UNED

TRABAJO FIN DE MASTER

Análisis forense en entornos Android orientado a la adquisición de inteligencia

Máster en Ciberseguridad

ALUMNO: Jesús Sevilla Sánchez

DIRECTORES: María de los Llanos Tobarra Abad

Antonio Robles Gómez

UNED

TRABAJO FIN DE MASTER

Análisis forense en entornos Android orientado a la adquisición de inteligencia

Máster en ciberseguridad

RESUMEN

El presente trabajo de fin de master constituye una extensión de la asignatura Análisis Forense, focalizado en los dispositivos móviles que montan sistemas operativos Android. Por un lado, se mostrarán los fundamentos teóricos que conforman este tipo de análisis forense digital, desde la importancia que en nuestras vidas juegan estos dispositivos, hasta comprender la necesidad de un análisis forense en este ámbito, junto con ello, las diversas fases, técnicas y procedimientos que caracterizan estas actividades forenses.

Por otro lado, se materializarán una serie de talleres de prácticas, buscando, no solo una muestra real de este tipo de análisis, sino una herramienta en sí misma, con el objeto de formar a cierto personal en esta disciplina, con un nivel de detalle que, partiendo del material y formación previa por parte del alumno, alcanza la propia resolución del profesorado.

A lo largo del presente proyecto, se han marcado una serie de objetivos, basados en la formación en la ciencia forense sobre dispositivos móviles, así como la conformación de una serie de talleres de prácticas. Su cumplimiento ha sido viable a través de unas bases teóricas que sostienen este tipo de ciencia forense, desde el conocimiento de las bases de un sistema operativo Android, hasta el paso por una serie de buenas prácticas sobre acciones forense en estos dispositivos. Junto con lo anterior la materialización/ejemplo de acción forense sobre sistemas Android, lo cual no solo refuerza, sino que demuestra los retos que supone “enfrentarse” a este tipo de dispositivos/sistemas operativos asociados.

This master's research project is an addition to the subject Forensic Analysis, focusing on mobile devices that use Android operating systems. On the one hand, it will show the theoretical foundations that make up this type of digital forensic analysis, from the importance that these devices play in our lives, to understanding the need for forensic analysis in this area, along with the various phases, techniques and procedures that characterise these forensic activities.

On the other hand, a series of practical workshops will materialise, seeking not only a real sample of this type of analysis, but a tool in itself, with the aim of training certain personnel in this discipline, with a level of detail that, starting from the material and previous training on the part of the student, reaches the very resolution of the teaching staff.

Throughout this project, a series of objectives have been set, based on mobile forensic science training on mobile devices, as well as the creation of a series of practical workshops. Its fulfilment has been feasible through theoretical bases that support this type of forensic science, from the knowledge of the basics of an Android operating system, to the passage through a series of good practices on forensic actions on these devices. Along with the above, the materialisation/example of forensic action on Android systems, which not only reinforces, but also demonstrates the challenges involved in "confronting" this type of device/operating system.

PALABRAS CLAVE

Android, Análisis forense digital, Artifacts, Android Debug Bridge, Android Virtual Device.

AGRADECIMIENTOS

En primer lugar, quisiera agradecer a mi tutora, María de los Llanos Tobarra Abad, no solo por su apoyo durante el desarrollo del presente trabajo, sino también, por su infinita paciencia a lo largo de la asignatura Análisis Forense. En segundo lugar, quisiera dar las gracias a mi esposa, María por su incondicional e incasable apoyo siempre presente. En tercer lugar, a mis padres María Isabel y José Antonio, que sin ellos nunca me habría embarcado en el mundo académico de la Ingeniería Informática. Y, por último, pero no por ello menos importante, a mis hermanos, Álvaro y David, con los que siempre he podido contar en los buenos, y malos momentos.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación y justificación

Los dispositivos electrónicos como teléfonos móviles, tablets o PCs se han convertido en un elemento esencial de nuestra vida, desde su empleo en el día a día para actividades de ocio, hasta su utilización como herramientas de un entorno laboral. Es tan alto el uso que hacemos de ellos, que una gran cantidad de puestos de trabajo no se concebirían si ellos.

Existen una amplia gama de estos dispositivos, desde dispositivos muy básicos dirigidos a pequeñas tareas de ofimática o llamadas de teléfono, hasta aquellos orientados a tareas más complejas, como el diseño gráfico, empleo de videojuegos…etc. Todos ellos forman parte de nuestra vida cotidiana y cada vez albergan más información personal, la cual, nos ha facilitado aspectos cotidianos de la vida, así como tareas en nuestro entorno de trabajo.

A pesar de las ventajas evidentes que nos han proporcionado los dispositivos electrónicos, como los smartphones, es importante recalcar que vivimos en una era de la información, nos encontramos en una interconexión entre dispositivos constante que como ocurre con todo gran invento, no siempre es empleado para fines lícitos.

No es ningún secreto que los dispositivos electrónicos son fuentes de múltiples ciberdelitos, desde el acceso no autorizado a un dispositivo de un tercero hasta delitos como ciberamenazas, estafas…etc. En este punto, un completo y adecuado análisis de toda la información relevante que esos dispositivos puedan contener se hace no fundamental, sino necesario para esclarecer estos delitos, que encuentran su herramienta en los sistemas de comunicación e información. Es en este punto donde entra al ruedo la importancia del Análisis forense digital.

El análisis forense digital, abarca una amplia amalgama de dispositivos y redes, sin embargo, este Trabajo Fin de Master, en adelante TFM, focalizará su estudio al análisis forense dirigido a los dispositivos móviles, y más concretamente a la plataforma Android.

El mundo es testigo de un cambio de los ordenadores personales a los smartphones. Según un informe de Ericsson, el número total de tráfico de datos alcanzará los 71 exabytes por mes en 2022 frente a los 8.8 exabytes en 2017, esto se debe en gran medida a la enorme demanda de smartphones. Estos teléfonos cada vez desplazan más el empleo de ordenadores personales, pues han pasado de un uso dedicado a las llamadas telefónicas desde cualquier lugar, a editar documentos, empleo de correo electrónico, acceso a Internet, empleo de GPS, así como permitir la gestión de tareas en un entorno laboral.

Como comenté en anteriores párrafos, los dispositivos electrónicos, y más concretamente los smartphones son auténticas fuentes de información personal: fotos con metadatos de localización,

conversaciones de aplicaciones chat, correo electrónico, incluso pueden almacenar un histórico de tus movimientos geográficos. Por todo esto, la adquisición de datos procedentes de un dispositivo móvil, se ha convertido en una evidencia con un valor incalculable, en investigaciones asociadas a casos criminales. En los tiempos que corren, es extraño que una investigación forense digital no afecte a un dispositivo móvil.

En concepto de ciberseguridad está alcanzando, una importancia crítica en el correcto desarrollo de una nación. Resulta muy común visualizar en las noticias la multitud de ataques que se efectúan en el marco de las tecnologías de la información. En este sentido hay dos pilares esenciales que sostienen una sólida seguridad en este ámbito: concienciación y formación.

Resulta fundamental contar con personal actualizado y formado que, en el marco del presente trabajo, posea un denso conocimiento en el ámbito del análisis forense digital. Este perfil debe extenderse no solo al evidente ámbito comercial, sino al policial/militar que garantice la seguridad de la nación.

Por otro lado, de nada sirve contar con unos grandes profesionales en el ámbito general de la ciberseguridad, sino se cuenta con un adecuado programa de concienciación para todos aquellos usuarios afectados por las tecnologías de la información. A fin de cuentas, en muchos aspectos, es el propio usuario habitual el principal vector de ataque.

A pesar de que en los párrafos anteriores he mencionado la ciberseguridad en un sentido amplio, destaco la rama del análisis forense digital y en concreto el focalizado en dispositivos móviles, los cuales, reforzando mis anteriores argumentos, constituyen en los tiempos que corren los dispositivos electrónicos, por delante de los PCs, más empleados en la conexión a Internet.

1.2 Objetivos

El análisis forense de dispositivos móviles es una rama del análisis forense digital. Dada la exponencial proliferación de dispositivos móviles y su, cade vez mayor, capacidad de almacenamiento de todo tipo de datos personales y del empleo de propio dispositivo, como los archivos *log*, las evidencias extraídas de los mismos se han convertido en un elemento esencial en cualquier tipo de incidente, desde los más livianos, hasta aquellos que cubre el código penal.

1.2.1 Objetivos Generales

Una formación sencilla y eficaz en proceso de análisis forense en dispositivos Android, constituye el foco fundamental del presente trabajo. Este proceso mantiene algunas similitudes con un análisis forense asociado a ordenadores personales, sin embargo, su constante actualización, las múltiples empresas fabricantes de los mismos y su portabilidad, así como las particularidades propias de los mismos, hace que sea un auténtico reto, el afrontar este tipo de análisis.

Como se explicará en sucesivos apartados, el análisis forense de dispositivos móviles conlleva una serie de pasos, desde el acceso al mismo, hasta la extracción y posterior análisis de las evidencias digitales, todo este proceso este asociado a una serie de herramientas, tanto gratuitas como de pago. El presente TFM buscará presentar una serie de casuísticas que permitan el análisis de diversos tipos de evidencias digitales asociadas a dispositivos móviles.

1.2.2 Objetivos Específicos

Para un adecuando entendimiento y familiarización con el proceso se análisis forense de dispositivos móviles, se va a conformar una estructura de talleres, los cuales permitirán ofrecer varias casuísticas, que permitirá al personal participante en los mismos vislumbrar la realidad y diversidad de abarca este tipo de análisis forense: centrado en la memoria interna del dispositivo, *artifacts* de aplicaciones móviles…etc.

El planeamiento y ejecución de estos talleres, constituye un objetivo en sí mismo, pues permitirá materializar todos los aspectos tóricos presentados a lo largo del estado del arte del presente trabajo.

1.3 Descripción del contenido del TFM

En el presente apartado, se va a efectuar una descripción resumida del contenido de los subsiguientes capítulos que conforman el presente trabajo:

- Capítulo 2. Estado del arte. Este apartado estará conformado por una serie de apartados, que comienzan con la evolución de la tecnología móvil, pasando por el concepto de análisis forense digital y móvil, la estructura Android y finalizando con una descripción de los principales *artifacts* en sistemas Android.
- Capítulo 3. Desarrollo el TFM. Este apartado muestra el levantamiento de un entorno de trabajo forense, así como la descripción de algunas herramientas de trabajo.
- Capítulo 4. Análisis de una tarjeta SD/almacenamiento interno. Apartado centrado en el primer taller del trabajo, focalizado en el análisis forense de la memoria interna o tarjeta SD de un dispositivo móvil.
- Capítulo 5. Empleo de herramientas *no root.* Este apartado busca la práctica con herramientas de análisis forense en entornos Android, sin requerir privilegios especiales sobre el dispositivo.
- Capítulo 6. Análisis de aplicaciones móviles. Se busca localizar, extraer y analizar los principales *artifacts* de algunas aplicaciones móviles.
- Capítulo 7. Conclusiones y líneas futuras. Se refleja el cumplimiento de los diferentes objetivos planteados, así como una serie de líneas de acción futuras.
- Capítulo 8. Bibliografía. Muestra las referencias documentales (libros, webs, artículos… etc) que a lo largo del trabajo se mencionan.

2 ESTADO DEL ARTE

2.1 Evolución de las tecnologías móviles y su aceptación social

Es evidente que los teléfonos móviles se han convertido en una parte esencial de nuestras vidas. Fue en 1983, cuando la empresa Motorola recibía la certificación procedente de la Federal Communications Commission (FCC), la cual suponía el punto de partida para la venta del Motorola DynaTAC 8000X [1] **,** ver Figura 2-1.

Figura 2-1 Motorola DynaTAC 8000X [1]

Desde el mismo inicio de su entrada en el mercado, la venta de estos dispositivos no ha dejado de crecer de manera exponencial. Tras casi 30 años desde el primer modelo comercial, el número de usuarios de los actuales smartphones alcanza los 7.000 millones, lo cual supone aproximadamente el 70% de la población mundial.

Según una investigación realizada por el Estudio General de Medios (EGM), el 92% de los usuarios de Internet accede a través de su dispositivo móvil, por encima tanto del portátil como del ordenador de sobremesa. Estos datos, junto con las cada vez mayores posibilidades que ofrece un dispositivo móvil: mensajería instantánea, todo tipo de trámites bancarios, compras online… etc, hacen que el ordenador personal pase a un segundo plano.

La razón de esta proliferación en los dispositivos móviles, se debe a la aparición de los llamados smartphones, que, según la Real Academia Española, se trata de terminales móviles que ofrecen servicios avanzados de comunicaciones (acceso a Internet y correo electrónico), así como servicios de agenda y organizador personal con un mayor grado de conectividad que un terminal convencional [2]

El primer Smartphone vio la luz el 15 de agosto de 1996, bautizado como Nokia 9000 Communicator, ver figura 2-2. Desde ese momento las posibilidades que ofrecía un dispositivo móvil fueron creciendo hasta al alcanzar las ya conocidas a día de hoy.

Figura 2-2 Nokia 9000 Communicator [16]

Las posibilidades que ofrece un Smartphones los han convertido en auténticos almacenes de información sensible, llegando a ser la propia información contenida, más valiosa que el propio dispositivo. Información que puede ir desde simples chats entre familiares, historiales de navegación, registros de localizaciones visitadas por el usuario… etc. En este punto es inevitable preguntarse cuan útil sería acceder a toda esta información en un caso de terrorismo o cualquier otro delito, ver figura 2-3.

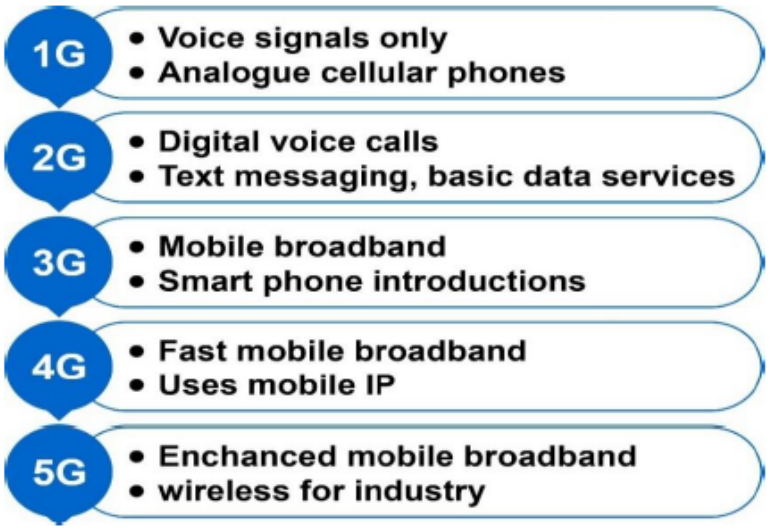


Figura 2-3 Evolución de las tecnologías de los dispositivos móviles

2.2 El análisis forense digital

En términos generales se puede definir la ciencia forense digital, como aquella, que se fundamenta en la identificación, preservación, análisis y presentación de datos almacenados en dispositivos electrónicos de una forma legal y aceptable [3], evitando cualquier intrusismo que los modifique.

Resulta importante resaltar, que esta disciplina, es aplicable tanto a investigaciones de delitos "tradicionales", tales como: homicidios, narcotráfico, terrorismo…etc. Como para aquellos directamente relacionados con las tecnologías de la información y comunicación, y en este ámbito, se incluirían tanto aquellos que afectan directamente a la conocida como tríada CIA: Confidencialidad, Integridad y Disponibilidad de la información o ciberdelitos en sentido estricto [4], como aquellos que emplean las TICs como medio para la comisión de delitos o ciberdelitos en sentido amplio [4].

En el marco del análisis forense digital, es posible distinguir seis fases que definen el proceso de análisis forense digital:

- Asegurar la escena (fotografías de los elementos, fotos del entorno, etc.).
- Identificación y recolección de evidencias.
- Preservación de evidencias (copias, cálculos de hashes, etc.).
- Documentar las evidencias (nº de series, marcas y modelos, lugar de la recolección de evidencias, fecha y hora, etc.).
- Análisis de las evidencias (Preparación del laboratorio forense, identificación de líneas temporales, evaluación de impactos, etc.).
- Redacción de informes (Ejecutivo, técnico).

Dentro del análisis forense digital, existen una multitud de tipologías basadas en distintos ámbitos, por un lado, encontramos el más evidente, en base al tipo de dispositivo en cuestión, como sería el basado en ordenadores, servidores, dispositivos móviles. Por otro lado, y muy en relación con el anterior, en base al sistema operativo que se monta, tanto centrados en ordenadores como Windows, Linux … etc, como en dispositivos móviles, tales como Android, Windows Phone, IOS, etc. Pero aparte de esta trivial clasificación, también existen tipologías de análisis forense digital centrado en el ámbito malware, de memoria RAM, sobre dispositivos de almacenamiento y especializados en la interconexión de redes.

Una evidencia electrónica o digital, es cualquier información almacenada o transmitida en forma digital, que cualquier parte en un proceso judicial puede emplear como prueba. El análisis forense digital está sustentado sobre evidencias digitales fundamentalmente, aunque también sobre evidencias de tipo físico, tales como fotografías del lugar de los hechos, de las conexiones de los dispositivos electrónicos implicados, sus periféricos, los propios dispositivos, …etc.

Debido al valor probatorio de las evidencias en los procesos legales, se debe aplicar un proceso determinado que permita garantizar su validez y admisión en un juicio. Aunque no se encuentra en ningún documento de referencia, es muy común afirmar que el principio que debe guiar cualquier procedimiento de obtención de evidencias es que, partiendo de la misma información, aplicando los pasos que se indiquen en el procedimiento, se deben obtener los mismos resultados.

Por todo lo anterior, resulta de gran importancia:

- Realizar, al menos, una copia de la información original.
- Tener mecanismos que permitan comprobar la integridad en cada paso.
- Documentar todos y cada uno de los pasos realizados para obtener la conclusión, con un nivel de detalle tal que se registren las herramientas empleadas, las versiones de las mismas y procedimientos específicos.

En España, el reconocimiento que se da a las evidencias digitales como fuentes de prueba, está recogido en la Ley de Enjuiciamiento Civil, artículos 299 a 386. A mayores la recogida, así como el tratamiento de evidencias digitales está recogido en la RFC 3227: "Directrices para la recopilación y

almacenamiento de evidencias digitales" [5] e ISO/IEC 27037:2016. Directrices para la identificación, recogida, adquisición y preservación de evidencias digitales [6].

2.3 El análisis forense en dispositivos móviles

La ciencia forense digital centrada en dispositivos móviles o mobile forensics, busca la extracción segura y análisis de evidencias almacenadas en este tipo de dispositivos. Está construida sobre tres pilares: acceso, extracción y análisis.

Los móviles son auténticas antenas portátiles, permiten la conexión mediante redes wifi, bluetooth… esto supone un auténtico reto para poder acometer un "sencillo" acceso a los dispositivos, pues existen todo tipo de aplicaciones que, a través, por ejemplo, de la red de datos GSM se puede hacer un borrado de todo el contenido del dispositivo. Por todo ello, es fundamental tratar de desconectarlo de cualquier tipo de red, así como introducir el dispositivo en una bolsa de Faraday, que evite que las antenas de los dispositivos interaccionen con cualquier tipo de red.

La adquisición de las evidencias responde a múltiples métodos, y es muy importante el adiestramiento constante no en un único método, pues al igual que ocurre con otras ramas forenses digitales, como la de los ordenadores, puede que un método sea únicamente válido para un solo tipo de evidencia, pero el analista debe tener la capacidad de adaptar el método a la situación.

Aunque el estudio y adiestramiento constante es un denominador común en cualquier analista forense digital, cobra un protagonismo especial en el caso de los dispositivos móviles. El rápido incremento en sus distintos tipos, fabricantes, así como sistemas operativos que montan, hacen de este tipo de análisis forense un auténtico reto, que requiere de una constante preparación y actualización para abordarlo.

2.3.1 La odisea del análisis forense en dispositivos móviles

Las evidencias digitales representan un reto en si para su adquisición y análisis como consecuencia de su volatilidad y sencillez de acceso, todo esto permite que los datos puedan ser borrados o modificados con sencillez por el propio dueño del dispositivo o sincronizarse con otros dispositivos que permitan la modificación de evidencias [7].

Entre las bases que hacen del análisis forense un auténtico "calvario" para el analista destacan:

- *Tipologías hardware*; los múltiples modelos a los que se debe enfrentar el analista son cada vez mayores, lo cual deriva en una constante necesidad de adaptación a los cambios que día a día definen la estructura hardware de un dispositivo móvil.
- *Balance de los sistemas operativos*; Resulta sencillo entender la supremacía de Windows sobre el resto de sistemas operativos, sin embargo, en el caso de los dispositivos móviles la variedad es mucho mayor, desde el famoso IOS de Apple, pasando por el Android de Google, el Microsoft Mobile SO… etc. A pesar de la mencionada variedad, la multitud de versiones que los soportan hace que dentro un mismo sistema operativo no sea trivial tratar dos versiones de un mismo SO.
- *Modificación de evidencias*; Como se comentó con anterioridad, resulta necesario evitar en la medida de lo posible cualquier modificación de las evidencias digitales al tratar de extraerlas, siendo especialmente complejo en el caso de dispositivos móviles.
- *Antiforense*; cada vez son más comunes estas técnicas que ocultan, ofuscan y bloquean información esencial en un análisis.
- *Contraseñas*; la dificultad de extracción se incrementa en este tipo de dispositivos si no se dispone de la contraseña de acceso, en cuyo caso se deben emplear técnicas de bypass que no siempre son efectivas.

- *Herramientas específicas*; la variedad en sí que envuelve el hardware y software de los dispositivos móviles obliga a que el analista disponga de una amplia variedad de medios.
- *La alterabilidad de los datos*; como se comentó en anteriores párrafos, uno de los aspectos que más caracteriza a las evidencias digitales es la sencillez en su modificación.
- *Mecanismos de reseteo*; resulta muy simple poner el teléfono en "valores de fábrica", su sencillez puede resultar en una puesta por error, lo cual inhabilitará cuasi por completo los datos contenidos.
- *Conectividad*; como ya se ha mencionado, las redes a las que tiene acceso un dispositivo móvil cubren desde la propia red móvil de comunicación móvil o GSM, pasando por WI-FI, bluetooth … etc. desde estas es posible modificar diversos aspectos del dispositivo, por ello es fundamental cortar con cualquier modificación con el exterior.
- *Aspectos legales*; debido a su habitual uso, resulta muy probable que un dispositivo móvil esté involucrado en algún tipo de crimen, que a veces, sobrepasan los límites geográficos de una nación, por ello, los analistas forenses especialistas en estos dispositivos deben ser conocedores del crimen en cuestión y estar familiarizados con el marco legal que lo envuelve.

2.3.2 El proceso de análisis forense en dispositivos móviles

A pesar de que cada dispositivo móvil dispone de características particulares, que hacen única la tarea del analista forense en este campo, es posible sistematizar el análisis forense en dispositivos móviles en cinco hitos: Preparación, acceso, adquisición, análisis y emisión de informes [8].

2.3.2.1 Preparación

Constituye el inicio de cualquier análisis forense digital. Una vez que se dispone del conocimiento necesario sobre las necesidades sobre el análisis forense del dispositivo, se debe organizar la totalidad de formatos que deben ser rellenados, como es el caso de la cadena de custodia, información y estudio del dispositivo, así como una preparación específica del laboratorio forense que se va a emplear.

2.3.2.2 Acceso

Resulta fundamental, desde el momento en el que tenemos acceso al móvil, evitar cualquier tipo de acción que pueda dañar o modificar los datos contenidos en el dispositivo, es por ello, que resulta muy recomendable transportar el dispositivo empleando bolsas que eviten el impacto de la electricidad estática.

A pesar de todo el nivel de cuidado que se debe tener, es importante explotar cualquier oportunidad que tengamos para facilitarnos el acceso a los datos contenidos en el aparato, entre dichas oportunidades cabe mencionar algunas de ellas:

- Resulta muy común que el dispositivo tenga habilitado el bloqueo de pantalla, por ello, en caso de que sea posible, es aconsejable deshabilitar esta opción.
- Si es posible, modificar las opciones de configuración del dispositivo para permitir accesos con mayores privilegios.
- Muchos dispositivos móviles, incluidos los sistemas Android, disponen de una opción que permite editar el tiempo que el teléfono permanece desbloqueado, modificando esta opción podemos evitar que se bloquee y así evitar la dificultad añadida que implica una extracción sobre un dispositivo en esas condiciones.

Se mencionó anteriormente, que un dispositivo móvil cuenta con varias opciones de acceso a redes inalámbricas, lo cual puede derivar en un bloqueo o borrado remoto, es por ello que, siempre que sea posible, el dispositivo debe ser aislado de cualquier red externa. Un método sería poner el teléfono en modo avión, lo cual no es eficaz para todo tipo de dispositivos, a mayores el teléfono puede ser transportado en una bolsa de Faraday, lo cual bloquea cualquier señal desde o hacia el dispositivo.

2.3.2.3 Adquisición

El método de extracción de datos procedentes de un dispositivo móvil, depende íntimamente del sistema operativo que monte el teléfono, así como el modelo del dispositivo, entre los tipos de adquisición de datos, destaca:

- La adquisición manual: resulta el método más trivial. Se basa en el propio empleo del interfaz de usuario del dispositivo para acceder a la información. Como es evidente, únicamente se podrá acceder a aquellos datos que estén visibles para el usuario, a parte, se trata de un método susceptible de modificar los datos.
- Adquisición lógica: Hace referencia a la extracción de archivos procedentes de un sistema de ficheros. Esta metodología permite la obtención de archivos tales como: registro de llamadas, teléfonos de contactos, localizaciones GPS, historial de navegación, información de aplicaciones de red (Skype, Facebook, etc.), historial de navegación, etc.
- Adquisición de sistemas de ficheros: se trata de un proceso lógico, y se basa en la extracción de la totalidad de un sistema de ficheros.
- Adquisición física: Consiste en realizar una copia bit a bit de un dispositivo de almacenamiento, al igual que en una imagen de un disco duro.

2.3.2.4 Análisis

Durante la fase de análisis, al igual que en el resto de etapas, resulta muy habitual y conveniente el empleo de diversas herramientas, no existe una única herramienta a emplear en todas las casuísticas, pues unas serán más recomendables para un tipo de datos en concreto o para un tipo de presentación, pero puede que obvien parte de los datos relevantes, los cuales deban ser cubiertos con otras herramientas.

Junto con la amalgama de herramientas con las que debe estar familiarizado el analista, debe completarse con un detallado conocimiento de los distintos tipos de datos que se le presenten, así como sus formas de presentación y orden, como los sistemas de ficheros asociados a distintos sistemas operativos.

2.3.2.5 Emisión de informes

De nada sirve un estricto transporte del dispositivo móvil, una cuidadosa extracción de datos y un detallado análisis, si no se documentan todos y cada uno de los pasos seguidos. El proceso de registrar las acciones llevadas a cabo debe comenzar desde el momento inicial. Algunos datos que es fundamental que permanezcan bien documentados son:

- La fecha y hora de inicio del proceso de análisis.
- El estado del móvil.
- La situación del teléfono cuando se adquirió.
- Marca, modelo, sistema operativo, versión del sistema operativo, etc.
- Toma de fotos del teléfono y sus componentes.
- Descripción de las herramientas empleadas durante el proceso de análisis forense, así como sus versiones.

La base de un buen informe forense digital, es preguntarse si otro analista sería capaz de reproducir todos y cada uno de los pasos descritos en el informe, obteniendo por lo tanto los mismos resultados.

Los datos obtenidos del teléfono deben ser adecuadamente presentados a los destinatarios, de cara a poder ser analizados a través de diferentes sistemas software en un futuro. A parte de una correcta presentación de los datos, fotos del estado de los datos en el teléfono son muy recomendables, lo cual hará del informe visualmente convincente.

2.4 Los sistemas Android

2.4.1 La evolución de los sistemas Android

Android es un sistema operativo para móviles basado en Linux, desarrollado por una aglomeración de compañías que forman el Open Handset Alliance (OHA). Desde sus inicios, ha experimentado una enorme evolución, desde septiembre de 2008, mes en el que vio la luz Android 1.0, hasta septiembre de 2021 con Android 12, última versión del sistema operativo hasta la fecha.

NOMBRE	VERSIÓN	FECHA DE LANZAMIENTO
APPLE PIE	1.0	SEP-2008
BANANA BREAD	1.1	FEB-2009
CUPCAKE	1.5	ABR-2009
DONUT	1.6	SEP-2009
ECLAIR	2.0-2.1	OCT-2009
FROYO	2.2-2.2.3	MAY-2010
GINGERBREAD	2.3-2.3.7	DIC-2010
HONEYCOMB	3.0-3.2.6	FEB-2011
ICE CREAM SANDWICH	4.0-4.0.5	OCT-2011
JELLY BEAN	4.1-4.3.1	JUL-2012
KITKAT	4.4-4.4.4	OCT-2013
LOLLIPOP	5.0-5.1.1	NOV-2014
MARSHMALLOW	6.0-6.0.1	OCT-2015
NOUGAT	7.0-7.1.2	JUN-2016
OREO	8.0-8.1	AGO-2017
PIE	9.0	AGO-2018
ANDROID 10	10.0	SEP-2019
ANDROID 11	11.0	SEP-2020
ANDROID 12	12.0	SEP-2021

Tabla 2-1 Versiones sistema operativo Android

Las constantes actualizaciones de versiones, ver tabla 2-1, que ha sufrido este sistema operativo, tienen un evidente impacto en las metodologías forenses aplicadas sobre ellas. Un claro ejemplo del impacto directamente relacionado con la evolución de Android, es el mecanismo de encriptación del disco duro o sus siglas en inglés FDE (Full Disk Encryption), lo cual permite el almacenamiento de

datos encriptados en el dispositivo. Las primeras versiones de Android, carecían de esta funcionalidad, facilitando la extracción de información por parte de los analistas.

El mecanismo FDE, no ha sido el único impacto en la ciencia forense digital dirigida a dispositivos móviles, con el tiempo y como consecuencia de una creciente mayor demanda de seguridad, han surgido funcionalidades tales como: kernel seguro, permisos sobre aplicaciones, entornos seguros de ejecución … etc. Todos ellos dirigidos a mejorar la seguridad de los dispositivos, en pos de una mayor tranquilidad para el usuario, pero dificultando las tareas de extracción y análisis de los datos contenidos en los dispositivos móviles.

2.4.2 Arquitectura de los dispositivos Android

Resulta fundamental, previo a entrar en materia forense, entender la estructura que conforma el sistema operativo Android, a mayores se entra en cierto detalle sobre las diferentes "capas" que lo definen.

Android, al igual que cualquier sistema operativo, constituye un software de enlace y gestión entre el usuario y el hardware, un medio a través del cual las aplicaciones hacen uso del "físico" del dispositivo. Este SO está dirigido a dispositivos móviles y tablets, permitiendo la gestión de su memoria, así como de los diversos procesos que ejecutan las tareas, asegura los aspectos de seguridad y se ocupa de incidencias en la red.

Es importante resaltar, que se trata de un software de código abierto o *open source,* lo cual implica que los fabricantes de dispositivos pueden acceder libremente a su Código Fuente, y modificarlo a su antojo, en base a las necesidades que se considere que cubra el dispositivo, lo cual tiene un fuerte impacto en la diversidad intrínseca asociada a los distintos modelos de dispositivos móviles.

El Sistema Operativo Android, está constituido por una serie de capas o *layers*, ver figura 2-4, ejecutándose una sobre otra. De cara a entender el ecosistema Android, es importante tener unas nociones básicas de cada capa y los cometidos de los que se responsabilizan [9].

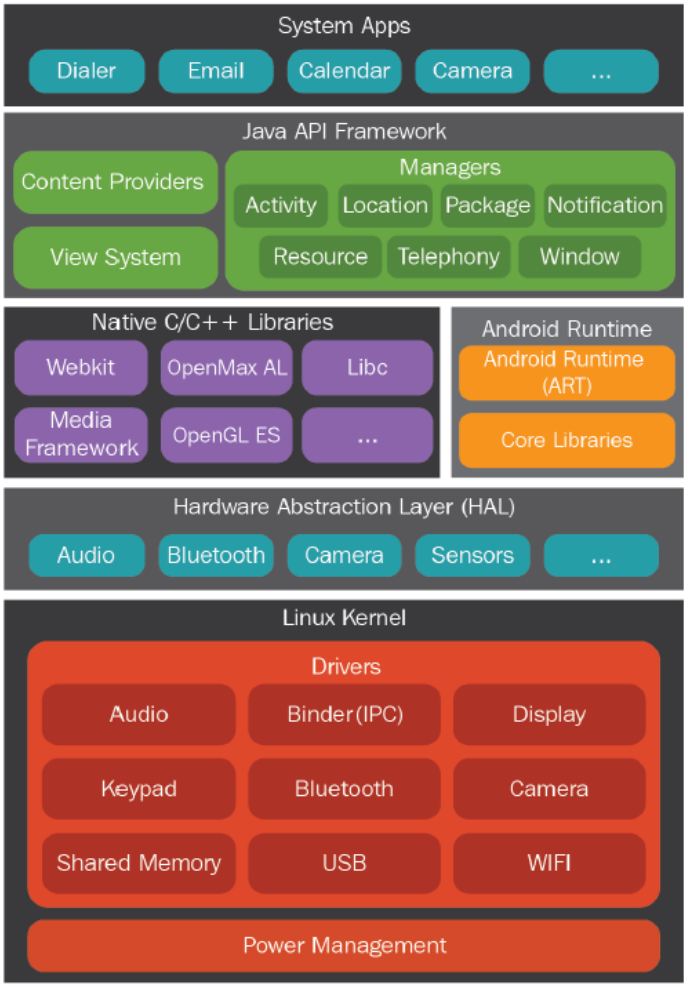


Figura 2-4 Capas del SO Android [7]

2.4.2.1 El Kernel

Como ocurre con cualquier Sistema operativo, el elemento más próximo, y que sirve como capa de abstracción entre el hardware del dispositivo, y el software, es el kernel o núcleo. En el caso del SO Android, está implementado sobre un kernel Linux.

Linux, es una plataforma portable, la cual puede ser compilada en múltiples tipos de hardware, de ahí la elección como núcleo de Android. El kernel contiene una serie software, conocidos como drivers, que permiten el control del hardware que subyace bajo él. Entre los drivers, destacan los relacionados con el WI-FI, audio, Bluetooth, Servicio de Bus Universal, etc.

2.4.2.2 Capa de Abstracción Hardware

La capa de abstracción hardware, o sus siglas en ingles HAL (Hardware Abstraction Level), está constituida por una serie de bibliotecas, las cuales conforman interfaces para un específico tipo de componente hardware, permitiendo al nivel más alto, la capa java API framework, trabajar con el hardware del dispositivo gracias a esas interfaces.

Gracias a esta capa, los fabricantes de hardware, pueden implementar diversas funcionalidades evitando realizar cambios en la capa más alta del Sistema operativo.

2.4.2.3 Bibliotecas nativas C/C++

El siguiente nivel del Sistema operativo Android, consiste en una serie de bibliotecas escritas en lenguaje C/C++, las cuales van a permitir a los dispositivos móviles manejar diversos tipos de datos. Entre las diversas bibliotecas, destaca la llamada biblioteca *media framework*, que constituye la principal interface que provee de servicios a las otras capas subyacentes. La biblioteca WebKit, provee de páginas web en los buscadores web, y la librería *Surface Manager* mantiene los gráficos.

2.4.2.4 Dalvik

Para entender el presente nivel, es importante desdoblarlo en dos apartados, en el primero se explicarán los fundamentos de la máquina virtual Dalvik.

Toda aplicación instalada en Android está escrita en lenguaje Java, cuando es compilado, se obtiene el conocido como bytecode, la máquina virtual Java permite hacer correr dicho bytecode, sin embargo, versiones anteriores al Android 5.0, hacían uso de la, ya mencionada, máquina virtual Dalvik, o sus siglas en inglés DVM, ver figura 2-5.

DVM permite correr bytecode java, el cual ha sido convertido con anterioridad a bytecode Dalvik, a través del compilador Dalvik.

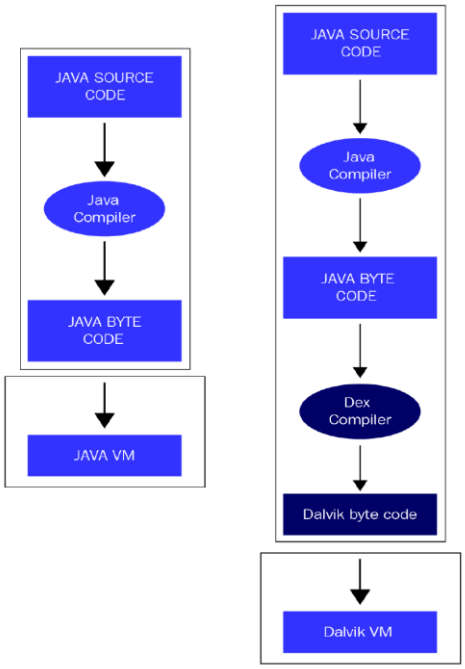


Figura 2-5 Comparativa JVM - DVM

DVM hace uso de compilación en tiempo de ejecución, lo cual traía ciertas mejoras de rendimiento, pues es muy apropiado en dispositivos con poca capacidad de almacenamiento, sin embargo, es más lento, puesto que la compilación se hace tras la instalación.

2.4.2.5 Android Run Time

Posteriormente a la versión 5 de Android, Dalvik fue desplazado por *Android Run Time*, o sus siglas en inglés ART. Entre las características que lo diferencian de DVM, destacan:

- Compilación anticipada, la cual permite compilar una aplicación en tiempo de instalación, y no en tiempo de ejecución, que implica mejoras en el rendimiento, pero requiere un mayor espacio de almacenamiento.
- Mejoras en el recolector de basuras.

- Mejoras en el desarrollo y depuración de aplicaciones, mediante mensajes más detallados.

2.4.2.6 Java API Framework

Esta capa es la responsable de manejar las funciones básicas del dispositivo móvil. Este es el nivel sobre el que las aplicaciones instaladas interactúan directamente con el dispositivo. Está dividido en una serie de bloques, entre los que destacan:

- Gestor de telefonía. Gestiona todas las llamadas de voz.
- Proveedor de contenido. Dirige la compartición de datos entre aplicaciones.
- Gestor de recursos. Gestiona diversos recursos empleados por las aplicaciones.

2.4.2.7 Capa de aplicación

Constituye el nivel que contiene los programas con los que el usuario interactúa con el dispositivo móvil.

Por un lado, existen las llamadas aplicaciones de sistema, las cuales consisten en una serie de programas preinstalados en el dispositivo, tales como: navegador por defecto, cliente de correo … etc. No pueden ser desinstaladas o modificadas por el usuario, puesto que son de solo lectura.

Por otro lado, el usuario puede instalar aplicaciones haciendo uso de plataformas de distribución, tales como Google Play.

2.4.3 Sistemas de ficheros en Android

Un sistema de ficheros constituye la forma de almacenamiento de un dispositivo de memoria, el cual estructura y organiza la escritura, lectura, búsqueda, almacenamiento y borrado de archivos de una manera concreta.

Resulta esencial desde el punto de vista forense comprender los distintos tipos de sistemas de ficheros que abarca Android, lo cual ayudará al analista a obtener conocimiento de como los datos son almacenados y recuperados. Cada sistema de ficheros, define las reglas de gestión de los archivos del volumen, como, por ejemplo, velocidad de recuperación de datos, tamaño de archivos, seguridad…etc.

Los sistemas Linux, y por lo tanto Android, admiten numerosas tipologías de sistemas de ficheros. A diferencia de los sistemas Windows, en Linux los accesos no se hacen por nombres de unidades o *drives,* sino que existe una única jerarquía en árbol, la cual representa el sistema de ficheros como una entidad, cada nuevo sistema de ficheros añadido se monta en este árbol, ver figura 2-6.

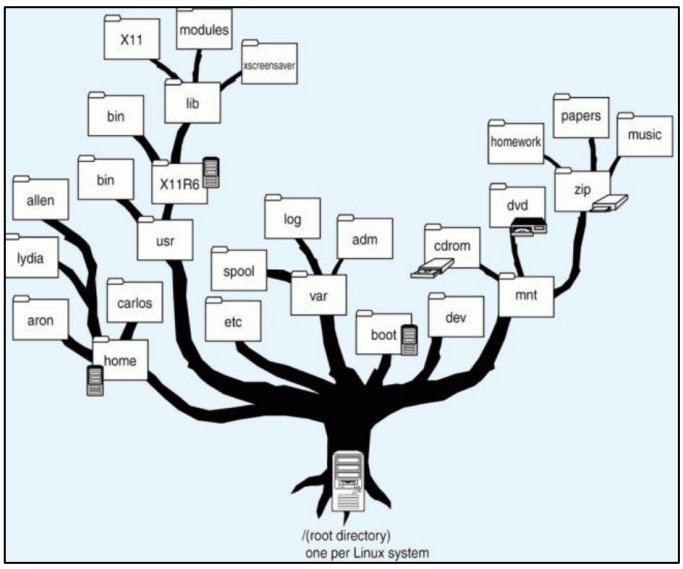


Figura 2-6 Sistema de ficheros en Linux [8]

Independientemente que se trate de un volumen que proceda de un sistema de almacenamiento local o externo, todos son integrados en un gran sistema de ficheros, el cual comienza en root ("/").

A continuación, se indican los principales sistemas de ficheros, disponibles en sistemas Android, ver tabla 2-3:

ExFAT	**Sistema de ficheros optimizado para memorias flash, no forma parte del kernel estándar de Linux.**
F2FS	**Sistema de ficheros de código abierto introducido por Samsung. Tiene en cuenta las características de las memorias flash NAND.**
JFFS2	**Se trata de un sistema de ficheros basado en una estructura de registros, para el empleo en memorias flash. Se trata del sistema de ficheros por defecto de memorias flash para *Android Open Source Project (ASOP)* desde la versión *Ice Cream Sandwich.***
YAFFS2	**Sistema de ficheros de código abierto de un solo subproceso, basado en una estructura de registros y lanzado en 2002. Diseñado para permitir rápidos accesos en memorias flash NAND. Presenta problemas en adquisiciones forenses debido al empleo del sistema de gestión *out of band*.**
RFS	**Admite memorias flash NAND en dispositivos Samsung. Puede resumirse como un sistema de ficheros FAT16 donde el *journaling* está habilitado a través de un registro de transacciones.**
EXT2/EXT3/EXT4	**Sistemas de ficheros extendidos (EXTended filesystem), surgen en 1992, dirigidos al kernel de Linux. El Journaling o registro diario, es la principal ventaja de EXT3 sobre EXT3. EXT4 gano gran preponderancia debido a su empleo en dispositivos móviles que implementaban procesadores dual-core, para los cuales el sistema de ficheros YAFFS2 presentaba un cuello de botella.**
FAT/VFAT	**De las siglas en ingles File Allocation Table y Virtual File Allocation Table. FAT 12, 16 Y 32, son compatibles con los controladores MSDOS. VFAT es una extensión de FAT32.** **FAT32 es compatible con la mayoría de los dispositivos Android. Muchas de las tarjetas SD están formateadas empleado este sistema de ficheros.**

Tabla 2-3 Sistemas de ficheros dispositivos Android

La anterior tabla recoge los principales sistemas de ficheros conocidos como: *flash-mermory filesystem* y *media-based fylesystems.* Sin embargo, no son los únicos sistemas de "ordenamiento" de archivos en dispositivos Android. Junto con los anteriores surgen otros conocidos como *pseudo*

filesystems, los cuales hacen referencia a "agrupaciones lógicas de archivos". A continuación, se indican los principales representantes de este tipo de sistemas de ficheros, ver tabla 2-4.

CGROUP	Permite una manera de acceder y definir ciertos parámetros del Kernel.
ROOTFL	Este sistema de ficheros, constituye uno de los principales componentes del sistema Android. Contiene toda la información necesaria para iniciar el dispositivo. Este sistema de ficheros está montado en "/" (carpeta root), por ende, sobre este sistema de ficheros se montan todos los demás.
PROCFS	Proporciona información detalladas acerca del Kernel, procesos y parámetros de configuración.
SYSFS	Almacena información sobre la configuración del dispositivo. Se encuentra montado en la carpeta /sys. Aunque a priori puede no considerase información de interés desde un punto de vista forense, lo cierto es que, puede permitir verificar la integridad de una evidencia digital.
TMPFS	Constituye un almacén temporal en el dispositivo, el cual almacena los archivos en la RAM. Suele estar montado en el directorio /dev.

Tabla 2-4 Pseudo Sistemas de Ficheros Android

2.4.4 Artifacs de los sistemas Androids

Una vez conocida la arquitectura de un sistema Android, así como las distintas tipologías de sistemas de ficheros, las cuales definen el cómo de la organización de la información, es fundamental conocer, que puede ser útil desde un punto de vista forense.

Toda acción realizada por un usuario siempre deja huellas, registro de llamadas, detalles de localización, historial de navegación… etc [10]. En terminología forense, se define *artifacs* como aquellos objetos que contienen datos y evidencias de que "algo ha sucedido" en el sistema, registran y almacenan diferentes eventos que ha realizado el sistema operativo, en resumen, componentes que ofrece un sistema y en los cuales reside información, que demuestra el paso del usuario.

Previo a entrar en detalles acerca de los principales artifacts de los sistemas Android, es fundamental comprender la estructura de particiones, así como los principales directorios que subyacen en los sistemas Android.

2.4.4.1 Particiones en sistemas Android

Una partición, es una unidad de almacenamiento lógico localizada en una sola unidad física de almacenamiento de datos. Permiten dividir el espacio de almacenamiento en secciones, las cuales pueden ser accedidas de manera independiente.

Aunque las particiones presentes en un sistema Android, pueden variar entre versiones y proveedores, algunas particiones están presentes en todos los sistemas Android, a continuación, se nombran las de mayor interés, ver tabla 2-5:

BOOT	Contiene la información necesaria para que el dispositivo pueda iniciarse.
CACHE	Contiene información a la que se ha accedido frecuentemente, así como registros de recuperación.
RECOVERY	Permite iniciar el dispositivo en modo recuperación, en el cual pueden realizarse acciones tales como: actualizaciones del dispositivo y operaciones de mantenimiento.
SYSTEM	Contiene el *Android framework*[1] , bibliotecas, archivos binarios del sistema, así como aplicaciones preinstaladas.
USERDATA	Constituye el almacenamiento interno del dispositivo para los datos de las aplicaciones. Contiene mucha información de interés forense. Almacena todos los datos de las aplicaciones instaladas.

Tabla 2-5 Principales particiones de sistemas Android

2.4.4.2 Directorios de interés

Comprender como Android organiza sus datos en archivos y carpetas, resulta fundamental para acometer un adecuado análisis forense. La jerarquía de archivos en los sistemas Android es muy similar a la de los sistemas Linux. En Linux, la jerarquía de archivos puede ser vista como un árbol, en el cual su punto más alto es llamado root, representado por el símbolo "/".

Con independencia de que se hable de un sistema de ficheros local o remoto, se encontrará siempre presente bajo root. La jerarquía de archivos en los sistemas Android es una versión personalizada de la existente en los sistemas Linux, puede cambiar en base al fabricante y a la versión Linux subyacente.

A continuación, se indicarán los principales directorios presentes en los sistemas Android, ver tabla 2-6, no se debe olvidar que un acceso completo a todos ellos, está supeditado a disponer de permisos root, o lo que es lo mismo acceso con máximos privilegios sobre el sistema.

/ACCT	Punto de montaje del grupo de control acct.

[1] Conjunto de API que permite a los desarrolladores escribir rápida y fácilmente aplicaciones para dispositivos Android.

	Proporciona la contabilización de los usuarios.
/CACHE	Se almacenan los datos a los que se accedido frecuentemente. Contiene información de interés desde un punto de vista forense, tal como: historial del navegador, imágenes y otros datos de aplicaciones.
/CONFIG	Contiene los archivos de configuración de SDCardFS[2], así como gadget USB.
/DATA/DATA	La mayor parte de la información perteneciente al usuario se almacena en esta carpeta. Contiene información de todas las aplicaciones. Tiene una especial importancia desde un punto de vista forense.
/DEV	Contiene archivos especiales asociados a todos los dispositivos. Punto de montaje para el sistema de ficheros tempfs.
/MNT	Punto de montaje de todos los sistemas de ficheros, así como tarjetas SD internas y externas.
/PROC	Permite el acceso a estructuras de datos del Kernel, es el punto de montaje del sistema de ficheros procfs.
/SBIN	Contiene archivos binarios de múltiples *demonios*[3]
/STORAGE	Contiene información acerca del contenido de tarjetas SD, así como almacenamiento interno del dispositivo. Cualquier aplicación con el permiso de escritura sobre almacenamiento externo, generará archivos en este directorio. Entre las carpetas que contiene, destaca Digital Camera Images, el cual es el directorio por defecto de las cámaras de los dispositivos móviles, en el cual se pueden encontrar: fotos, videos tomados por la cámara.
/SYSTEM	Almacena bibliotecas, binarios del sistema, así como otros archivos de sistema. Además, aquellas aplicaciones preinstaladas en el dispositivo también se encuentran en este directorio.

Tabla 2-6 Principales directorios en sistemas Android

[2] Capa de emulación FAT32 que forma parte directamente del kernel.
[3] Proceso que se ejecuta en segundo plano en lugar de ser controlado por el usuario.

2.4.4.3 Aplicaciones Android

Junto con la información que subyace en los principales directorios de los sistemas Android, resulta de vital interés toda la información asociada a las aplicaciones instaladas en el dispositivo. Como se mencionó con anterioridad, las aplicaciones pueden clasificarse en: aplicaciones de sistema, y aplicaciones instaladas por el usuario.

Dado el carácter personal que lleva impresa una aplicación, los datos almacenados por la misma contienen una cantidad muy valiosa de información forense. Entre la información asociada a este tipo de datos destacan: mensajes de texto y chat, emails, fotografías, vídeos, historial de navegación, datos asociados a aplicaciones instaladas, etc.

Los datos pertenecientes a las aplicaciones pueden ser almacenados tanto en elementos externos e internos. En el caso de dispositivos de almacenamiento externo, tales como tarjetas SD[4], la información puede ser contenida en cualquier localización. Sin embargo, en lo relativo al almacenamiento interno del dispositivo, el directorio está predefinido, concretamente en /data/data, seguido por el nombre del paquete asociado a la aplicación. Por ejemplo, los datos asociados a la aplicación se encuentran en */data/data/com.whatsapp*.

Los datos relativos a las distintas aplicaciones instaladas en un dispositivo Android, pueden almacenarse en las siguientes localizaciones, ver tabla 2-7:

Preferencias compartidas	proporcionan un marco para almacenar pares clave-valor de tipos de datos primitivos en formato XML. Los diversos archivos XML pueden contener informaciones muy útiles durante un análisis forense, tal como nombres de cuentas o contraseñas.
Almacenamiento interno	Localizados en el directorio /data/data. Los datos almacenados aquí son privados y no pueden ser accedidos por otras aplicaciones. Incluso el propietario del dispositivo no puede ver los archivos, a menos que disponga de máximos privilegios. Los paquetes asociados a las distintas aplicaciones, con tienen una serie de carpetas, entre las que destaca la carpeta *bases de datos*, la cual contine información de gran valor forense.
Almacenamiento externo	Los dispositivos de almacenamiento externo no tienen un nivel de seguridad tan elevado como el interno, de hecho, los datos almacenados aquí son públicos, de tal forma que otras aplicaciones, con los adecuados permisos, pueden acceder a ellos.
Red	La red puede ser una gran fuente de información en términos generales en el ámbito digital, y en especial para dispositivos móviles, cuya conexión

[4] Secure Digital

	a la red es constante.

Tabla 2-7 Tipología de almacenamiento de los datos de aplicaciones

2.4.4.4 Principales Artifacs

La profundidad del análisis forense sobre dispositivos Android, va a depender de la capacidad de acceso sobre el dispositivo. Existen dos tipos de usuarios: con privilegios o *rooted* y sin privilegios o *non-rooted.* Por defecto, los sistemas operativos Android no permiten una escalada de privilegios a los usuarios, por lo que un usuario habitual será *non-rooted.*

Para un análisis completo se requiere un profundo acceso y recuperación de los diferentes *artifacs*. Los accesos root, permiten un acceso completo al sistema de particiones. El sistema de particiones almacena la totalidad de los datos relativa al usuario, aplicaciones, así como el sistema de ficheros de cada partición.

Como se ha definido anteriormente, los *artifacts* constituyen las trazas o huellas dejadas por un usuario de forma inconsciente o accidental, esto constituye información muy valiosa en un posible procedimiento judicial.

Los *artifacs,*ver tablas 2-8 y 2-9 ,van a variar en función de la marca, modelo, así como de la versión del sistema operativo, y junto con lo anterior, en función a si se trata de un móvil básico o *feature phone*[5], o un smartphone.

Se trata de información muy sensible, cualquier pequeña acción sobre ellos, puede modificar significativamente los datos contenidos, por ello es fundamental una cuidadosa adquisición del dispositivo, así como un metódico acceso a la información contenida.

TIPOLOGÍA	ARTIFACT
HARDWARE	MARCA, MODELO, NÚMERO IMEI, NÚMERO DE SERIE.
GENERADO POR EL USUARIO	LISTA DE CONTACTOS, SMS, MMS (enviados, recibidos, en borrador y borrados), CALENDARIO Y NOTAS.
GENERADOS POR EL DISPOSITIVO	REGISTRO DE LLAMADAS

Tabla 2-8 *Artifacs* que pueden ser extraídos de un dispositivo básico.

TIPOLOGÍA	ARTIFACTS
HARDWARE	MARCA, MODELO, NÚMERO IMEI, NÚMERO DE SERIE.
GENERADO POR EL USUARIO	LISTA DE CONTACTOS, SMS, MMS (enviados, recibidos, en borrador y borrados), CALENDARIO, NOTAS, FOTOS, VÍDEOS, MAPAS Y GRABACIONES.

[5] Teléfonos móviles que únicamente permiten funciones fundamentales, como llamar, o enviar y recibir mensajes.

GENERADOS POR EL DISPOSITIVO	REGISTRO DE LLAMADAS
INTERNET	CUENTAS ONLINE, HISTORIAL DE NAVEGACIÓN, EMAILS…
APLICACIONES INSTALADAS	REGISTROS DE CHAT, APLICACIONES DUALES…

Tabla 2-9 *Artifacs* que pueden ser extraídos de un smartphone.

A continuación, se va a efectuar un recorrido por principales ficheros y directorios que representan algunos de los principales *artifacs* de dispositivos Android, ver tabla 2-10:

CONTACTOS	localizados en el archivo *contacts2.db* en el directorio */data/data/com.android.providers.contacts/databases*
HISTORIAL DE LLAMADAS	Toda información relacionada con llamadas entrantes, salientes y perdidas, puede ser localizado en el archivo *calllog.db* en el directorio */data/data/com.Android.providers.contacts/databases*
SIM[6]	Información relacionada con la tarjeta SIM, tal como el ICCID[7], número de teléfono y el MCC[8]/MNC[9], estos últimos permiten identificar el operador de la red, puede ser localizada en el archivo *telephony.db*, en el directorio */data/data/com.android.providers.telephony/databases*
SMS[10]/MMS[11]	Información asociada a mensajes de texto puede ser encontrada en el archivo *mmssms.db*, en el directorio */data/data/com.Android.providers.telephony/databases*
DESCARGAS DE INTERNET	Información asociada a las descargas de archivos desde Internet, puede ser localizada en el archivo *downloads.db*¸en el directorio */data/data/com.android.providers.downloads/databases*
WHATSAPP	Información asociada a los contactos WhatsApp puede localizarse en el archivo *wa.db*, la información asociada a mensajes en el archivo *msgstore.db*, ambos en el directorio */data/data/com.whatsapp/databases*
FACEBOOK	Información relacionada con el perfil de usuario, puede ser localizada en el archivo de base de datos *pref_db*, la relacionada con los amigos del usuario en el archivo

[6] Subscriber Identity Module.
[7] Integrated Circuit Card Identifier: número de serie único que tiene cada tarjeta SIM.
[8] Mobile Country Code
[9] Mobile Network Code
[10] Short Message Service
[11] Multimedia Message Service

	contacts_db2, y la asociada a mensajes de Facebook en *threads_db2*. Todos ellos en el directorio */data/data/com.facebook.katana/databases*

Tabla 2-10 Principales *artifacs* en Android

3 DESARROLLO DEL TFM

3.1 El laboratorio forense Android

3.1.1 La estación de trabajo

Previo al inicio del examen de la información extraída de dispositivos móviles, es esencial disponer de un entorno de trabajo totalmente estéril, con las herramientas necesarias de extracción y/o análisis de evidencias. Es muy importante contar únicamente con aquellas herramientas que sean necesarias, en un entorno de trabajo especialmente dirigido a este cometido.

Para este tipo de tareas resultan de gran utilidad las máquinas virtuales, las cuales permiten disponer no solo de un entrono con aquellos elementos necesarios, sino en una situación de "aislamiento", respecto al entorno de la máquina anfitrión. Durante los ejercicios prácticos o talleres, se hará uso de una máquina virtual Windows 10 [11] para el software de virtualización VMware player 16 [12], esta será nuestra estación de trabajo que contendrá aquellas aplicaciones tanto de simulación de dispositivos móviles, como de análisis forense, ver figura 3-1.

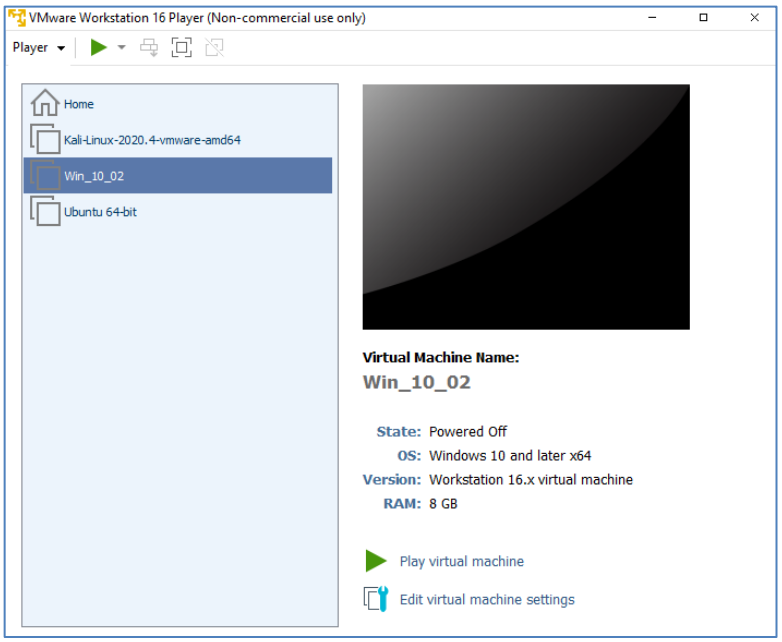


Figura 3-1 *Interface* principal del software VMware Player 16

A lo largo del desarrollo y resolución de los talleres se hará uso del software Android Studio [13], que se describirá en detalle posteriormente. Para disponer de un empleo estable en la máquina virtual es necesario configurar una serie de parámetros mínimos: se requiere una reserva de 8GB de memoria RAM, ver figura 3-2, así como la activación de virtualización en el procesador virtual de la máquina, ver figura 3-3.

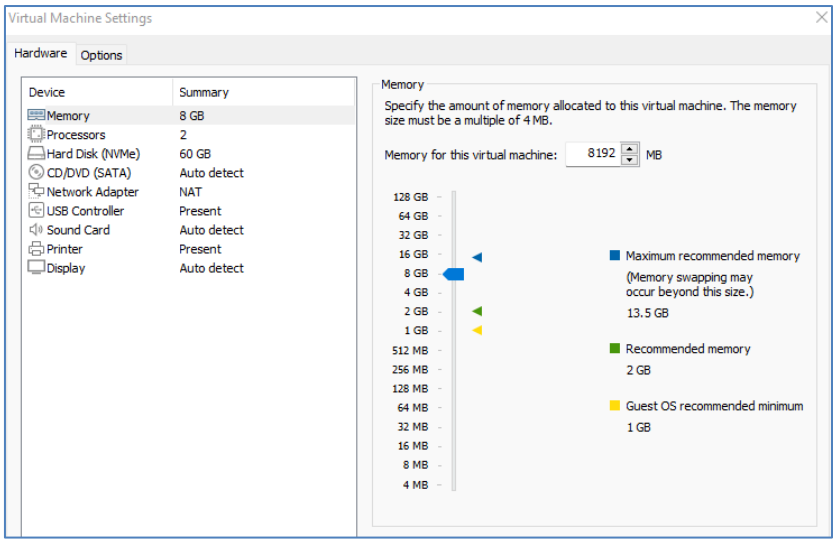


Figura 3-2 Detalle de la configuración de memoria RAM

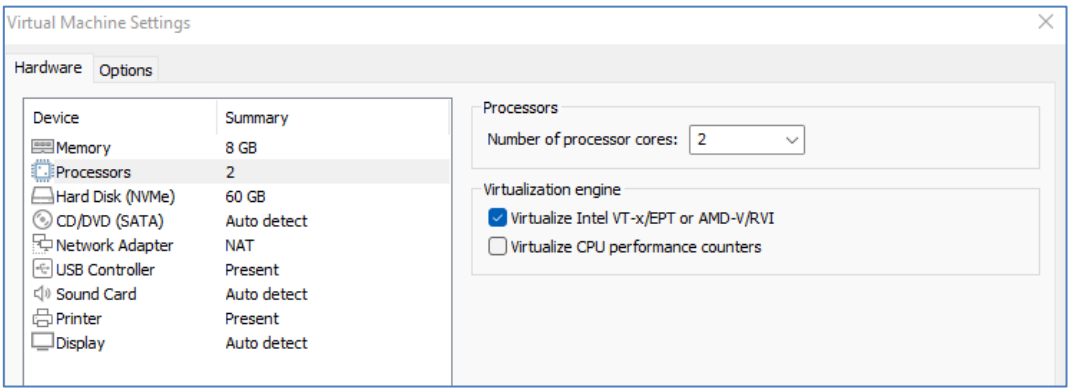


Figura 3-3 Detalle configuración de virtualización

De cara a mantener un entorno limpio desde un punto de vista forense, son de gran utilidad los conocidos como *snapshot*[12], desgraciadamente el software player 16 no cuenta con una opción por defecto, sin embargo, el fichero que contiene la máquina virtual puede copiarse en otra localización a modo de copia de seguridad de un momento concreto. Esto es especialmente útil cuando se analiza algún tipo de malware, ya que permite recuperar la máquina saneada de nuevo.

[12] Copia de seguridad de una máquina virtual, permite reestablecerla a un estado anterior.

3.1.2 Android Studio

A lo largo del desarrollo de los talleres, se emplearán tanto teléfonos físicos, como virtuales, en este último punto entra a jugar la herramienta Android Studio, ver figura 3-4, la cual nos permitirá levantar un emulador de dispositivo móvil con un sistema operativo Android.

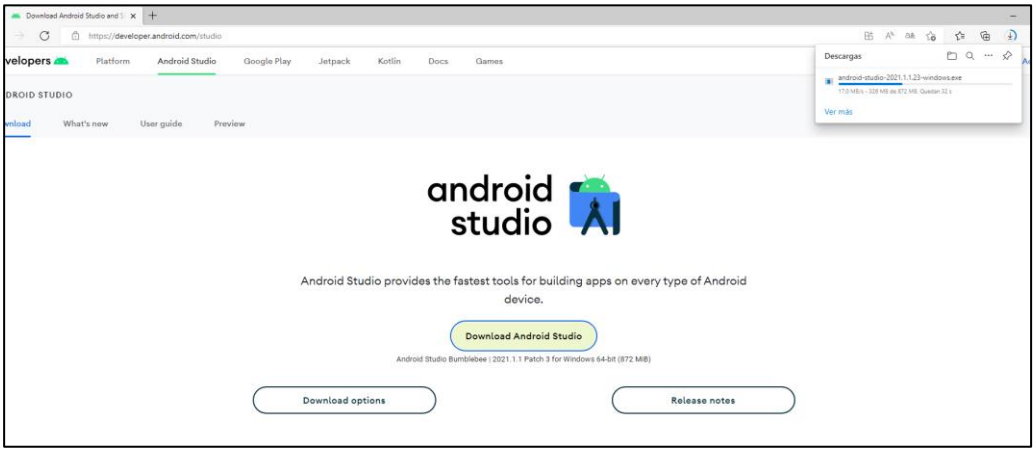


Figura 3-4 Web descarga Android Studio

En primer lugar, debe crearse un nuevo proyecto, ver figura 3-5, lo cual contiene todo lo que define el lugar de trabajo para una aplicación, desde el código fuente y recursos, hasta código de prueba y configuraciones de compilación.

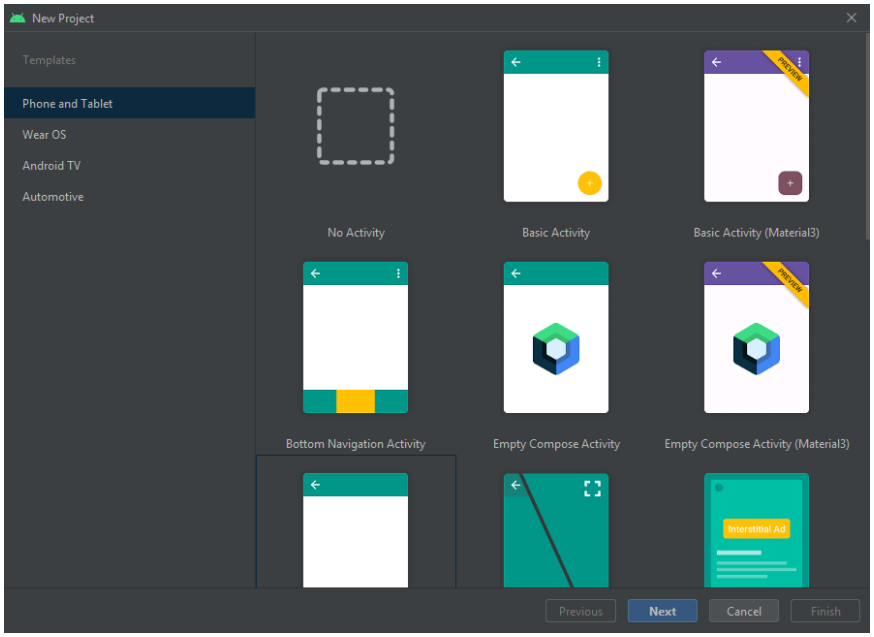


Figura 3-5 Selección de un nuevo proyecto

Una vez creado un nuevo proyecto, configuramos un nuevo dispositivo virtual Android, ver figura 3-6 y 3-7 ,elemento sobre el cual se centrarán las prácticas.

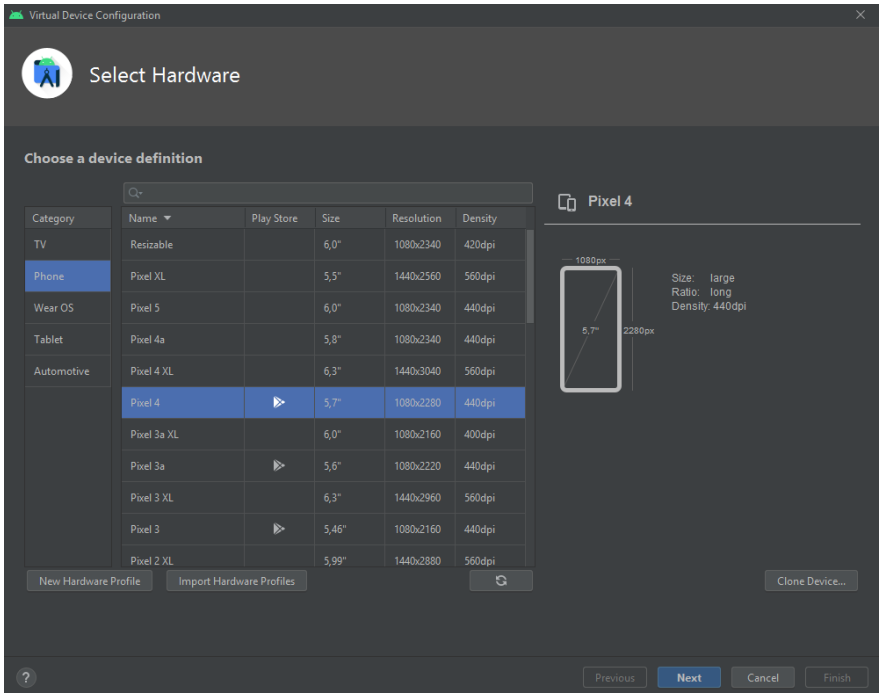


Figura 3-6 Selección del hardware del AVD

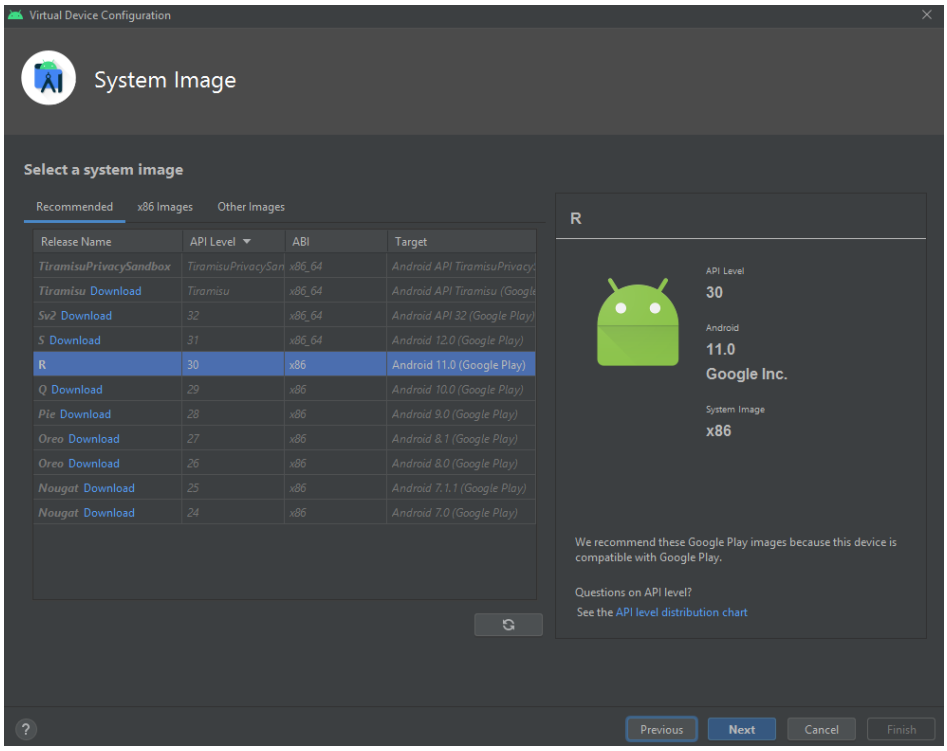


Figura 3-7 Selección de la versión del SO

Tras la creación del proyecto y del dispositivo virtual podremos lanzarlo, ver figura 3-8, haciendo uso de él como si de un teléfono físico se tratase.

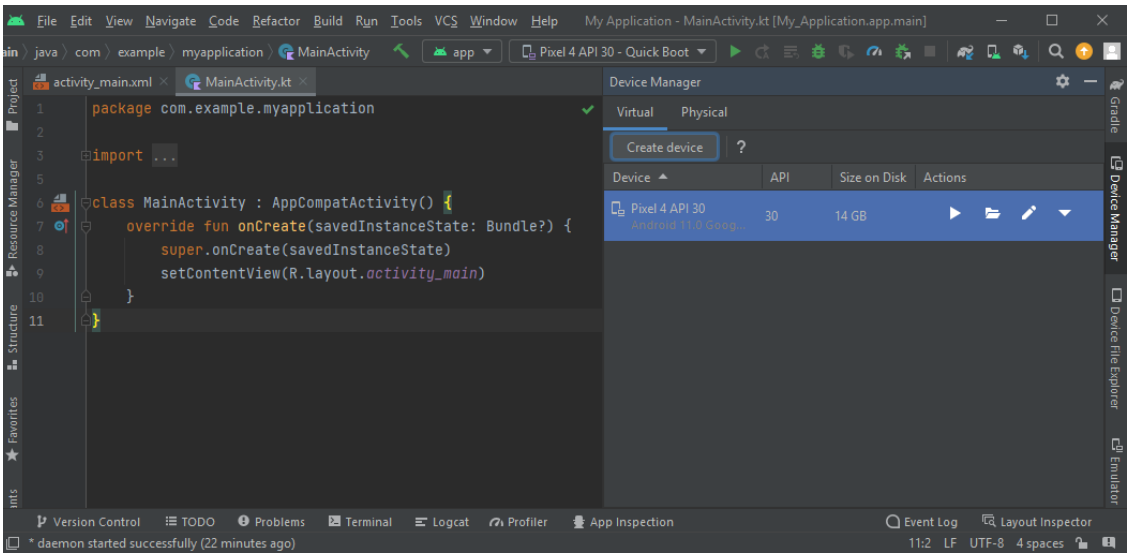


Figura 3-8 Interface principal tras la creación del proyecto y el AVD

Los dispositivos virtuales, no solo son una excelente herramienta de desarrolladores para crear y probar aplicaciones para móviles, a mayores, permite a los analistas forenses entender cómo se comportan ciertas aplicaciones, así como sus efectos en los dispositivos.

El emulador, ver figura 3-9, puede emplearse para crear cuentas de email, instalar aplicaciones, así como navegar por Internet, ver figura 3-10. Resulta una herramienta de gran interés desde un punto de vista forense, permitiendo extraer y analizar los diferentes *artifacts* como si de un dispositivo móvil físico se tratase.

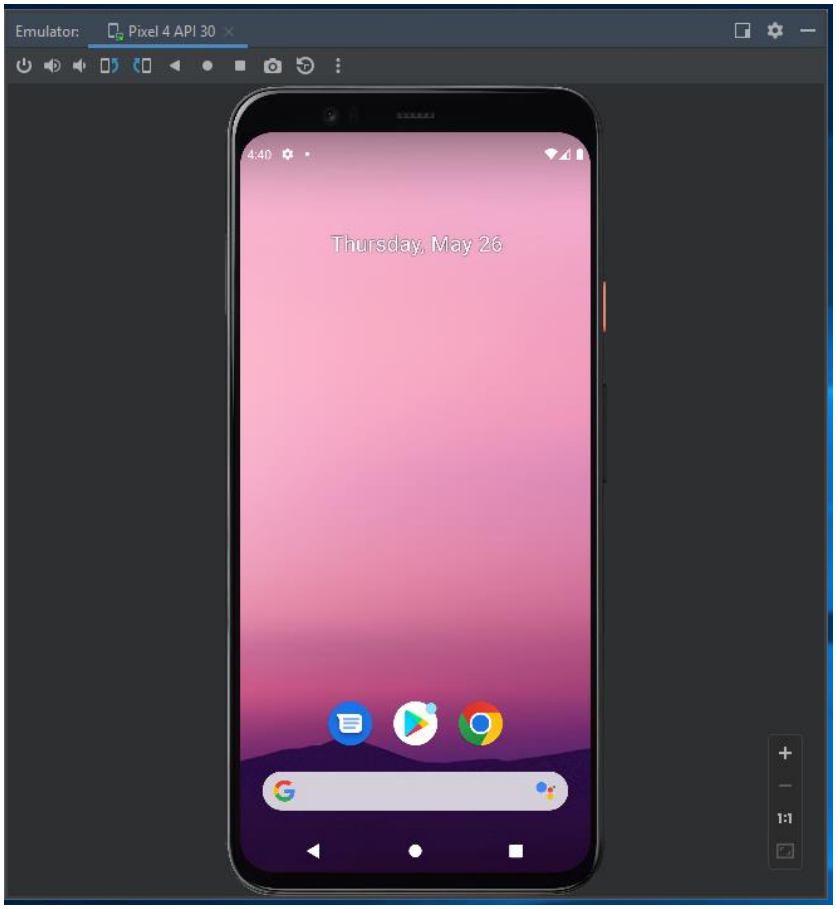


Figura 3-9 Vista principal de un AVD PIXEL 4

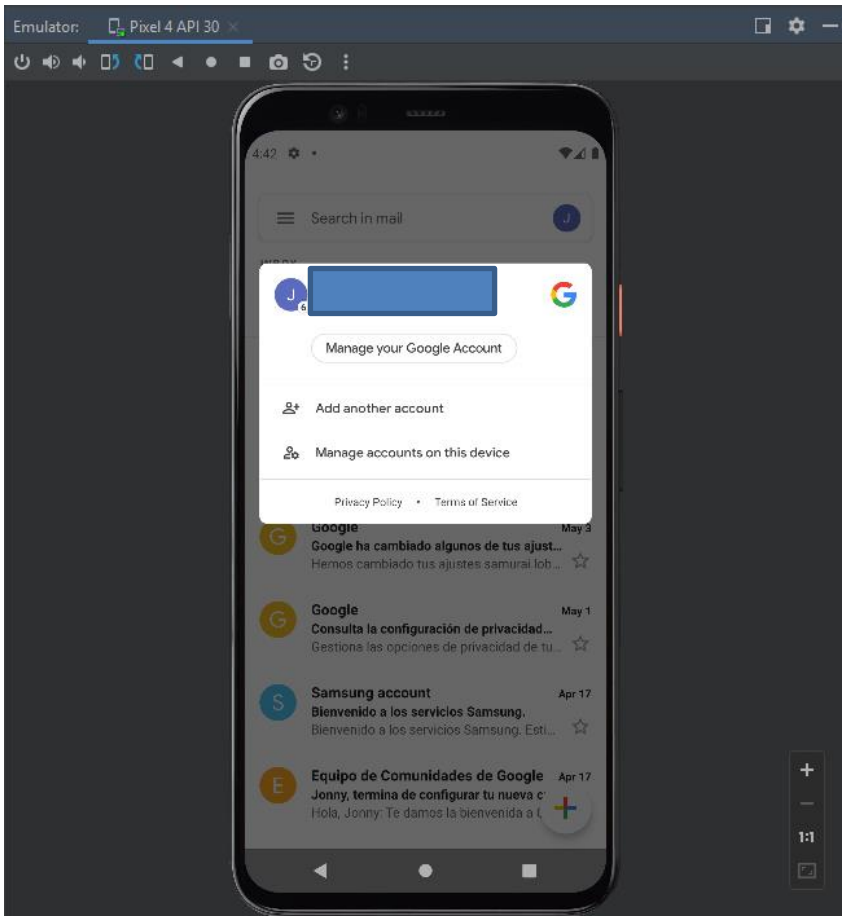
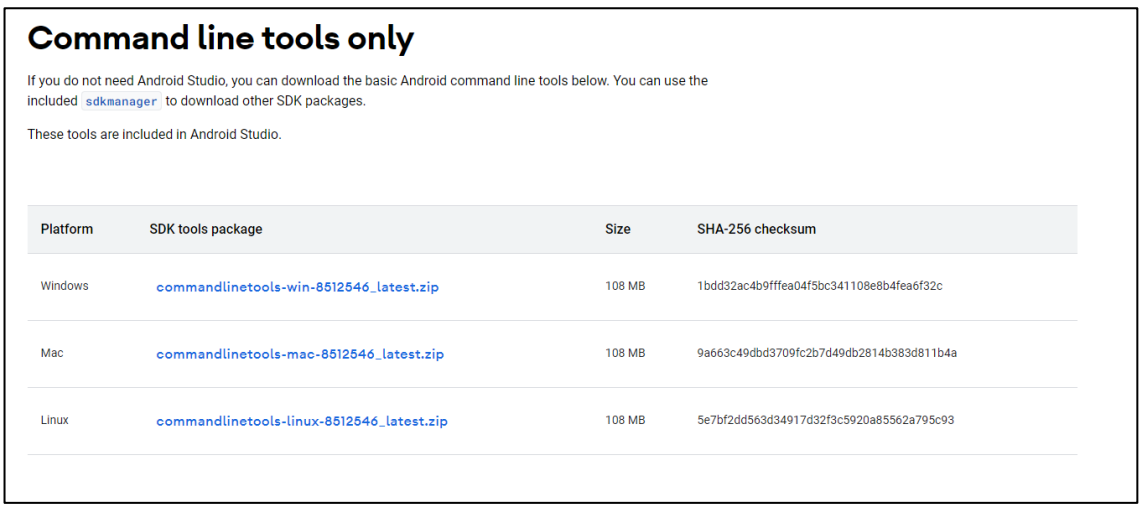


Figura 3-10 GMAIL en AVD

3.1.3 Android Debug Bridge (ABD)

Esta herramienta va a jugar un papel fundamental en el proceso de análisis forense de dispositivos Android. En el presente trabajo la instalación se realizará a través del propio Android Studio, pero puede instalarse de manera independiente a través de *Android Software Development Kit (SDK)*, en el apartado *Command Line Tools only* [13], ver figura 3-11.



Command line tools only

If you do not need Android Studio, you can download the basic Android command line tools below. You can use the included `sdkmanager` to download other SDK packages.

These tools are included in Android Studio.

Platform	SDK tools package	Size	SHA-256 checksum
Windows	commandlinetools-win-8512546_latest.zip	108 MB	1bdd32ac4b9fffea04f5bc341108e8b4fea6f32c
Mac	commandlinetools-mac-8512546_latest.zip	108 MB	9a663c49dbd3709fc2b7d49db2814b383d811b4a
Linux	commandlinetools-linux-8512546_latest.zip	108 MB	5e7bf2dd563d34917d32f3c5920a85562a795c93

Figura 3-11 Sección de descarga Android SDK

ADB permite comunicar el dispositivo móvil con el laboratorio forense a través de instrucciones en líneas de comando. Para trabajar con ABD, la opción *USB-Debugging*, ver figura 3-12, debe estar habilitada. Esta opción suele encontrarse en opciones de desarrolladores, la cual suele estar oculta. En el caso de un Samsung J3, el procedimiento es el siguiente:

1.Dirigirse al icono de ajustes.

2.Desplazarse a *Acerca del teléfono*.

3.Pinchar en *Información del Software.*

4.Pinchar 5 veces en *número de compilación* para activar el modo desarrollador y hacerlo visible.

5.Volver a ajustes y verás el *modo desarrollador*.

6. Activar la opción: *depurador por USB.*

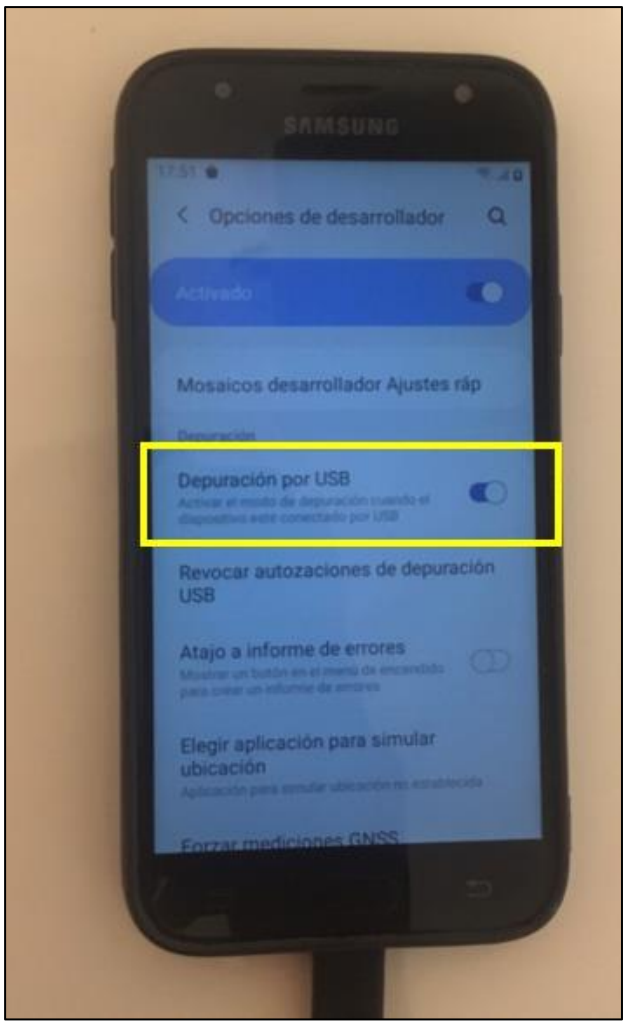


Figura 3-12 Opción *Depuración por* USB en Sansung J3

Una vez habilitada la opción *Depuración por USB*, en el dispositivo correrá el proceso *ADB Daemon*, el cual buscará constantemente una conexión USB. Normalmente este proceso no corre con

privilegios, y salvo que el dispositivo este rooteado, no permitirá el acceso a los datos de aplicaciones. En la estación de trabajo, se iniciará el programa adb, el cual está localizado generalmente en: *C:\Users\USER0\AppData\Local\Android\Sdk\platform-tools*, resulta muy recomendable añadir esta localización a la variable de entorno *path*. Una vez situados en una consola de comandos, basta con teclear adb, ver figura 3-13, para lanzarlo, en primer lugar, chequeará si el proceso ADB está ya ejecutado, y en caso contrario iniciará uno.

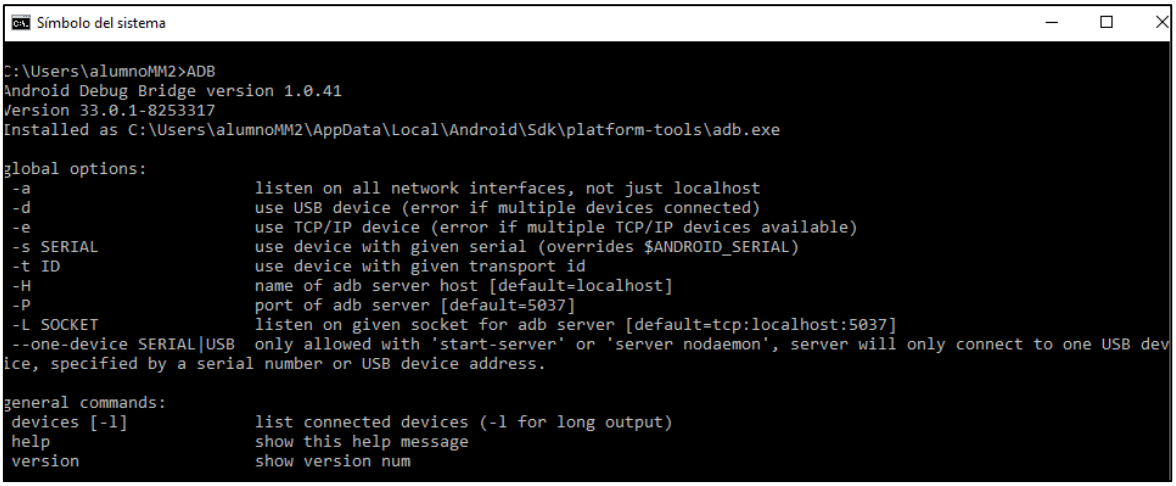


Figura 3-13 Salida por pantalla tras ejecutar el comando ADB

Como se ha comentado anteriormente, se trata de una herramienta fundamental, que permite la comunicación con el dispositivo móvil, y con ello la adquisición de evidencias asociadas a él. A continuación, se mostrará una visión general de sus capacidades.

En primer lugar, se va a indicar como adb permite listar todos los dispositivos móviles conectados. Los emuladores que tengamos levantados también aparecerán, ver figura 3-14, en el presente caso se tiene levantado un dispositivo virtual *pixel4*, así como una conexión por USB a un Samsung J3, en este último caso nos preguntará si damos permiso para la conexión.

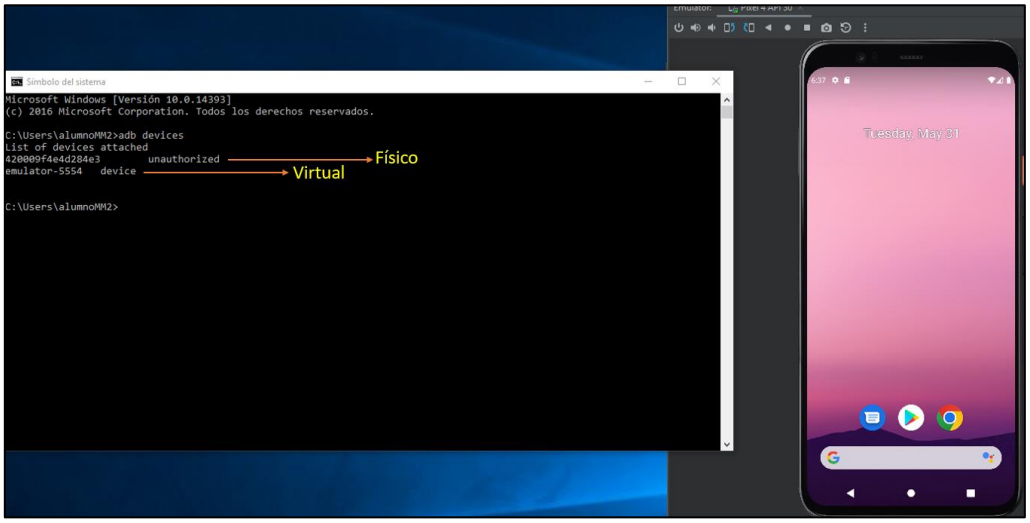


Figura 3-14 Listado de dispositivos conectados (uno sin autorización)

Es posible ver como uno de los dispositivos, el físico concretamente, aparece como no autorizado, esto es debido a que aún no hemos permitido el acceso desde el propio dispositivo.

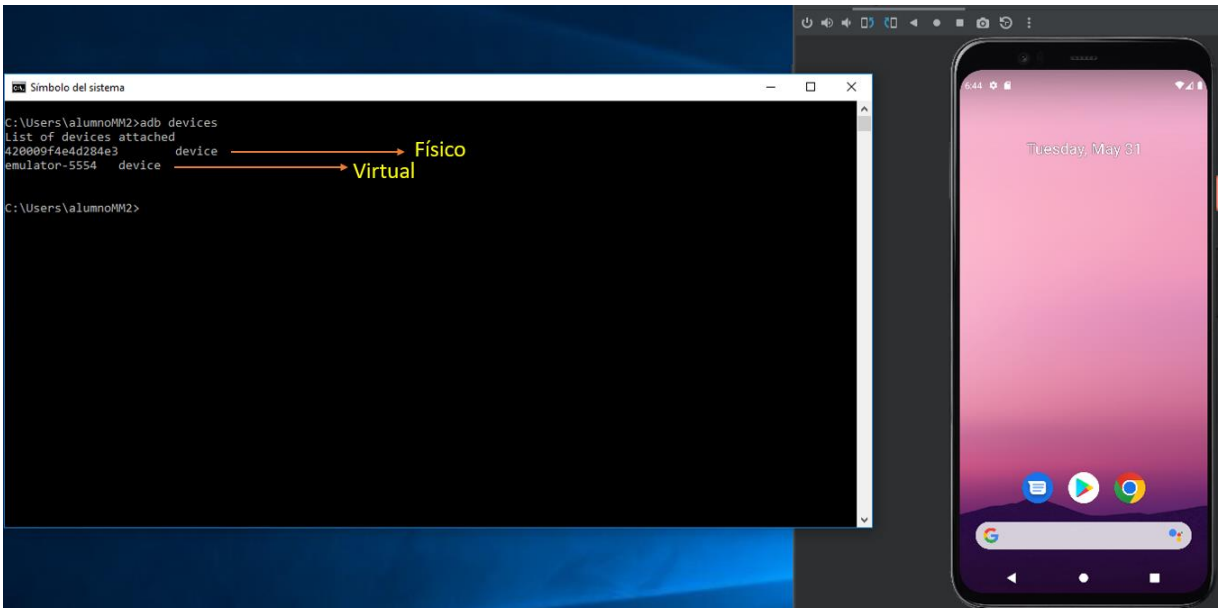


Figura 3-15 Listado de dispositivos conectados ambos autorizados

En este momento ya podemos acceder a cualquiera de ambos dispositivos, ver figura 3-15, para ello se hará uso de la instrucción *Shell*, ver figura 3-1. En el caso de disponer de varios dispositivos conectados, se debe emplear el comando *adb -s <nº de serie del dispositivo > Shell.*

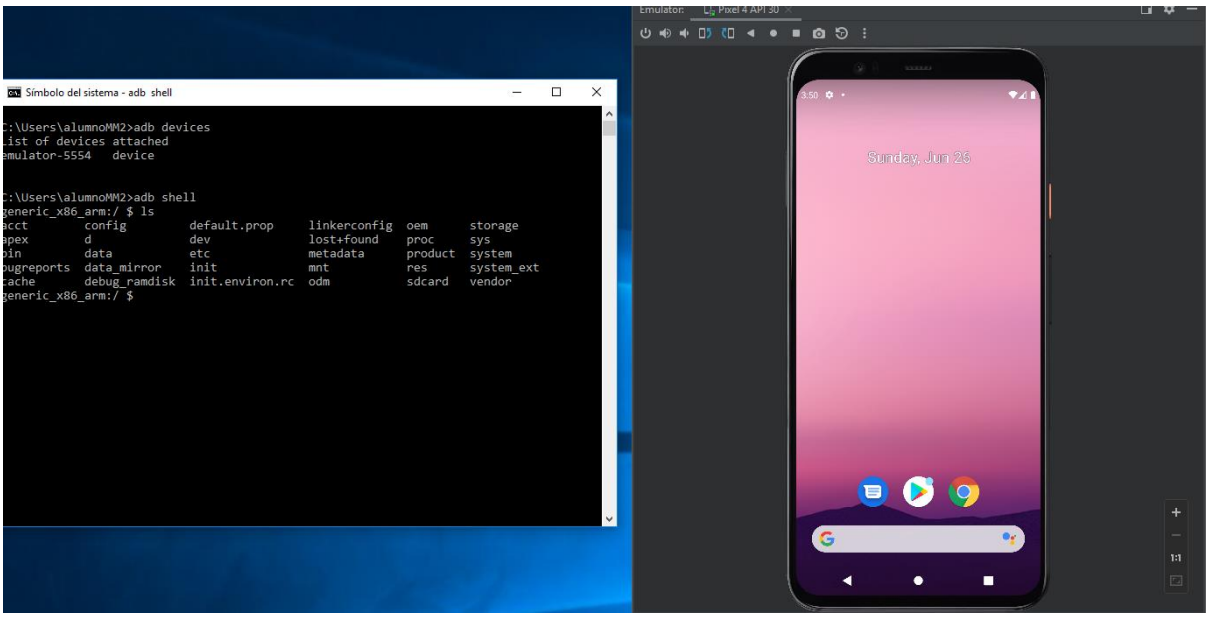


Tabla 3-1 Empleo del comando *shell*

Como se ha mencionado con anterioridad, el sistema operativo Android corre sobre un kernel de Linux, el comando adb Shell, nos permite acceder a una Shell de Linux que nos permitirá interactuar con el sistema de ficheros del dispositivo Android.

Para aquellos que estén familiarizados con las distribuciones de Linux, la Shell de Linux es un programa que permite la interacción con el dispositivo empleando comandos de Linux, a continuación, se mostrará a modo de ejemplo el empleo de los más representativos, figura 3-16, figura 3-17 y figura 3-18:

LS	PERMITE LISTAR ARCHIVOS Y DIRECTORIOS ASOCIADOS AL DIRECTORIO EN EL QUE NOS ENCONTREMOS. -a: muestra archivos ocultos -c: muestra archivos por marcas de tiempo -R: muestra a mayores los directorios
CAT	PERMITRE LEER UNO O MÁS ARCHIVOS, Y LOS MUESTRA POR PANTALLA.
CD	A TRAVÉS DEL COMANDO CD, SE CAMBIA DE UN DIRECTORIO A OTRO.
CP	PERMITE COPIAR UN ARCHIVO DESDE UNA LOCALIZACIÓN ORIGEN A UNA DESTINO. /$ cp [opciones] <origen> <destino>
CHMOD	PERMITE MODIFICAR LOS PERMISOS SOBRE UN ARCHIVO O UN DIRECTORIO. /$ chmod [option] file
DD	EL COMANDO DD PERMITE: COPIAR UN ARCHIVO, CONVIRTIENDOLO Y FORMATEANDOLO EN BASE A LOS OPERANDOS. RESULTA MUY UTIL PARA CREAR UNA COPIA BIT A BIT DEL DISPOSITIVO ANDROID. /$ dd if=<archivo origen> of=/sdcard/ejemplo.image
RM	PERMITE BORRAR ARCHIVOS Y DIRECTORIOS. /$ rm <archivo>
GREP	EMPLEADO PARA BUSCAR ARCHIVOS, O EL CONTENIDO DE UN ARCHIVO, EN BASE A UN PATRÓN DE BÚSQUEDA.

PWD	DEVUELVE POR PANTALLA EL DIRECTORIO ACTUAL.
MKDIR	PERMITE CREAR UN NUEVO DIRECTORIO. /$ mkdir [opciomes] <nombre del directorio>
EXIT	PERMITE SALIR DE LA SHELL.

Tabla 3-2 Principales comandos de LINUX.

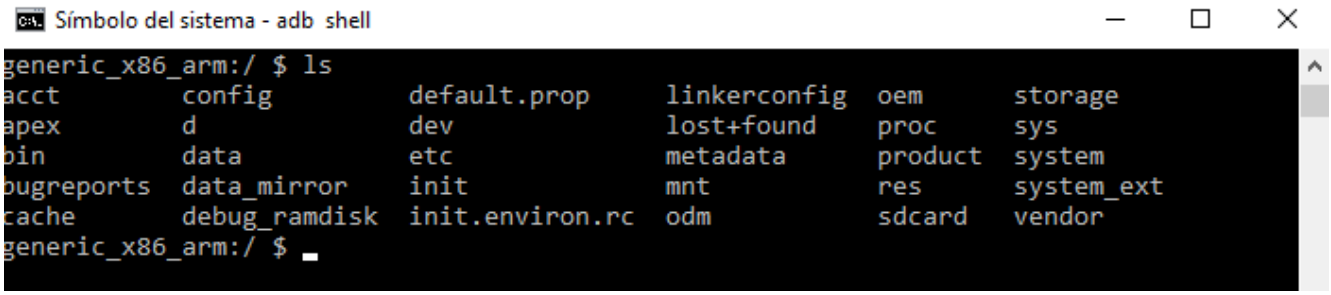


Figura 3-16 Ejemplo de empleo comando *ls*

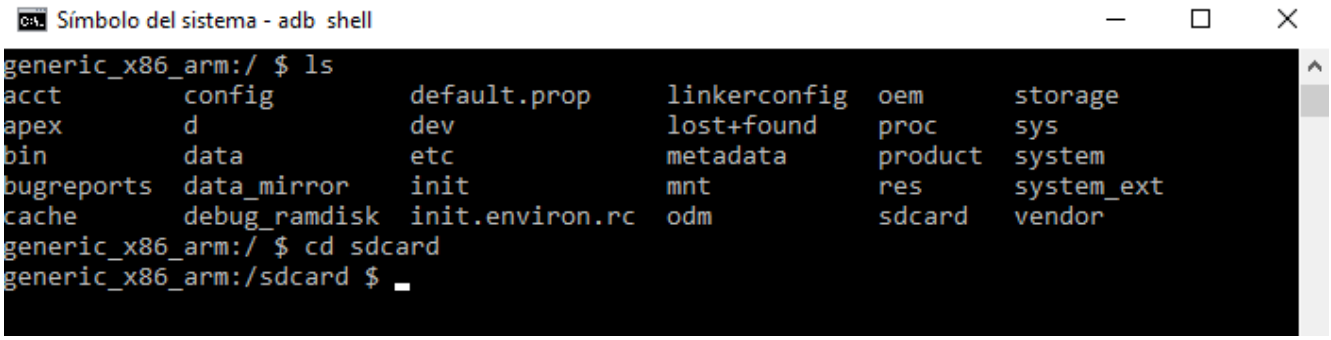


Figura 3-17 Ejemplo de empleo comando *cd*

Figura 3-18 Ejemplo de empleo comando *pwd*

Junto con los principales comando de los sistemas Linux, ver tabla 3-2, resulta fundamental conocer una serie de opciones, aparte de *devices* y *Shell*, que permite el comando *adb*, estas opciones serán esenciales a la hora de acometer distintos requisitos que precisará el análisis forense sobre dispositivos Android.

En determinadas ocasiones, será necesario instalar ciertas aplicaciones en el dispositivo, de cara a asegurar ciertos privilegios para una adquisición completa. Por supuesto, todas estas acciones deliberadas sobre el dispositivo deben ser detalladamente documentadas y justificadas, para ello se hará uso del comando *install:*

adb install <programa a instalar>

Junto con posibles instalaciones de aplicaciones sobre el dispositivo, será necesario extraer información del dispositivo, de cara a efectuar un análisis más detallado, o para preservar evidencias. Para ello se emplea el comando pull, ver figura 3-21*:*

adb pull <origen en el dispositivo> <destino en el laboratorio local>

Es importante resaltar, que en un dispositivo Android únicamente podremos extraer evidencias desde directorios autorizados, por ejemplo, no podremos extraer directamente nada desde el directorio /data/data/, sin embargo, sí desde el /sdcard.

También podremos volcar ficheros procedentes de nuestro laboratorio en el dispositivo Android, ver figura 3-19 y figura 3-20, haciendo uso del comando *push.*

adb push <fichero origen en laboratorio local> <destino en el dispositivo>

De manera similar a lo que ocurría con el comando *pull,* el comando *push* únicamente se podrá emplear sobre directorios en los que el usuario tenga privilegios.

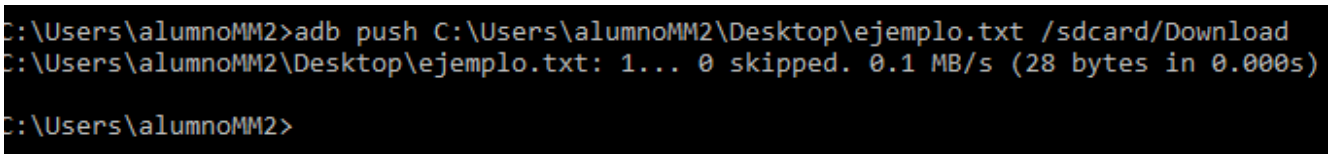


Figura 3-19 Ejemplo de empleo del comando *push*

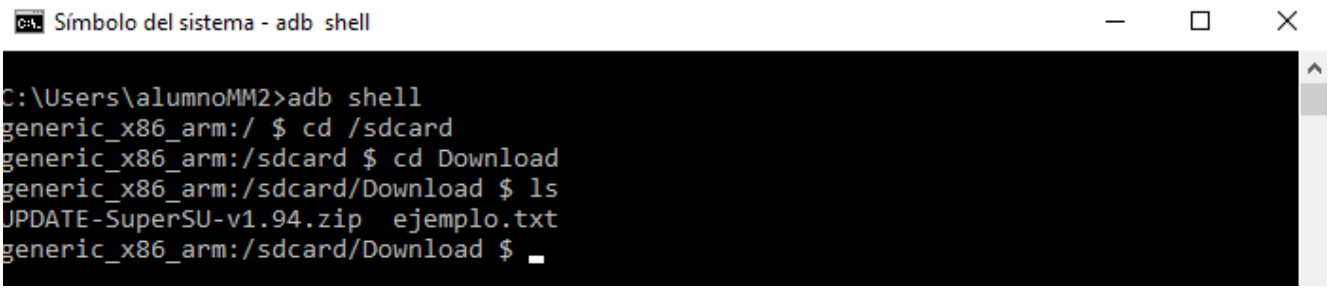


Figura 3-20 Verificación del archivo introducido en el dispositivo

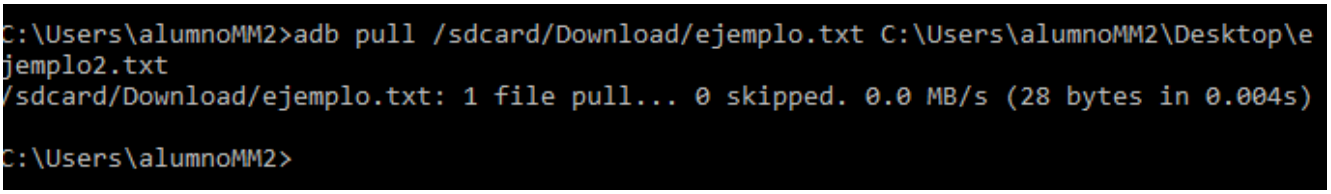


Figura 3-21 Ejemplo de empleo del comando *pull*

3.2 Herramientas en el marco de una adquisición lógica

La adquisición lógica hace referencia, a aquella que no realiza una copia bit a bit, y por tanto no permite la extracción/recuperación de información borrada. Requiere una comunicación con el sistema operativo.

El Sistema operativo, elegirá que información está al alcance del analista, podría asemejarse a realizar un "copia y pega" de datos procedentes del dispositivo, en caso de que exista información oculta o borrada, no será copiada en el destino.

Es muy importante tener presente, que el factor limitante en la extracción de información procedente de dispositivos móviles, son los permisos que el usuario tenga sobre los datos almacenados, como vimos anteriormente, existen ciertas ubicaciones y datos que a los que no es posible acceder sin permisos *ROOT*. En el caso de información procedente de aplicaciones, la excepción se encuentra en el caso de que dichos datos se localicen en la SD card, en cuyo caso podrán ser accedidos sin necesidad de *rootear* el dispositivo.

No se debe olvidar, que la decisión de *rootear* un dispositivo móvil, debe estar de acuerdo con la legislación local, puesto que, la aceptación de evidencias de un dispositivo *rooteado* cambia según la jurisdicción.

3.2.1 ADB BACKUP

Esta función implementada por GOOGLE desde la versión 4.0 de Android, permite a un analista (o un usuario) efectuar una copia de recuperación o back up de datos, incluidos los de ciertas aplicaciones, en la estación de trabajo. Esta función no requiere de privilegios root.

A pesar de los aparentes beneficios de esta herramienta, no todas las aplicaciones permiten efectuar una copia de recuperación, esta va a depender del desarrollador de la misma, si permite o no la realización de copias de seguridad. Al mismo tiempo, este método no podrá emplearse si el dispositivo está bloqueado.

El formato de la instrucción ADB BACKUP es el siguiente:

adb backup [-f <file>] [-apk|-noapk] [-obb|-noobb] [-shared|-noshared] [-all] [-

system|-nosystem] [<packages...>]

A continuación, se explicará el significado de las distintas opciones o *-flags*, ver tabla 3-3 y figuras 3-22 y 3-23*:*

-f	Permite especificar el archivo de salida para la copia de seguridad. Si no se indica nada, se empleará el directorio actual.
[-apk|noapk]	Elige si se desea efectuar back up del archivo .apk, por defecto la opción es -noapk.
[-obb|-noobb]	Elige si se desea realizar back up de los archivos. obb (expansión de APK), por defecto -nooobb.
[-shared|-noshared]	Elige sí o no se efectúa back up del almacenamiento compartido y de la tarjeta SD. Por defecto -noshared

[-all]	Permite efectuar back up de todas aquellas aplicaciones instaladas, en las que el desarrollador ha permitido esta opción.
[-system|-nosystem]	Permite elegir si se incluyen aplicaciones del sistema, por defecto -system.
[<packages>]	Permite indicar el paquete de datos para una aplicaciones específica.

Tabla 3-3 Opciones de la herramienta adb backup

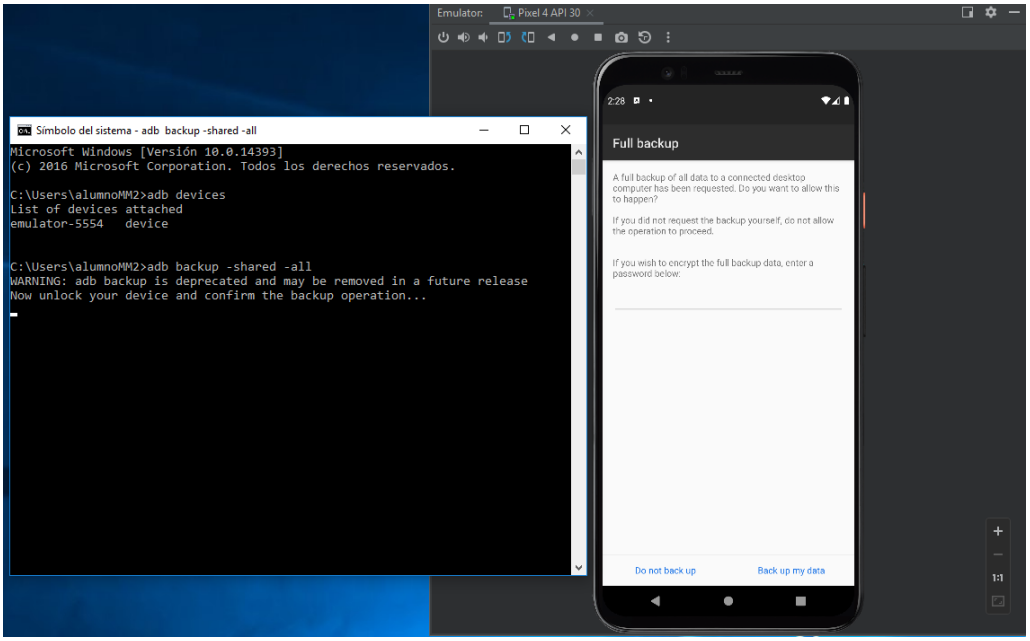


Figura 3-22 Empleo herramienta backup, solicitud de autorización al usuario

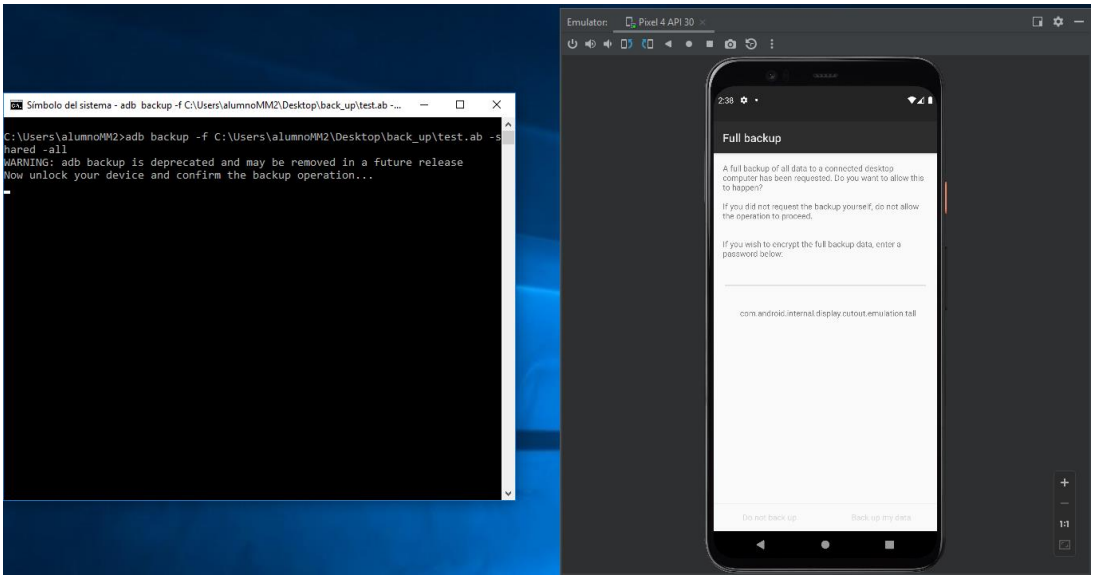


Figura 3-23 Empleo de herramienta backup

Una vez obtenido el archivo *ab*[13], el cual es posible abrirlo convirtiéndolo en primera instancia en un .TAR, ver figura 3-24, veremos un par de directorios: *app* y *shared*, ver figura 3-25. Para convertir el archivo ab, existen multitud de herramientas, en este caso se va a emplear *android backup processor* [14].

```
C:\Users\alumnoMM2\Desktop\android-backup-tookit-20210819\android-backup-tookit\android-backup-processor\executable>java -jar abp.jar unpack
C:\Users\alumnoMM2\Desktop\back_up\test.ab  C:\Users\alumnoMM2\Desktop\back_up\test.tar

C:\Users\alumnoMM2\Desktop\android-backup-tookit-20210819\android-backup-tookit\android-backup-processor\executable>
```

Figura 3-24 Empleo herramienta Android Backup Processor

Nombre	Fecha de modifica...	Tipo	Tamaño
apps	03/07/2022 16:45	Carpeta de archivos	
shared	03/07/2022 16:45	Carpeta de archivos	

Figura 3-25 Directorios procedentes de archivo *.ab*

El directorio *app*, ver figura 3-26, contiene datos procedentes del directorio /data/data con la opción backup activo, mientras que el directorio *shared*, ver figura 3-27, contiene la información procedente de la tarjeta SD.

Nombre	Fecha de modifica...	Tipo	Tamaño
android.auto_generated_rro_product__	03/07/2022 16:45	Carpeta de archivos	
com.android.bips	03/07/2022 16:45	Carpeta de archivos	
com.android.bips.auto_generated_rro_pr...	03/07/2022 16:45	Carpeta de archivos	
com.android.bluetoothmidiservice	03/07/2022 16:45	Carpeta de archivos	
com.android.bookmarkprovider	03/07/2022 16:45	Carpeta de archivos	
com.android.camera2	03/07/2022 16:45	Carpeta de archivos	
com.android.carrierconfig.auto_generate...	03/07/2022 16:45	Carpeta de archivos	
com.android.carrierdefaultapp	03/07/2022 16:45	Carpeta de archivos	
com.android.cellbroadcastreceiver	03/07/2022 16:45	Carpeta de archivos	
com.android.contacts	03/07/2022 16:45	Carpeta de archivos	
com.android.cts.ctsshim	03/07/2022 16:45	Carpeta de archivos	
com.android.cts.priv.ctsshim	03/07/2022 16:45	Carpeta de archivos	
com.android.dialer	03/07/2022 16:45	Carpeta de archivos	
com.android.dreams.basic	03/07/2022 16:45	Carpeta de archivos	
com.android.egg	03/07/2022 16:45	Carpeta de archivos	
com.android.emergency	03/07/2022 16:45	Carpeta de archivos	
com.android.emulator.radio.config	03/07/2022 16:45	Carpeta de archivos	
com.android.externalstorage	03/07/2022 16:45	Carpeta de archivos	
com.android.htmlviewer	03/07/2022 16:45	Carpeta de archivos	
com.android.internal.display.cutout.emu...	03/07/2022 16:45	Carpeta de archivos	
com.android.internal.display.cutout.emu...	03/07/2022 16:45	Carpeta de archivos	
com.android.internal.display.cutout.emu...	03/07/2022 16:45	Carpeta de archivos	
com.android.internal.display.cutout.emu...	03/07/2022 16:45	Carpeta de archivos	

Figura 3-26 Contiendo del directorio app

[13] Se trata de un archivo TAR que ha sido comprimido con un algorithmo *Deflate*.

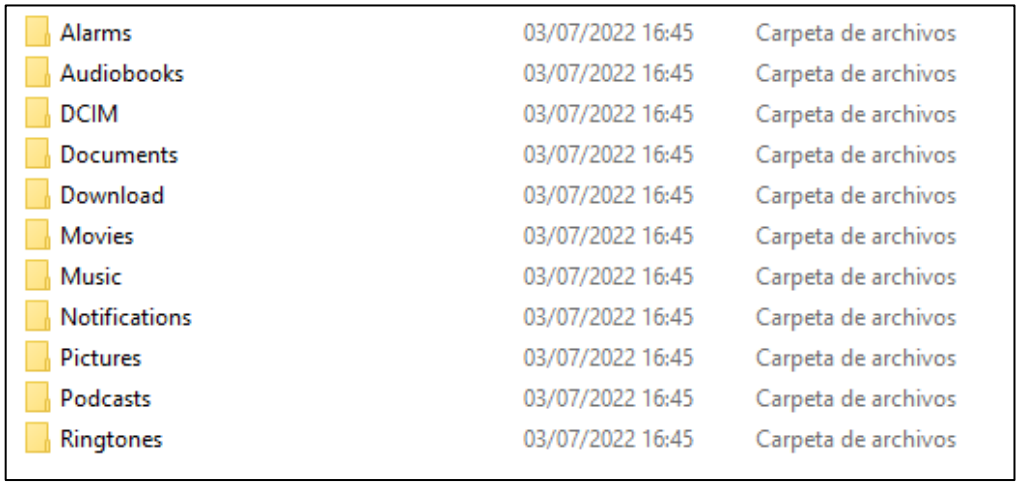


Figura 3-27 Contenido del directorio shared

3.2.2 ADB DUMPSYS

Dumpsys se trata de una herramienta del Sistema operativo Android, concebida para conocer el estado de los distintos servicios corriendo en el dispositivo. A pesar de su finalidad desde el punto de vista del desarrollador, puede permitir la adquisición de información de interés desde un punto de vista forense. Esta herramienta no requiere de un acceso root, sin embargo, precisa de habilitar la opción de depuración por USB para permitir su correcta ejecución.

La herramienta *dumpsys* permite la ejecución de una serie de servicios, los cuales van a variar en función a la versión del Sistema operativo. Para conocer las opciones que permite *dumpsys* basta ejecutar la instrucción: *adb -s< nº serie del dispositivo > shell service list*, ver figura 3-28.

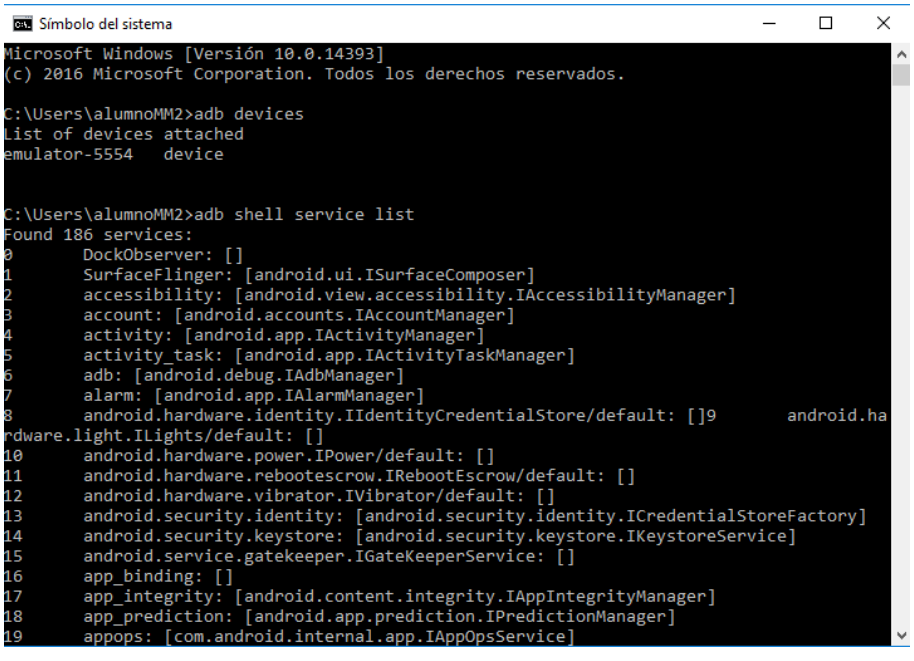


Figura 3-28 Servicios de la herramienta dumpsys

A continuación, se describirán aquellas opciones que tienen un mayor interés, desde un punto de vista forense, ver tabla 3-4.

IPHONESUBINFO	Permite conocer el IMEI del dispositivo.
BATTERYSTAT	Empleado para saber el empleo de las aplicaciones que están en ejecución. Permite conocer que aplicación ha sido empleada de manera reciente.
PROCSTATS	Este servicio permite conocer el empleo de procesador por parte de las aplicaciones que están corriendo. Permite conocer que aplicaciones se han empleado de manera reciente. *–HOURS X*, permite saber el porcentaje de empleo de la memoria en las últimas x horas, ver figura 3-29.
USER	Permite conocer la última información de logeo para cada usuario, ver figura 3-30. Debemos tener en cuenta, que únicamente un usuario puede estar logeado simultáneamente, viendo la información del último logeo podemos identificar quien inició sesión por última vez.
APP OPS	Permite conocer los permisos asignados a cada aplicación, y con ello saber la última vez que la aplicación empleó un determinado permiso, ver figura 3-31.
WI-FI	Devuelve una lista de SSID, cuya conexión ha sido guardada, ver figura 3-32.
NOTIFICATION	Devuelve información sobre notificaciones activas, lo cual puede ser útil para guardar el estado de un dispositivo al que se ha accedido, o incluso conocer que aplicación ha ejecutado una determinada notificación.
CONCLUSIONS	Sin especificar un servicio concreto, devolverá todos los servicios disponibles.

Tabla 3-4 Opciones herramienta dumpsys

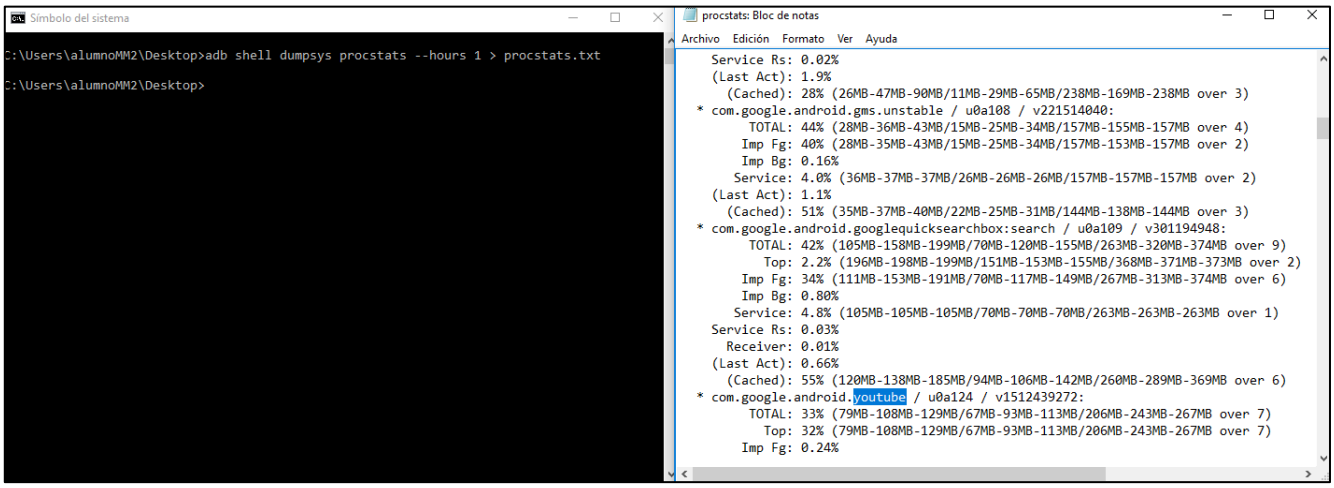


Figura 3-29 Ejemplo de empleo servicio procstats

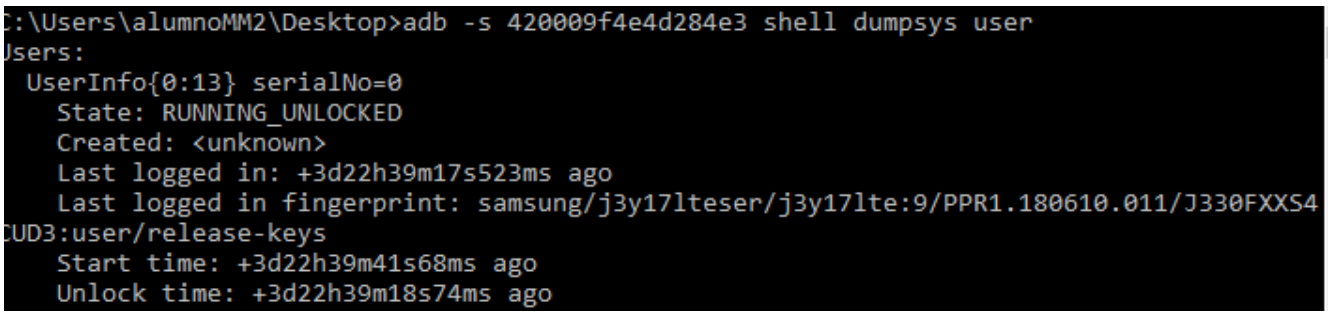


Figura 3-30 Ejemplo de empleo servicio user

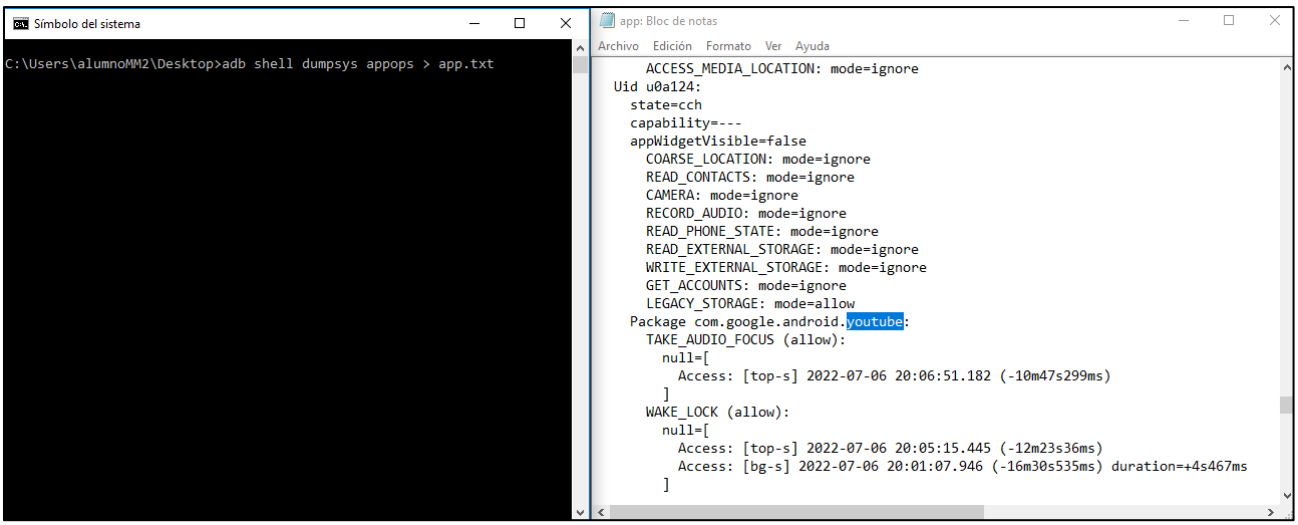


Figura 3-31 Ejemplo empleo servicio AppOps

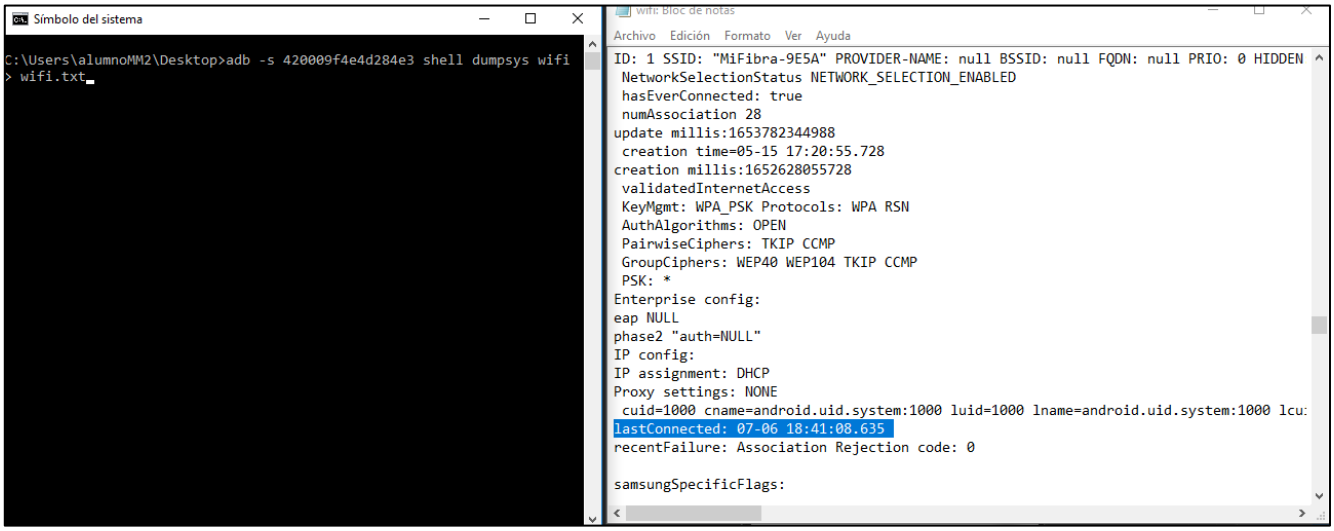


Figura 3-32 Ejemplo de uso servicio WIFI

3.2.3 HELIUM

La aplicación *helium*, permite realizar sincronización de aplicaciones y copias de respaldo en sistemas operativos Android. La razón de su estudio, es debido a que permite la extracción de información que *ADB BACKUP* no puede, como es el caso del registro de SMS y llamadas.

Su empleo requiere de dos aplicaciones, una instalada en la estación de trabajo y la otra en el dispositivo móvil [15], ver figura 3-33.

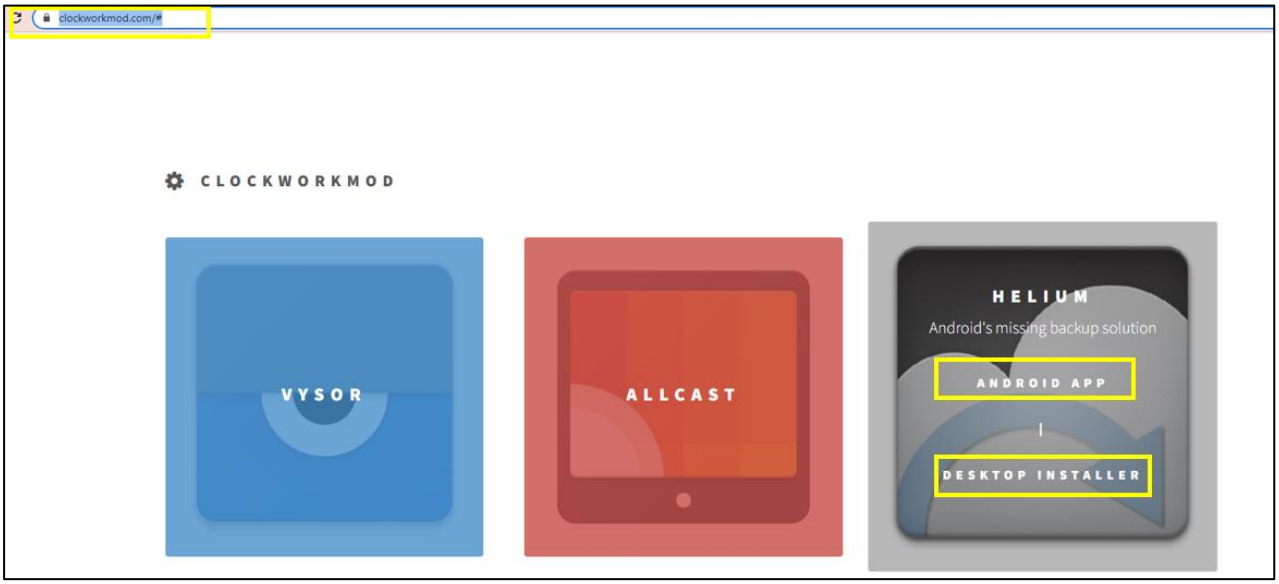


Figura 3-33 Web descarga aplicación *helium*

Una vez instaladas ambas aplicaciones, iniciamos la aplicación de la estación de trabajo, donde se nos indicará que conectemos el dispositivo con la aplicación *helium* instalada, ver figura 3-34.

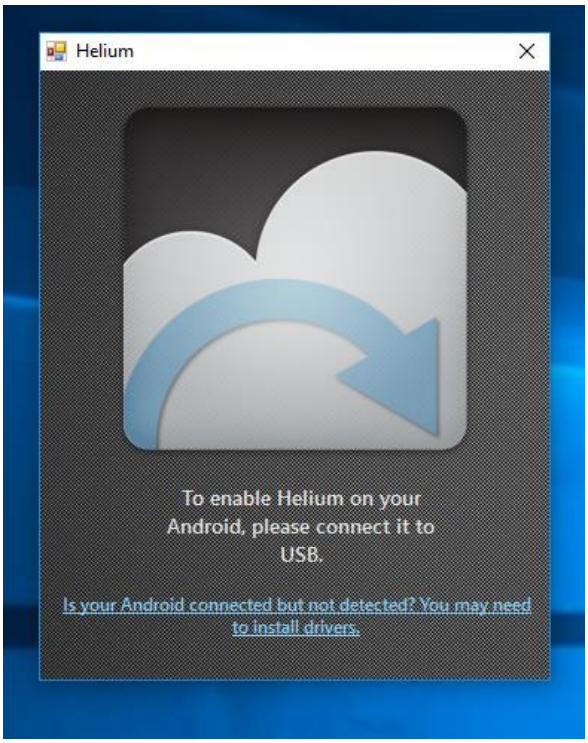


Figura 3-34 Pantalla de inicio *helium* en estación de trabajo

Al finalizar la sincronización, podremos indicar desde el dispositivo el tipo de backup que queremos, ver figura 3-35. Es importante resaltar, que una vez sincronizadas las aplicaciones del dispositivo y de la estación de trabajo, podemos desconectar el dispositivo móvil. Ambos, deben encontrarse en la misma red wifi.

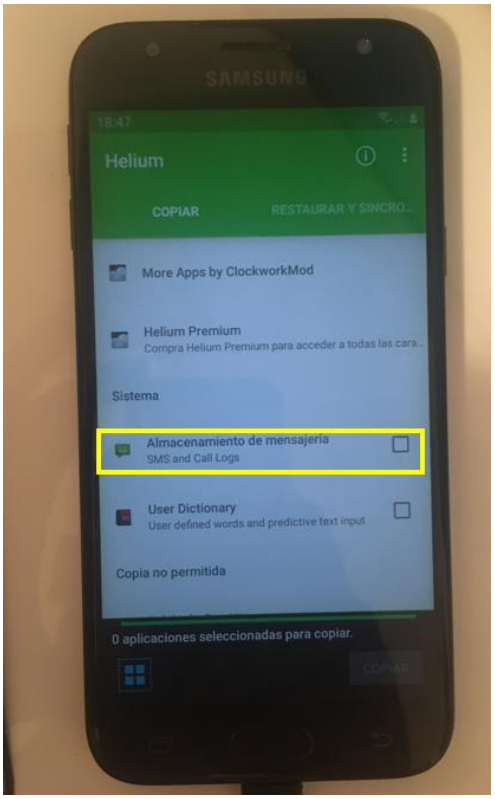


Figura 3-35 Pantalla helium tras sincronizar con la estación de trabajo

En este caso, se le indicará efectuar una copia del registro de sms y llamadas de teléfonos. A continuación, se clicará en la opción *descargar en PC.*

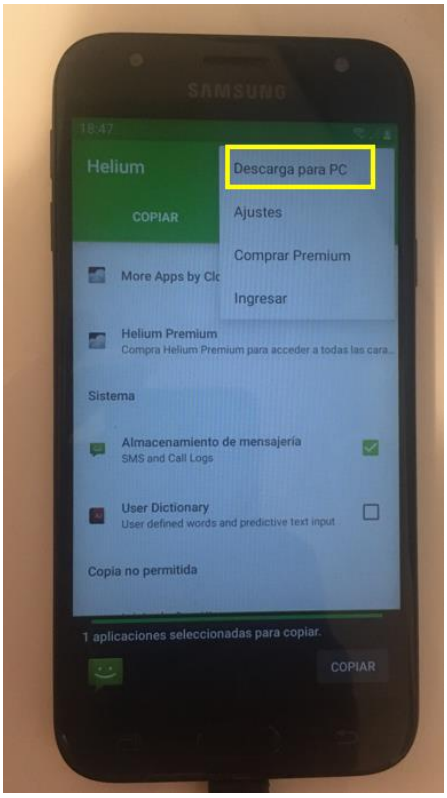


Figura 3-36 Opción de descarga a PC

Tras el paso anterior, se iniciará el *helium server* en el dispositivo móvil, donde se indicará la IP de conexión y el puerto del servicio, así como el protocolo a emplear.

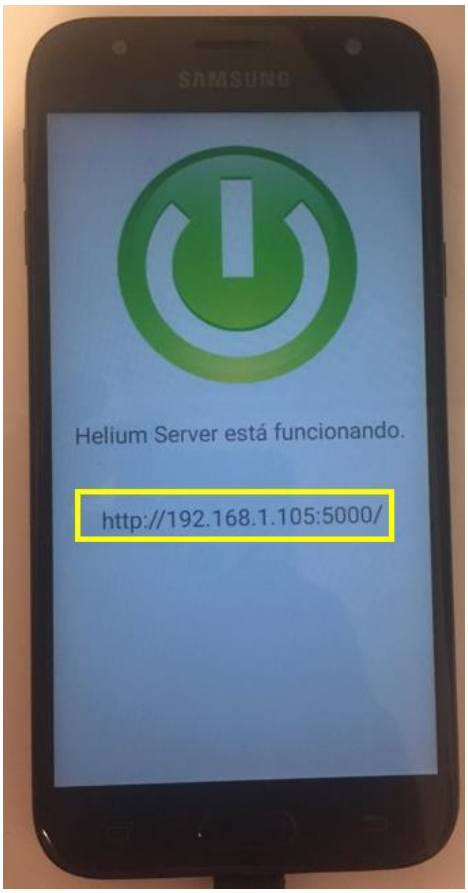


Figura 3-37 Activación del *helium server*

Una vez que el servidor se encuentra activo en el dispositivo móvil, ver figura 3-37, desde la estación de trabajo accedemos al mismo, y se procede a descargar el registro de sms y llamadas, ver figura 3-38.

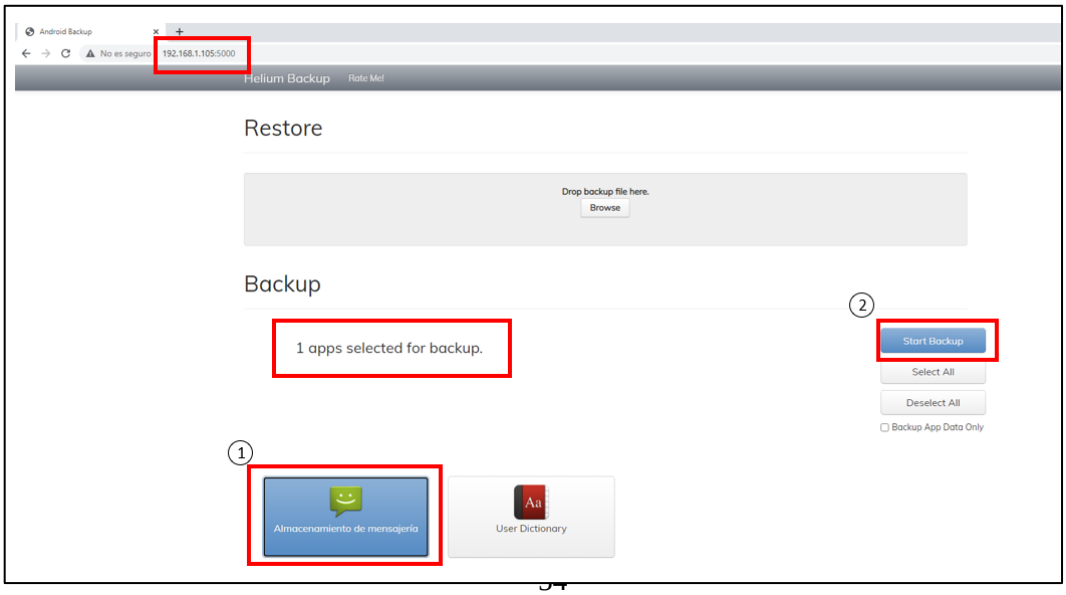


Figura 3-38 Acceso al *helium server*.

Tras realizar la copia de seguridad, dispondremos de un archivo de especial interés: *com.android.providers.telephony.ab*, en esta ocasión se hará uso de la aplicación *helium backup extractor*, ver figura 3-39.

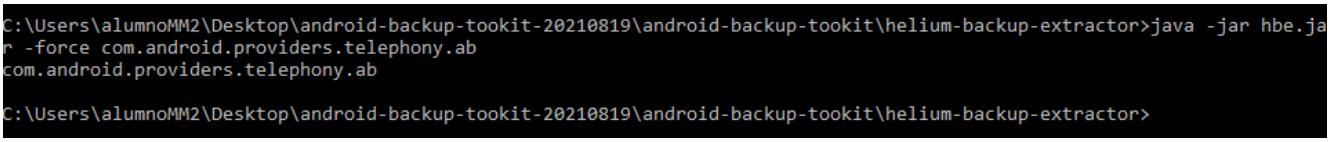


Figura 3-39 Empleo de la herramienta hbe.jar

Como consecuencia de aplicar la herramienta anterior, se obtendrá un directorio llamado *apps\com.android.providers.telephony\cb*, en el encontraremos el fichero: *custom.cb*, el cual podemos abrir con la herramienta wordpad, ver figura 3-40.

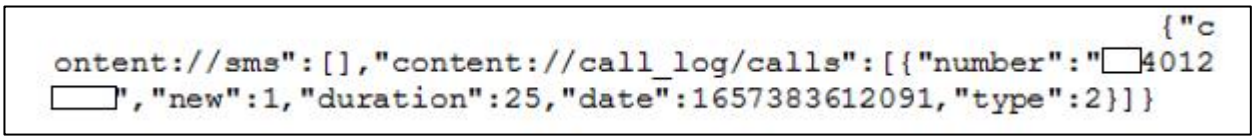


Figura 3-40 Contenido del fichero *custom.cb*

En el contenido del fichero, podemos ver: el número contactado, la duración de la llamada, así como la fecha de realización de la misma en formato *tiempo Unix*.

Es evidente, que esta herramienta no parece la más adecuada desde un punto de vista forense, pero en ocasiones es la única forma de extraer cierto tipo de información del dispositivo, razón por la cual debe estudiarse y practicar su empleo.

3.2.4 Métodos root para la adquisición de evidencias.

Hasta ahora se han analizado distintos métodos de adquisición lógica en un marco sin privilegios, sin embargo, esto nos limita el análisis de la información contenida en las distintas aplicaciones instaladas en el dispositivo, todas ellas en la partición /DATA/DATA. Como se ha comentado con anterioridad, el acceso a este tipo de datos está restringido a un usuario con privilegios, el cual no es el usuario habitual del dispositivo móvil.

En el presente apartado, se partirá de un dispositivo rooteado, para extraer los ficheros procedentes de los paquetes de aplicaciones. En primer lugar, se procederá a volcarlos a un punto donde un usuario sin privilegios si pueda extraer mediante la opción *pull* de la herramienta *adb*, a continuación, haciendo uso de ella los datos serán volcados en la estación de trabajo.

El presente AVD, ha sido rooteado haciendo uso de la herramienta Magisk. Es sencillo comprobar si un dispositivo ha sido rooteado, basta con lanzar una shell, y emplear la instrucción SU, tras lo cual se pasará del símbolo *$* al símbolo *#*, ver figura 3-41.

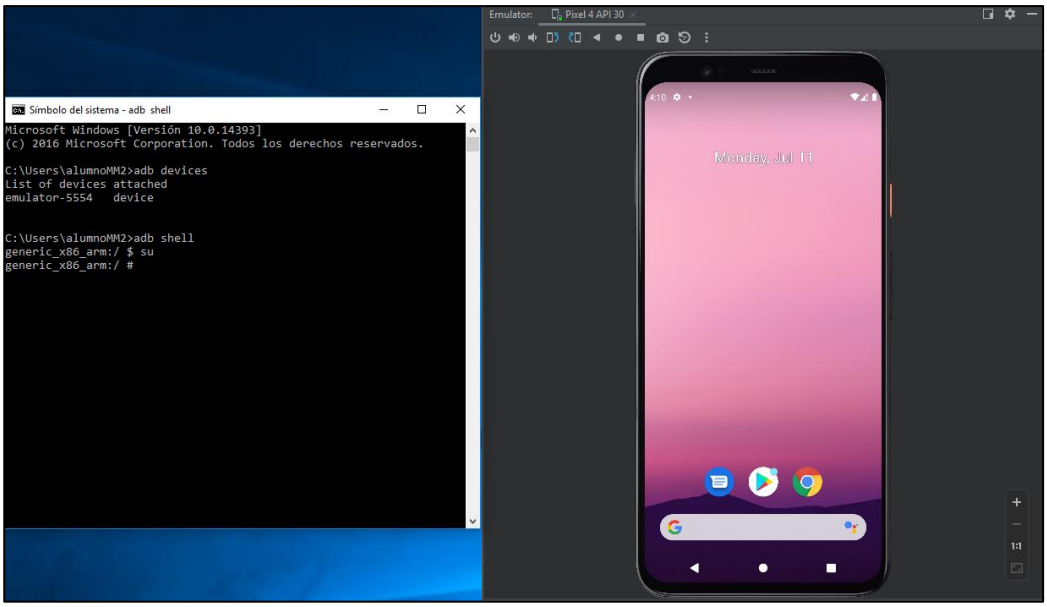


Figura 3-41 Comprobación privilegios root en dispositivo Android

Una vez alcanzado la escalada de privilegios, es posible ver todas las aplicaciones instaladas en el dispositivo inspeccionando el directorio /DATA/DATA. Para ello, basta con navegar hasta dicho directorio, y ejecutar el comando LS, ver figura 3-42.

```
C:\Users\alumnoMM2>adb shell
generic_x86_arm:/ $ su
generic_x86_arm:/ # ls
acct        d             etc             mnt       sdcard
apex        data          init            odm       storage
bin         data_mirror   init.environ.rc oem       sys
bugreports  debug_ramdisk linkerconfig    proc      system
cache       default.prop  lost+found      product   system_ext
config      dev           metadata        res       vendor
generic_x86_arm:/ # cd /data/data
generic_x86_arm:/data/data # ls
android
android.auto_generated_rro_product__
com.android.backupconfirm
com.android.bips
com.android.bips.auto_generated_rro_product__
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.bookmarkprovider
com.android.calllogbackup
com.android.camera2
com.android.carrierconfig
com.android.carrierconfig.auto_generated_rro_product__
com.android.carrierdefaultapp
com.android.cellbroadcastreceiver
com.android.certinstaller
com.android.chrome
com.android.companiondevicemanager
com.android.contacts
com.android.cts.ctsshim
```

Figura 3-42 Comando LS sobre directorio /DATA/DATA

Sin embargo, desde un punto de vista forense, interesa un fichero más "idóneo" para ser anexado en un informe forense, por ello, se recurrirá al fichero */data/system/packages.list.* Este archivo, puede ser extraído copiándolo en una localización accesible por la herramienta pull, como es el caso de /sdcard, o copiando su contenido en un nuevo fichero .list, ver figura 3-43.

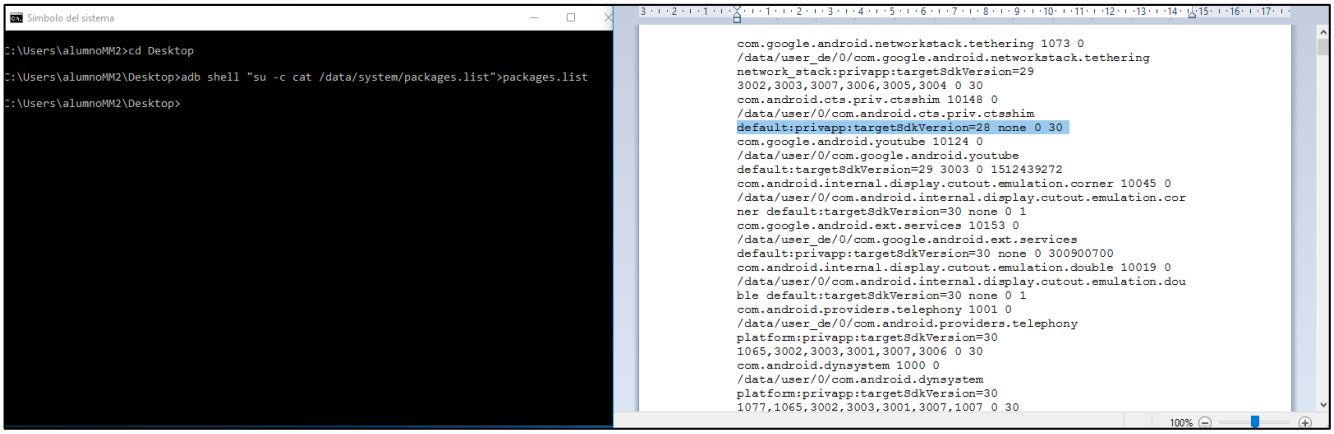


Figura 3-43 Volcado del fichero *packages.list.*

Junto con el anterior archivo, resulta de gran interés el fichero: package-usage.list, ver figura 3-44, el cual como su propio nombre indica, permite conocer el último uso dado a cada una de las aplicaciones instaladas. Este fichero no es la "verdad absoluta" pues refleja si la aplicación ha sido actualizada o a enviado alguna notificación, lo cual no implica su uso por parte del usuario.

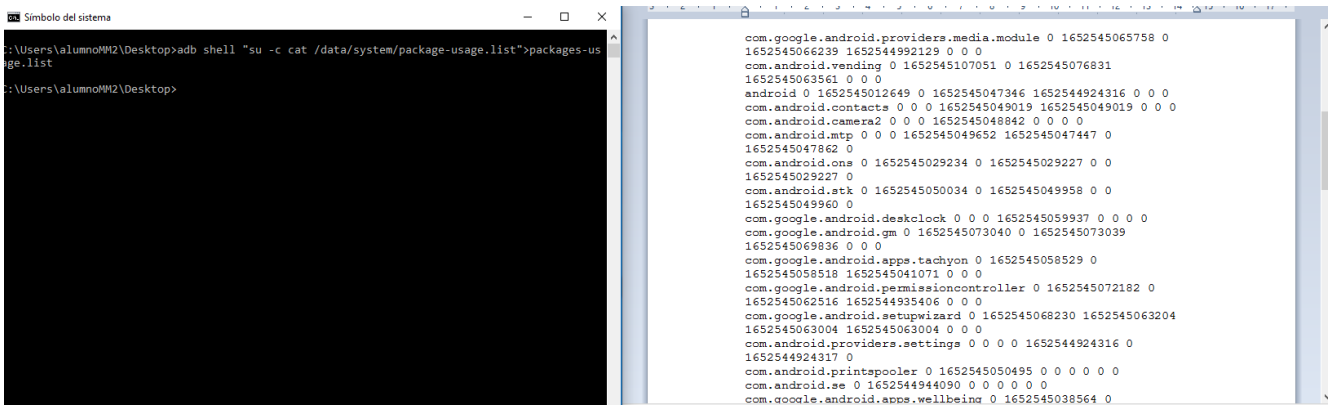


Figura 3-44 Volcado del fichero *package-usage.list*

No en todas las ocasiones, será viable poder volcar directamente cierta información a una localización en la estación de trabajo. A veces es preciso, relocalizar las evidencias a puntos accesibles por el comando *pull*, como es el caso de una tarjeta SD esterilizada procedente del analista forense, en determinadas circunstancias no es posible una opción alternativa, por todo ello, se reitera la importancia de documentar cada paso realizado.

En esta ocasión se van a generar una serie de entradas en el listín telefónico del AVD, ver figura 3-45, tras lo cual se extraerán ciertas evidencias que permitirán analizar los datos procedentes del listín.

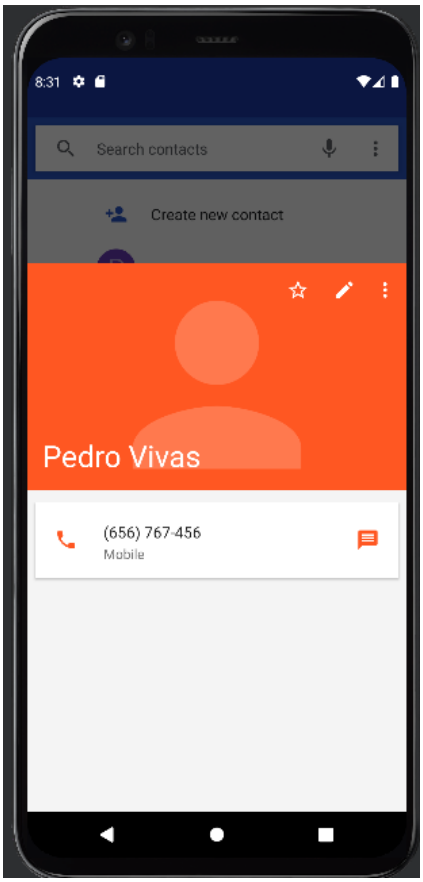


Figura 3-45 Entrada en el listín del AVD.

Se procede a copiar, con privilegios, el archivo *contacts2.db* en el directorio */storage/Nº-Nº/Documents*, el cual forma parte de la tarjeta SD del analista, ver figura 3-46. A continuación, a través del comando *pull* se volcará a la estación de trabajo, ver figura 3-47.

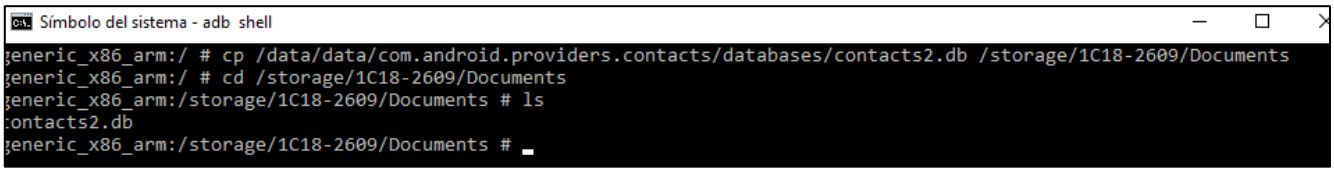


Figura 3-46 Copia del archivo *contacts2.db* en tarjeta SD.

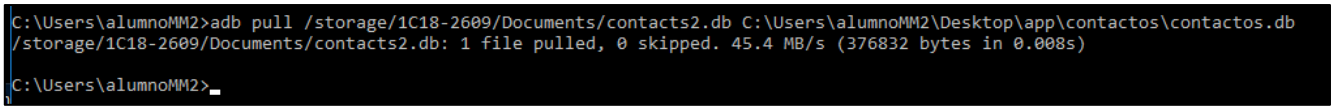


Figura 3-47 Volcado del archivo de contactos de la tarjeta SD a la estación de trabajo.

Una vez que se dispone del fichero en el laboratorio forense, se procede a analizarlo a través de la aplicación DB BROWSER (SQLite), ver figura 3-48.

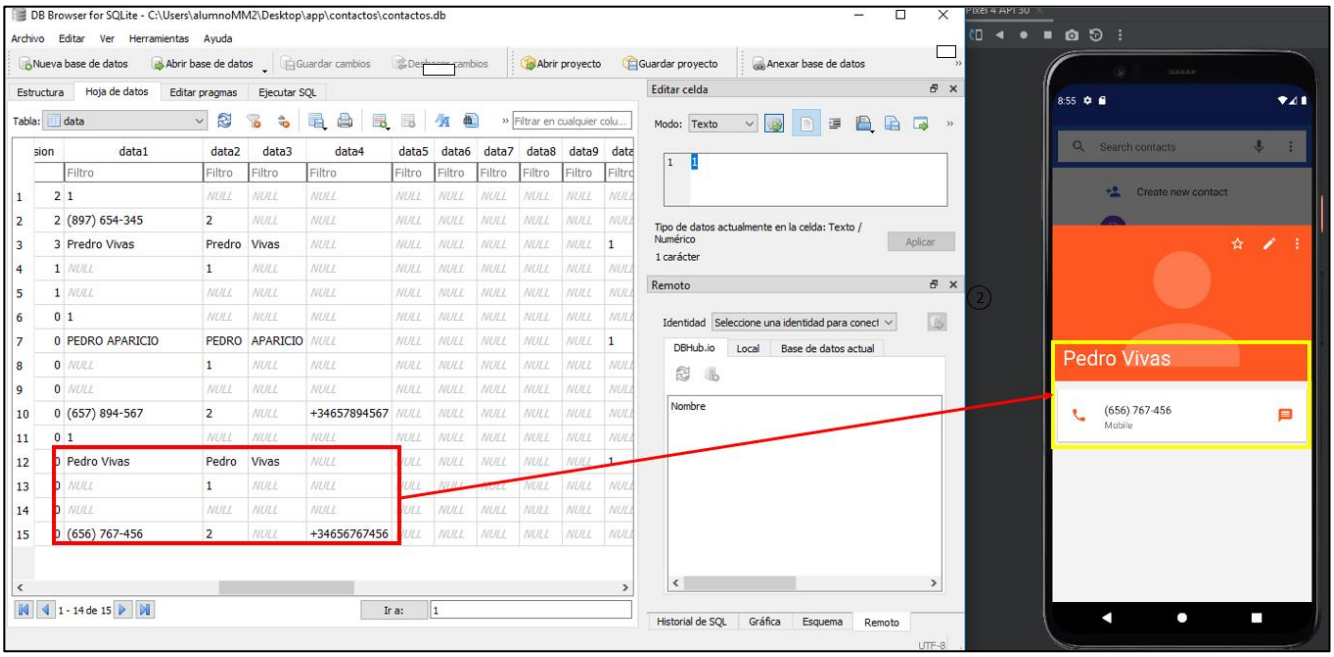


Figura 3-48 Análisis del listín telefónico de un dispositivo Android

3.3 Metodología basada en talleres

Una vez conocidas las bases que conforman el análisis forense sobre dispositivos Android, así como los elementos y herramientas que definen un laboratorio forense de esta índole, se introducirá en el presente apartado las bases comunes que van a constituir una serie de talleres prácticos, dirigidos a consolidar y adquirir cierto nivel de habilidad en la presente rama del análisis forense digital, así como sentar unas bases para materializar una formación en este ámbito.

Se desarrollarán un total de tres talleres de trabajo, en los subsiguientes capítulos del TFM, con diversidad de objetivos y herramientas. A continuación, se describirán con detalle los diferentes apartados que van a definir cada uno de ellos:

- Objetivos del taller: En este apartado, se van a numerar la finalidad perseguida para el presente taller.
- Conocimientos previos requeridos: Cada uno de los talleres implica unas ciertas bases previas, necesarias para una adecuada resolución y cumplimiento de los objetivos descritos en el apartado anterior.
- Preparación del taller: En este apartado se indicarán las necesidades software y hardware requeridas para una adecuada resolución. Se identificará el hardware con cierto nivel de detalle, así como las versiones del software requerido.

- Guía del estudiante: Constituye el enunciado del caso práctico. En él se presentará el taller al estudiante, así como los pasos que debe realizar, junto con los entregables solicitados por el profesorado.
- Resolución del taller para el docente: Se resolverán completamente y con gran nivel de detalle descriptivo, los diferentes talleres, con la finalidad de demostrar el cumplimiento de los objetivos descritos y la factible resolución de los mismos.
- Discusión del taller: cada práctica irá acompañado de un apartado de conclusiones, que busca plantear una serie de cuestiones al estudiante, con el objeto de facilitar una reflexión sobre las distintas lecciones aprendidas.

En los sucesivos tres capítulos se desarrollarán tres talleres, con una distribución de apartados descrita en el párrafo anterior. El primer taller se centrará en la memoria interna/ tarjeta SD de un dispositivo móvil, es segundo estará focalizado en herramientas de adquisición sin privilegios root sobre el dispositivo, por último, el tercer taller mostrará las principales *artifacs* derivados de algunas conocidas aplicaciones móviles.

4 ANÁLISIS DE UNA TARJETA SD/ALMACENAMIENTO INTERNO

4.1 Objetivos

El presente taller estará centrado, en la adquisición lógica, preservación y análisis de información contenida en un dispositivo Android, a continuación, se enumerarán los objetivos que lo fundamentan:

- Familiarizarse con el adiestramiento forense a través de un dispositivo real.
- Familiarizarse con el empleo de la herramienta ABD.
- Profundizar en el sistema de ficheros Android.
- Efectuar adquisición lógica de información contenida en una tarjeta SD/almacenamiento interno.
- Identificar las ventajas e inconvenientes de este tipo de adquisición.

4.2 Conocimientos previos

Para el correcto aprovechamiento del desarrollo del taller, el alumno precisará de una serie de conocimientos previos:

- Conocer el concepto de análisis forense digital, y más concretamente centrado en dispositivos móviles.
- Tener un conocimiento básico de las fases que conforman el análisis tanto digital, como en el caso concreto de dispositivos móviles.
- Conocer el concepto de evidencia digital, así como las características que lo singularizan de otro tipo de información digital.
- Conocer los principales *artifacs* asociados a un dispositivo Android.
- Conocer de manera básica la herramienta ABD, y su opción PULL.
- Disponer de un conocimiento básico del sistema de ficheros Linux, así como de sus instrucciones principales.
- Disponer de un conocimiento básico del sistema de ficheros Android, más concretamente de los directorios asociados al *sdcard.*

4.3 Preparación

En el presente taller, cada alumno dispondrá de las siguientes herramientas para la resolución de los ejercicios:

- Terminal de usuario: 512 GB disco duro, 16 GB RAM, Sistema operativo Windows 10/11de 64 bits.
- Hipervisor VMware Player 16
- Máquina virtual Windows 10 (laboratorio forense)
    - Reserva de 8 GB en la VM
    - Android Studio
    - Herramienta ADB
    - AVD generada a través de la herramienta Android Studio
- Dispositivo Android físico

El teléfono móvil dispondrá de una serie de fotografías a modo de evidencias digitales.

4.4 Guía del estudiante

En el presente apartado se procederá a enunciar el ejercicio al estudiante, así como describir los diferentes pasos requeridos para su resolución, junto con ello se le indicará el entregable del taller.

La información anteriormente descrita, que será entregada al estudiante se dividirá en una serie de apartados.

4.4.1 Descripción preliminar del incidente

El director de la empresa STARK S.L, Anthony Timothy Stark, ha contactado con nuestra empresa de análisis forense digital, debido a que tiene ciertas sospechas de que uno de sus empleados a fotografiado información, de nivel de clasificación SECRETO, de las estaciones de trabajo.

En los periodos laborales, y dentro de las oficinas, está prohibido el empleo de teléfonos móviles personales. Sin embargo, gracias a las cámaras de seguridad, se ha visto a un empleado fotografiando la pantalla de su PC, así como el empleo reiterado de su dispositivo personal en horario laboral.

Tras conseguir los permisos legales necesarios, se ha podido tener acceso al propio dispositivo, un SAMSUNG J3 de 2017, el cual por obligación expresa del juez, no podrá ser rooteado.

Se ha sufrido un robo de información, para la resolución del caso podemos ir resolviendo una serie de cuestiones:

- ¿De qué accesos no root disponemos?
- ¿Qué datos de interés podemos extraer del dispositivo? ¿IMEI, nº de tlf…?
- ¿Cuáles son los directorios de interés accesibles a un usuario sin privilegios?
- ¿marcas de tiempo de los ficheros de interés?

4.4.2 Evaluación

Como resultado deberéis entregar un informe pericial de vuestras pesquisas, en él debe verse reflejado lo siguiente:

- Versionado de las herramientas empleadas en el laboratorio forense.
- Descripción detallada, con capturas de pantalla, de todos los pasos dados.
- Cálculo de hashes de todas las evidencias adquiridas.
- Conclusiones, donde se indicará si se considera que el dueño del dispositivo robó información clasificada de la empresa STARK S.L.

4.5 Resolución para el profesor

En el presenta apartado, se materializará la resolución del taller desde el punto de vista del profesor, cumpliendo todos los requisitos demandados al alumno, comprobando una resolución viable y un cumplimiento de los objetivos descrito de manera eficaz.

En primer lugar, se indicarán las herramientas, junto con sus versiones:

- Hipervisor VMware WorkStation Player 16: 16.2.4 build-20089737.
- VM WINDOWS 10 (laboratorio forense) pro Enterprise edition: WINDOWS 10 ENTERPRISE EDITION 2016 LTSB, 1607.
- ANDROID DEBUG BRIDGE:1.0.41.
- MULTIHASHER: 2.8.2

A continuación, se presentará un pequeño reportaje fotográfico del dispositivo del sospechoso, ver figuras 4-1 y 4-2:

Figura 4-1 Dispositivo Android fotografía 1

Figura 4-2 Dispositivo Android fotografía 2

Seguidamente iniciamos nuestro laboratorio forense, y con él una consola de comandos para el empleo de la herramienta ADB, ver figura 4-3:

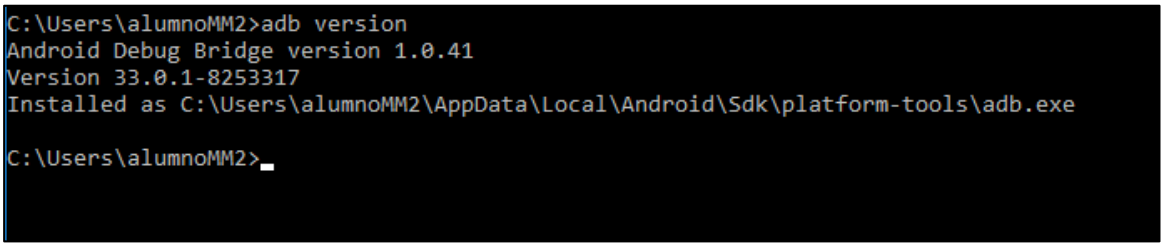


Figura 4-3 Herramienta ABD utilizada durante el caso práctico

A continuación, se procederá a conectar el dispositivo al laboratorio forense, ver figura 4-4, haremos uso de su propio cable original de carga y transmisión de datos. Para un posible acceso, el dispositivo debe estar desbloqueado, activado el depurador por USB y autorizar la depuración por USB, en este último mensaje se nos indicará la huella digital de la clave RSA.

Figura 4-4 Verificación del acceso al dispositivo

El siguiente paso será obtener y almacenar en nuestro laboratorio forense información de interés relativa al dispositivo y al usuario, lo cual nos permite crear una identidad asociada al dispositivo.

En primer lugar, se obtendrá el IMEI del dispositivo, lo cual se volcará en un txt y almacenaremos en nuestro laboratorio, ver figuras 4-5 y 4-6:

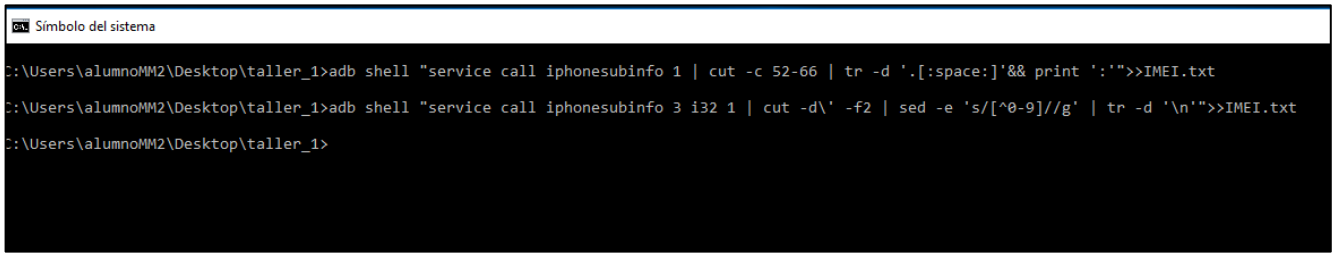


Figura 4-5 Obtención y volcado de ambos nº IMEI del dispositivo

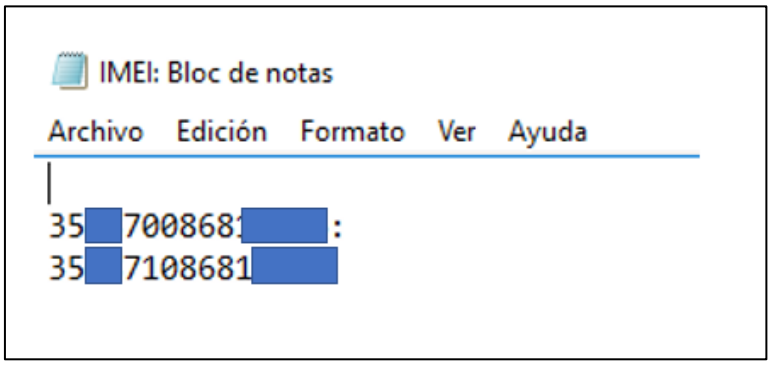


Figura 4-6 IMEI del dispositivo

Continuado con datos procedentes del dispositivo, obtendremos la versión del sistema operativo Android instalado en el dispositivo, ver figura 4-7, recordemos que esto es importante, pues hay ciertos cambios entre las distintas versiones:

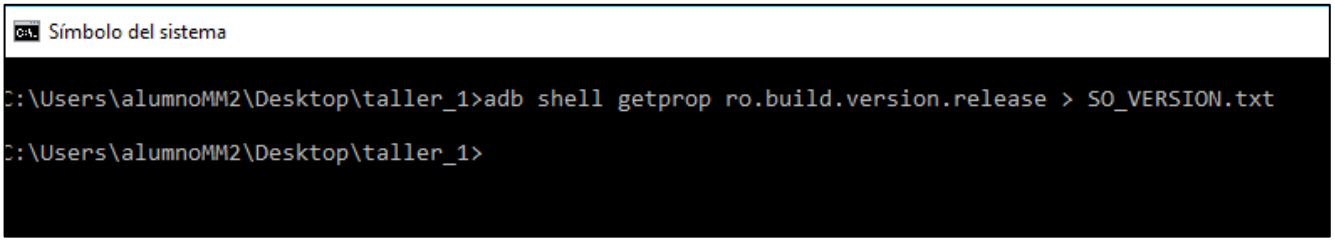


Figura 4-7 Obtención de la versión del SO Android

A mayores se buscará información relativa al usuario, ver figura 4-8, empleando la herramienta dumpsys:

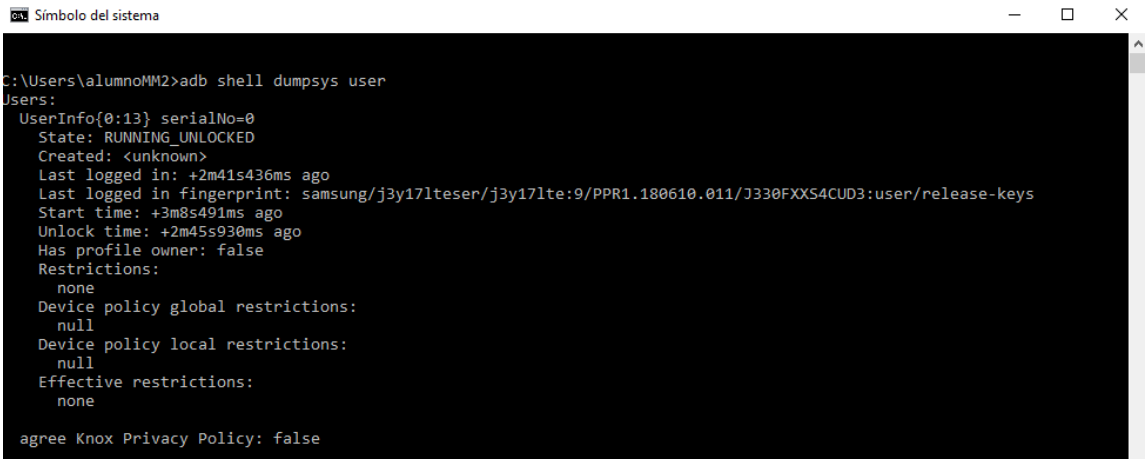


Figura 4-8 Datos del usuario a través de dumpsys

Puede verse como el último inicio de sesión se ha producido hace 2 minutos, lo cual demuestra que el dispositivo ha sido apagado hace poco tiempo. Resulta fundamental preservar toda información extraída, ver figura 4-9, por ello se volcará a un fichero de texto:

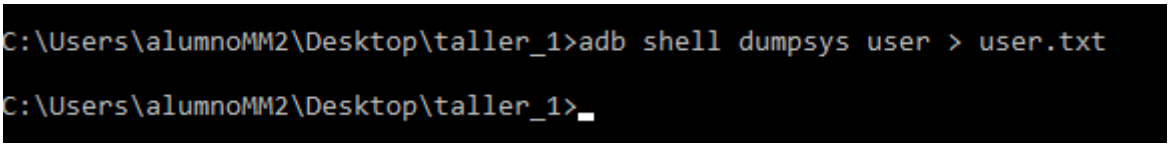


Figura 4-9 Volcado de la información del usuario a un archivo *txt*

A mayores es posible comprobar el número del teléfono asociado a la tarjeta SIM, a través de la instrucción *iphonesubinfo*,ver figura 4-10 , la cual también volcaremos como evidencia:

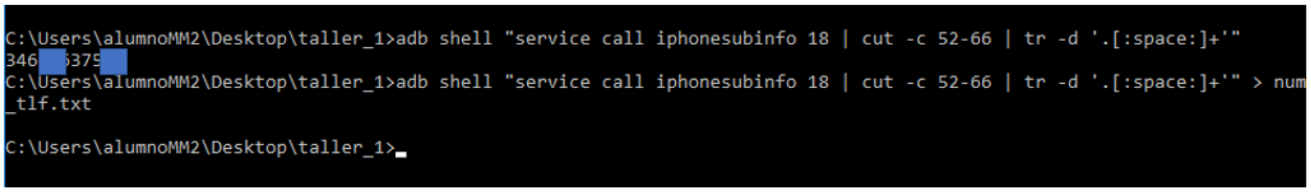


Figura 4-10 Extracción y volcado del número de teléfono

Llegados a este punto se va a proceder a calcular el hash de las diferentes evidencias extraídas, y a realizar una copia de las mismas, asegurando la preservación de los ficheros, para ello se hará uso de la herramienta multihasher, ver figura 4-11.

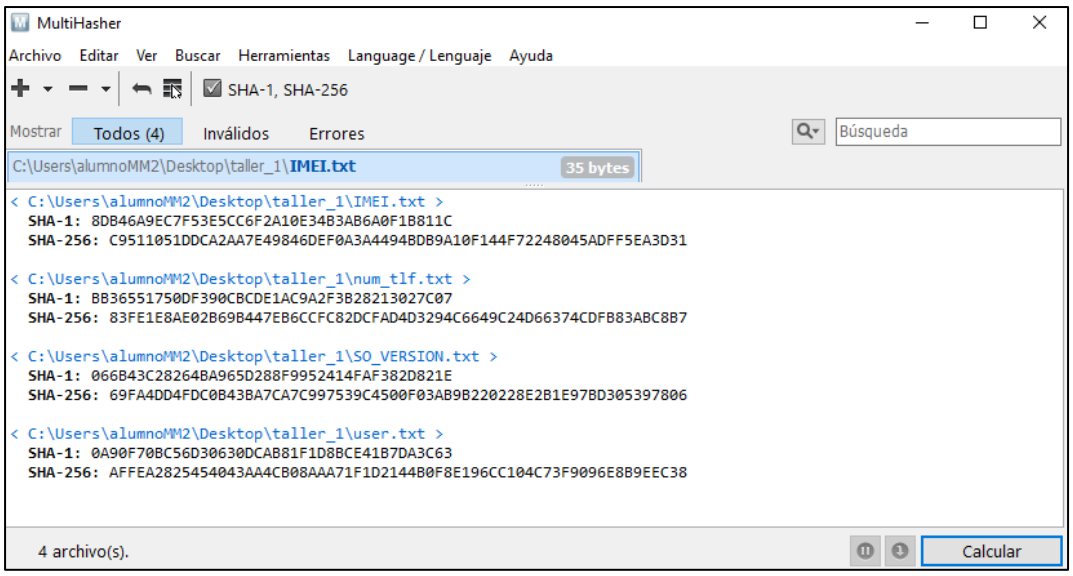


Figura 4-11 Cálculo de hashes con MULTIHASHER

A continuación, se buceará por el almacenamiento interno/tarjeta SD, ver figura 4-12, buscando evidencias que puedan aportar luz a la investigación sobre el sospechoso.

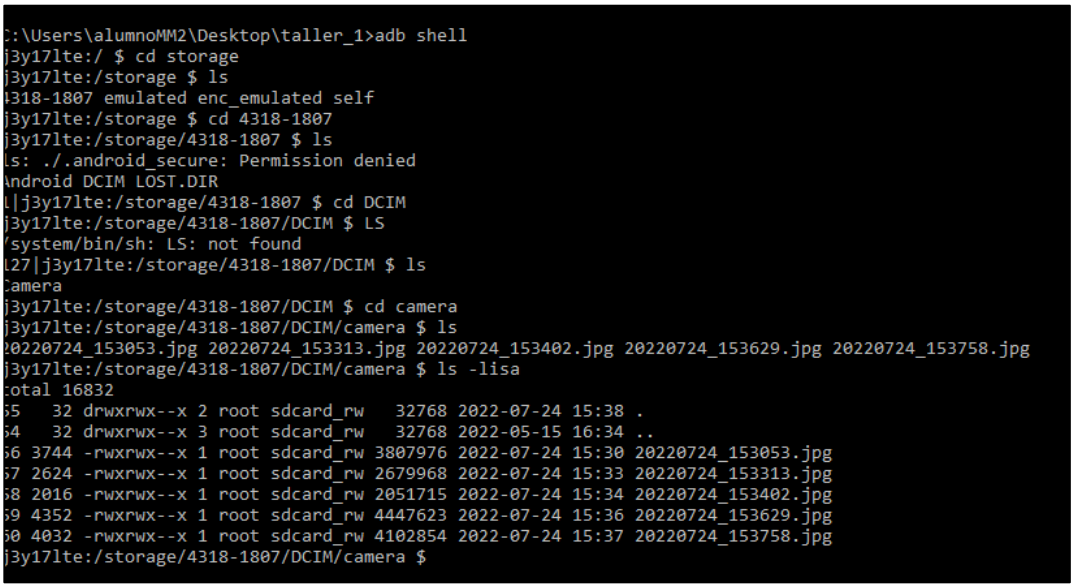


Figura 4-12 Búsqueda de evidencias en la tarjeta SD del dispositivo

Es posible ver la fecha de última modificación: 24-07-22, dato que podría verificarse con las imágenes de las cámaras del circuito cerrado de televisión. A mayores podemos ver los tiempos MAC, ver figura 4-13, de cada fotografía:

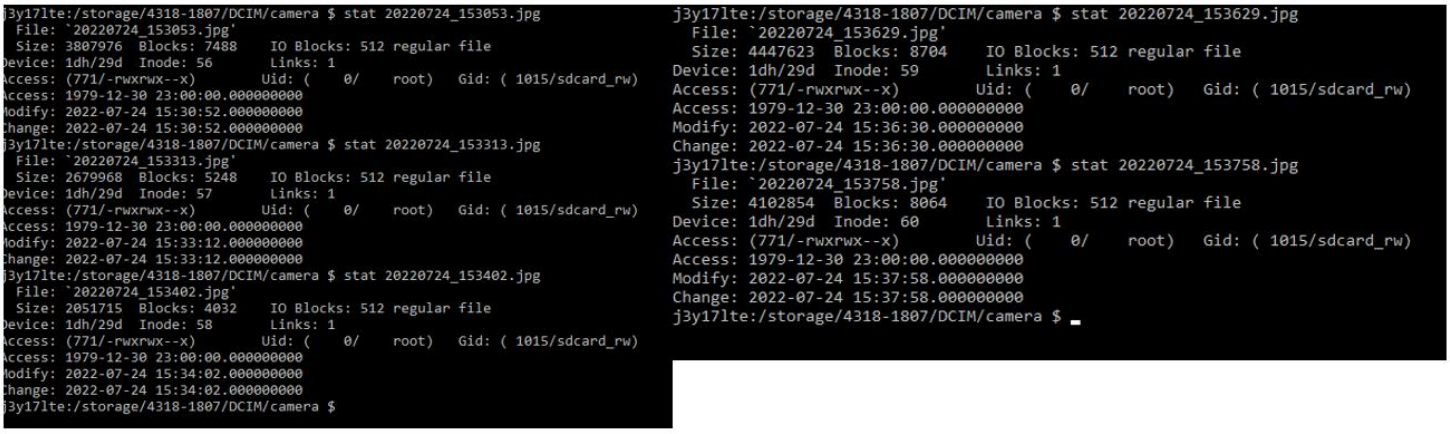


Figura 4-13 Tiempos MAC de los ficheros localizados en la tarjeta SD

Seguidamente se procede a su volcado, ver figura 4-14, a través de la herramienta *PULL*, almacenándolos en el laboratorio forense:

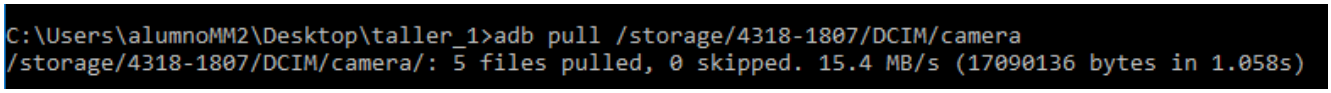


Figura 4-14 Volcado del directorio *camera* en el laboratorio forense

A través de la herramienta *MULTIHASHER* se calcula el hash de las evidencias extraídas, ver figura 4-15, y se realiza una copia de las mismas:

```
< C:\Users\alumnoMM2\Desktop\taller_1\camera\20220724_153053.jpg >
  SHA-1: 5C6E002BCCF8626E081735B1810B5E52265D27DF
  SHA-256: 8A12E369ECCA72558A730AE53427A7B81053AB7B533E0B4F91D4ECDA4A79CBBC

< C:\Users\alumnoMM2\Desktop\taller_1\camera\20220724_153313.jpg >
  SHA-1: C03369CCCEFCA3E91A3E00AC672368FDA16637B6
  SHA-256: 0C614DA733416A1C960857808045096B95E6A7D9101B262CC72E41796D7F5DA1

< C:\Users\alumnoMM2\Desktop\taller_1\camera\20220724_153402.jpg >
  SHA-1: 39ECB6D32CF6351A580551A4515F0D8DEBB8686C
  SHA-256: 976C4B891798A66C0571A4981BC5ACB83FD762FD330B3161B75D1C708530085A

< C:\Users\alumnoMM2\Desktop\taller_1\camera\20220724_153629.jpg >
  SHA-1: 695F7BF9BC0DD6102076A28752022F6B9557E2A7
  SHA-256: 44D311CED408BC2EB8D4292AC412C3A54E5B80FE8A16AFBE988FCBA9ED48BABE

< C:\Users\alumnoMM2\Desktop\taller_1\camera\20220724_153758.jpg >
  SHA-1: CFE11980B1CC35442B7F15CFE075CFF1E3BDD10C
  SHA-256: 034290C9DC923B3735D4C259AFC7F35751BAEBD11450A4A841BA0587D30E159A
```

Figura 4-15 Cálculo del HASH de los ficheros localizados en el directorio *camera* del dispositivo móvil

Sobre las copias realizada se comprueba su contenido, ver figura 4-16, permitiendo verificar si se ha obtenido información clasificada del dispositivo:

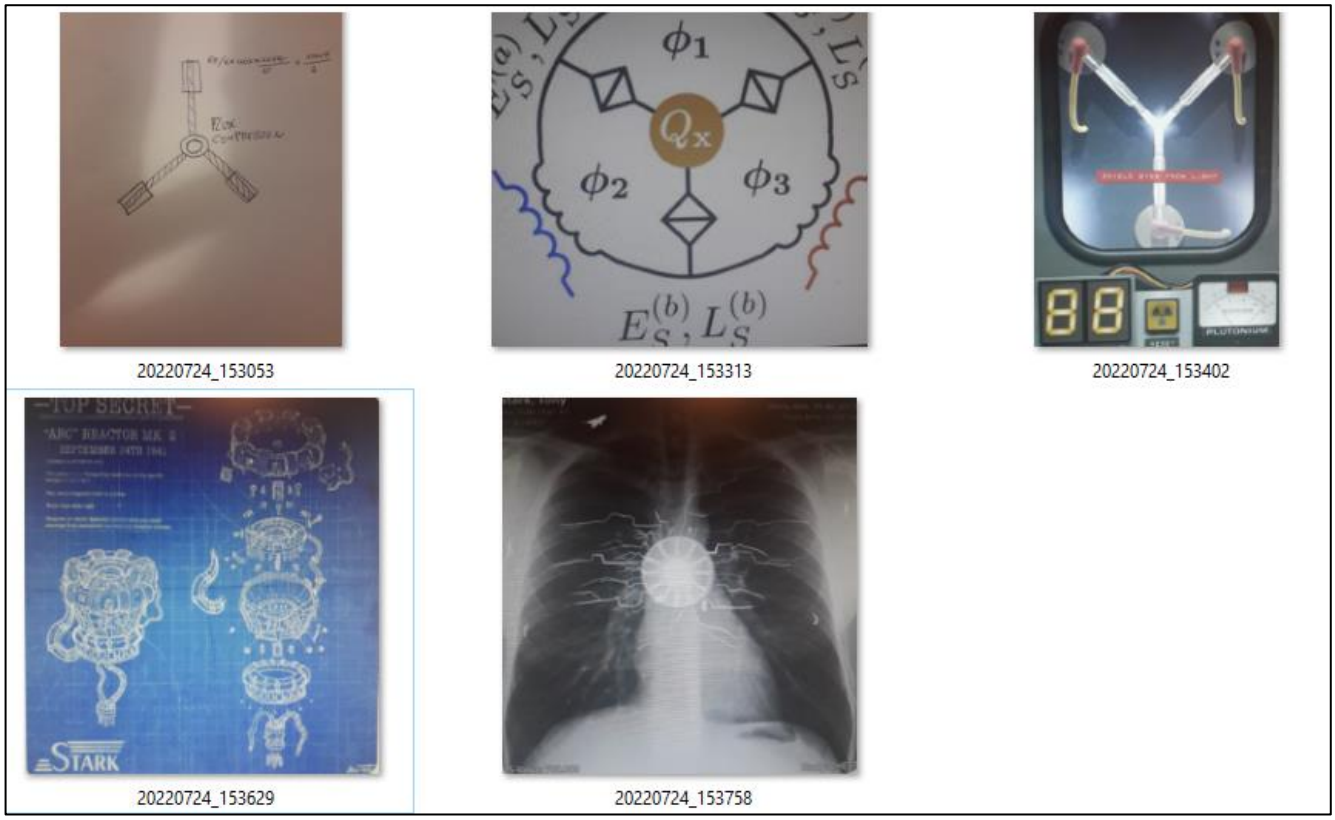


Figura 4-16 Imágenes encontradas en el dispositivo del sospechoso.

En último lugar, se esperan una serie de conclusiones que el estudiante debe extraer de la práctica realizada, este apartado es completamente libre, sin embargo, hay ciertos elementos que se esperan:

- El acceso a través de la herramienta ABD implica el desbloqueo del dispositivo.
- Este método se restringe únicamente a los accesos que un usuario habitual tiene permitido.
- Al no ser una adquisición física no pueden localizarse archivos borrados.

Las limitaciones de este método son evidentes, sin embargo, datos como los tiempos MAC y la extracción de evidencias procedentes del dispositivo, así como el volcado de información de interés, permite disponer de una serie de herramientas básicas para un futuro informe pericial.

4.6 Discusión

Los dispositivos móviles constituyen auténticos "diarios" de todas nuestras acciones. Disponer de acceso a las distintas particiones asociadas al dispositivo permite un conocimiento muy amplio del usuario del mismo.

En el presente taller, se pretende familiarizarse con el acceso al dispositivo a través de la herramienta *ABD*, así como adquirir buenas prácticas en el trato de todas las evidencias, con todo ello podemos hacernos las siguientes preguntas.

¿Podemos verificar que el sospechoso es el dueño del dispositivo con la información extraída?

¿Es posible asegurar que fue él quien realizó las fotografías?

¿Se le puede condenar por ello?

¿Podemos asegurar que las fotografías fueron realizadas en el momento en el que el sospechoso fue capturado por las cámaras de vigilancia?

¿Cuántos permisos se precisa que el dispositivo conceda para este tipo de adquisiciones?

No debemos olvidar, que los analistas forenses no buscan incriminar o dar opinión sobre la comisión de un delito, sino proporcionar herramientas o evidencias que permitan extraer conclusiones verídicas en un proceso judicial.

5 EMPLEO DE HERRAMIENTAS *NO ROOT*

5.1 Objetivos

El presente taller estará centrado, en la adquisición lógica, preservación y análisis de información contenida en un dispositivo Android, a continuación, se enumerarán los objetivos que lo fundamentan:

- Familiarizarse con el adiestramiento forense a través de un dispositivo real.
- Familiarizarse con el empleo de la herramienta ADB.
- Profundizar en el sistema de ficheros Android.
- Familiarizarse con la opción ADB, *dumpsys*.
- Familiarizarse con la opción ADB, *backup.*
- Familiarizarse con la herramienta de adquisición lógica *helium.*
- Identificar y analizar los principales *artifacs* adquiridos con las anteriores herramientas.
- Identificar las ventajas e inconvenientes de este tipo de adquisición.

5.2 Conocimientos previos

Para el correcto aprovechamiento del desarrollo del taller, el alumno precisará de una serie de conocimientos previos:

- Conocer el concepto de análisis forense digital, y más concretamente centrado en dispositivos móviles.
- Tener un conocimiento básico de las fases que conforman el análisis tanto digital, como en el caso concreto de dispositivos móviles.
- Conocer los principales *artifacs* asociados a un dispositivo Android.
- Conocer el concepto de evidencia digital, así como las características que lo singularizan de otro tipo de información digital.
- Estar familiarizado con el empleo de un AVD, así como su generación a través de la herramienta *Android Studio.*
- Conocer de manera básica la herramienta ABD, junto con su opción DUMPSYS y BACKUP.
- Conocer de manera básica la herramienta HELIUM, así como las opciones que ofrece.

- Disponer de un conocimiento básico del sistema de ficheros Linux, así como de sus instrucciones principales.
- Disponer de un conocimiento básico del sistema de ficheros Android.

5.3 Preparación del taller

En el presente taller, cada estudiante dispondrá de las siguientes herramientas para la resolución de los ejercicios:

- Terminal de usuario: 512 GB disco duro, 16 GB RAM, Sistema operativo Windows 10/11de 64 bits.
- Hipervisor VMware Player 16.
- Máquina virtual Windows 10 (laboratorio forense).
  - Reserva de 8 GB en la MV.
  - Android Studio.
  - Herramienta ADB.
- Dispositivo Android físico con aplicación helium instalada.

El teléfono móvil dispondrá de una serie de fotografías, así como de llamadas y SMS realizados desde el dispositivo a modo de evidencias.

5.4 Guía del estudiante

En el presente apartado se procederá a enunciar el ejercicio al estudiante, así como describir los diferentes pasos requeridos para su resolución, junto con ello se le indicará el entregable del taller.

La información anteriormente descrita, que será entregada al estudiante se dividirá en una serie de apartados:

5.4.1 Descripción preliminar del incidente

El director de la empresa STARK S.L, Anthony Timothy Stark, ha contactado con nuestra empresa de análisis forense digital, debido a que tiene ciertas sospechas de que uno de sus empleados a fotografiado información de clasificación SECRETO de las estaciones de trabajo, a mayores se tienen fuertes sospechas de haber contactado con la empresa rival INDUSTRIAS HUMMER S.L.

En los periodos laborales, y dentro de las oficinas, está prohibido el empleo de teléfonos móviles personales. Sin embargo, gracias a las cámaras de seguridad, se ha visto a un empleado fotografiando la pantalla de su PC, así como el empleo reiterado de su dispositivo personal en horario laboral.

Tras conseguir los permisos legales necesarios, se ha podido tener acceso al propio dispositivo, un SAMSUNG J3 de 2017, el cual por obligación expresa del juez, no podrá ser rooteado.

Se ha sufrido un robo de información, para la resolución del caso podemos ir resolviendo una serie de cuestiones:

- ¿De qué accesos no root disponemos?
- ¿Qué datos de interés podemos extraer del dispositivo? ¿IMEI, nº de teléfono…?
- ¿Podemos verificar el empleo del dispositivo en el entorno laboral?
- ¿Cuáles son los directorios de interés accesibles a un usuario sin privilegios?
- ¿existe alguna herramienta que permita volcar la información accesible no root, del dispositivo?
- ¿Marcas de tiempo de los ficheros de interés?
- ¿Es posible acceder a información sobre llamadas y SMS?

- ¿Se puede trazar una línea de tiempo sobre los principales eventos?

5.4.2 Evaluación

Como resultado deberéis entregar un informe pericial de vuestras pesquisas, en él debe verse reflejado lo siguiente:

- Versionado de las herramientas empleadas en el laboratorio forense.
- Descripción detallada, con capturas de pantalla, de todos los pasos dados.
- Cálculo de hashes de todas las evidencias adquiridas.
- Conclusiones, donde se indicará si se considera que el dueño del dispositivo robó información clasificada de la empresa STARK S.L, así como su posible contacto con la empresa INDUSTRIAS HUMMER S.L.

5.5 Resolución del profesor

En el presente apartado, se materializará la resolución del taller desde el punto de vista del profesor, cumpliendo todos los requisitos demandados al estudiante, comprobando una resolución viable y un cumplimiento de los objetivos descrito de manera eficaz.

En primer lugar, se indicarán las herramientas, junto con sus versiones:

- Hipervisor VMware WorkStation Player 16: 16.2.4 build-20089737.
- VM WINDOWS 10 (laboratorio forense) pro Enterprise edition: WINDOWS 10 ENTERPRISE EDITION 2016 LTSB, 1607.
- ANDROID DEBUG BRIDGE:1.0.41.
- MULTIHASHER: 2.8.2
- Herramienta HELIUM: 1.1.4.6
- JAVA: 1.8.0_341
- ANDROID BACKUP TOOLKIT

En primera instancia se presentará un breve reportaje fotográfico del dispositivo incautado del sospechoso ver figuras 5-1 y 5-2:

Figura 5-1 Fotografía dispositivo Android 1

Figura 5-2 Fotografía dispositivo Android 2

A continuación, siguiendo en la línea de la guía del estudiante se obtendrá una serie de información de interés forense relativa al dispositivo, desde los números IME, ver figura 5-3, pasando por la verificación del teléfono asociado a la tarjeta SIM, y la posible verificación del empleo del dispositivo móvil en el entorno laboral.

En primer lugar, se volcará el IMEI asociado al dispositivo:

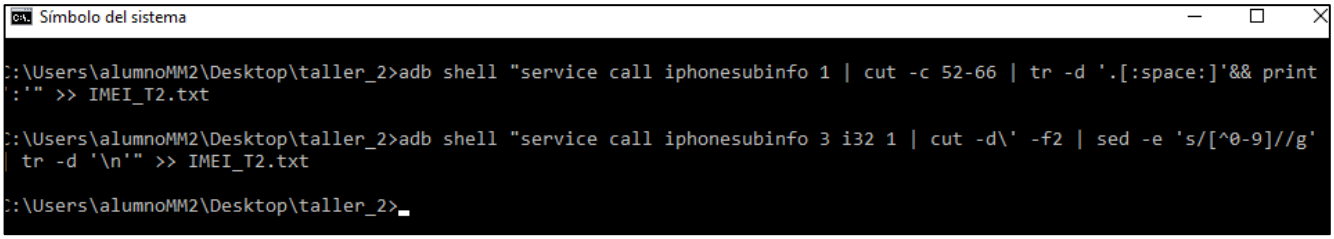


Figura 5-3 Volcado IMEI.

Con esta información se podrá identificar el dispositivo GSM a nivel mundial, dato que es trasmitido por el propio dispositivo al conectarse a una red, ver figura 5-4.

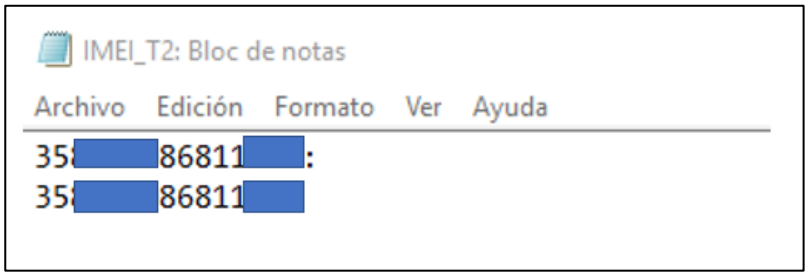


Figura 5-4 Nº IMEIs del dispositivo

El siguiente dato que se va a volcar es la versión del SO del dispositivo, ver figuras 5-5 y 5-6, este dato es de gran interés pues existen ciertas diferencias desde un punto de vista forense entre los diferentes SO de Android:

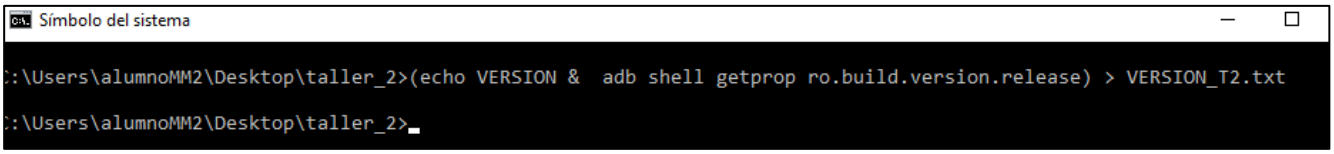


Figura 5-5 Volcado de la versión del SO

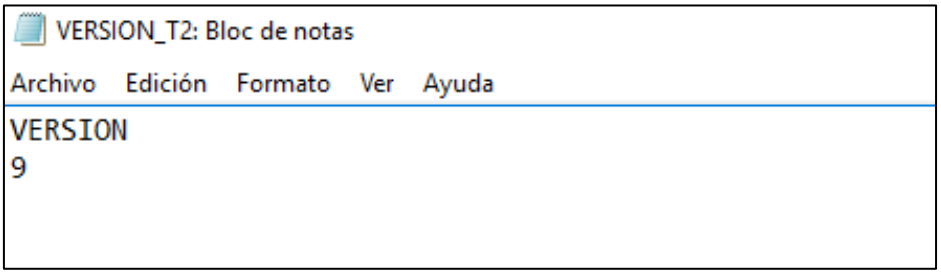


Figura 5-6 Versión del SO del dispositivo

Es posible comprobar que se trata de un Android 9, conocido como PIE, como se ha comentado anteriormente un estudio detallado confirmaría las características de interés forense de las que dispone esta versión de Android.

También resulta de gran interés aquella información que a través de la herramienta edición *dumpsys* se pueda obtener del dispositivo, ver figura 5-7:

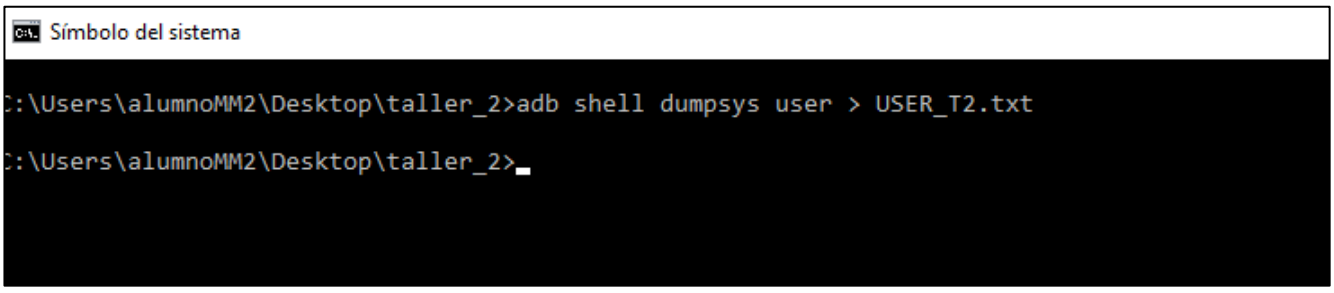


Figura 5-7 Volcado de información relativa a el/los usuarios

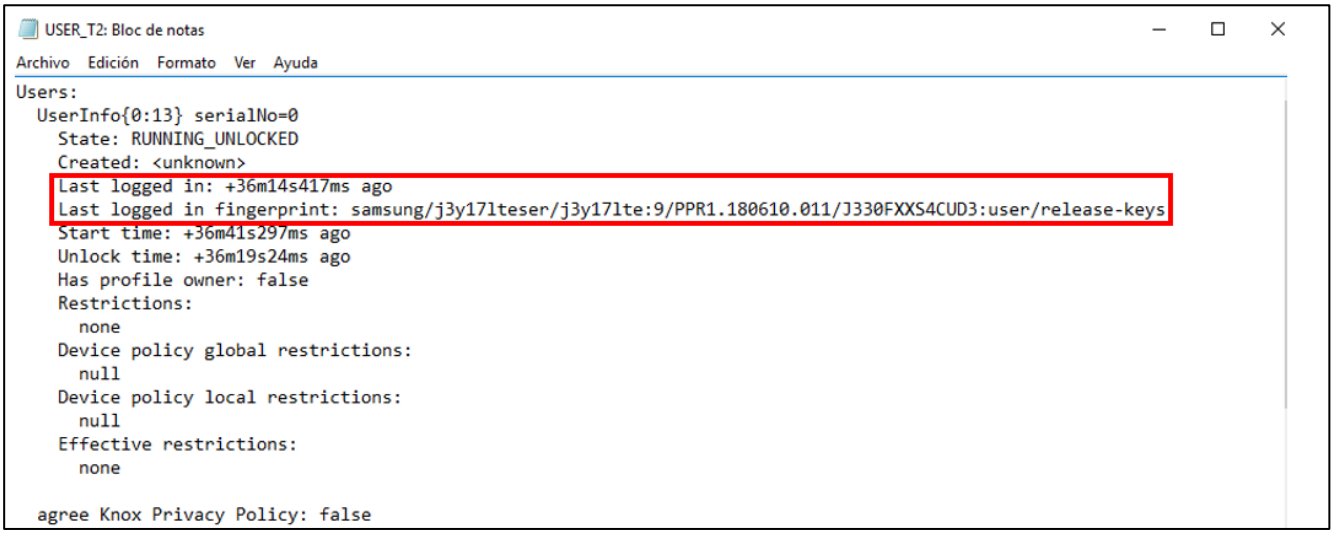


Figura 5-8 Información del ususario a través de la opción user

Del volcado anterior se pueden obtener datos como el último logeo, ver figura 5-8, así como confirmar/ampliar varias características del dispositivo, como la versión del firmware, la versión del SO …

A continuación, se procederá a obtener el número de teléfono asociado a la SIM del dispositivo, ver figuras 5-9 y 5-10:

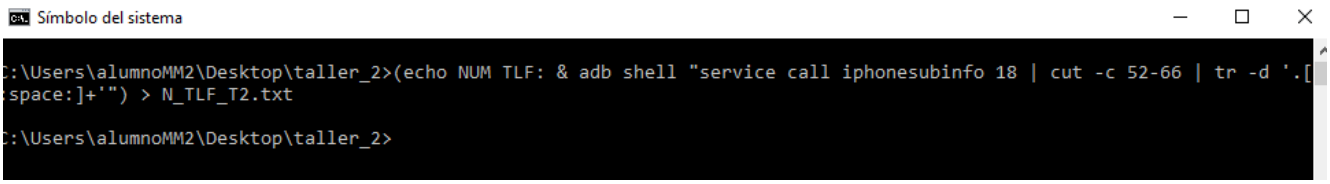


Figura 5-9 Volcado del nº de tlf asociado a la SIM

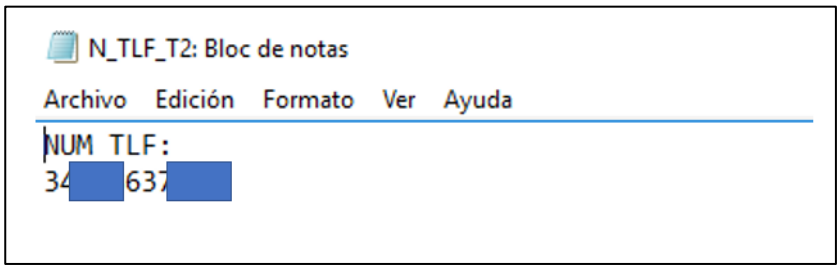


Figura 5-10 Nº teléfono asociado a la SIM del dispositivo

Seguidamente, se entrará en detalle sobre los procesos ejecutados en el dispositivo, en primer lugar, se empleará la opción appops, lo cual nos identificará los permisos asociados a los procesos, ver figura 5-11.

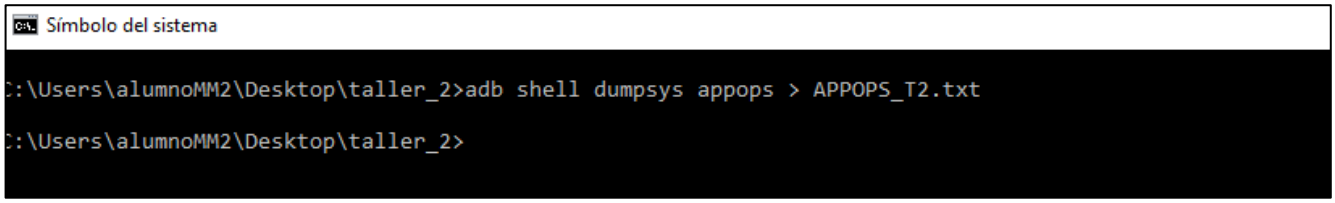


Figura 5-11 Volcado de los datos que ofrece la opción appops

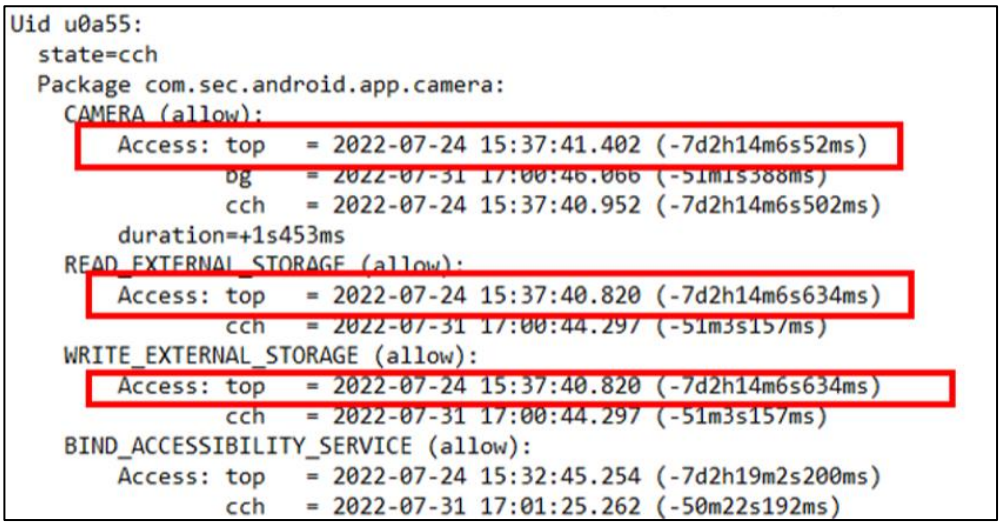


Figura 5-12 Datos del proceso ...camera

A través de APPOPS se obtiene información muy interesante, a través de los permisos dados a los procesos ejecutados en el dispositivo. Destaca en concreto el proceso u0a55, ver figura 5-12, asociado a la cámara, en ella pueden verse una serie de permisos, y junto a ellos, instantes de uso de dichos permisos, como es el caso de WRITE_EXTERNAL_STORAGE el cual nos indica su uso el 24 de julio de 2022, dato que podríamos comparar con los tiempos MAC de las posibles fotografías que se localicen en el dispositivo.

Junto con la opción APPOPS, se empleará PROCSTAT, ver figura 5-13, la cual permitirá visualizar el % de uso del procesador para cada una de las aplicaciones empleadas por el usuario:

```
C:\Users\alumnoMM2\Desktop\taller_2>adb shell dumpsys procstats > PROCSTAT_T2.txt

C:\Users\alumnoMM2\Desktop\taller_2>adb shell dumpsys procstats --HOURS 168 > PROCSTA_168_T2.txt

C:\Users\alumnoMM2\Desktop\taller_2>adb shell dumpsys procstats --hours 168 > PROCSTA_168_T2.txt

C:\Users\alumnoMM2\Desktop\taller_2>adb shell dumpsys procstats --hours 171 > PROCSTA_171_T2.txt

C:\Users\alumnoMM2\Desktop\taller_2>adb shell dumpsys procstats --hours 96 > PROCSTA_96_T2.txt

C:\Users\alumnoMM2\Desktop\taller_2>
```

Figura 5-13 Volcado de la opción PROCSTATS

Para esta opción de *dumpsys*, conviene comparar los distintos porcentajes de empleo del procesador en distintos hitos horarios: actual, últimos 4 días, últimas 7 días, 8 días y 10 días. Aunque no da unos resultados concluyentes si nos permite asentar cierta información obtenida de la opción anterior.

Del empleo de la opción APPOPS obtuvimos un dato temporal de interés, como fue la fecha: 24/07/22, lo cual se trata en horas de más de 168.

Comparando las distintas opciones horarias: actual, últimos cuatro días, últimos 171 horas u últimas dos semanas obtenemos los siguientes datos, ver figuras 5-14, 5-13, 5-14, 5-16 y 5-17:

```
* com.sec.android.app.camera / u0a55 / v900219300:
      TOTAL: 0,03%
    Receiver: 0,03%
    (Cached): 29% (3,6MB-3,9MB-4,6MB/0,00-7,0KB-44KB/0,00-7,0KB-44KB over 7)
```

Figura 5-14 PROCSTATS del momento actual

```
* com.sec.android.app.camera / u0a55 / v900219300:
      TOTAL: 0,20% (64MB-65MB-65MB/30MB-30MB-30MB/0,00-15MB-30MB over 2)
        Top: 0,17% (64MB-65MB-65MB/30MB-30MB-30MB/0,00-15MB-30MB over 2)
    Receiver: 0,02%
 (Last Act): 0,88% (37MB-38MB-39MB/4,4MB-4,5MB-4,5MB/0,00-3,7MB-4,5MB over 6)
    (Cached): 12% (3,6MB-8,3MB-36MB/0,00-417KB-3,5MB/0,00-123KB-1,9MB over 19)
```

Figura 5-15 PROCSTATS de los últimos 4 días

```
* com.sec.android.app.camera / u0a55 / v900219300:
      TOTAL: 0,23% (64MB-65MB-65MB/30MB-30MB-30MB/0,00-15MB-30MB over 2)
        Top: 0,20% (64MB-65MB-65MB/30MB-30MB-30MB/0,00-15MB-30MB over 2)
    Receiver: 0,03%
 (Last Act): 0,83% (37MB-38MB-39MB/4,4MB-4,5MB-4,5MB/0,00-3,7MB-4,5MB over 6)
    (Cached): 12% (3,6MB-7,8MB-36MB/0,00-378KB-3,5MB/0,00-111KB-1,9MB over 21)
```

Figura 5-16 PROCSTAT de los últimos 171 (dato similar al resultado de APPOPS)

```
* com.sec.android.app.camera / u0a55 / v900219300:
        TOTAL: 0,22% (64MB-65MB-65MB/30MB-30MB-30MB/0,00-15MB-30MB over 2)
          Top: 0,19% (64MB-65MB-65MB/30MB-30MB-30MB/0,00-15MB-30MB over 2)
     Receiver: 0,03%
  (Last Act): 0,77% (37MB-38MB-39MB/4,4MB-4,5MB-4,5MB/0,00-3,7MB-4,5MB over 6)
    (Cached): 12% (3,6MB-7,8MB-36MB/0,00-378KB-3,5MB/0,00-111KB-1,9MB over 21)
```

Figura 5-17 PROCSTATS de las últimas dos semanas

De los diversos datos tomados, puede deducirse un pequeño pico coincidente con la marca de tiempo obtenida de la opción APPOPS.

A mayores, es posible verificar si ha habido algún tipo de conexión wifi en el entorno laboral, ver figura 5-18 y 5-19, lo cual sabemos por las normas de seguridad interna de la empresa, que está prohibido, a través de la opción WIFI:

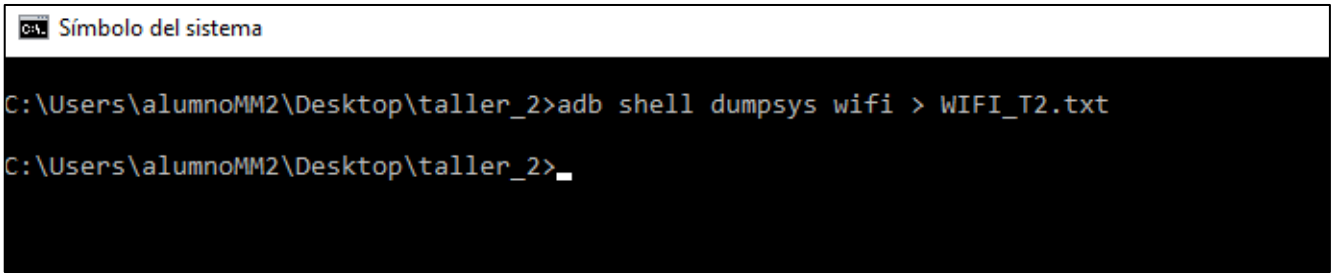


Figura 5-18 Volcado de datos wifi

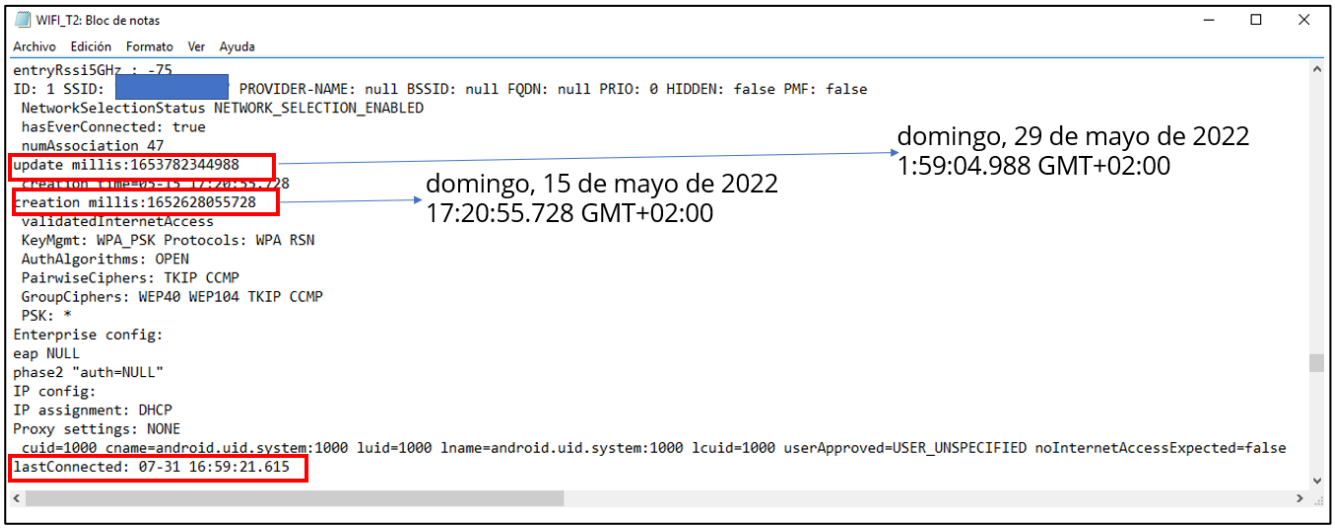


Figura 5-19 Datos de la red wifi empresarial

La figura 5-19 demuestra que el sospechoso sí se ha conectado a la red empresarial, únicamente disponible en los distintos despachos del edificio, y donde está prohibida el uso de dispositivos personales.

Antes de continuar con las posibilidades que ofrece la siguiente herramienta se realizará el hash de las evidencias obtenidas, ver figura 5-20:

```
< C:\Users\alumnoMM2\Desktop\taller_2\APPOPS_T2.txt >
  SHA-1: 63F07ED0773B4CB5918E4E059EEF579D31889DF7
  SHA-256: 6F2B4D5C4164BCBEA266720B2FEBB355AFA5784B2A4038B1B3D51A31EF4766B7

< C:\Users\alumnoMM2\Desktop\taller_2\IMEI_T2.txt >
  SHA-1: A82CAD36D89D6FB13ACCAB9406662B5EA7D7A3BA
  SHA-256: C2974708 4B0ABEBA3F556215859ECBF672DA5E92567F9C07964830320A45E349

< C:\Users\alumnoMM2\Desktop\taller_2\N_TLF_T2.txt >
  SHA-1: 4DA2FEB43949428D8DF10F08A9849E6A9AEFC88A
  SHA-256: 754060D0088CB75062E90632FE8D72BF6629A25521E3550949D06B0160F9A5A0

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTA_96_T2.txt >
  SHA-1: 9ED475C84E532D60FB2D2D1B06617DA75CF2B6E8
  SHA-256: 41F9EE5EEE142B9BC5FE5FC2B86957156AD7663BB3F436E83EE6F39207812491

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTA_168_T2.txt >
  SHA-1: 330FE0A8D93C6E7ED20D7B43AA117A012E881FEF
  SHA-256: 01DD1F6FD8F13956578F1222E1791065EC4B8A91F5004A068BADA8EC7A3D1F9C

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTA_171_T2.txt >
  SHA-1: 35F57450B594AEA58835032F3FACF2160FA2E07C
  SHA-256: 6EB0CF5B3E07C4B9DCEC1682E304B929C7D26ADA07AAC89EBAC05E730C4854A2

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTA_240_T2.txt >
  SHA-1: BC15826D8206CD55C6EA010A694C89449A309AA4
  SHA-256: A6F63E939B3C2E90E2FA3238B8731B1618DC9B43AB7B7ED21BA4C9C3365ACC84

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTA_360_T2.txt >
  SHA-1: 5C5A47FF04E9249DDB690BEC73250BA2E369C58D
  SHA-256: 722E0833572F3D5AEB380C31CF7C5D2EDDB9992EA24B28F96C1A12D6AA816BBF

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTA_480_T2.txt >
  SHA-1: 07B3112014FB8C09B27EA45C234E52FDAC234A9F
  SHA-256: 92B8B0F45071682107A0863AF3DBA75608FE2740E3BC5AE2E1B46D2D7D6DAFF8

< C:\Users\alumnoMM2\Desktop\taller_2\PROCSTAT_T2.txt >
  SHA-1: 0F9E1B01D758C269ADC1AF7B136C42D7BB73D7ED
  SHA-256: 010D7D6786C643DE3B812C05A734043692CB62D6668CC2C831D2184F16000543

< C:\Users\alumnoMM2\Desktop\taller_2\USER_T2.txt >
  SHA-1: 77FCF7FAF9EFE2AC514CC647AA78B575B2FF888D
  SHA-256: 53AD663EEA5EEB529BCD3E742CF250A96075ED2AD279024AE6546BE67A3564CA

< C:\Users\alumnoMM2\Desktop\taller_2\VERSION_T2.txt >
  SHA-1: 421C27B4B94A6A50304F9785E58373D2395A694F
  SHA-256: 89EA011D21F5B99964D4503493A0E919878E2552B2B0FF948DAD5D5B651EAB8A

< C:\Users\alumnoMM2\Desktop\taller_2\WIFI_T2.txt >
  SHA-1: 4EEC7EFE7032E3C81FDB6ACAFF710576E59F4056
  SHA-256: 3515B131134B662B53BCFD418A78DA06E114252F571CA6F30A903F1E86FFB241
```

Figura 5-20 Cálculo de hashes de las evidencias obtenidas

A continuación, se recurrirá a la herramienta BACKUP, para forzar una copia de recuperación de los datos del dispositivo, aunque el eje central serán los datos procedentes del almacenamiento interno y la tarjeta SD, también se obtendrán los datos de aplicaciones que tengan activada la opción de BACKUP, ver figura 5-21:

```
C:\Users\alumnoMM2>adb backup -f C:\Users\alumnoMM2\Desktop\back_up\back_up_T2.ab
-shared -all
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

Figura 5-21 Empleo de la herramienta backup

Tras esto, deberemos interactuar con el dispositivo para autorizar la copia de seguridad y asignarle una contraseña. Una vez finalizado el proceso de backup se volcará un archivo. ab que lo pasaremos a TAR, a través de la herramienta *Android backup processor*, donde *hola* es la contraseña asignada para la copia de seguridad, ver figura 5-22:

```
C:\Users\alumnoMM2\Desktop\android-backup-tookit-20210819\android-backup-tookit\android-backup-processor\executable>java -jar abp
.jar unpack C:\Users\alumnoMM2\Desktop\back_up\back_up_T2.ab C:\Users\alumnoMM2\Desktop\back_up\back_up_T2.tar hola
```

Figura 5-22 Paso del fichero .ab a TAR

Llegados a este punto ya podemos inspeccionar el contenido de la copia de seguridad, y con ello verificar si el sospechoso dispone de contenido clasificado, concretamente en el directorio shared, ver figura 5-23:

Figura 5-23 Contenido de la copia de seguridad

Figura 5-24 Contenido de la tarjeta SD del dispositivo

En este caso, es posible verificar, que en la tarjeta SD del dispositivo se encuentra información clasificada de la empresa STARK S.L, ver figura 5-24. Para finalizar con las evidencias obtenidas vamos a vislumbrar los tiempos MAC de los archivos obtenidos directamente desde el contenido backup del laboratorio, naturalmente los tiempos de creación y acceso se habrán modificado, pero no el de modificación:

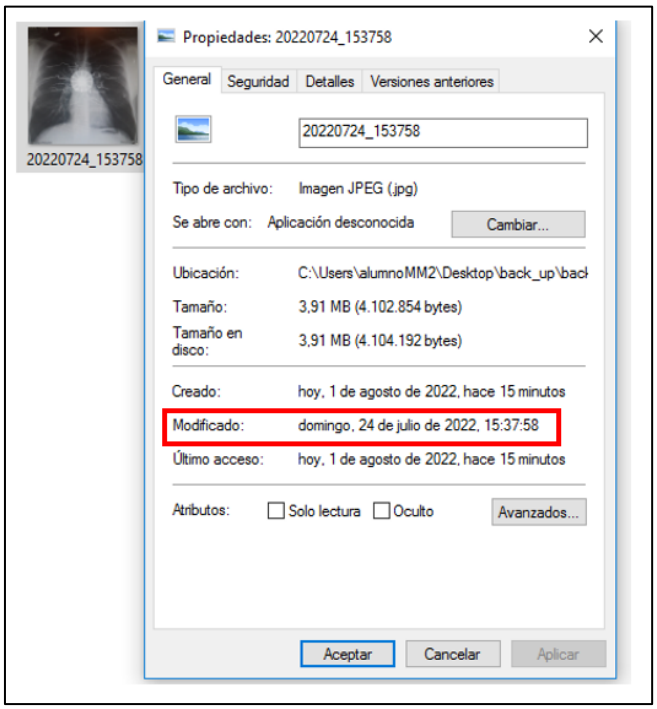


Figura 5-25 Tiempo de modificación del archivo

Es posible ver la coincidencia temporal de los ficheros, ver figura 5-25, con los tiempos obtenidos de la opción APPOPS de la herramienta DUMPSYS, lo cual da fuertes indicios de la toma de fotos empleando la cámara del dispositivo.

A continuación, se obtienen los hashes relativos a los ficheros volcados a través de la copia de seguridad, ver figura 5-26:

```
< C:\Users\alumnoMM2\Desktop\back_up\back_up_T2\shared\1\DCIM\Camera\20220724_153053.jpg >
  SHA-1: 5C6E002BCCF8626E081735B1810B5E52265D27DF
  SHA-256: 8A12E369ECCA72558A730AE53427A7B81053AB7B533E0B4F91D4ECDA4A79CBBC

< C:\Users\alumnoMM2\Desktop\back_up\back_up_T2\shared\1\DCIM\Camera\20220724_153313.jpg >
  SHA-1: C03369CCCEFCA3E91A3E00AC672368FDA16637B6
  SHA-256: 0C614DA733416A1C960857808045096B95E6A7D9101B262CC72E41796D7F5DA1

< C:\Users\alumnoMM2\Desktop\back_up\back_up_T2\shared\1\DCIM\Camera\20220724_153402.jpg >
  SHA-1: 39ECB6D32CF6351A580551A4515F0D8DEBB8686C
  SHA-256: 976C4B891798A66C0571A4981BC5ACB83FD762FD330B3161B75D1C708530085A

< C:\Users\alumnoMM2\Desktop\back_up\back_up_T2\shared\1\DCIM\Camera\20220724_153629.jpg >
  SHA-1: 695F7BF9BC0DD6102076A28752022F6B9557E2A7
  SHA-256: 44D311CED408BC2EB8D4292AC412C3A54E5B80FE8A16AFBE988FCBA9ED48BABE

< C:\Users\alumnoMM2\Desktop\back_up\back_up_T2\shared\1\DCIM\Camera\20220724_153758.jpg >
  SHA-1: CFE11980B1CC35442B7F15CFE075CFF1E3BDD10C
  SHA-256: 034290C9DC923B3735D4C259AFC7F35751BAEBD11450A4A841BA0587D30E159A
```

Figura 5-26 Cálculo de hashes de los ficheros localizados en la tarjeta SD

Para finalizar se recurrirá a la herramienta helium, de cara a obtener evidencias relativas a SMS y llamadas telefónicas realizadas desde el dispositivo del sospechoso. Para ello, debemos tener instalada la versión Android en el dispositivo, así como la versión desktop en el laboratorio. Es fundamental que el laboratorio y el dispositivo estén conectados a la misma red, ver figura 5-27:

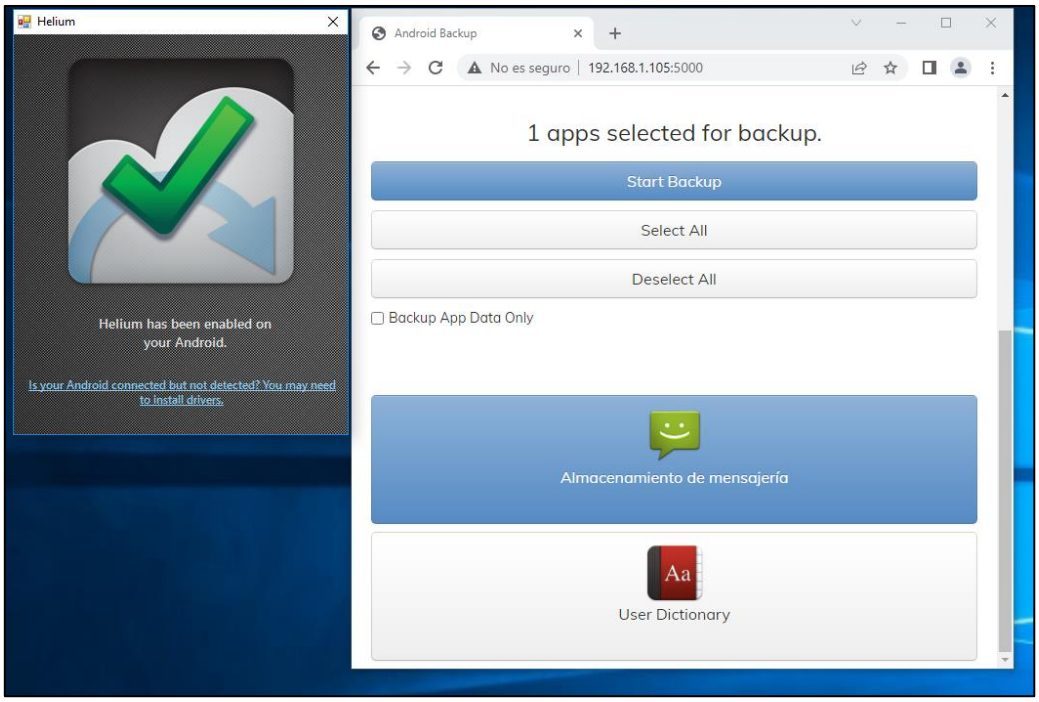


Figura 5-27 Empleo de la herramienta Helium

Se obtiene como consecuencia un archivo llamado: *com. android. Android. providers*, que a través de la herramienta *helium back up extractor*, se obtendrá el archivo custom. cb en el directorio \apps\com.android.providers.telephony\cb, ver figura 5-28:

Figura 5-28 Datos de las llamadas realizadas por el sospechoso

A través de esta información sería posible conocer con quien se ha estado comunicando el sospechoso, y si permite sostener los argumentos acusatorios de la empresa STARK S.L.

En último lugar, se esperan una serie de conclusiones que el alumno debe extraer de la práctica realizada, este apartado es completamente libre, sin embargo, hay ciertos elementos que se esperan de él/ella:

- Los métodos de adquisición de evidencias presentados implican la posibilidad de desbloqueo del dispositivo, así como la activación de la opción de depuración por USB.
- La herramienta backup obliga a una aprobación desde el dispositivo, y por tanto una interacción con el mismo.
- La herramienta helium obliga a una instalación en el propio dispositivo del sospechoso, lo que modifica naturalmente el contenido original del dispositivo.
- Con los datos obtenidos, en un entorno judicial se podría contribuir a demostrar la culpabilidad del sospechoso, o al menos que desde ese dispositivo se han perpetrado acciones prohibidas por la empresa.

A pesar de las claras desventajas de los métodos anteriormente expuestos, queda demostrado la complejidad asociada al análisis forense de dispositivos móviles sin modificar lo más mínimo el contenido del dispositivo, por ello es esencial documentar todos y cada uno de los pasos realizados, reduciendo las posibilidades de que la evidencia pueda ser desestimada.

5.6 Discusión

En el presente taller, se pretende familiarizar con el acceso al dispositivo a través de la herramienta *ABD*, el uso de herramientas de adquisición como DUMPSYS, BACKUP y HELIUM, así como adquirir buenas prácticas en el trato de todas las evidencias, con todo ello podemos hacernos las siguientes preguntas:

¿Podemos verificar que el sospechoso es el dueño del dispositivo con la información extraída?

¿Es posible asegurar que fue él quien realizó las fotografías?

¿Se le puede condenar por ello?

¿Podemos asegurar que las fotografías fueron realizadas en el momento en el que el sospechoso fue capturado por las cámaras de vigilancia?

¿Cuántos permisos se precisa que el dispositivo conceda para este tipo de adquisiciones?

¿Podemos asegurar que el dispositivo ha permanecido en un área restringida para dispositivos personales?

No debemos olvidar, que los analistas forenses no buscan incriminar o dar opinión sobre la comisión de un delito, sino proporcionar herramientas o evidencias que permitan extraer conclusiones verídicas en un proceso judicial.

6 ANÁLISIS DE APLICACIONES MÓVILES

6.1 Objetivos

El presente taller estará centrado en la adquisición lógica, preservación y análisis de información procedente de aplicaciones móviles en sistemas Android, a continuación, se enumerarán los objetivos que lo fundamentan:

- Familiarizarse con el adiestramiento forense haciendo uso de AVDs.
- Familiarizarse con el empleo de la herramienta ABD.
- Profundizar en el sistema de ficheros Android.
- Familiarizarse con la identificación y adquisición de *artifacs* de algunas aplicaciones.
- Familiarizarse con el análisis de *artifacts* de aplicaciones.
- Identificar las ventajas e inconvenientes de este tipo de adquisiciones.

6.2 Conocimientos previos

Para el correcto aprovechamiento del desarrollo del taller, el alumno precisará de una serie de conocimientos previos:

- Conocer el concepto de análisis forense digital, y más concretamente centrado en dispositivos móviles.
- Tener un conocimiento básico de las fases que conforman el análisis forense tanto digital, como en el caso concreto de dispositivos móviles.
- Conocer los principales *artifacs* asociados a un dispositivo Android, concretamente de las principales aplicaciones instaladas en un dispositivo.
- Conocer el concepto de evidencia digital, así como las características que lo singularizan de otro tipo de información digital.
- Estar familiarizado con el empleo de un AVD, así como su generación a través de la herramienta *Android Studio.*
- Disponer de un conocimiento básico del sistema de ficheros Linux, así como de sus instrucciones principales.
- Disponer de un conocimiento básico del sistema de ficheros Android.

6.3 Preparación del taller

En el presente taller, cada estudiante dispondrá de las siguientes herramientas para la resolución de los ejercicios:

- Terminal de usuario: 512 GB disco duro, 16 GB RAM, Sistema operativo Windows 10/11de 64 bits.
- Hipervisor VMware player 16.
- Máquina virtual Windows 10 (laboratorio forense).
    - Reserva de 8 GB en la MV.
    - Android Studio.
    - Herramienta ADB.
    - AVD generada a través de la herramienta Android Studio y rooteada a través de la herramienta Magisk.

La AVD dispondrán de una serie de aplicaciones sobre las que se procederá a realizar las adquisiciones de evidencias, y los posteriores análisis.

6.4 Guía del estudiante

En el presente apartado se procederá a enunciar el ejercicio al estudiante, así como describir los diferentes pasos requeridos para su resolución, junto con ello se le indicará el entregable del taller.

La información anteriormente descrita, que será entregada al estudiante se dividirá en una serie de apartados:

6.4.1 Descripción preliminar del incidente

En el presente taller, no se presentará una situación "simulada" de un entorno en el que se ha producido un incidente, sino que se enumerarán una serie de ejercicios, relativos a los objetivos del presente taller:

- Ejercicio 1: Acceso a un dispositivo móvil, adquisición y análisis de los principales *artifacts* de la aplicación *contactos*.
- Ejercicio 2: Acceso a un dispositivo móvil, adquisición y análisis de los principales *artifacts* del diccionario del usuario.
- Ejercicio 3: Acceso a un dispositivo móvil, adquisición y análisis de los principales *artifacts* de la aplicación *Google keep*.

6.4.2 Evaluación

Como resultado se deberá entregar un informe pericial de las pesquisas, en él debe verse reflejado lo siguiente:

- Versionado de las herramientas empleadas en el laboratorio forense.
- Descripción detallada, con capturas de pantalla, de todos los pasos dados.
- Cálculo de hashes de todas las evidencias adquiridas.
- Conclusiones, donde se reflejarán los inconvenientes y ventajas de estas adquisiciones, así como las dificultades encontradas.

6.5 Resolución del profesor

En el presente apartado, se materializará la resolución del taller desde el punto de vista del profesor, cumpliendo todos los requisitos demandados al alumno, comprobando una resolución viable y un cumplimiento de los objetivos descrito de manera eficaz.

En primer lugar, y común a todos los ejercicios se presentará el listado de herramientas y versiones a emplear para la resolución del taller:

- Hipervisor VMware WorkStation Player 16: 16.2.4 build-20089737.
- VM WINDOWS 10 (laboratorio forense) pro Enterprise edition: WINDOWS 10 ENTERPRISE EDITION 2016 LTSB, 1607.
- ANDROID DEBUG BRIDGE:1.0.41.
- MULTIHASHER: 2.8.2
- JAVA: 1.8.0_341
- SQLite: 3.12.2

A continuación, se resolverán los diferentes ejercicios de manera individual:

6.5.1 Ejercicio 1

En el presente ejercicio se accederá a un dispositivo móvil Android, en este caso a través de una AVD, y se localizará, volcará y analizarán los principales *artifacts* relativos a la aplicación contactos. Antes de ello, el alumno dispondrá de una serie de contactos ya generados por el profesorado, ver figura 6-1:

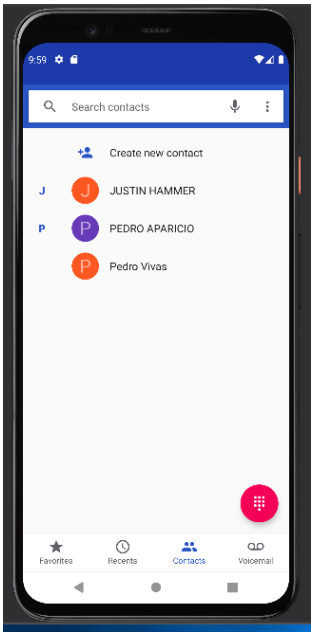


Figura 6-1 Contactos del AVD

A continuación, se procederá al acceso del dispositivo a través de la herramienta ABD, es importante recordar que este dispositivo ha sido rooteado de cara poder acceder a directorios no permitidos para un usuario sin privilegios, ver figura 6-2.

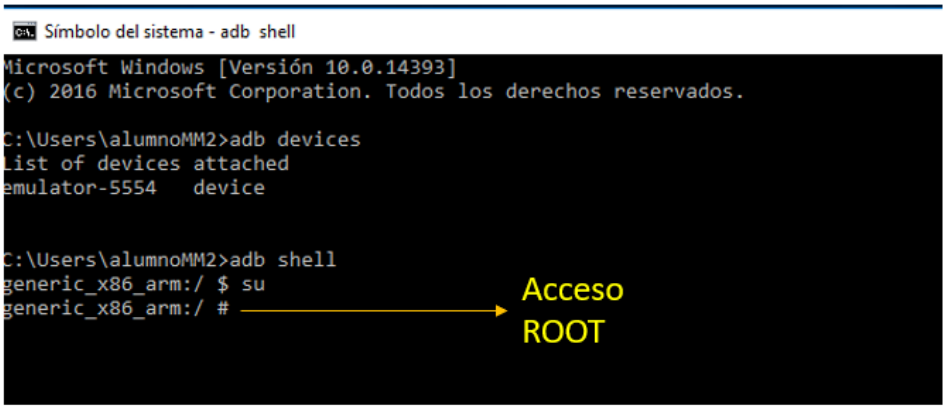


Figura 6-2 Acceso al dispositivo y escalada de privilegios

Una vez demostrados los privilegios root, nos dirigimos al directorio: */data/data/com.android.providers.contacts/databases*, donde se localiza el archivo *contacts2.db*, ver figura 6-3:

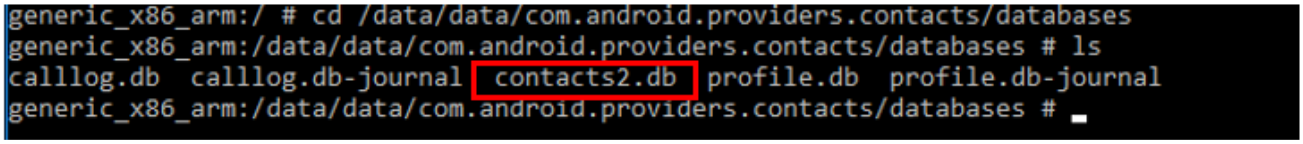


Figura 6-3 Acceso al artifact de *contactos*

Seguidamente, se calcula el hash del *artifacts* localizado, a través de herramientas de linux , como es el caso del comando SHA256SUM, ver figura 6-4:

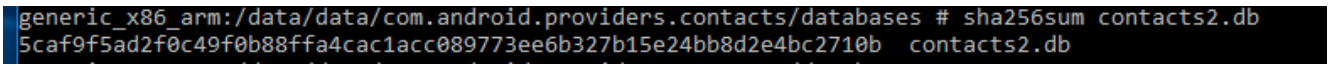


Figura 6-4 Cálculo del hash a través de herramientas linux

Una de las opciones para proceder a su adecuada extracción es copiarlo a un directorio accesible por un usuario sin privilegios, en este caso se empleará el directorio *storage/Nº-Nº/Documents*, lo cual forma parte de la tarjeta SD del analista, ver figura 6-5:

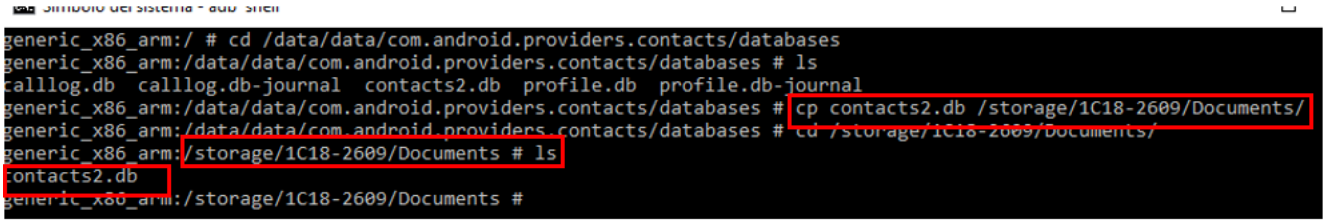


Figura 6-5 Copia de la base de datos de contactos en la tarjeta SD del analista

Previo a la adquisición del *artifacts*, resulta de interés conocer los tiempos MAC que desde el sistema operativo del dispositivo se reflejan en dicho *artifacts*, lo cual resulta muy útil para el trazado de una línea de tiempos relativa a una investigación forense, para ello se empleará la instrucción STAT, ver figura 6-6:

```
1|generic_x86_arm:/data/data/com.android.providers.contacts/databases # stat contacts2.db
  File: contacts2.db
  Size: 376832    Blocks: 744     IO Blocks: 512  regular file
Device: fd04h/64772d    Inode: 131093   Links: 1        Device type: 0,0
Access: (0660/-rw-rw----)       Uid: (10062/  u0_a62)   Gid: (10062/  u0_a62)
Access: 2022-05-10 18:20:16.718474062 +0000
Modify: 2022-08-03 10:05:15.396000000 +0000
Change: 2022-08-03 10:05:15.396000000 +0000
generic_x86_arm:/data/data/com.android.providers.contacts/databases #
```

Figura 6-6 Tiempos MAC asociados a la base de datos de contactos

A continuación, haciendo uso de la herramienta PULL, ver figura 6-7, se procederá a la adquisición del fichero, para su posterior análisis a través de la herramienta SQLite:

```
C:\Users\alumnoMM2>adb pull /storage/1C18-2609/Documents/contacts2.db C:\Users\alumnoMM2\Desktop\taller_3
/storage/1C18-2609/Documents/contacts2.db: 1 file pulled, 0 skipped. 54.3 MB/s (376832 bytes in 0.007s)
```

Figura 6-7 Volcado del archivo de contactos en el laboratorio forense

Seguidamente, se calculará el hash de la evidencia extraída a través de la herramienta MULTIHASHER, ver figura 6-8:

Figura 6-8 Cálculo del hash del fichero contactos.db

Una vez extraído del fichero, el análisis es viable a través del gestor SQLite, donde se identifican una serie de tablas de interés:

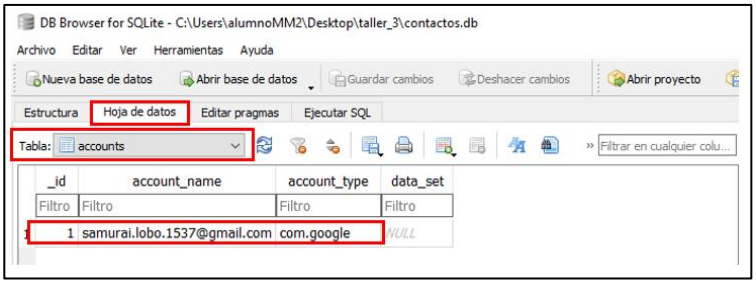


Figura 6-9 Contenido de la tabla *accounts*

En la figura 6-9, pueden verse las distintas cuentas Google que han sido registradas por el usuario en el dispositivo. A continuación, se presentará la tabla de *contacts*:

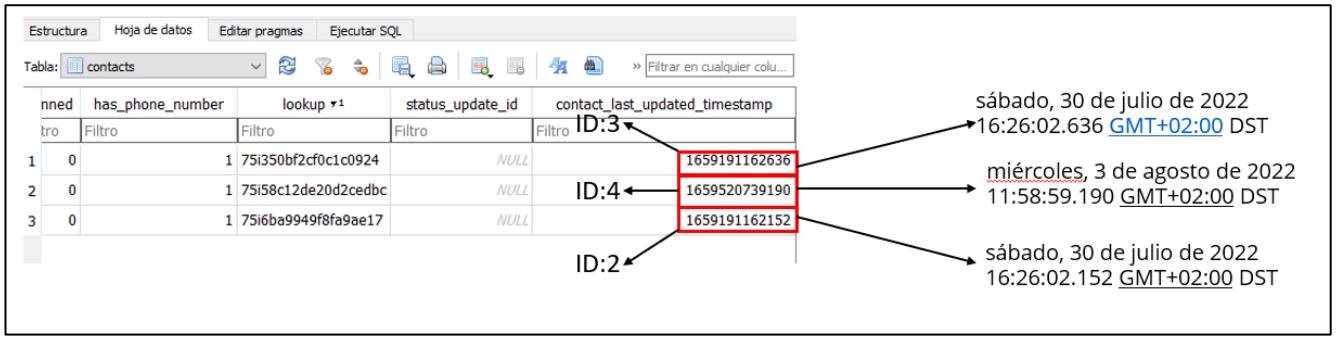


Figura 6-10 Contenido de la tabla *contacts*

La figura 6-10 muestra un contenido muy interesante, a priori no parece que llame la atención, sin embargo, refleja tres contactos (los tres del AVD), así como un tiempo de última actualización de los teléfonos, los cual puede identificarse bien con el momento de creación del contacto o su última edición, por ejemplo, para añadir algún dato más.

A través de la columna *id* o *name_raw_contact_id*, puede verse la correlación entre la presente tabla y la tabla *phone_lookup*, ver figura 6-11*:*

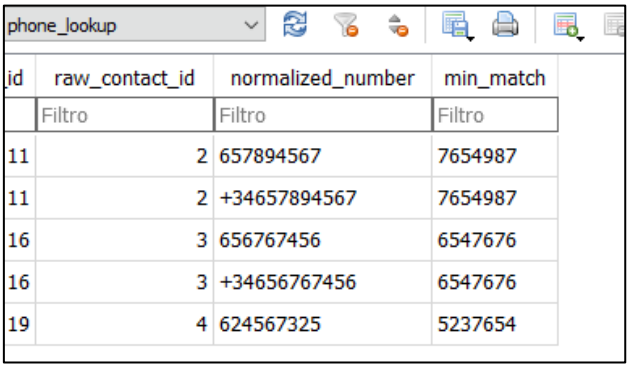
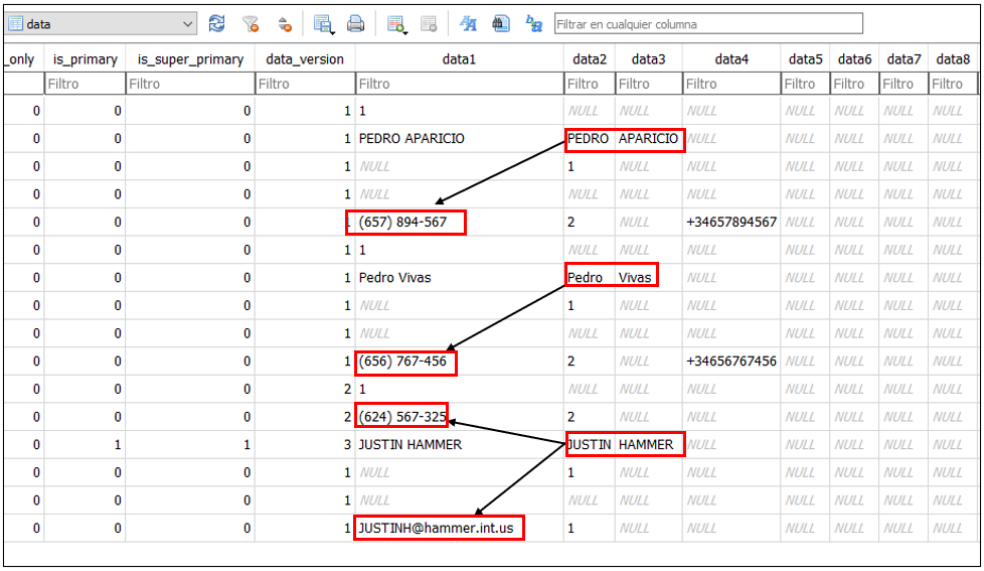


Figura 6-11 Contenido de la tabla *phone lookup*

Para finalizar, se mostrará parte del contenido de la tabla *data*, la cual nos permitirá localizar los teléfonos de contactos, junto con sus nombres asociados y algún dato más de interés, como pueden ser cuentas asociadas a los contactos, ver figura 6-12:



data

Filtrar en cualquier columna

_only	is_primary	is_super_primary	data_version	data1	data2	data3	data4	data5	data6	data7	data8
Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
0	0	0	1	1	NULL	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	PEDRO APARICIO	PEDRO	APARICIO	NULL	NULL	NULL	NULL	NULL
0	0	0	1	NULL	1	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	(657) 894-567	2	NULL	+34657894567	NULL	NULL	NULL	NULL
0	0	0	1	1	NULL	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	Pedro Vivas	Pedro	Vivas	NULL	NULL	NULL	NULL	NULL
0	0	0	1	NULL	1	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	(656) 767-456	2	NULL	+34656767456	NULL	NULL	NULL	NULL
0	0	0	2	1	NULL	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	2	(624) 567-325	2	NULL	NULL	NULL	NULL	NULL	NULL
0	1	1	3	JUSTIN HAMMER	JUSTIN	HAMMER	NULL	NULL	NULL	NULL	NULL
0	0	0	1	NULL	1	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL
0	0	0	1	JUSTINH@hammer.int.us	1	NULL	NULL	NULL	NULL	NULL	NULL

Figura 6-12 Información de la tabla *data*

6.5.2 Ejercicio 2

En el presente ejercicio se realizará un análisis de los principales *artifacts* de la herramienta diccionario de usuario de un dispositivo Android, para ello se partirá de un AVD con algunas palabras introducidas, ver figura 6-13:

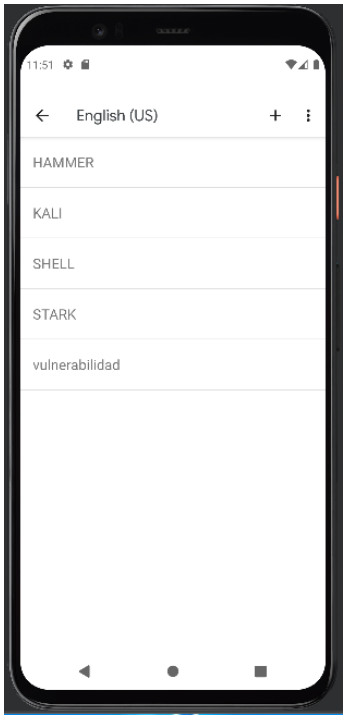


Figura 6-13 Palabras introducidas en el diccionario de usuario

Esta herramienta constituye una potente fuente de información para el analista, pues contiene palabras empleadas por el usuario que han sido introducidas en el mismo, evitando ser marcadas por el auto corrector, esto es muy interesante pues con gran probabilidad serán palabras empleadas frecuentemente por el usuario del dispositivo.

En primer lugar, se accederá al directorio */data/data/com.android.providers.userdictionary/databases,* en dicha localización nos encontraremos con los siguientes ficheros, el acceso a dicho directorio está condicionado a disponer de permisos de root sobre el sistema operativo, ver figura 6-14:

```
C:\Users\alumnoMM2>adb shell
generic_x86_arm:/ $ su
generic_x86_arm:/ # cd /data/data/com.android.providers.userdictionary
generic_x86_arm:/data/data/com.android.providers.userdictionary # cd databases
generic_x86_arm:/data/data/com.android.providers.userdictionary/databases # ls
user_dict.db  user_dict.db-journal
generic_x86_arm:/data/data/com.android.providers.userdictionary/databases #
```

Figura 6-14 Contenido del directorio *databases*

Seguidamente se volcará el fichero base de datos user_dict.db en una localización accesible para un usuario sin privilegios, en este caso, en una tarjeta SD perteneciente al analista, ver figura 6-15:

```
generic_x86_arm:/storage/1C18-2609/Documents # ls
user_dict.db
```

Figura 6-15 Localización del fichero en la tarjeta SD del analista

Por último, se extraerá el *artifact* a través de la herramienta pull, localizándose en el laboratorio forense local, ver figura 6-16:

```
C:\Users\alumnoMM2>adb pull /storage/1C18-2609/Documents/user_dict.db C:\Users\alumnoMM2\Desktop\taller_3
/storage/1C18-2609/Documents/user_dict.db: 1 file pulled, 0 skipped. 5.9 MB/s (16384 bytes in 0.003s)
```

Figura 6-16 Volcado del fichero objetivo sobre el laboratorio forense

Seguidamente se calculará el hash, tanto en el propio sistema operativo Android, ver figura 6-17 como a través de la herramienta MULTIHASHSER, ver figura 6-18:

```
generic_x86_arm:/storage/1C18-2609/Documents # sha256sum user_dict.db
f316c7f07ed3dd3a274260f1b57943fddb80d8551d24a2e03716ab8264c3cdad  user_dict.db
```

Figura 6-17 Cálculo del hash empelando herramienta de linux

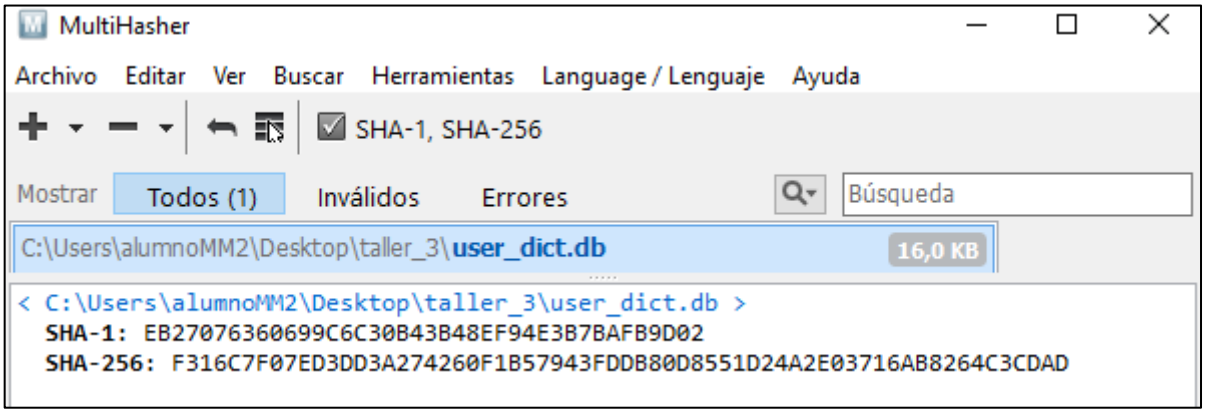
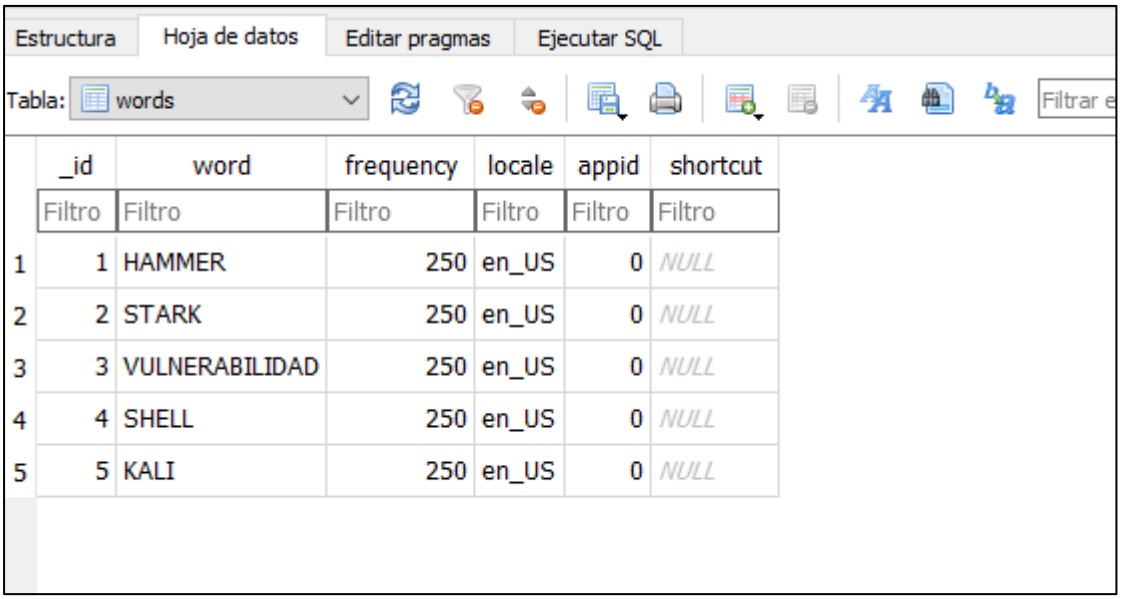


Figura 6-18 Cálculo del hash a través de la herramienta MULTIHASHER

Una vez volcado del fichero de interés, haciendo uso de la herramienta SQLite, se procederá a inspeccionar su contenido, ver figura 6-19:



	_id	word	frequency	locale	appid	shortcut
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	HAMMER	250	en_US	0	NULL
2	2	STARK	250	en_US	0	NULL
3	3	VULNERABILIDAD	250	en_US	0	NULL
4	4	SHELL	250	en_US	0	NULL
5	5	KALI	250	en_US	0	NULL

Figura 6-19 Contenido del artifact asociado al diccionario del usuario

6.5.3 Ejercicio 3

El presente ejercicio se basa en efectuar un análisis forense sobre la aplicación GOOGLE KEEP sobre una AVD. Se trata de una aplicación de notas/recordatorios que permite avisar al usuario no solamente en un determinado momento, sino si se encuentra en una localización específica.

El paquete/directorio que contiene toda la información relativa a esta aplicaciones: com.google.android.keep. El *artifact* principal sobre la presente aplicación será keep.db, contenido en el directorio ya mencionado.

En primer lugar, se efectúa la conexión sobre la AVD, a través de la herramienta ABD. Una vez establecida la conexión se escala a privilegios ROOT, ver figura 6-20, se debe recordar que la AVD empleada ha sido rooteada.

```
C:\Users\alumnoMM2>adb shell
generic_x86_arm:/ $ su
generic_x86_arm:/ # cd /data/data
```

Figura 6-20 Conexión al AVD y escalada de privilegios

Seguidamente, nos dirigimos al directorio de datos asociado a la aplicación GOOGLE KEEP, el cual contiene todos los archivos asociados a la aplicación, ver figura 6-21 :

```
generic_x86_arm:/data/data # cd com.google.android.keep
generic_x86_arm:/data/data/com.google.android.keep # ls
cache  code_cache  databases  files  lib  no_backup  shared_prefs
generic_x86_arm:/data/data/com.google.android.keep # cd databases
generic_x86_arm:/data/data/com.google.android.keep/databases # ls
-1_threads.notifications.db          gnp_database-shm  pseudonymous_room_notifications.db
-1_threads.notifications.db-journal  gnp_database-wal  pseudonymous_room_notifications.db-shm
1_threads.notifications.db           growthkit.db      pseudonymous_room_notifications.db-wal
1_threads.notifications.db-journal   growthkit.db-shm  samurai.lobo.1537@gmail.com_room_notifications.db
accounts.notifications.db            growthkit.db-wal  samurai.lobo.1537@gmail.com_room_notifications.db-shm
accounts.notifications.db-journal    keep.db           samurai.lobo.1537@gmail.com_room_notifications.db-wal
gnp_database                         keep.db-journal
```

Figura 6-21 Directorio asociado a aplicación GOOGLE KEEP

A continuación, se procede a calcular el hash del fichero keep.db, a través de la herramienta sha256sum de Linux, ver figura 6-22:

```
generic_x86_arm:/data/data/com.google.android.keep/databases # sha256sum keep.db
8f7769bd718884ce06c61a1a56ea179e6410c5c8582635524d0041327f9dc980  keep.db
```

Figura 6-22 Cálculo del hash sobre el fichero keep.db

El siguiente paso es trasladar el fichero a una ubicación accesible. Se simulará que se ha introducido una SD CARD esterilizada por el analista en el dispositivo, ver figura 6-23:

```
generic_x86_arm:/data/data/com.google.android.keep/databases # cp keep.db /storage/1C18-2609/Documents
```

Figura 6-23 Copia del fichero keep.db en la tarjeta SD

Para proceder a la correcta extracción, se emplea la herramienta PULL sobre el laboratorio forense,ver figura 6-24, de esta forma se podrá proceder a su análisis con la herramienta SQLite:

```
C:\Users\alumnoMM2>adb pull /storage/1C18-2609/Documents/keep.db C:\Users\alumnoMM2\Desktop\taller_3
/storage/1C18-2609/Documents/keep.db: 1 file pulled, 0 skipped. 44.7 MB/s (372736 bytes in 0.008s)
```

Figura 6-24 Volcado del fichero keep.db en el laboratorio forense

El siguiente paso será realizar el cálculo del hash a través de la herramienta MULTIHASHER, ver figura 6-25:

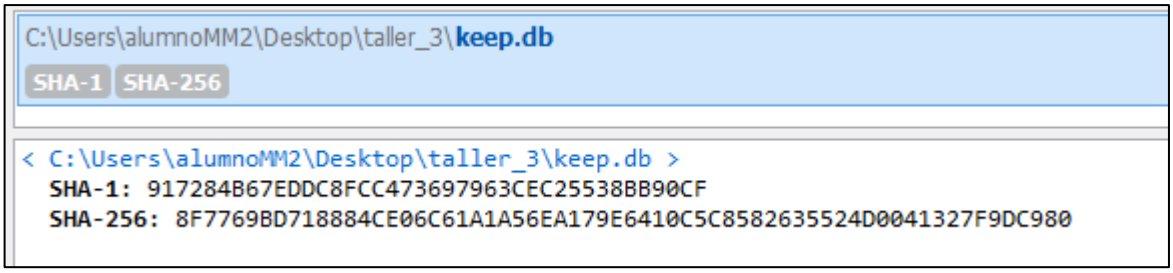
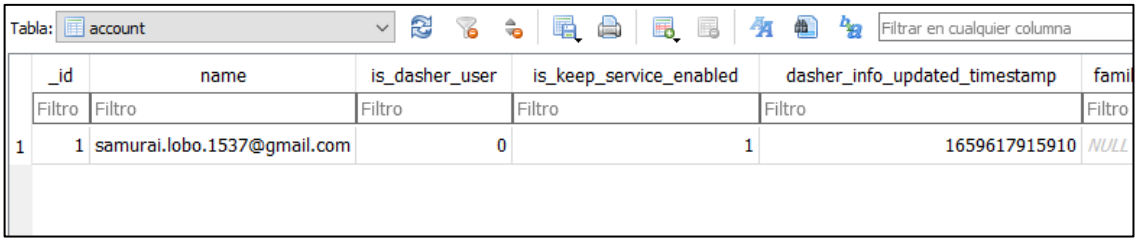


Figura 6-25 Hash del fichero keep.db a través de la herramienta MULTIHASHER

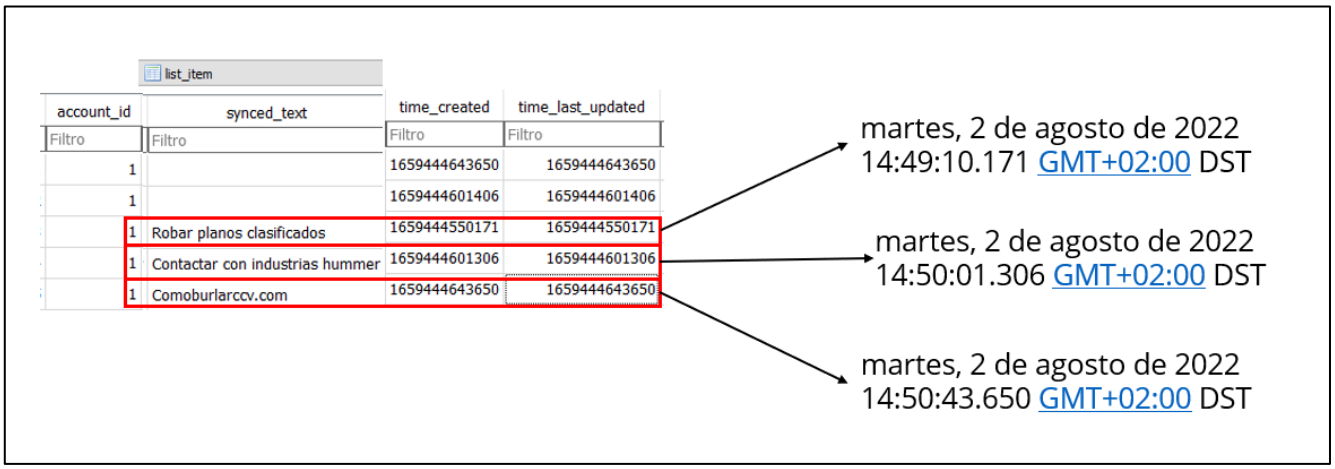
Una vez volcada la evidencia, se procede a su análisis a través de la aplicación SQLite, de esta forma se analizarán las distintas estructuras de datos que contiene el fichero:



	_id	name	is_dasher_user	is_keep_service_enabled	dasher_info_updated_timestamp	fami
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	samurai.lobo.1537@gmail.com	0	1	1659617915910	NULL

Figura 6-26 Contenido de la tabla *account*

En la figura 6-26, pueden verse la única cuenta identificada en el dispositivo, con un identificador asociado.



account_id	synced_text	time_created	time_last_updated
Filtro	Filtro	Filtro	Filtro
1		1659444643650	1659444643650
1		1659444601406	1659444601406
1	Robar planos clasificados	1659444550171	1659444550171
1	Contactar con industrias hummer	1659444601306	1659444601306
1	Comoburlarccv.com	1659444643650	1659444643650

Figura 6-27 Contenido de la tabla *list_item*

De la figura 6-27, puede derivarse el contenido de las diferentes notas asociadas a una cuenta de usuario, a mayores se obtiene el *time stamp* asociado a cada una de las notas, lo que permite una herramienta para el trazado de líneas temporales sobre las acciones del sospechoso.

En último lugar, se esperan una serie de conclusiones que el alumno debe extraer de la práctica realizada, este apartado es completamente libre, sin embargo, hay ciertos elementos que se esperan de él/ella:

- Los métodos de adquisición de evidencias presentados implican la posibilidad de desbloqueo del dispositivo, así como la activación de la opción de depuración por USB.
- El dispositivo debe haber sido rooteado, lo cual implica cierta modificación de los datos almacenados en el mismo.
- Se requiere del empleo de una localización intermedia, en el caso del ejercicio, a través de una SD extraíble procedente del analista, sería posible reubicar los datos en el almacenamiento interno accesible por el usuario, pero no sería recomendable al modificar posibles datos que hayan sido borrados por el usuario.
- Los datos extraídos constituyen evidencias asociadas a los contactos almacenados, palabras del diccionario, así como una lista de tareas, pueden proporcionar información muy útil en un entorno judicial, sin embargo, resulta esencial documentar y justificar cada uno de los pasos dados, en especial el hecho de rootear el dispositivo.

Resulta evidente, las precondiciones que se deben cumplir para perpetrar la adquisición y posterior análisis realizados en el presente taller, a mayores hay una clara manipulación de los datos contenidos en el dispositivo, sin embargo, en ocasiones, es la única manera de efectuar una adquisición de información procedente de este tipo de dispositivos, todo lo cual demuestra la densa complejidad que el análisis forense procedente de dispositivos móviles representa.

6.6 Discusión

En el presente taller, se pretende familiarizar con la localización, adquisición y análisis de diversos *artifacts* procedentes de una serie de aplicaciones, así como adquirir buenas prácticas en el trato de todas las evidencias, con todo ello podemos hacernos las siguientes preguntas:

¿Es posible extraer un listado completa de contactos del dispositivo?

¿Es posible trazar una línea de tiempos en relación a los contactos almacenados?

A través de la información derivada de la aplicación diccionario ¿Qué tipo de información se puede extraer? ¿por qué es importante los datos extraídos?

En relación a la aplicación GOOGLE KEEP ¿es posible trazar una línea de tiempos asociada a los eventos? ¿Qué tipo de información se puede extraer?

7 CONCLUSIONES Y LÍNEAS FUTURAS

7.1 Conclusiones

A lo largo del presente trabajo de fin de master, ha quedado patente la gran complejidad que supone el análisis forense digital, focalizado en dispositivos móviles. A pesar de constituir una rama del análisis forense digital, se han vislumbrado múltiples diferencias con otras ramas, que han derivado en dificultades para lograr un adecuado análisis con una modificación mínima del dispositivo.

Se planteó al inicio del presente trabajo, un objetivo general basado en la formación en las diferentes fases del análisis forense sobre dispositivos Android. Este objetivo, como su propio nombre indica, constituye una finalidad relativamente ambigua, en gran medida alcanzada a través del paso por las diferentes fases del análisis forense sobre dispositivos móviles, sus herramientas y diversas prácticas realizadas, sin embargo, alcanzar completamente dicho objetivo, requiere de un estudio constante por parte del analista. A lo largo del presente trabajo se ha pasado por los aspectos fundamentales que caracterizan este tipo de actividad forense, a pesar de ello, el presente objetivo requiere de una mayor profundidad y un ejercicio constante.

Como objetivo específico, se materializaron tres sencillos talleres, un primer taller dirigido sobre la tarjeta SD y memoria interna accesible de un dispositivo Android, un segundo taller focalizado en el empleo de una serie de herramientas específicas sin necesidad de privilegios root, y un tercer taller dirigido a diversos *artifacts* sobre algunas aplicaciones móviles de interés. Su planificación y ejecución, también alimentó al objetivo general planteado. El desarrollo de los tres talleres conllevó no solo el desarrollo de los mismos, sino el planteamiento de los objetivos perseguidos, el conocimiento previo necesario del alumno, así como el material mínimo necesario. Con todo ello, considero completado el objetivo específico planteado al inicio del trabajo, permitiendo no únicamente el empleo en si de ciertas herramientas, sino la planificación que requiere tratar de transmitir este tipo de formación. Sin olvidar que la profundidad y complejidad de los talleres es naturalmente escalable, incluyendo un mayor número de herramientas y *artifacts*.

Para finalizar el presente apartado, considero esencial destacar las palpables diferencias entre este tipo de análisis forense y el focalizado a ordenadores personales, de sobremesa, etc,. Desde el inicio de la actividad forense, las dificultades son reconocibles, ejemplo de ello es el cuidado que ha de tenerse en el tratamiento y transporte de estos dispositivos. Como se ha comentado desde el inicio del trabajo, los dispositivos móviles son “cuadernos de bitácora” del usuario que los emplea, siendo una rica fuente de información y por lo tanto de interés forense.

El presente trabajo, no solo ha tratado de recorrer desde una visión teórica los fundamentos que conforman este tipo de análisis forense, sino palpar las dificultades derivadas del mismo, y a mayores

construir talleres de formación para propiciar la educación en esta disciplina. Poco a poco, los dispositivos móviles están eclipsando a los ordenadores de sobre mesa, y es por ellos y por la dificultad demostrada que su análisis forense supone, que se debe fomentar una formación sólida y constante en esta rama del análisis forense digital.

7.2 Líneas futuras

En el presente apartado, se indicarán una serie de ideas que permiten en unos casos completar y en otros incrementar la complejidad, de los diferentes aspectos desarrollados a lo largo del presente trabajo.

1. Diversas técnicas de *rooteo* de un dispositivo Android. Se ha comentado la necesidad, en determinadas ocasiones, de disponer de acceso con privilegios sobre el sistema operativo del dispositivo móvil. Como una posible línea futura, sería viable mostrar las diversas opciones para *rootear* un dispositivo Android, e incluso, plantearlo como un taller más de formación.
2. Técnicas de desbloqueo para el acceso a un dispositivo Android. Como ha podido verse a lo largo de los talleres, el empleo de la herramienta ABD ha estado condicionado a la posibilidad de desbloqueo del propio dispositivo, para lo cual es preciso conocer: ese posible PIN, patrón o contraseña. No en todas las ocasiones, el desbloqueo del dispositivo se obtiene de manera trivial, por ello, considero de interés su formación y extensión de este trabajo en dicho sentido.
3. Incremento del número de aplicaciones a analizar. En el tercer taller, únicamente se han mostrado, a nivel práctico, tres aplicaciones móviles, sin embargo, como se ha mostrado a lo largo del trabajo, existen multitud de las mismas, todas ellas con una serie de artifacts asociados. Como una primera idea de ampliación, considero que sería de interés incorporar las aplicaciones de uso muy reiterado, como es el caso de FACEBOOK, así como WHATSAPP, GMAIL, etc,. Focalizando su formación en talleres, indicando y mostrando los principales *artifacts* de interés.
4. Extender el análisis forense a un entorno malware. Dada la complejidad y especialización que supone la disciplina de análisis MALWARE, ya sea en un entorno de sistemas operativos de escritorio, o dirigidos a dispositivos móviles, implica una disciplina aparte. A modo de extensión, resulta viable incluir un cierto nivel de documentación e incluso formación en este ámbito, indicando las diversas técnicas tanto dinámicas, como estáticas para su análisis.
5. Conformar el presente trabajo como un curso de formación nivel básico, centralizado en un ámbito policial y militar. Formación asociada a un plan de estudios, así como a una planificación temporal y de costes.

8 BIBLIOGRAFÍA

[1] R. Ramirez Pino, El teléfono movil y la vida cotidiana, Barcelona, 2008.

[2] «REAL ACADEMIA ESPAÑOLA,» [En línea]. Available: https://www.rae.es/.

[3] R. McKemmish, What is forensic computing?, 1999.

[4] R. H. B. Alicia Gil Gil, Cibercriminalidad, DYKINSON, 2019.

[5] «RFC 3227,» [En línea]. Available: https://www.ietf.org/rfc/rfc3227.txt.

[6] «ISO 27037,» [En línea]. Available: https://www.iso27001security.com/html/27037.html.

[7] D. T. R. T. Oleg Skulkin, Learning Android Forensics, PacktPub, 2018.

[8] O. S. H. M. S. B. Rohit Tamma, Practical Mobile Forensics, PacktPub, 2020.

[9] «Android para desarrolladores,» [En línea]. Available: http://developer.android.com.

[10] N. R. Koppolu, «Android Mobile Artifacts: A Treasure Trove of Digital Evidence in Crime Investigation,» *International Research Journal of Engineering and Technology (IRJET)*, 2021.

[11] Microsoft, «Microsoft Edge Developer/Virtual machines,» [En línea]. Available: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/#downloads.

[12] VMware, «VMware workstation player,» [En línea]. Available: https://www.vmware.com/es/products/workstation-player/workstation-player-evaluation.html.

[13] Android, «Android Studio/Download,» [En línea]. Available: https://developer.android.com/studio.

[14] «SOURCEFORGE,» [En línea]. Available: https://sourceforge.net/projects/android-backup-processor/.

[15] «clockworkmod,» [En línea]. Available: https://www.clockworkmod.com/#.

[16] «WIKIPEDIA,» [En línea]. Available: https://en.wikipedia.org/.