipos de datos en este almacenamiento. Como resultado de esto, aparecen nuevas rutas de archivos como `misc_de`, `misc_ce`, `system_de` y `system_ce` en la carpeta `/data`.



```

vbox86p:/data # pwd
/data
vbox86p:/data # ls
adb          app-lib      dalvik-cache media      ota          rollback    system_de    tombstones  vendor_ce
anr          app-private data         mediadm    ota_package rollback-observer tombstones  vendor_de
apex         app-staging drm          misc       per_boot    server_configurable_flags unencrypted
app          backup      gsi          misc_ce     preloads    ss          system
app-asec     bootchart   local        misc_de     property    system      user_de
app-ephemeral cache        lost+found  ntc         resource-cache system_ce    user
vbox86p:/data #
  
```

Figura 23. Rutas dentro de la carpeta `/data`.

Desde una perspectiva forense, este es un cambio muy importante porque lo que esto también significa es que, en los dispositivos que ejecutan Android Nougat, `/data/data` no es la única ubicación donde se almacenan los artefactos.

Por ejemplo, la ubicación de los datos de los SMS en los dispositivos antiguos se almacenaba en `/data/com.android.providers.telephony/databases/smsmms.db` y la ubicación de los datos SMS en los dispositivos Nougat se almacena en la ruta `/user_de/0/com.android.providers.telephony/databases/smsmms.db`.

En un teléfono rooteado, el comando `adb pull` puede ejecutarse de la siguiente manera para extraer las bases de datos de la aplicación de Dropbox:



```

C:\android-sdk\platform-tools>adb.exe pull /data/data/com.dropbox.android/databases C:\temp
pull: building file list...
pull: /data/data/com.dropbox.android/databases/prefs.db-journal -> C:\temp/prefs.db-journal
pull: /data/data/com.dropbox.android/databases/prefs.db -> C:\temp/prefs.db
pull: /data/data/com.dropbox.android/databases/db.db-journal -> C:\temp/db.db-journal
pull: /data/data/com.dropbox.android/databases/db.db -> C:\temp/db.db
4 files pulled. 0 files skipped.
1753 KB/s (140352 bytes in 0.078s)
  
```

Figura 24. Comando `adb pull`.

Del mismo modo, en un teléfono rooteado, toda la carpeta `/data` puede ser extraída de esta manera. Como se muestra en la siguiente imagen, contenido completo del

directorio /data en el dispositivo Android puede copiarse en el directorio local de la máquina. El directorio de datos completo se extrajo en 97 segundos. El tiempo de extracción variará dependiendo de la cantidad de datos que residan en /data.

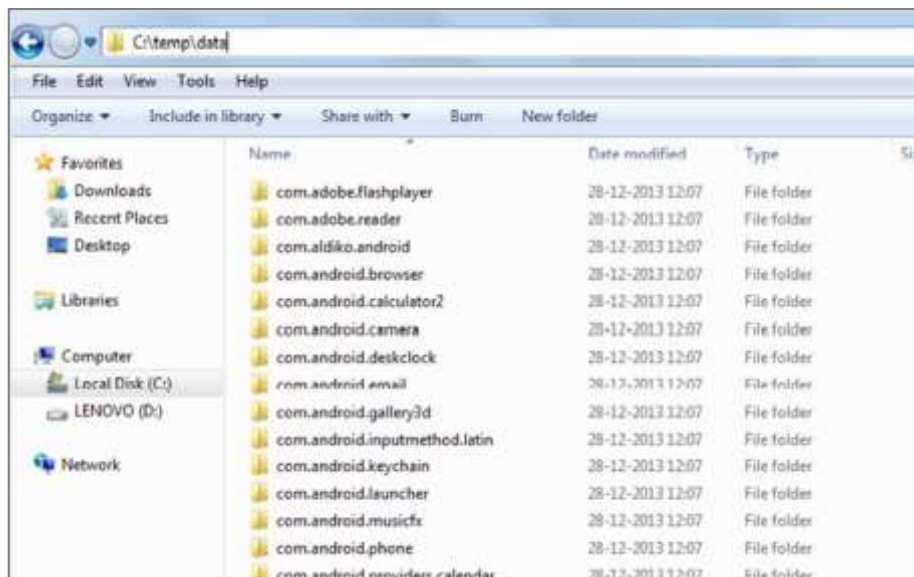


Figura 25. El directorio /data extraído a una estación de trabajo forense.

En un dispositivo no rooteado, un comando pull en el directorio /data no extrae los archivos, como se muestra en la siguiente imagen, ya que el usuario de la shell no tiene permiso para acceder a esos archivos:

```
C:\android-sdk\platform-tools>adb.exe pull /data C:\temp
pull: building file list...
0 files pulled. 0 files skipped.
```

Figura 26. Comando ADB pull en dispositivo no rooteado.

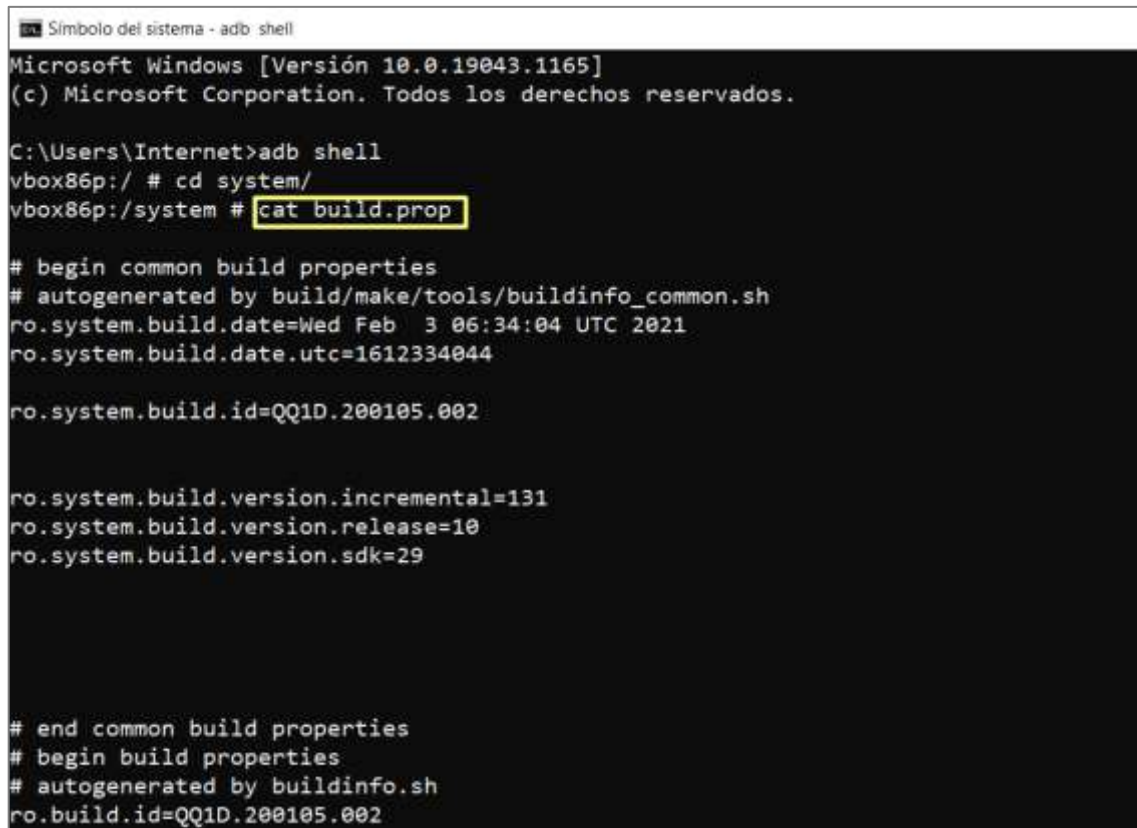
Ejemplo de extracción de una apk de un terminal móvil

<https://www.neoguias.com/extraer-archivos-apk-de-apps-de-android-sin-rootear/>

### Extrayendo la información del dispositivo

Conocer los detalles de su dispositivo Android, como el modelo, la versión, y más, ayudará a su investigación. Por ejemplo, cuando el dispositivo está dañado físicamente y esto prohíbe

el examen de la información del dispositivo puede obtener detalles sobre el dispositivo ejecutando el siguiente comando en la carpeta /system:



```
Símbolo del sistema - adb shell
Microsoft Windows [Versión 10.0.19043.1165]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Internet>adb shell
vbox86p:/ # cd system/
vbox86p:/system # cat build.prop

# begin common build properties
# autogenerated by build/make/tools/buildinfo_common.sh
ro.system.build.date=Wed Feb 3 06:34:04 UTC 2021
ro.system.build.date.utc=1612334044

ro.system.build.id=QQ1D.200105.002

ro.system.build.version.incremental=131
ro.system.build.version.release=10
ro.system.build.version.sdk=29

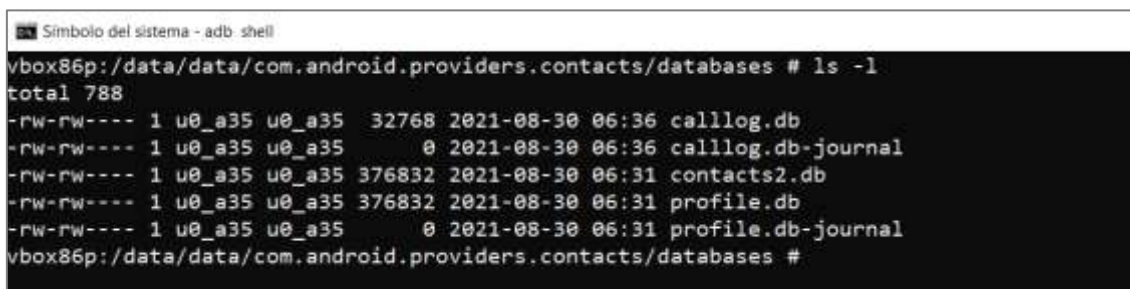
# end common build properties
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=QQ1D.200105.002
```

Después de extraer la información del dispositivo, ahora extraeremos los registros de llamadas.

### Extracción de registros de llamadas

El acceso a los registros de llamadas de un teléfono es a menudo necesario durante una investigación para confirmar ciertos eventos.

La información sobre los registros de llamadas se almacena en el archivo contacts2.db ubicado en /data/data/com.android.providers.contacts/databases/.



```

Simbolo del sistema - adb shell
vbox86p:/data/data/com.android.providers.contacts/databases # ls -l
total 788
-rw-rw---- 1 u0_a35 u0_a35 32768 2021-08-30 06:36 calllog.db
-rw-rw---- 1 u0_a35 u0_a35 0 2021-08-30 06:36 calllog.db-journal
-rw-rw---- 1 u0_a35 u0_a35 376832 2021-08-30 06:31 contacts2.db
-rw-rw---- 1 u0_a35 u0_a35 376832 2021-08-30 06:31 profile.db
-rw-rw---- 1 u0_a35 u0_a35 0 2021-08-30 06:31 profile.db-journal
vbox86p:/data/data/com.android.providers.contacts/databases #

```

Figura 27. Ficheros con las bases de datos en formato sqlite en los contactos en un dispositivo android.

Se puede utilizar el navegador SQLite para ver los datos presentes en este archivo después de extraerlo a una carpeta local en la estación de trabajo forense.

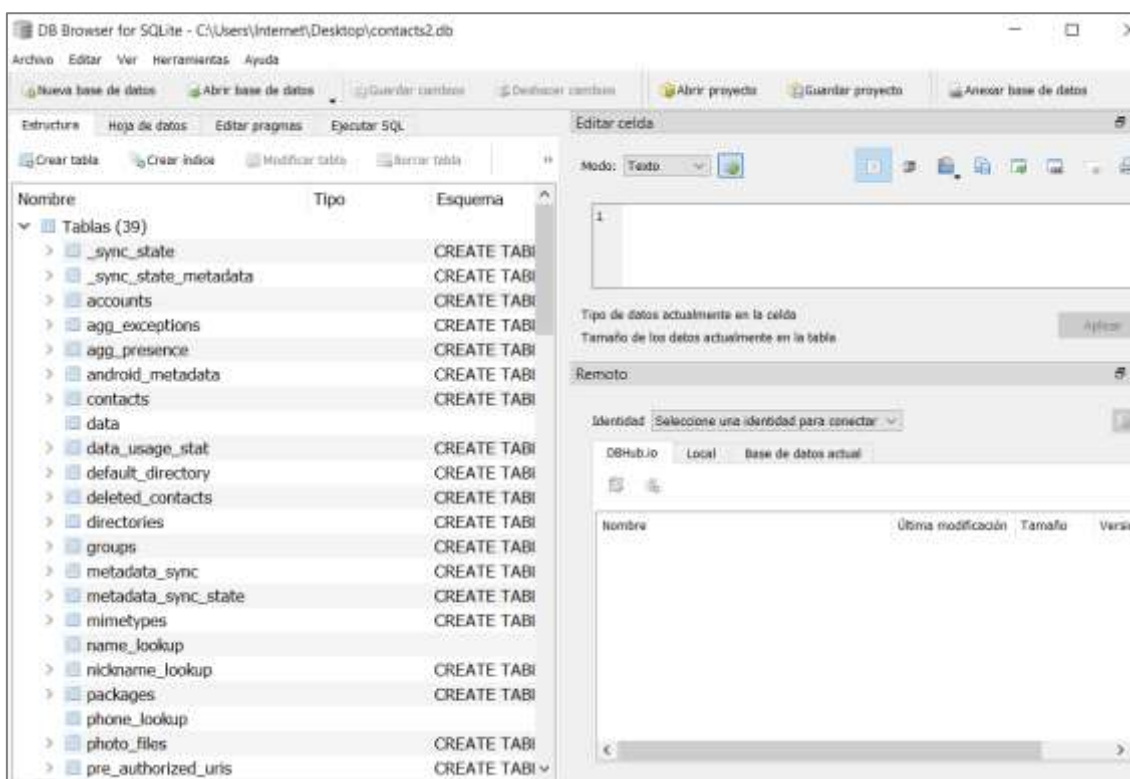


Figura 28. Estructura de la base de datos almacenada en el fichero contacts2.db.

Veamos cómo extraer los registros de llamadas siguiendo estos pasos:



1. Como se muestra en la siguiente captura de pantalla, utilizando el comando `adb pull`, los archivos `.db` necesarios pueden ser extraídos a una carpeta en la estación de trabajo forense.



Figura 29. El archivo `contacts2.db` copiado en una carpeta local.

2. Tenga en cuenta que las aplicaciones utilizadas para realizar llamadas pueden almacenar los detalles del registro de llamadas en la carpeta de la aplicación correspondiente. Todas las aplicaciones de comunicación deben ser examinadas para los detalles del registro de llamadas, como se indica a continuación:

```
/data/data/com.android.providers.contacts/databases
vbox86p:/data/data/com.android.providers.contacts/databases # ls -l
total 788
-rw-rw---- 1 u0_a35 u0_a35 32768 2021-08-30 06:36 calllog.db
-rw-rw---- 1 u0_a35 u0_a35 0 2021-08-30 06:36 calllog.db-journal
-rw-rw---- 1 u0_a35 u0_a35 376832 2021-08-30 06:31 contacts2.db
-rw-rw---- 1 u0_a35 u0_a35 376832 2021-08-30 06:31 profile.db
-rw-rw---- 1 u0_a35 u0_a35 0 2021-08-30 06:31 profile.db-journal
```

Figura 30. Fichero con información importante relacionada con contactos y llamadas.

```
C:\Users\Internet\Desktop>adb pull /data/data/com.android.providers.contacts/databases/calllog.db-journal
/data/data/com.android.providers.contacts/databases/calllog.db-journal: 1 file pulled, 0 skipped.

C:\Users\Internet\Desktop>adb pull /data/data/com.android.providers.contacts/databases/contacts2.db
/data/data/com.android.providers.contacts/databases/contac...file pulled, 0 skipped. 69.9 MB/s (376832 bytes in 0.005s)

C:\Users\Internet\Desktop>adb pull /data/data/com.android.providers.contacts/databases/profile.db
/data/data/com.android.providers.contacts/databases/profil...file pulled, 0 skipped. 189.5 MB/s (376832 bytes in 0.003s)
```

Figura 31. Extracción de ficheros `.db` con la herramienta `adb`.

Ahora, abra el archivo contacts2.db utilizando el Navegador SQLite (navegando a Archivo | Abrir base de datos) y navegue por los datos presentes en las diferentes tablas. La tabla de llamadas presente en el archivo contacts2.db proporciona información sobre el de llamadas. La siguiente captura de pantalla destaca el historial de llamadas junto con el nombre, número, duración y fecha:

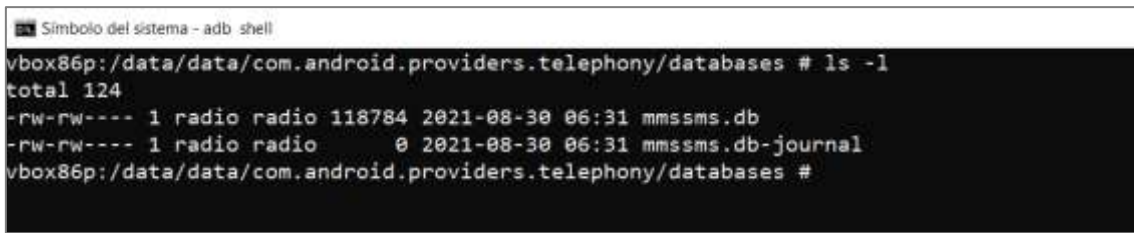
Nombre	Tipo	Esquema
android_metadata		CREATE TABLE android_metadata (locale TEXT)
calls		CREATE TABLE calls (_id INTEGER PRIMARY KEY AUTOINCREMENT, number TEXT, presentation INTEGER NOT NULL DEFAULT 1, post_dial_digits TEXT NOT NULL DEFAULT "", via_number TEXT NOT NULL DEFAULT "", date INTEGER, duration INTEGER, data_usage INTEGER, type INTEGER, features INTEGER NOT NULL DEFAULT 0, subscription_component_name TEXT, subscription_id TEXT, phone_account_address TEXT, phone_account_hidden INTEGER NOT NULL DEFAULT 0, sub_id INTEGER, new INTEGER, name TEXT, number_type INTEGER, number_label TEXT, countryiso TEXT, voicemail_uri TEXT, is_read INTEGER, geocoded_location TEXT, lookup_uri TEXT, matched_number TEXT, normalized_number TEXT, photo_id INTEGER NOT NULL DEFAULT 0, photo_uri TEXT)
_id	INTEGER	"_id" INTEGER
number	TEXT	"number" TEXT
presentation	INTEGER	"presentation" INTEGER NOT NULL DEFAULT 1
post_dial_digits	TEXT	"post_dial_digits" TEXT NOT NULL DEFAULT ""
via_number	TEXT	"via_number" TEXT NOT NULL DEFAULT ""
date	INTEGER	"date" INTEGER
duration	INTEGER	"duration" INTEGER
data_usage	INTEGER	"data_usage" INTEGER
type	INTEGER	"type" INTEGER
features	INTEGER	"features" INTEGER NOT NULL DEFAULT 0
subscription_component_name	TEXT	"subscription_component_name" TEXT
subscription_id	TEXT	"subscription_id" TEXT
phone_account_address	TEXT	"phone_account_address" TEXT
phone_account_hidden	INTEGER	"phone_account_hidden" INTEGER NOT NULL DEFAULT 0
sub_id	INTEGER	"sub_id" INTEGER DEFAULT -1
new	INTEGER	"new" INTEGER
name	TEXT	"name" TEXT
number_type	INTEGER	"number_type" INTEGER
number_label	TEXT	"number_label" TEXT
countryiso	TEXT	"countryiso" TEXT
voicemail_uri	TEXT	"voicemail_uri" TEXT
is_read	INTEGER	"is_read" INTEGER
geocoded_location	TEXT	"geocoded_location" TEXT
lookup_uri	TEXT	"lookup_uri" TEXT
matched_number	TEXT	"matched_number" TEXT
normalized_number	TEXT	"normalized_number" TEXT
photo_id	INTEGER	"photo_id" INTEGER NOT NULL DEFAULT 0
photo_uri	TEXT	"photo_uri" TEXT

Figura 32. Estructura de la tabla con la información de las llamadas del dispositivo.

### Extracción de SMS/MMS

Durante el curso de una investigación, se le puede pedir que recupere los mensajes de texto que fueron enviados y entregados a un dispositivo móvil en particular. Por lo tanto, es importante entender dónde se almacenan los detalles y cómo acceder a los datos. El archivo `mmssms.db`, que está presente en `/data/data/com.android.providers.telephony/databases`, contiene los detalles necesarios.





```
Simbolo del sistema - adb shell
vbox86p:/data/data/com.android.providers.telephony/databases # ls -l
total 124
-rw-rw---- 1 radio radio 118784 2021-08-30 06:31 mmsms.db
-rw-rw---- 1 radio radio      0 2021-08-30 06:31 mmsms.db-journal
vbox86p:/data/data/com.android.providers.telephony/databases #
```

Figura 33. Ficheros relacionados con le logs de los mensajes sms/mms.

Al igual que con los registros de llamadas, debe asegurarse de que las aplicaciones capaces de de mensajería sean examinadas en busca de registros de mensajes relevantes utilizando el siguiente comando:

```
adb.exe pull /data/data/com.android.providers.telephony C:\N-temp
```



```
vbox86p:/data/data/com.android.providers.telephony/databases # ls -l
total 124
-rw-rw---- 1 radio radio 118784 2021-08-30 06:31 mmsms.db
-rw-rw---- 1 radio radio      0 2021-08-30 06:31 mmsms.db-journal
vbox86p:/data/data/com.android.providers.telephony/databases # exit
C:\Users\Internet\Desktop adb pull /data/data/com.android.providers.telephony/databases
/data/data/com.android.providers.telephony/databases/: 2 files pulled, 0 skipped, 32.1 MB/s (118784 bytes in 0.004s)
```

Figura 34. Extracción de los ficheros relacionados con los mensajes sms, mms utilizando la herramienta adb.

Esto dará la siguiente salida:

Nombre	Tipo	Esquema
part	Table	CREATE TABLE part (_id INTEGER PRIMARY KEY AUTOINCREMENT, mid INTEGER, seq INTEGER DEFAULT 0, ct...
pdu	Table	CREATE TABLE pdu (_id INTEGER PRIMARY KEY AUTOINCREMENT, thread_id INTEGER, date INTEGER, date_sen...
pending_msgs	Table	CREATE TABLE pending_msgs (_id INTEGER PRIMARY KEY, proto_type INTEGER, msg_id INTEGER, msg_type INT...
rate	Table	CREATE TABLE rate (sent_time INTEGER)
raw	Table	CREATE TABLE raw (_id INTEGER PRIMARY KEY, date INTEGER, reference_number INTEGER, count INTEGER, seq...
sms	Table	CREATE TABLE sms (_id INTEGER PRIMARY KEY, thread_id INTEGER, address TEXT, person INTEGER, date INTEG...
sqlite_sequence	Table	CREATE TABLE sqlite_sequence(name, seq)
sr_pending	Table	CREATE TABLE sr_pending (reference_number INTEGER, action TEXT, data TEXT)
threads	Table	CREATE TABLE threads (_id INTEGER PRIMARY KEY AUTOINCREMENT, date INTEGER DEFAULT 0, message_coun...
words	Table	
words_content	Table	CREATE TABLE 'words_content'('docid INTEGER PRIMARY KEY, 'c0_id', 'c1index_text', 'c2source_id', 'c3table_to...
words_segdir	Table	CREATE TABLE 'words_segdir'('level INTEGER, idx INTEGER, start_block INTEGER, leaves_and_block INTEGER, end...
words_segments	Table	CREATE TABLE 'words_segments'('blockid INTEGER PRIMARY KEY, block BLOB)
Índices (4)	Index	
addrMsgIdIndex	Index	CREATE INDEX addrMsgIdIndex ON addr (msg_id)
partMidIndex	Index	CREATE INDEX partMidIndex ON part (mid)
threadIdDateIndex	Index	CREATE INDEX threadIdDateIndex ON sms (thread_id, date)
typeThreadIdIndex	Index	CREATE INDEX typeThreadIdIndex ON sms (type, thread_id)
Vistas (2)	View	
pdu_restricted	View	CREATE VIEW pdu_restricted AS SELECT * FROM pdu WHERE (msg_box=1 OR msg_box=2) AND (m_type!=130)
sms_restricted	View	CREATE VIEW sms_restricted AS SELECT * FROM sms WHERE type=1 OR type=2
Disparadores (26)	Trigger	
addr_cleanup	Trigger	CREATE TRIGGER addr_cleanup DELETE ON pdu BEGIN DELETE FROM addr WHERE msg_id=old_id;END
cleanup_delivery_and_read...	Trigger	CREATE TRIGGER cleanup_delivery_and_read_report AFTER DELETE ON pdu WHEN old.m_type=128 BEGIN DELI...
delete_mms_pending_on_d...	Trigger	CREATE TRIGGER delete_mms_pending_on_delete AFTER DELETE ON pdu BEGIN DELETE FROM pending_msgs
delete_mms_pending_on_u...	Trigger	CREATE TRIGGER delete_mms_pending_on_update AFTER UPDATE ON pdu WHEN old.msg_box=4 AND new.msg...
insert_mms_pending_on_in...	Trigger	CREATE TRIGGER insert_mms_pending_on_insert AFTER INSERT ON pdu WHEN new.m_type=130 OR new.m_ty...
insert_mms_pending_on_u...	Trigger	CREATE TRIGGER insert_mms_pending_on_update AFTER UPDATE ON pdu WHEN new.m_type=128 AND new.m...
mms_words_delete	Trigger	CREATE TRIGGER mms_words_delete AFTER DELETE ON part BEGIN DELETE FROM words WHERE source_id =
mms_words_update	Trigger	CREATE TRIGGER mms_words_update AFTER UPDATE ON part BEGIN UPDATE words SET index_text = NEW.to...
part_cleanup	Trigger	CREATE TRIGGER part_cleanup DELETE ON pdu BEGIN DELETE FROM part WHERE mid=old_id;END

Figura 35. Estructura de la tabla donde se almacenan los mensajes MMS y SMS.

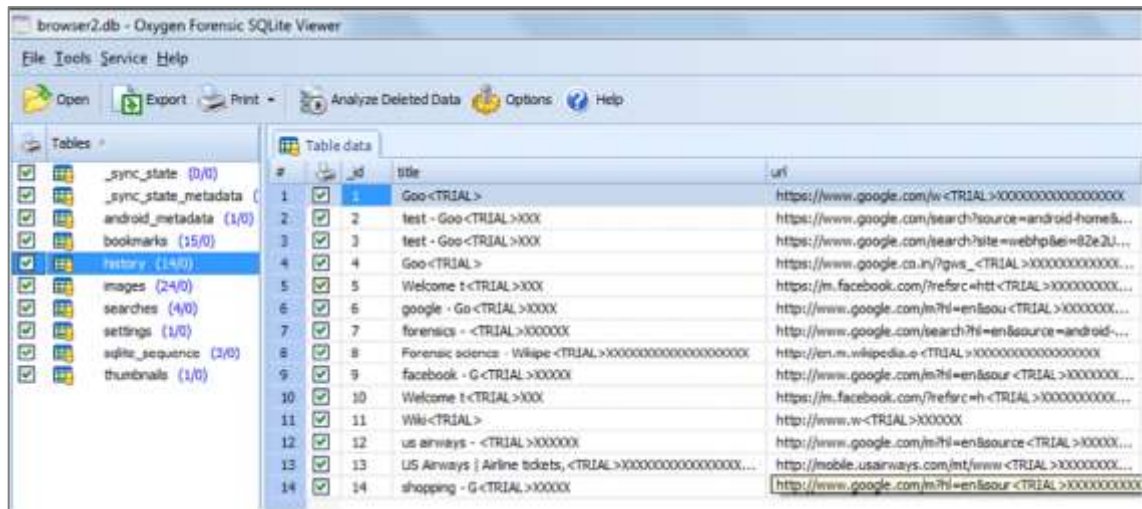
### Extracción de la información del historial del navegador

La extracción de la información del historial del navegador es una tarea que a menudo se requiere de un forense. Aparte del navegador por defecto de Android, se pueden utilizar diferentes aplicaciones de navegador en un teléfono Android, como Firefox Mobile y Google Chrome.

Todos estos navegadores almacenan su historial de navegación en el formato SQLite .db. Para nuestro ejemplo, estamos extrayendo datos del navegador por defecto de Android a nuestra estación de trabajo forense.

Estos datos están localizados en /data/data/com.android.browser. El archivo llamado browser2.db contiene los detalles del historial del navegador.

La siguiente imagen muestra los datos del navegador, representados por Oxygen Forensic SQLite Viewer. Tenga en cuenta que la versión de prueba ocultará cierta información:



#	id	title	url
1	1	Goo<TRIAL>	https://www.google.com/w<TRIAL>XXXXXXXXXXXXXXXXXXXX
2	2	test - Goo<TRIAL>XXX	https://www.google.com/search?source=android-home&...
3	3	test - Goo<TRIAL>XXX	https://www.google.com/search?site=webhp&ie=82e2U...
4	4	Goo<TRIAL>	https://www.google.ca/in/?gvs_<TRIAL>XXXXXXXXXXXX...
5	5	Welcome t<TRIAL>XXX	https://m.facebook.com/?refsrc=htt<TRIAL>XXXXXXXXXXXX...
6	6	google - Go<TRIAL>XXXX	https://www.google.com/m?hl=en&source=TRIAL>XXXXXXXX...
7	7	forensics - <TRIAL>XXXXXX	http://www.google.com/search?hl=en&source=android-...
8	8	Forensic science - Wikip<TRIAL>XXXXXXXXXXXXXXXXXXXX	http://en.m.wikipedia.o<TRIAL>XXXXXXXXXXXXXXXXXXXX
9	9	facebook - G<TRIAL>XXXXXX	http://www.google.com/m?hl=en&source=TRIAL>XXXXXXXX...
10	10	Welcome t<TRIAL>XXX	https://m.facebook.com/?refsrc=h<TRIAL>XXXXXXXXXXXX...
11	11	Wiki<TRIAL>	http://www.w<TRIAL>XXXXXX
12	12	us airways - <TRIAL>XXXXXX	http://www.google.com/m?hl=en&source=TRIAL>XXXXXX...
13	13	US Airways   Airline tickets,<TRIAL>XXXXXXXXXXXXXXXXXXXX...	http://mobile.usairways.com/int/www<TRIAL>XXXXXXXXXXXX...
14	14	shopping - G<TRIAL>XXXXXX	http://www.google.com/m?hl=en&source=TRIAL>XXXXXXXXXXXX...

Figura 36. El archivo browser2.db en Oxygen Forensic SQLite Viewer.

Hay que tener en cuenta que el comportamiento antes mencionado podría cambiar si se utiliza el modo de incógnito del navegador. Varios de los detalles que se han visto no se almacenan en el dispositivo si se utiliza el modo incógnito del navegador.

### Análisis de los chats de redes sociales/IM

Las redes sociales y las aplicaciones de chat de mensajería instantánea, como Facebook, Twitter y WhatsApp revelan datos sensibles que podrían ser útiles durante la investigación de cualquier caso.

El análisis es prácticamente el mismo que con cualquier otra aplicación de Android. Descargue los datos a una estación de trabajo forense y analice los archivos .db para averiguar si puede obtener alguna información sensible. Por ejemplo, veamos la aplicación de Facebook e intentemos ver qué datos se pueden extraer.

Primero, extraemos la carpeta /data/data/com.facebook.katana y navegamos hasta la carpeta carpeta databases.

```

Simbolo del sistema - adb shell
root@vbox86p:/data/data/com.facebook.katana/databases # ls
composer_db
composer_db-journal
contacts_db2
contacts_db2-journal
offline_lwi_mutations_db
offline_lwi_mutations_db-journal
offline_mode_db
offline_mode_db-journal
prefs_db
prefs_db-journal
root@vbox86p:/data/data/com.facebook.katana/databases #

```

Figura 37. Contenido de la carpeta databases para Facebook.

El archivo fb.db presente en esta carpeta contiene la información que está asociada a la cuenta del usuario. La tabla friends\_data contiene información sobre los nombres de los amigos del usuario, junto con sus números de teléfono, ID de correo electrónico y fechas de nacimiento, como se muestra en la siguiente imagen.

	id	user id	first name	last name	cell	other	email	birthday month
1		1 100004087623668	Lavanya				lavanya @gn	2
2		2 100000005601801	Pranav	M				-3
3		3 100004630714031	Sujata	P	+919			4
4		4 100000818058433	Sudha	C			sudha @yah	1
5		5 100003499121241	Vasu	N	+919		vasu i@	7
6		6 100003191641671	Mekha	A	+9101		n @redd	12
7		7 1033892411	Sai	BI	+9195		sai@i@	9
8		8 100002190061552	Vara	K			vara @hoo.co	3
9		9 10000232888334	Kalun	A	+9186	3	k @vind@gmail.i	6
10		10 100000103323292	E	R	+919		prtha @dy@y	-1
11		11 562618335	Mukesh	K	+9198	1	mukesh @yahc	2

Figura 38. Base de datos de Facebook extraída con adb.

Del mismo modo, se pueden analizar otros archivos para averiguar si se puede recopilar alguna información sensible presentes en la carpeta /data/data, se puede obtener información sobre la geolocalización, los eventos del calendario, las notas del usuario, etc.

## Resumen

Los dispositivos móviles modernos almacenan una amplia gama de información, como SMS, registros de llamadas, historial del navegador, mensajes de chat, detalles de localización, etc. De ahí que a menudo sean un factor clave en varios casos criminales, reconstrucción de eventos, casos corporativos y legales, y más.

La ciencia forense de los dispositivos móviles también tiene sus propios retos y conceptos que se salen de los límites de la ciencia forense digital tradicional.

Hay que tener mucho cuidado al manipular el dispositivo, desde la fase de admisión de pruebas hasta la fase de archivo. Los examinadores responsables de los dispositivos móviles deben comprender los diferentes métodos de adquisición y las complejidades de la manipulación de los datos durante el análisis. Extraer datos de un dispositivo móvil es la mitad del trabajo a realizar.

El sistema operativo, las características de seguridad y el tipo de teléfono inteligente determinarán la cantidad acceso a los datos.

Es importante seguir unas prácticas forenses sólidas y asegurarse de que las pruebas no se alteren durante la investigación.

