Adquisición de dispositivos móviles con sistema operativo Android

Lic. Gerardo Nilles, Lic. Gastón Silva, Lic. Gaston Semprini

Informática Forense. Poder judicial de Río Negro. Laprida 292. Viedma. Rio Negro.
gnilles@jusrionegro.gov.ar, gsilva@jusrionegro.gov.ar.
gsemprini@jusrionegro.gov.ar

Abstract. La cantidad creciente de dispositivos móviles con sistema operativo Android incautados en los secuestros de dispositivos tecnológicos dieron lugar a que desde el área se investigaran las mejores técnicas y herramientas para realizar la correcta adquisición de los mismos.
Este trabajo presenta las técnicas investigadas y la metodología aplicada por el área utilizando herramientas libres y enmarcadas dentro de un procedimiento operativo estandarizado.

Keywords: Adquisición, Dispositivos móviles, Android, Imagen en Vivo.

1 Introducción

En los últimos años los dispositivos tecnológicos han experimentado grandes avances.

Estos adelantos tecnológicos incorporan los dispositivos móviles, los cuales se han convertido en una extensión del ser humano, creándose una gran dependencia por las aplicaciones que contienen; ejemplo de esta afirmación, son los aparatos que se suspenden cuando se dejan de mirar o los que comprenden cuando se emiten ordenes por voz, siendo capaces de responder en diferentes idiomas. [1]

Con el uso de dispositivos móviles comienza un proceso de sustitución de la PC, que se da primero en la priorización del uso de uno sobre otro para acceder a Internet y luego como único dispositivo de acceso. Esto sucede especialmente en los segmentos socioeconómicos más bajos así como entre los más jóvenes.

El móvil como principal dispositivo de conexión es más importante entre los usuarios de hasta 31 años identificados como nativos digitales, y en las mujeres, mientras que la computadora se mantiene entre los hombres de más de 53 años.

En Argentina para más del 40% de los usuarios de Internet el dispositivo móvil es el principal medio de acceso. Más aún, para el 6% de quienes usan esta red, el móvil es el único dispositivo de acceso, permitiendo su uso a segmentos antes desconectados o que debían recurrir a espacios públicos, limitando entonces su utilidad. [2]

Los avances en tecnología móvil hacen que cada vez haya que resignar menos funcionalidad a la hora de usar un dispositivo móvil frente a una PC. Con capacidades similares o superiores por el agregado de la movilidad, en particular los Smartphones, se posicionan como dispositivos de interés al llevar adelante una investigación que involucre accesos a internet, comunicaciones, distribución de imágenes con contenido sexual, etc.

2 Sobre la investigación forense

Por lo expuesto anteriormente, es esperable que sea cada vez mayor la cantidad de celulares, principalmente Smartphones, incautados en los secuestros de dispositivos tecnológicos.

Cuando en una investigación forense se cuenta con un celular para peritar, uno de los principales desafíos es determinar la mejor manera de adquirir la evidencia, es decir, cómo pueden extraerse los datos relevantes contenidos en un dispositivo. Para esto se debe contar con un conocimiento sólido de las características de hardware y software del dispositivo. También resulta imprescindible contar con procedimientos operativos estandarizados que establezcan los lineamientos sistemáticos mínimos de trabajo para garantizar la calidad del servicio ofrecido, conformando así un modelo de trabajo pericial escalable para afrontar la demanda creciente de actividades forenses [3]. Estos procedimientos deben basarse en las buenas prácticas de la disciplina.

Estadísticamente, en el laboratorio de informática forense del Poder Judicial de Río Negro, un 75% de los dispositivos móviles aportados como evidencia cuentan con distintas versiones del sistema operativo Android. Según la consultora de tecnología Gartner, el 86.2 % de los dispositivos vendidos en el año 2016 contaban con el sistema operativo Android, representando un aumento del 4 por ciento en comparación con el mismo periodo del año anterior. El crecimiento de Android se mantiene principalmente en los fabricantes de teléfonos provenientes de Asia, concluye el estudio. Samsung tuvo el 22.3 por ciento de cuota siendo el fabricante con más participación. [4]

Teniendo en cuenta las estadísticas propias y la tendencia del mercado global de dispositivos móviles, se consideró necesario en este laboratorio abordar la problemática de la adquisición de dispositivos móviles con sistema operativo Android. Se realizaron pruebas de concepto de las distintas técnicas, utilizando tanto herramientas licenciadas como open source. De las pruebas realizadas y el análisis de los resultados obtenidos se pudo elaborar el procedimiento operativo estandarizado para la adquisición de este tipo de dispositivos.

3 Tecnología Android

Android es una pila de software que incluye un sistema operativo, middleware y una capa aplicaciones para que el teléfono pueda realizar funciones más allá de la funcionalidad de telefonía clásica.

Android es una plataforma abierta y completa para dispositivos móviles. Incluye un sistema operativo, interfaz de usuario y aplicaciones.

El diseño de Android está basado en el Kernel de Linux en su versión 2.6, razón por la cual cuenta con las características de ser libre, gratuito y multiplataforma, siendo creado principalmente para dispositivos móviles, entre ellos, los teléfonos inteligentes, Tablet, relojes y televisores. [1]

Algunas de sus características principales son las siguientes:

- Almacenamiento. Utiliza SQLite, una base de datos que se emplea para almacenar datos en el teléfono.
- Mensajería. Android es compatible con los SMS y MMS, también corre aplicaciones de mensajería instantánea como por ejemplo WhatsApp.
- Navegador. Cuenta con un navegador de Internet básico que funciona con el motor JavaScript V8.
- Soporte de Java. En su interior Android cuenta con una arquitectura en Java, pero en su exterior, no cuenta con una máquina virtual basada en este lenguaje.
- Entorno de desarrollo. Los desarrolladores pueden utilizar cualquier software que les permite crear aplicaciones en Java como por ejemplo Eclipse (integrado en Android).
- Google Play Store. Android cuenta con una tienda de aplicaciones donde los desarrolladores publican sus aplicaciones, estas amplían el número de funciones que realiza el sistema operativo de fábrica.

- Bluetooth. lleva conectividad Bluetooth de forma nativa.
- Multitarea. En Android, podemos dejar aplicaciones corriendo en segundo plano sin gastar muchos recursos del teléfono.

4 Arquitectura Android

Al ser un sistema operativo de código abierto, su arquitectura está formada por varias capas que facilitan el desarrollo y creación de aplicaciones [5]:

- **Kernel de Linux**. El núcleo actúa como una capa de abstracción entre el hardware y el resto de las capas de la arquitectura. El desarrollador no accede directamente a esta capa, sino que debe utilizar las librerías disponibles en capas superiores. De esta forma se evita tener que conocer las características precisas de cada teléfono. Si es necesario hacer uso de la cámara, el sistema operativo se encarga de utilizar la que incluya el teléfono, sea cual sea. Para cada elemento de hardware del teléfono existe un controlador dentro del kernel que permite utilizarlo desde el software.

  El kernel también se encarga de gestionar los diferentes recursos del teléfono (energía, memoria, etc.) y del sistema operativo en sí: procesos, elementos de comunicación, etc.

- **Librerías**. Están escritas en C o C++ y compiladas para la arquitectura hardware específica del teléfono. Estas normalmente están hechas por el fabricante, quien también se encarga de instalarlas en el dispositivo antes de ponerlo a la venta. El objetivo de las librerías es proporcionar funcionalidad a las aplicaciones para tareas que se repiten con frecuencia, evitando tener que codificarlas cada vez y garantizando que se llevan a cabo de la forma "más eficiente".

  Entre las librerías incluidas habitualmente se encuentran OpenGL (motor gráfico), Bibliotecas multimedia (formatos de audio, imagen y video), Webkit (navegador), SSL (cifrado de comunicaciones), FreeType (fuentes de texto), SQLite (base de datos), entre otras.

- **Máquina virtual**. El componente principal del entorno de ejecución de Android es la máquina virtual Dalvik (variación de la máquina virtual de Java). Las aplicaciones se codifican en Java y son compiladas en un formato específico para que esta máquina virtual las ejecute. La ventaja de esto es que las aplicaciones se compilan una

única vez y de esta forma estarán listas para distribuirse con la total garantía que podrán ejecutarse en cualquier dispositivo Android que disponga de la versión mínima del sistema operativo que requiera la aplicación.

- **Framework de aplicaciones**. La mayoría de los componentes de esta capa son librerías Java que acceden a los recursos de las capas anteriores a través de la máquina virtual Dalvik.

- **Aplicaciones**. En la última capa se incluyen todas las aplicaciones del dispositivo, tanto las que tienen interfaz de usuario como las que no, las nativas (programadas en C o C++) y las administradas (programadas en Java), las que vienen preinstaladas en el dispositivo y aquellas que el usuario ha instalado. [1]

Las versiones del Sistema Android dan inicio en el 2007 con su versión beta, para el siguiente año fue lanzada su versión 1.0, a partir del año 2009 las actualizaciones y nuevas versiones han sido denominadas en orden alfabético.

5 Adquisición de dispositivos Android

Es importante entender las distintas técnicas de adquisición sobre dispositivos móviles y el tipo de evidencia que permiten obtener. [6]

En el laboratorio de informática forense se aplican tres técnicas de adquisición sobre dispositivos móviles, la adquisición manual, la adquisición lógica y la adquisición física. Esta última puede obtenerse por hardware o por software, siendo la realización de una imagen "En vivo" del dispositivo una técnica de software. Para todas estas técnicas es necesario que el perito tenga acceso al dispositivo. Es decir, que el mismo se encuentre desbloqueado o que se conozca su patrón o código de desbloqueo.

Gráfico 1: Niveles de Adquisición

En la figura se presentan las técnicas mencionadas. A medida que se recorre la pirámide desde abajo hacia arriba, las técnicas son más invasivas sobre el dispositivo y requieren más tiempo y mayor nivel de entrenamiento.

El tipo de adquisición de evidencia que se practique sobre un dispositivo móvil dependerá de las características del mismo y de los puntos de pericia de la investigación. Se intentará dar respuesta a los puntos de pericia utilizando los métodos menos invasivos posibles.

5.1 Adquisición Manual

La adquisición o extracción manual requiere manipular el dispositivo y navegar por su contenido registrando fotográficamente la información descubierta. Esta técnica es agobiante si se intenta registrar gran cantidad de datos, también es propensa a errores debido a la excesiva manipulación del dispositivo.

5.2 Adquisición Lógica

La adquisición o extracción lógica implica la extracción de datos que se encuentran almacenados o asignados en el dispositivo, junto a la utilización de su sistema operativo, cable de conexión y software de sincronización o aplicaciones de transferencias de archivos desarrolladas por terceros. Esto permite la adquisición de la mayoría de los datos en tiempo real del dispositivo. Entre los tipos de datos se incluyen registros de llamadas, registros de llamadas de la tarjeta SIM eliminados, detalles del teléfono (IMEI/ESN), entradas del directorio telefónico, SMS's, imágenes, vídeos, archivos de audio y más.

En la mayoría de los casos, no se puede realizar la extracción lógica en dispositivos bloqueados.

A diferencia de los métodos de extracción física, el método de extracción lógica es más fácil y rápido de realizar por las herramientas de extracción, ya que está limitado a la cantidad de datos que puede extraer. Este método no permite obtener información que haya sido eliminada.

Para la extracción lógica de datos se pueden utilizar diferentes técnicas.

1. Comando adb

Es una herramienta del paquete de desarrollo de Android con Licencia Publica General. Esta herramienta de línea de comando permite comunicarse con el dispositivo móvil, obteniendo información y copiándola en la estación de

trabajo forense. Si no se tiene acceso root no se copiaran aquellos archivos para los cuales no se tenga permiso.

Para poder ejecutar comandos adb es necesario activar la depuración USB en el dispositivo.

2. Resguardos

Se deben conocer que tipos de resguardos existen para luego analizar la tarjeta SD del dispositivo, como así también, si es posible, la computadora, notebook o netbook del usuario, donde puedan existir resguardos del dispositivo analizado.

3. Herramienta AFLogical

Es una herramienta que se distribuye en forma libre para organismos de seguridad. [7]

Para utilizar esta herramienta se debe habilitar la depuración usb en el dispositivo. El programa permite extraer datos en formato CSV (valores separados por coma) y un archivo info.xlm que brinda información detallada del dispositivo y las aplicaciones instaladas.

5.3 Adquisición Física

Para permitir el análisis más completo y detallado del dispositivo, la extracción física accede a capas de datos adicionales, tanto en el espacio asignado como no asignado, que se almacenan en la memoria física del teléfono. Estas capas incluyen tres diferentes grupos de contenidos pertinentes para los investigadores: Contenido "lógico" por ejemplo, registros de llamadas en teléfonos inteligentes, contenido eliminado y contenido que el teléfono recoge sin ninguna acción y a veces sin el consentimiento del usuario, por ejemplo: logs de aplicaciones, redes wifi, ubicaciones GPS, historial web, encabezados de correos electrónicos y datos EXIF en imágenes y datos del sistema.

Las técnicas de extracción física pueden ser por Hardware o Software.

Por Hardware: son métodos que conectan hardware al dispositivo o físicamente extraen los componentes del dispositivo móvil. El equipamiento requerido y su respectiva capacitación suelen ser muy costosos.

El proceso de extracción física por hardware instala código de programación en el dispositivo para omitir el bloqueo, instala y ejecuta código en la RAM

para leer la memoria flash y transfiere los datos a la estación forense. Este proceso se realiza con el dispositivo móvil en "rescue mode" o "download mode", operando en este modo, los dispositivos móviles están diseñados para permitir la inserción de una pequeña pieza de código llamada boot loader dentro de la RAM durante el inicio. [8]

Por Software: son técnicas que se ejecutan como programas en el dispositivo con acceso de usuario root y obtienen una imagen física de todas las particiones de datos.

Este tipo de extracción requiere acceso al dispositivo como usuario root. El acceso root a un sistema operativo permite un control privilegiado del mismo, el rooteo de un dispositivo Android es similar al acceso de los permisos administrativos en Linux o en cualquier otro sistema operativo similar a Unix. Al cambiar los privilegios de acceso se producen modificaciones al dispositivo, además el procedimiento de acceso como usuario root varía según el fabricante y la versión de Android. Por lo tanto resulta ser una técnica con muchos obstáculos y agobiante para el perito. [9]

5.4 Imagen "En vivo" de un dispositivo Móvil

En el laboratorio de informática forense del Poder Judicial de Rio Negro se optó por obtener las imágenes físicas de todas las particiones de un dispositivo móvil a través de Software, realizando una imagen "en vivo" del dispositivo.

Para realizar una imagen en vivo es necesario:

1. Una conexión entre la estación de trabajo forense y el dispositivo móvil a peritar. La conexión es vía USB.

2. Un "exploit" al teléfono que nos permita tener acceso root. Un exploit es un programa que aprovecha una vulnerabilidad para tomar ventaja de esta. En este caso acceso como usuario root y control total sobre el dispositivo

3. Ejecutar un comando que realice la copia.

Se debe conectar el dispositivo a la estación forense a través de un cable USB. La comunicación con el dispositivo será a través de comandos adb, por lo tanto es necesario activar la depuración USB en el dispositivo y tener instalado en la estación de trabajo el SDK Android.

Como se mencionó anteriormente el proceso de rooteo varía según el fabricante y versión de Android. Se utilizan distintos mecanismos:

- Aplicaciones que se ejecutan desde la estación de trabajo forense, accediendo vía usb al dispositivo para intentar el acceso root.
- Aplicaciones que instalan el exploit al dispositivo via adb.
- Acceso al modo de recuperación, modificando una parte de la ROM.

En todos los casos hay que tener en cuenta que es un proceso riesgoso que además de anular la garantía puede llegar a dañar el dispositivo, por lo tanto la implementación de estas técnicas debe ser probada previamente en el laboratorio para minimizar los daños o pérdida de datos en los dispositivos.

No existe una técnica o herramienta que permita el rooteo universal de todos los dispositivos. En el laboratorio se utiliza el software towel root, que se instala vía adb al dispositivo. Este método funciona para la mayoría de los kernels previos a junio de 2014. Para los demás casos se puede consultar online por un método específico de rooteo para el dispositivo en cuestión.

Una vez obtenido el acceso root es necesario ejecutar comandos que permitan realizar la copia. Se utiliza el comando de Linux dd. Este comando generalmente no está disponible en las distribuciones Android, por lo tanto debe ser instalado via adb.

La ejecución de este comando dará como resultado un archivo en formato .dd, que será la imagen en vivo del dispositivo. Esta será copiada a la estación de trabajo forense donde se podrán extraer y resguardar las particiones que deban ser analizadas posteriormente. Una de las particiones de mayor interés será la ***userdata.***

6 Procedimiento Operativo

SOP. Imagen en vivo de un dispositivo Android
Propósito:

Este procedimiento pertenece a la etapa de preservación de dispositivos móviles.

Alcance:

Este procedimiento se aplica exclusivamente a dispositivos Android.

Equipamiento:

Hardware:

a. Computadora Forense

b. Cable usb

Software:

a. Android SDK. Instalado en la Computadora forense
b. Drivers.
c. Aplicaciones de rooteo, administrador de Super usuario y comandos Linux extras.

Limitaciones:

El dispositivo debe estar desbloqueado o conocer su patrón de desbloqueo.
El dispositivo debe contar con espacio suficiente para las aplicaciones de rooteo y administración.
Los resultados dependerán de las capacidades y limitaciones de las herramientas elegidas, como así también la experiencia del perito.

Procedimiento:

Los pasos del procedimiento deben ser documentados con suficiente detalle, de manera que permita a otro forense, competente en la misma área, ser capaz de identificar que se ha hecho y evaluar los resultados independientemente.

1. Preparación
   a. Encender el dispositivo
   b. Configurarlo en modo Avión
   c. Activar la depuración usb.
2. Conexión a la estación de trabajo
   a. Conectar el dispositivo via USB
   b. Instalar drivers en la computadora forense.
3. Realización de la imagen.
   a. Instalar y ejecutar software de rooteo.
   b. Instalar y ejecutar software de administración de Super Usuario
   c. Instalar comandos Linux extra (dd)
   d. Ejecutar comando dd para realizar la copia forense del dispositivo en la computadora forense.

7 Validez de la técnica

A diferencia de la adquisición de dispositivos tradicionales, donde se realiza una copia bit a bit de su medio de almacenamiento, pudiendo calcular el hash

del mismo para garantizar su integridad, la adquisición de un dispositivo móvil no es tan simple. El medio de almacenamiento de un dispositivo tradicional es solo almacenamiento, mientras que un dispositivo móvil es un sistema completo que incluye almacenamiento. La realización de la imagen en vivo de un dispositivo Android requiere conectarlo a una pc y ejecutar comandos sobre el mismo, lo cual modifica los datos del dispositivo. Si bien este tipo de técnicas confronta con algunos principios tradicionales de la informática forense, en los últimos años están siendo aceptadas por la comunidad profesional, siempre que estas modificaciones menores para la introducción del software de vuelco de datos sean practicadas en un entorno controlado de laboratorio y considerando procedimientos de trabajo formalmente establecidos que garanticen su repetibilidad y reproducibilidad.

La validez de esta técnica será respaldada con una correcta documentación de cada paso realizado para la obtención de la imagen, evitando además las modificaciones innecesarias.

Con respecto a la “solidez forense” de este método puede decirse que establecer un estándar absoluto que dicte "preservar todo pero no cambiar nada" es incompatible con otras disciplinas forenses. [10]

Los puristas argumentan que la adquisición forense no debería alterar la fuente de evidencia original de ninguna manera. Sin embargo, disciplinas forenses tradicionales tales como análisis de ADN muestran que la solidez forense no requiere que la fuente original no sea alterada.

Cuando se toman muestras de material biológico quedan manchas o rasguños en la evidencia original. A pesar de estos cambios que ocurren durante la preservación, estos métodos son considerados sólidos y el ADN es admitido generalmente como evidencia.

8 Conclusiones

La creciente demanda de pericias sobre dispositivos móviles con tecnología Android plantea un desafío para los peritos informáticos. La adquisición de dichos dispositivos no es una tarea trivial y si bien la experiencia del perito es importante al momento de determinar la mejor manera de realizar una extracción, cada dispositivo con sus variantes de fabricantes y versiones de sistema operativo aporta un grado de incertidumbre en esta etapa del proceso.

Como se mencionó anteriormente, en el laboratorio de informática forense se intenta adquirir la evidencia digital de los dispositivos móviles utilizando las técnicas menos invasivas posibles. De esta manera, solo se intenta realizar una imagen en vivo del dispositivo cuando los puntos de pericia así lo requieren.

Según los datos estadísticos del laboratorio, se pudo realizar una imagen en vivo en el 60% de los casos en que se intentó. Esta técnica presenta sus principales limitaciones al no poder lograr acceso privilegiado (root) en los dispositivos más nuevos.

Se incluye la obtención de la imagen en vivo de dispositivos en el marco de un procedimiento operativo estandarizado a fin de otorgarle el marco formal adecuado que permita ofrecer rigurosidad y control de calidad en la integración de métodos y técnicas que utiliza el laboratorio.

Este procedimiento forma parte del manual de operaciones que regula las actividades del personal del área y como tal está sujeto a revisiones y modificaciones periódicas con el objetivo de mantener su correctitud y eficacia.

9 Referencias:

1. Larrota Ardila Luz Stella, Martinez Zabala Jeimy Marcela, Orjuela López Viviana Francenet. Diseño de una guía para la auditoría de análisis forense en dispositivos móviles basados en tecnología Android para la legislación colombiana. 2014

2. Carrier y Asociados. Cerrando la brecha con LTE. http://www.carrieryasoc.com//wp-content/uploads/5.%20Cerrando%20la%20brecha%20con%20LTE.pdf

3. Leopoldo Sebastián Gómez. Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados.
SID 2015, 15º Simposio Argentino de Informática y Derecho.

4. Gartner Newsroom. Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016. http://www.gartner.com/newsroom/id/3415117.

5. Android Architecture. http://elinux.org/Android_Architecture.

6. Rick Ayers Sam Brothers Wayne Jansen. NIST Special Publication 800-101 Revision 1. Guidelines on Mobile Device Forensics. Mayo 2014.

7. HOWTO: Use AFLogical OSE for Logical Forensics of an Android Device. https://santoku-linux.com/howto/howto-use-aflogical-ose-logical-forensics-android/

8. EXPLAINING CELLEBRITE UFED DATA EXTRACTION PROCESSES.
http://www.cellebrite.com/pages/explaining-cellebrite-ufed-data-extraction-processes

9. Maria Elena Darahuge. Luis E. Arellano Gonzalez . Manual de Informática Forense II.. Errepar 2012.

10. Eoghan Casey and Gerasimos J. Stellatos. The Impact of Full Disk Encryption on Digital Forensics.