FORENSE DIGITAL EN DISPOSITIVOS MÓVILES BAJO SISTEMA OPERATIVO ANDROID 7.1 O SUPERIOR

HUGO ERNESTO MOLINA RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2019

FORENSE DIGITAL EN DISPOSITIVOS MÓVILES BAJO SISTEMA OPERATIVO ANDROID 7.1 O SUPERIOR

HUGO ERNESTO MOLINA RODRÍGUEZ

Monografía para optar por el título de Especialista en Seguridad Informática

Director/Asesor de opción de trabajo de grado

MARTÍN CAMILO CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2019

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., 18 de marzo de 2019

DEDICATORIA

Quiero dedicar mi trabajo de grado a Dios, a mi hijo, mi madre, mi familia en general y a los docentes de la universidad.

A Dios agradezco por permitirme tener todas las bendiciones que implican poder desarrollar este trabajo de grado como mi trabajo, mi salud, el tiempo e infinidad de bendiciones que me permitieron escribir estas líneas.

A mi hijo, Sebastián David Molina, quien es mi motivación para seguir adelante en cada una de las actividades académicas que realizo con la ilusión de poder brindarle un mejor futuro y de demostrarle que todo lo que queremos realizar se puede con determinación, motivación, dedicación y con amor por lo que hacemos.

A mi madre por estar siempre pendiente de mí y apoyarme en cada uno de los pasos que doy, por ser esa fuente de inspiración junto con mi hijo para ser un mejor profesional, hombre, hijo, padre y compañero.

A los todos los profesores que me acompañaron en este proceso, que me guiaron y me aconsejaron para obtener el conocimiento necesario para realizar este trabajo de grado.

AGRADECIMIENTOS

Mi especial agradecimiento es para la universidad que con sus políticas y beneficios que brindan a los egresados me permitieron crecer profesionalmente por medio del postgrado en seguridad informática.

También agradezco a cada uno de mis compañeros con quienes compartí, aprendí y crecí en cada uno de los pasos que me llevan a obtener este amado título de especialista.

CONTENIDO

GLOSARIO

Kernel: También es conocido como el núcleo del sistema operativo. Es el software que se encarga de administrar los recursos del hardware que contenga un dispositivo restringiendo el acceso a solo aplicaciones autorizadas.

Archivos DEX: Es un formato diseñado para Android el cual es muy eficiente y ocupa un espacio reducido de memoria.

ROOT: Corresponde a la modificación del sistema operativo Android el cual permite tener permisos de super usuario sobre el sistema operativo.

Análisis Forense: El análisis forense en el procedimiento estructurado y bajo ciertas técnicas que permiten reconstruir una secuencia de sucesos de un incidente de seguridad de la información. Este análisis tiene la capacidad de responder el quien realizó la actividad irregular, cómo la ejecutó, desde dónde, cuándo y las acciones que ejecuto para comprometer el sistema.

Incidente de Seguridad de la Información: Para la norma ISO 27000 de Seguridad de la información, un incidente de seguridad es "uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información."[1]

Imagen Forense: Es un mecanismo de copia binaria de un medio electrónico de almacenamiento en el cual se incluyen no solo los espacios ocupados por archivos informáticos sino también los espacio borrados.

Delito informático: Es toda acción declarada en la ley colombiana, 1273 de 2009, que atentan contra la confidencialidad, integridad y disponibilidad de la información.

Prueba: Es componente físico o digital que permite mostrar con una determinación razonable o argumentada la ejecución de una acción o un suceso.

---

[1] Norma ISO/IEC 27000:2014(E). Information technology — Security techniques — Information security management systems — Overview and vocabulary. 15 de enero de 2014. p. 3.

Evidencia: Es una secuencia de pruebas que nos permite dar por hecho la ejecución de una acción o un suceso y determinar la valides de una proposición.

Cadena de Custodia: Es un procedimiento metódico y controlado que garantiza que la evidencia se recolectó de manera satisfactoria de la escena del delito y que esta evidencia no presenta ninguna alteración en su integridad. Este procedimiento inicia desde la recolección de las evidencias hasta la entrega de la misma a un juez como material probatorio de los hechos.

RESUMEN

Con el auge de los dispositivos móviles, como equipos electrónicos que hacen parte de IoT, las personas confían y entregan su información para que estos gestionen de alguna manera la información personal o corporativa[2]. Esta actividad ya es una tendencia a nivel mundial y está siendo parte de la cultura o idiosincrasia humana, tanto es así, que los ciber delincuentes utilizan a los dispositivos móviles como un vector de ataque para cumplir con metas ilegales.

De acuerdo con lo anterior es necesario realizar un estudio monográfico que permita analizar técnicas forenses digitales en dispositivos móviles con s/o Android 7.1, o superior con validez legal en Colombia de acuerdo con la ley 1564 DE 2012, código de procedimiento civil, en su artículo 243 donde indica "Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares"[3] y con la ley Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones en sus artículos 2, 10 y 11[4]. Es así como se ve la pertinencia de tener claridad sobre la arquitectura y del funcionamiento de estos dispositivos para conocer de mejor manera sus patrones o forma de trabajar para lograr recolectar evidencia que se pueda analizar y determinan las causas de un evento o incidente de seguridad de la información.

Además de tener la claridad la arquitectura y funcionamiento de los dispositivos móviles, se debe conocer el estudio y evaluación de aplicaciones que sean funcionales y confiables para el análisis forense de dispositivos móviles bajo el sistema operativo Android en su versión 7.1 o superior.

---

[2] Deloitte. Consumo móvil en Colombia. [En línea]. Bogotá: Deloitte. Disponible en https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil(VF1).pdf

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1564 DE 2012 (12, julio, 2012). Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. CONGRESO DE LA REPÚBLICA. Bogotá D. C., 2012. 109 p.

[4] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 DE 1999 (121, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. CONGRESO DE LA REPÚBLICA. Bogotá D. C., 1999. 1-3 p.

En esta monografía vamos a identificar las características funcionales del sistema operativo Android, la arquitectura del S.O., las herramientas tecnológicas que son funcionales y confiables para el análisis forense y los pasos para ejecutar un proceso de análisis forense a un dispositivo móvil.

Finalmente, esta monografía busca concluir un proceso integral de recolección de técnicas forenses digitales en dispositivos móviles con S/O Android 7.1, o superior y que sea un mecanismo de aprendizaje para la sociedad y lectores de este documento.

INTRODUCCION

Hoy el día el incremento de dispositivos móviles en el diario vivir de la sociedad humana es una necesidad que las personas tienen para poderse comunicar con otras personas por medio de redes intercomunicadas con estos dispositivos[5]. Es un fenómeno que ha crecido desde que llegó la revolución digital a la vida humana y no tiende a disminuir su uso, por el contrario, tiende a crecer a medida que evoluciona la tecnología.

Así como estos cambios tecnológicos traen beneficios que permiten que las personas puedan optimizar sus recursos y tiempo al poder realizar una teleconferencia desde cualquier lugar, o realizar pagos de servicios desde su dispositivo móvil, también traen grandes desafíos en términos de seguridad de la información y nuevas oportunidades para los delincuentes que desean cometer sus ilícitos sin exponerse demasiado.

Este trabajo analiza las técnicas forenses digitales en dispositivos móviles tomando como guía las buenas prácticas de estándares internacionales como lo es la NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response o el Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 de la Organización De Estados Americanos. Detalla los pasos esenciales que se deben tener en cuenta para realizar un peritaje informático exitoso sobre dispositivos móviles. Tomaremos como referencia de esta investigación un dispositivo móvil, Android, con un sistema operativo 7.1 o superior sin rooteo y con rooteo para poder determinar el alcance del análisis forense en este tipo de dispositivos. y busca ampliar las habilidades que son indispensables para un especialista de seguridad informática para que pueda enfrentarse con los retos que trae el mundo de la ciberseguridad tanto a nivel mundial como a nivel laboral y personal.

Finalmente, el propósito es generar conocimiento a la comunidad interesada en obtener estas habilidades para su ámbito laboral o personal.

[5] Deloitte. Óp. Cit., p 4.

1 PROBLEMA DE INVESTIGACION

1.1 ANTECEDENTES DEL PROBLEMA

Los sistemas de información cobran cada vez más importancia en la vida y evolución humana, así lo dice indica la empresa Tech Crunch, donde estima que existirán más de 6 mil millones de usuarios de smartphones en el 2020[6]. Con este aumento de dispositivos móviles crece el riesgo de que estos dispositivos puedan verse comprometidos en delitos informáticos por medio de un programa maligno diseñado específicamente para este tipo de tecnologías por los ciberdelincuentes.

Investigadores de la universidad de Cambridge identificaron que el 87% de los teléfonos inteligentes con sistema operativo Android estaba expuestos con al menos una vulnerabilidad crítica en sus sistemas.[7]

Uno de los vectores más utilizados por los ciberdelincuentes es el desarrollo de aplicaciones móviles con código malicioso que permite que el atacante tome provecho del dispositivo a su antojo. Así lo demuestra un estudio realizado por la empresa Dark Reading, donde identificaron que el malware en aplicaciones de banca aumentó en el tercer trimestre del año 2015 debido al alto uso de los usuarios para utilizar este medio para realizar pagos de servicios, facturas, transferencias y todas aquellas funcionalidades que les permite realizar una banca móvil.[8]

1.2 PLANTEAMIENTO DEL PROBLEMA

De acuerdo con lo estipulado en la ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones, en su artículo 11 donde especifica que:

---

[6] Tech Crunch. 6.1B Smartphone Users Globally By 2020, Overtaking Basic Fixed Phone Subscriptions. [En línea]. Bogotá: Tech Crunch. Disponible en https://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/#.n7ibu3d:RPIH

[7] BERESFORD, Alastair. Security Metrics for the Android Ecosystem. [En línea]. Bogotá: University of Cambridge. Disponible en https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

[8] CHICKOWSKI, Ericka. Mobile Malware Makes Mobile Banking Treacherous. [En línea]. Bogotá: Dark Reading. Disponible en https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

> Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.[9]

De acuerdo con la mencionada ley, la recolección de evidencia, conservación y su presentación debe contener el principio de confiabilidad para que una evidencia tenga algún valor probatorio ante un juez esta debe mantener los principios del peritaje como: Objetividad, Autenticidad y Conservación, Legalidad, Idoneidad, inalterabilidad y documentación.[10]

Realizar un análisis forense requiere de un conocimiento experto y habilidades en la recolección, conservación y presentación de la evidencia ante un juez para que estas pruebas cumplan con lo requerido en ley 1564 DE 2012, código de procedimiento civil, en su artículo 243 y la ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones en sus artículos 2, 10 y 11. . Es así, que este trabajo busca establecer una guía para lograr desarrollar un análisis forense a un dispositivo móvil con sistema operativo Android 7.1, o superior cumpliendo con las premisas y requerimiento del manejo de la evidencia digital para que esta tenga todo el valor legal en Colombia, de acuerdo con las leyes mencionadas en este párrafo, y pueda ser presentada como una prueba fehaciente en un caso determinado.

---

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 DE 1999 (121, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. CONGRESO DE LA REPÚBLICA. Bogotá D. C., 1999. 1-3 p.

[10] ACURIO DEL PINO, Santiago. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0. [En línea]. Bogotá: Organización De Estados Americanos. Disponible en https://www.oas.org/juridico/english/cyb_pan_manual.pdf

1.3 FORMULACION DEL PROBLEMA

¿Cómo realizar un análisis forense a un dispositivo móvil con sistema operativo Android 7.1, o superior? Debido al incremento exponencial a nivel mundial sobre el uso de dispositivo móviles que realiza actualmente las empresas y personas para su uso personal y mantenerse conectados en el mundo digital[11], crecen las vulnerabilidades y amenazas que pueden llevar a que un riesgo se materialice. Aunque muchas personas no tengan el conocimiento técnico, un dispositivo móvil puede llegar a estar involucrado en un incidente de ciberseguridad afectando su confidencialidad, integridad o disponibilidad del dispositivo, información o de los servicios que este presta, siendo esta característica uno de los mayores riesgos que sufre un usuario de un dispositivo móvil[12].

Por otro lado, la falta de conocimiento para identificar si un dispositivo móvil está comprometido con un software malicioso conlleva a que las personas o empresas no conozcan la manera de enfrentar este incidente de seguridad de la información o cómo actuar cuando su dispositivo móvil se ve involucrado en un delito informático o fue víctima de un ciberdelincuente.

Un estudio realizado por Threat Intelligence Report de Nokia, identificó que el malware en el año 2016 fue superior en un 95% con respecto al año anterior. Llegando a identificar 12 millones de muestras de malware en dispositivos Nokia.[13]

Este estudio ayuda identificar la cantidad de software malicioso que existe a nivel mundial y la velocidad vertiginosa con la que crece, siendo esta la razón por la cual es importante identificar los pasos y buenas practicar a la hora de recolección de evidencias en dispositivos móviles.

[11] Tech Crunch, Óp. cit.
[12] BERESFORD, Alastair, Óp. cit., p 4.
[13] Nokia Threat Intelligence Laboratories. Nokia Threat Intelligence Report. [En línea]. Bogotá: Nokia Threat Intelligence Laboratories. Disponible en https://onestore.nokia.com/asset/201094

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar un estudio monográfico que permita analizar técnicas forenses digitales en dispositivos móviles con s/o Android 7.1, o superior con validez legal en Colombia de acuerdo con su normatividad.

2.2 OBJETIVOS ESPECÍFICOS

1. Identificar la arquitectura del S.O. de dispositivos móviles Android.
2. Reconocer las características funcionales del sistema operativo Android que permiten ejecutar un análisis forense sobre estos dispositivos.
3. Identificar las herramientas tecnológicas que sean funcionales y confiables para el análisis forense de dispositivos móviles bajo el sistema operativo Android en su versión 7.1 o superior.
4. Ejecutar un proceso de análisis forense a un dispositivo móvil con sistema operativo Android en su versión 7.1 o superior.

3 JUSTIFICACIÓN

Es importante mencionar qué la monografía pretende ser un documento de conocimiento para la sociedad, para que las personas puedan realizar un proceso de análisis forense para a un dispositivo móvil con sistema operativo Android en su versión 7.1 o superior. En su mayoría, los ingenieros, las empresas, el gobierno y sociedad en general no tienen conocimiento sobre cómo gestionar un incidente de seguridad donde se ve involucrados dispositivos móviles y es necesario abordar estos temas y explicar cómo se debe realizar una investigación forense de acuerdo con cada una de sus fases y como se debe analizar las evidencias digitales que puede tener un dispositivo móvil sin afectar su integridad como evidencia.

El conocimiento que se plasma en este trabajo permite que cualquier persona que lea este trabajo comprenda y adquiera las bases para lograr realizar una investigación forense cumpliendo con los requerimientos mínimos que establece la normatividad legal colombiana en sus leyes, Ley 1564 DE 2012, código de procedimiento civil, en su artículo 243 y la Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones en sus artículos 2, 10 y 11.

4 MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

Android Fue diseñado originalmente por estadounidense Andy Rubin, quien creo la compañía Android Inc. en el año 2003. Con Android Inc. Andy buscaba desarrollar software para smartphones y desarrollar contenidos innovadores que permitieran la evolución de estos dispositivos.[14]

"Con el éxito que estaba teniendo Android Inc. Google centró su atención en este startup y viendo que estaba alienada con sus intereses decidió comprarla en el año 2005". Sin embargo, con la compra por parte de Google, Andy Rubin, paso a ser trabajador de Google como vicepresidente de ingeniería de Google supervisando el desarrollo de Android.[15]

Finalmente, Android fue presentado en el 2007 a nivel mundial como un avance tecnológico y evolución de los sistemas operativos para dispositivos móviles. "De esta manera se da inicio a una de las plataformas más usados a nivel mundial para dispositivos inteligentes con más del 80% para su uso en el 2017"[16].

Android se basa en el kernel de Linux, el cual es un sistema operativo abierto en el cual la comunidad contribuye para su desarrollo y es esta característica que le ha ayudado a surgir a través del tiempo porque no solo la comunidad puede interactuar

[14] Blog Historia de la Informática, Iván. Android. [En línea]. Bogotá: histinf.blogs.upv.es. Disponible en https://histinf.blogs.upv.es/2012/12/14/android/

[15] RAMÍREZ, Iván. Historia y evolución de Android: cómo un sistema operativo para cámaras digitales acabó conquistando los móviles. [En línea]. Bogotá: xatakandroid. Disponible en https://www.xatakandroid.com/sistema-operativo/historia-y-evolucion-de-android-como-un-sistema-operativo-para-camaras-digitales-acabo-conquistando-los-moviles

[16] Pcmag Noticias. El 99.6% del mercado móvil le pertenece a Android y iOS. [En línea]. Bogotá: pcmag. Disponible en http://latam.pcmag.com/sistemas-operativos-moviles/18490/news/el-996-del-mercado-movil-le-pertenece-a-android-y-ios

con el sistema operativo sino también los grandes fabricantes de smartphones como LG, Samsung, HTC, Nokia, entre otros.[17]

Desde sus inicios Android ha tenido varias versiones, cada una con nuevas características en comparación con su antecesora. Una de las principales características es que desde la versión 1.5 Cupcake, se lleva un orden alfabético y con nombres relacionados a postres o dulces debido a que su creador ama los productos dulces. Las versiones oficiales de Android son[18]:

- Android 1.5. Cupcake.
- Android 1.6. Donut.
- Android 2.1. Eclair.
- Android 2.2. Froyo.
- Android 2.3. Gingerbread.
- Android 3.0. Honeycomb.
- Android 4.0. Ice Cream Sandwich.
- Android 4.1. Jelly Bean.
- Android 5.0. Lollipop.
- Android 6.0. Marshmallow.
- Android 7.0. Nougat.
- Android 8.0. Oreo.
- Android 9.0. Pie.

Debido al incremento exponencial a nivel mundial sobre el uso de dispositivos móviles con sistema operativo Android que realiza actualmente las empresas y personas para su uso personal y mantenerse conectados en el mundo digital, crecen las vulnerabilidades y amenazas que pueden llevar a que un riesgo se materialice[19]. Investigadores de la universidad de Cambridge identificaron que el 87% de los teléfonos inteligentes con sistema operativo Android estaba expuestos

[17] BÁEZ, Manuel. Introducción a Android. [En línea]. Bogotá: xatakandroid. Disponible en https://s3.amazonaws.com/academia.edu.documents/34556195/android.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1552618190&Signature=d7T%2FkaVJBYHN4pp%2FHAJM6wlm3eA%3D&response-content-disposition=inline%3B%20filename%3DG_-Te_C_Introduccion_a_Android.pdf
[18] BÁEZ, Manuel. Óp. cit., p 2.
[19] Tech Crunch, Óp. cit.

con al menos una vulnerabilidad crítica en sus sistemas.[20] demostrando que se puede llegar atacar a un dispositivo móvil afectando su confidencialidad, integridad o disponibilidad del dispositivo, información o de los servicios que este presta. Es por esto que nos lleva a preguntarnos. ¿Cómo realizar un análisis forense a un dispositivo móvil con sistema operativo Android 7.1, o superior?

Es necesario tener las habilidades y conocimientos que nos ayuden a identificar las causas de los eventos que generan la materialización de un riesgo a través de un dispositivo inteligente con sistema operativo Android 7.1 o superior. Como se mencionó anteriormente, Android en el sistema operativo más utilizado en el mundo con cerca del 80% del mercado mundial[21]. Así mismo, es muy común ver que estos dispositivos se encuentren involucrados en incidentes de seguridad; como ser parte de una red botnet o simplemente que fueron utilizados para realizar actos ilícitos. Es importante lograr obtener información que permitan identificar los hechos ocurridos en estos dispositivos.

Actualmente se cuenta con una gran cantidad de herramientas que nos ayudan a realizar un proceso forense, alguna de ellas con pagas y otras no, o simplemente son open source. Dentro de estas herramientas tenemos:

Tabla 1. Herramientas forenses digitales

Tipo	Herramienta	Descripción	Página Oficial
Bloqueadores hardware	Tableau Digital Intelligence	Son dispositivos físicos que se conectar de entre el equipo del investigador forense y el disco al cual se busca realizar el proceso forense. De esta manera estos dispositivos permiten mantener la integridad impidiendo la escritura sobre el disco de almacenamiento al cual se esté realizando un proceso forense.	https://www.guidancesoftware.com/tableau/hardware?types=Forensic-Bridges https://digitalintelligence.com/products/ultrablock

[20] BERESFORD, Alastair. Óp. cit., p 4.
[21] Pcmag Noticias. El 99.6% del mercado móvil le pertenece a Android y iOS. [En línea]. Bogotá: pcmag. Disponible en http://latam.pcmag.com/sistemas-operativos-moviles/18490/news/el-996-del-mercado-movil-le-pertenece-a-android-y-ios

Bloqueadores software	Tequila: Es un sistema operativo basado en Linux, desarrollado en Latinoamérica, especializado para la informática forense. Su interfaz gráfica es fácil de entender y al ser una versión libre su soporte es limitado	su principal característica es que son sistemas operativos basado en Linux especializados para realizar tareas de análisis forense. Una de sus funciones que puede funcionar como bloqueadores. Al ser sistemas operativos pueden controlar el uso del hardware donde se encuentren instalados o en ejecución. Dada esta característica, estos sistemas operativos bloquean la escritura de los puertos USB de los equipos donde están instalados. De esta manera, cualquier dispositivo que se instale por el puerto USB solo funcionará en modo lectura.	https://tequila-so.org/
	Caine: Es un sistema operativo basado en Linux, desarrollado en Italia, especializado para la informática forense. Su interfaz gráfica es fácil de entender y al ser una versión libre su soporte es limitado		https://www.caine-live.net/
	SANS DFIR:	es una appliance virtual basado en Linux, especializado para la informática forense. Tiene una gran cantidad de características que la hace una de las mejores distribuciones para realizar este tipo auditorías	https://digital-forensics.sans.org/
Herramientas	Encase	Es una de las herramientas más completas a nivel mundial para la toma y análisis de imágenes forenses, contiene una gran cantidad de funcionalidades que optimizan el proceso de búsquedas de evidencias. Con tiene una versión libre la cual es bastante limitada y su versión pro es bastante costosa	https://www.guidancesoftware.com/encase-forensic
	Autopsy	Es una plataforma especializada para la ejecución de actividades de informática forense, esta aplicación es multiplataforma trabajando en sistemas operativos como Linux y Windows. Su interfaz gráfica es fácil de entender y al ser una versión libre su soporte es limitado	https://www.sleuthkit.org/autopsy/.
	adb Shell	Android Debug Bridge, adb, es una herramienta que permite a un dispositivo móvil, con sistema operativo Android, tenga comunicación con el equipo del investigador forense. De esta manera el investigador puede analizar de manera más profunda un dispositivo móvil sin limitarse solo a los recursos compartidos o a la tarjeta de almacenamiento masivo adicional que contenga el equipo móvil	http://adbshell.com/
	FTK Access data	Es una herramienta que contiene su versión libre la cual permite realizar toma de imágenes forenses bit a bit, pero para el análisis de esta es necesario adquirir su versión pro. El soporte para su versión profesional es bastante bueno.	https://accessdata.com/products-services/forensic-toolkit-ftk

Sistema Operativo	Santoku	Es un sistema operativo basado en Linux especializado para realizar el análisis forense a dispositivos móviles, análisis de malware en dispositivos móviles y análisis de seguridad en dispositivos móviles. Su interfaz gráfica permite que sea muy amigable de usar	https://santoku-linux.com.
	DEFT	Digital Evidence & Forensics Toolkit es un sistema operativo basado en Linux concebido para realizar tareas especificas y especializadas en análisis de evidencia digital.	http://www.deftlinux.net/
	ADIA	Appliance for Digital Investigation and Analysis. Es una appliance virtual montada sobre CenOS 7 la cual contiene una serie de herramientas enfocadas a la solución de incidentes relacionados con Informática forense.	https://forensics.cert.org/appliance/README.html

Este trabajo se basa su desarrollo de herramientas libres de código open source, el cual también aceptado para realizar procesos forenses por su validez legal y funcionalidad. Dentro de este software tenemos:

- ✓ ADB Shell.
- ✓ Santoku.

4.2 MARCO CONCEPTUAL

Para poder ejecutar un análisis de evidencia digital se requiere una persona con conocimientos como perito informático.

Un perito informático es una persona con conocimientos especializados en informática, hacking, recolección y análisis de evidencias digitales. “Su función principal consiste en el análisis de elementos informáticos, en busca de aquellos datos que puedan constituir una prueba o indicio útil para el litigio jurídico al que ha sido asignado”[22].

El perito informático debe seguir una serie de fases que ayude a guiar de una manera más amable la investigación.

[22] BASSINI, Andrés. El perito informático y la prueba pericial. [En línea]. Bogotá: Derechopenalonline.com. Disponible en http://derechopenalonline.com/el-perito-informatico-y-la-prueba-pericial/

“Fases del proceso del manejo de una evidencia”[23]:

- ✓ Fase 1- Aislamiento de la escena.
- ✓ Fase II - Identificación de fuentes de información, pasos iniciales de adquisición de información.
- ✓ Fase III - Recolección y examinación de información.
- ✓ Fase IV - Análisis de la información
- ✓ Fase V - Reporte

Asimismo, aparte de seguir las fases del proceso forense, también debe seguir una serie de actividades que permitan recolectar información integra y que sea susceptible a ser corroborada en el proceso judicial o incriminatorio que sea expuesto el caso. Estas actividades corresponden a:

Información imágenes de discos duros: Consiste en la generación de las imágenes de datos que conciernen al caso en investigación.

Recreación de una imagen de disco: Consiste en la reproducción de la imagen obtenida en el paso anterior. Para esta actividad se recomienda siempre trabajar con una copia de la imagen original, así mismo, utilizar programas especializados para este fin como lo son: FTK, Encase, Autopsy, CAIN y Santoku.

Revisar una evidencia: En esta fase se realizará un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser.

Algunas de las herramientas que ayudan al proceso investigativo forense son:

Herramientas para análisis forense autopsy: Autopsy® es un programa fácil de usar, basado en GUI, que le permite analizar de forma eficiente discos duros y teléfonos

[23] Ministerio de Tecnologías de la Información y Comunicaciones. Seguridad y privacidad de la información. Guia No. 13. [En línea]. Bogotá: Mintic. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

inteligentes. Tiene una arquitectura de plug-in que le permite encontrar módulos complementarios o desarrollar módulos personalizados en Java o Python.

Herramientas de recolección de información anti-forense: El término de evasión forense o anti-forense se refiere a las técnicas de eliminación y/o de ocultación de pruebas para complicar o imposibilitar la efectividad del análisis forense, existen herramientas que ayudan con la eliminación de todo este tipo de evidencias. Por ejemplo; RuneFS Tool, The Defilers Toolkit, Necrofile Tool, Klismafile Tool, entre otros.

Análisis de imágenes de discos: Con la información recolectada de la evidencia principal, procedemos a realizar un análisis con estas etapas:

- ✓ Análisis de la información prioritaria.
- ✓ Generación de listado de archivos comprometidos con el caso.
- ✓ Obtención de la línea de tiempo de la evidencia.
- ✓ Generación de informe final.

Recolección y conocimiento de los elementos que puede tener una evidencia: La Evidencia Digital o la prueba electrónica es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio. las evidencias deben ser:

- ✓ Relevante: debe pertenecer al caso real.
- ✓ Material: la evidencia debe demostrar o refutar los hechos que afectan a la cuestión ante el tribunal (que suele ser: "hizo el acusado cometer el delito que se le acusó a").
- ✓ Competente: la evidencia debe ser demostrada, ser realmente lo que pretende ser.

Se aplican todas las fases del proceso de peritaje de una evidencia: Es indispensable que todos los pasos anteriormente descritos sean ejecutados por el perito informático de una manera independiente y con el debido cumplimiento de los pasos o fases descritas con el fin de poder certificar las evidencias recolectadas para que un juez pueda determinar la inocencia o culpabilidad de un individúo.

Sin embargo, en su mayoría, los ingenieros, las empresas, el gobierno y sociedad en general no tienen conocimiento sobre cómo gestionar un incidente de seguridad donde se ve involucrados dispositivos móviles y es necesario abordar estos temas y explicar cómo se debe realizar una investigación forense de acuerdo a cada una de sus fases presentadas y como se debe analizar las evidencias digitales que puede tener un dispositivo móvil sin afectar su integridad como evidencia y las leyes que los regulan.

Este trabajo debe mejorar de manera significativa el impacto social a través del conocimiento que se plasmara para que cualquier persona que lea este trabajo, comprenda y tenga bases para lograr realizar una investigación forense cumpliendo con los requerimientos mínimos que establece la normatividad legal colombiana para el manejo de evidencias digitales.

4.3 MARCO ESPACIAL

Este trabajo se desarrolla en la ciudad de Bogotá D.C., Colombia, en la cual existen leyes, normatividades, frameworks, tanto nacionales como internaciones que permiten el desarrollo de este trabajo.

4.4 MARCO LEGAL

En Colombia existe leyes, como la ley 1273 del 2008 ley de delitos informáticos, el régimen probatorio en el Derecho Colombiano se encuentra consagrado en el Código de Procedimiento Civil, Sección tercera, Título XIII, ley 1564 DE 2012, código de procedimiento civil, en su artículo 243 y la ley 527 de 1999, Por medio de

la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones en sus artículos 2, 10 y 11.

A nivel internacional existen estándares que se toman como referencias de buenas prácticas para el adecuado manejo de evidencia digital. Algunos de estos estándares internacionales son: International Organization on Computer Evidence - IOCE, la Convención de Cybercrimen expuesta por la Comunidad Europea, el Digital Forensic Research Workshop-DFRWS 2001, donde establecen lineamientos o frameworks para el desarrollo de recolección de evidencia digital manual, NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response o el Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 de la Organización De Estados Americanos.

5 DESARROLLO DE LA PROPUESTA

5.1 CAPITULO 1. ARQUITECTURA DEL SISTEMA OPERATIVO ANDROID

Es sistema operativo de Android es uno de los sistemas operativos más usados a nivel mundial para dispositivos móviles, como: SmartPhones, Tabletas, SmartTV, SmartWatch, entre una infinidad de dispositivo móviles.

Android se basa en el kernel del sistema operativo Linux y está dividido por 5 capas que permiten su correcto funcionamiento, estas capas son:

- Kernel de Linux.
- Capa de abstracción de hardware.
- Librerías nativas de C/C++ / Runtime de Android.
- Marco de API de JAVA.
- Aplicaciones del sistema.

La arquitectura basada en las capas mencionadas anteriormente es la vigente desde Android 5.0 hacia adelante.

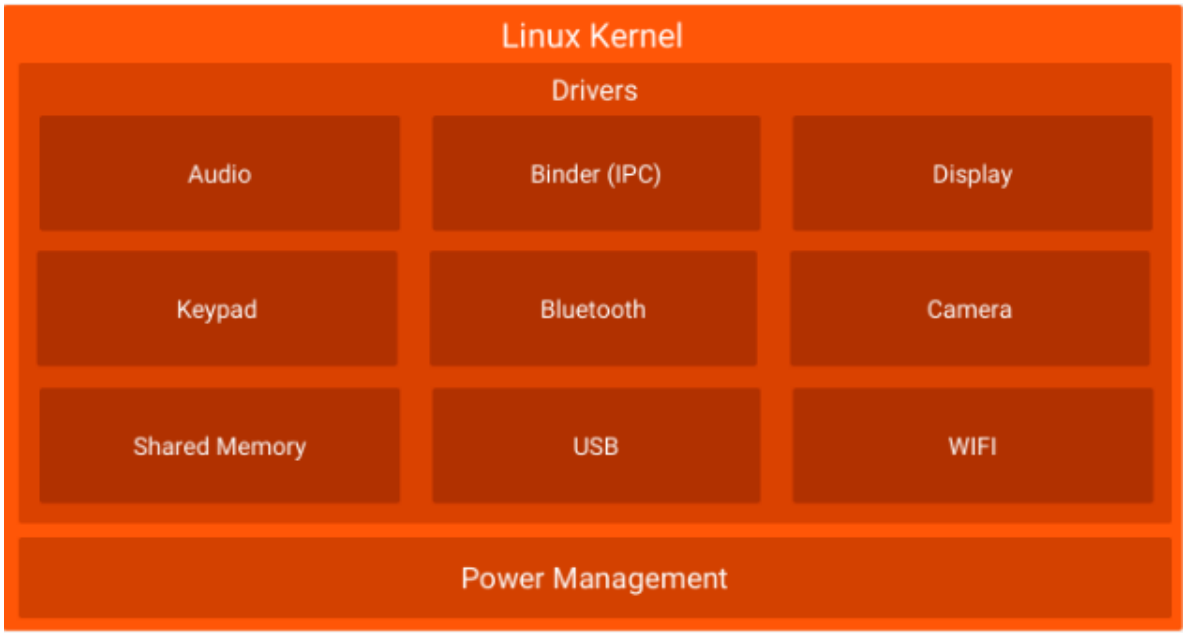
5.1.1 Kernel de Linux:

El kernel o núcleo es la base de todo el sistema operativo de Android, es el software responsable de la administración de todos los elementos de hardware con contiene el dispositivo. Así mismo, controla cuales son la aplicaciones o software que puede tener acceso a cada una de estas funcionalidades.

En términos de un dispositivo móvil, el kernel permite gestionar la memoria compartida, WiFi, los puertos USB, teclado, Bluetooth, Cámara, Audio, Binder (IPC) y Display.

En la imagen 1, vemos cómo está compuesta la capa base de la arquitectura del sistema operativo Android.

Imagen 1: Kernel de Android



Fuente: https://developer.android.com/guide/platform/?hl=es-419

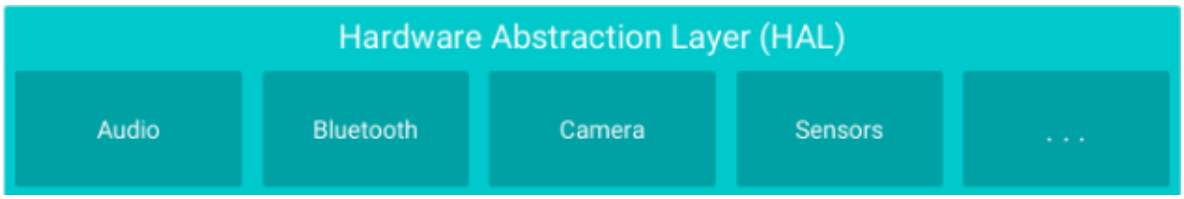
5.1.2 Capa de abstracción de hardware:

La capa de abstracción de hardware tiene como funcionalidad detectar dispositivos, administra aplicaciones y dispositivos de almacenamiento de tal manera que la capa de API de Java pueda utilizarlas para ejecutar el funcionamiento de las características del hardware. Es decir que facilita la comunicación entre el software y el hardware del dispositivo móvil.

Estas características dependen del modelo del dispositivo móvil, pero a nivel general tenemos: Audio, Bluetooth, Cámara, Sensores, Display, Flash y otros sensores o elementos de hardware que tenga el dispositivo móvil.[24]

En la imagen 2, vemos cómo está compuesta la capa base de abstracción de hardware del sistema operativo Android.

Imagen 2: Capa de abstracción de hardware



Fuente: https://developer.android.com/guide/platform/?hl=es-419

5.1.3 Librerías nativas de C/C++ - Runtime de Android:

Esta capa está dividida por dos módulos esenciales:

- Runtime de Android
- Librerías nativas de C/C++

Runtime de Android: Este módulo se encarga de ejecutar los procesos que cada de las APPs o tiempo de ejecución de Android (ART) que requieren para su

[24] CHSOSUNAL20161912551. Capa de Abstracción de Hardware (HAL). [En línea]. Bogotá: CHSOSUNAL20161912551. Disponible en https://chsosunal20161912551.wordpress.com/2016/03/15/capa-de-abstraccion-de-hardware-hal/

funcionamiento. Trabaja por medio de una máquina virtual de JAVA liviana denominada Dalvink. Esta máquina virtual es mucho más eficiente que una máquina virtual de JAVA convencional debido a que Dalvink requiere de menos recursos para su funcionamiento, como es el caso de los dispositivos móviles donde sus recursos como memoria y procesador son limitados. A partir de Android 5, se realizó una mejora sobre la máquina virtual de JAVA evolucionado una máquina virtual denominada ART mejorando la eficiencia de ejecución en un 33%.[25]

Este módulo ejecuta varia maquina virtuales las cuales consumen la menor cantidad de memoria RAM ejecutando archivos DEX.

"En las funciones de Runtime de Android tenemos"[26]:

- compilación ahead-of-time (AOT) y just-in-time (JIT);
- recolección de elementos no usados (GC) optimizada;
- mejor compatibilidad con la depuración, como un generador de perfiles de muestras dedicado, excepciones de diagnóstico detalladas e informes de fallos, y la capacidad de establecer puntos de control para controlar campos específicos

Librerías nativas de C/C++:

Este modulo contiene una gran cantidad de librerías que pueden ser utilizadas por las aplicaciones de capa superior. De esta manera se ahora tiempos y esfuerzos en la creación de códigos para hacer funcionar el hardware del dispositivo. La capa siguiente se encarga de suministrar la API para exponer estas librerías y que las aplicaciones las pueda utilizar[27].

[25] androidcurso.com. Arquitectura de Android. [En línea]. Bogotá: Android Curso. Disponible http://www.androidcurso.com/index.php/tutoriales-android-fundamentos/31-unidad-1-vision-general-y-entorno-de-desarrollo/99-arquitectura-de-android

[26] developer.android.com. Arquitectura de la plataforma. [En línea]. Bogotá: Developers. Disponible https://developer.android.com/guide/platform/?hl=es-419

[27] androidcurso.com. Óp. Cit.

En la imagen 3, vemos cómo está compuesta la capa Librerías nativas de C/C++ - Runtime del sistema operativo Android.

Imagen 3: Librerías nativas de C/C++ - Runtime de Android

Fuente: https://developer.android.com/guide/platform/?hl=es-419

5.1.4 Marco de API de JAVA:

Esta capa es la responsable de enlazar todo el software del dispositivo con el hardware del mismo por medio de la API internas que contiene el Sistema Operativo. Android al ser un sistema Operativo abierto utiliza recursos abiertos para facilitar su desarrollo, en este caso utiliza lenguaje JAVA para la creación de las APIs internas que permiten la comunicación entre los diferentes módulos, las aplicaciones y las máquinas virtuales que se requieres para el correcto funcionamiento del dispositivo móvil.[28]

Dentro de los beneficios que tenemos al utilizar esta arquitectura tenemos:

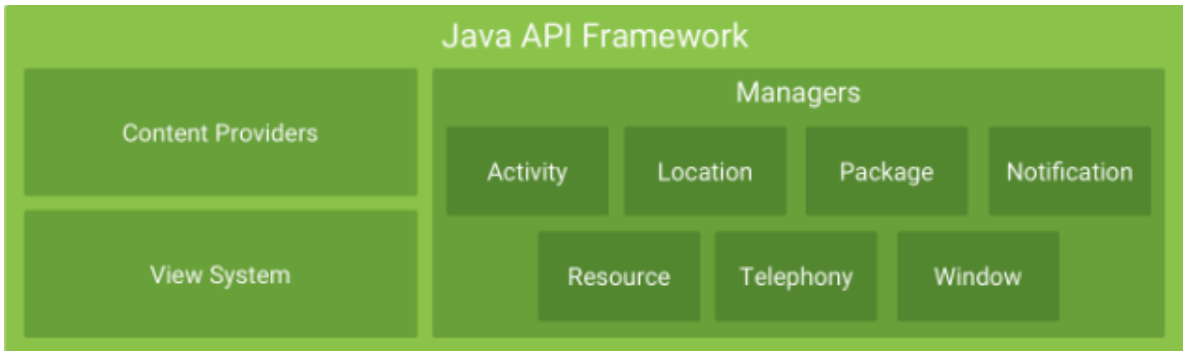
- Facilidad al desarrollar la interfaz de usuario.
- Acceso a recursos sin necesidad de código, se utiliza cadenas localizadas.
- Visualización de notificaciones en la barra de estado de la pantalla principal del dispositivo.

[28] androidcurso.com. Óp. Cit.

- Acceso de datos de otras apps, como app de contactos.

En la imagen 4, vemos el Marco de API de JAVA del sistema operativo Android.

Imagen 4: Marco de API de JAVA



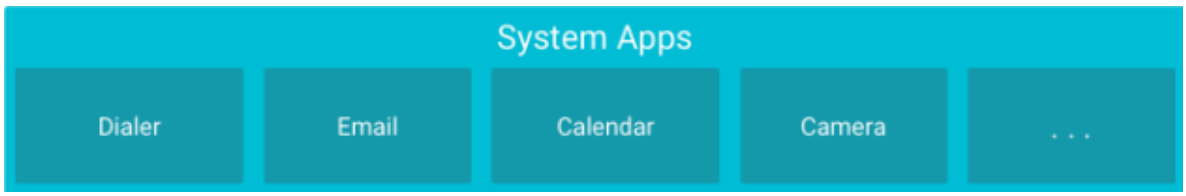
Fuente: https://developer.android.com/guide/platform/?hl=es-419

5.1.5 Aplicaciones del sistema:

Esta es la capa más alta de la arquitectura del sistema operativo Android. Es en eta capa donde se ejecutan tanto las APPs nativas del sistema operativo como las APPs que el usuario decide instalar.

En la imagen 5, vemos la capa de Aplicaciones del sistema operativo Android.

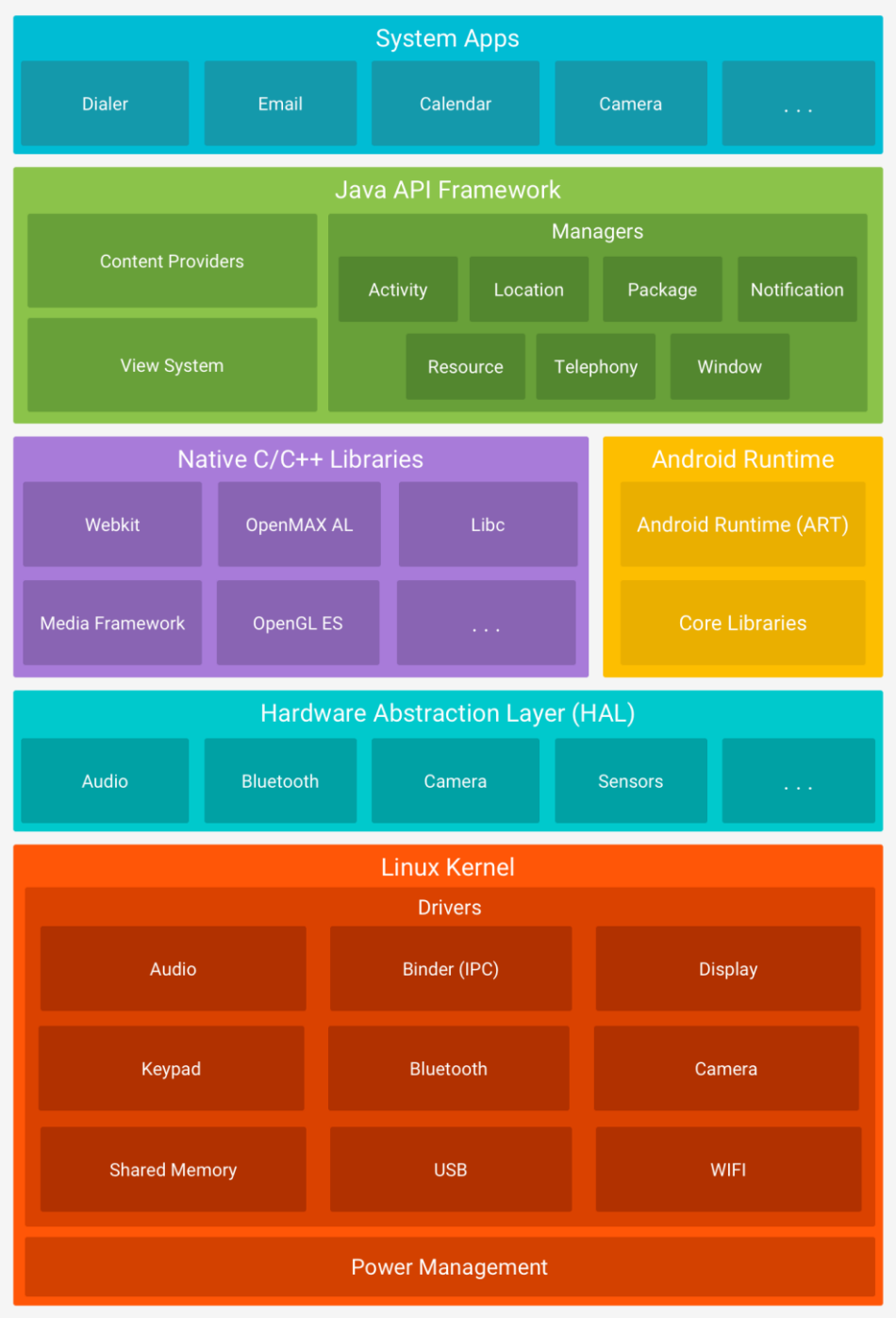
Imagen 5: Aplicaciones del sistema



Fuente: https://developer.android.com/guide/platform/?hl=es-419

En la imagen 6, vemos todas las capas de arquitectura del sistema operativo Android.

Imagen 6: Arquitectura del sistema operativo Android



Fuente: https://developer.android.com/guide/platform/?hl=es-419

5.2 CAPITULO 2. RECONOCER LAS CARACTERÍSTICAS FUNCIONALES DEL SISTEMA OPERATIVO ANDROID QUE PERMITEN EJECUTAR UN ANÁLISIS FORENSE SOBRE ESTOS DISPOSITIVOS.

El sistema operativo para dispositivos móviles denominado Android Nougat abarca a toda la familia de la versión 7.x. es la antepenúltima versión del famoso sistema operativo de Google el cual tiene como versiones superiores Android 8.0. Oreo y Android 9.0. Pie.

Android Nougat es considerado la versión más segura hasta el momento de su publicación teniendo como referencia las siguientes características[29].

- Mejoras en el modelo de cifrado: Hasta las versiones anteriores de Android Nougat, se utilizaba el patrón de desbloqueo al inicio del sistema operativo para descifrar la información contenida en el dispositivo. Ahora con la versión Android Nougat y su nueva funcionalidad de Direct Boot, se optimiza este proceso y permite dejar habilitado solo la alarma y las llamadas sin necesidad de descifrar el dispositivo.
- Cambios de arquitectura de multimedia: Android Nougat hace un cambio notable en su arquitectura de multimedia, este cambio mitiga las vulnerabilidades encontradas en versiones anteriores como es el caso de Marshmallow. Android Nougat, controla de manera eficiente los permisos requerido para acceder a los recursos de multimedia que son administrados por el sistema operativo.
- Mejoras en la seguridad de en las aplicaciones: Estas mejoras permitirán a los desarrolladores compartir datos entre aplicaciones por medio de un módulo denominado Content Providers.

[29] Zamora José. Por qué Android 7.0 Nougat es la versión más segura. [En línea]. Bogotá: El Androide libre. 2016., 1 p. Disponible en https://elandroidelibre.elespanol.com/2016/09/las-mejoras-seguridad-android-nougat.html

- Debido a sus cambios en el kernel del sistema operativo, Nougat, restringe el acceso al directorio de las aplicaciones “/data/data” con el fin de tener mas control sobre los usuarios que acceden a estos recursos.
- Nougat incorpora un nuevo modulo llamado Network Security Config, el cual permite hacer la gestión de entidades certificadoras, CA, o brindar confianza a un certificado auto firmado por una entidad conocida.
- Nougat mejora el módulo OTA de actualización del sistema operativo, permitiendo recibir de manera más eficiente las actualizaciones.
- El sistema de archivos Android cambia de acuerdo con el fabricante del dispositivo. Actualmente, tenemos dos sistemas de archivos utilizados por Android, el primerio de ellos es ext4, fourth extended filesystem, el cual es utilizado en sistemas operativos Linux. El segundo es f2fs, Flash Friendly File System, el cual fue desarrollado por SAMSUNG y es considerado más eficiente que el formato de archivos EXT4.
- Todos los dispositivos móviles vienen sin permisos administrador o root desde la fábrica. Sin embargo, algunas personas entusiastas de la tecnología y dispositivos móviles alteran esta característica del sistema operativo para tener más privilegios sobre los archivos del sistema operativo y lograr hacer modificaciones a su gusto.

De acuerdo a las características implementadas por Google observamos como el fabricante ha mejorado la seguridad de su sistema operativo a tal punto que realizar un proceso forense sobre un dispositivo móvil es cada día más complejo. Incluso, para realizar un proceso forense exitoso sobre todo el dispositivo móvil es necesario que este tenga privilegios root para poder analizar los archivos del sistema operativo, aplicaciones, configuración para tener más probabilidades de encontrar la secuencia de los hechos presentados sobre el dispositivo.

Si el equipo no es root, el análisis forense será limitado, básicamente con alcance al almacenamiento masivo del dispositivo y no a sus archivos del sistema. Siendo este el caso, se requiere una autorización del juez para poder habilitar permisos de

root sobre el dispositivo, siendo esta actividad delicada debido a que altera la evidencia y se puede perder toda credibilidad del caso.

5.3 CAPITULO 3. IDENTIFICAR LAS HERRAMIENTAS TECNOLÓGICAS QUE SEAN FUNCIONALES Y CONFIABLES PARA EL ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES BAJO EL SISTEMA OPERATIVO ANDROID EN SU VERSIÓN 7.1 O SUPERIOR.

En la actualidad existe una gran cantidad de herramientas, tanto pagas como open source, que nos pueden ayudar a realizar una investigación forense en un dispositivo móvil. Algunas de estas herramientas son:

5.3.1 Bloqueadores hardware y software:

Una vez el investigador forense informático ha realizado el proceso de toma de pruebas, evidencias, embalaje y cadena de custodia, procede a realizar el análisis de las pruebas obtenidas para determinar la existencia de evidencias que permitan reconstruir en una línea de tiempo los hechos ocurridos.

Como es primordial mantener la integridad de las pruebas y evidencias recolectadas, el investigador forense debe utilizar un mecanismo que le permita cumplir con esta premisa. Para esto, al momento de analizar los dispositivos de almacenamiento masivo utilizar dispositivos llamados bloqueadores, los cuales pueden ser físicos, hardware, o digitales, software.[30]

Hardware: Son dispositivos físicos que se conectar de entre el equipo del investigador forense y el disco al cual se busca realizar el proceso forense. De esta manera estos dispositivos permiten mantener la integridad impidiendo la escritura sobre el disco de almacenamiento al cual se esté realizando un proceso forense.

[30] ACURIO DEL PINO, Santiago. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0. [En línea]. Bogotá: Organización De Estados Americanos. Disponible en https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Las marcas más representativas son:

1. Tableau, su página oficial es https://www.guidancesoftware.com/tableau/hardware?types=Forensic-Bridges.
2. Digital Intelligence: su página oficial es https://digitalintelligence.com/products/ultrablock

Software: su principal característica es que son sistemas operativos basado en Linux especializados para realizar tareas de análisis forense. Una de sus funciones que puede funcionar como bloqueadores. Al ser sistemas operativos pueden controlar el uso del hardware donde se encuentren instalados o en ejecución. Dada esta característica, estos sistemas operativos bloquean la escritura de los puertos USB de los equipos donde están instalados. De esta manera, cualquier dispositivo que se instale por el puerto USB solo funcionará en modo lectura.

Los sistemas operativos mas representativos para realizar esta labor son:

1. Tequila: Es un sistema operativo basado en Linux, desarrollado en Latinoamérica, especializado para la informática forense. Su interfaz gráfica es fácil de entender y al ser una versión libre su soporte es limitado. su página web es https://tequila-so.org/
2. Caine: Es un sistema operativo basado en Linux, desarrollado en Italia, especializado para la informática forense. Su interfaz gráfica es fácil de entender y al ser una versión libre su soporte es limitado. Su página web es https://www.caine-live.net/
3. SANS DFIR: es una appliance virtual basado en Linux, especializado para la informática forense. Tiene una gran cantidad de características que la hace una de las mejores distribuciones para realizar este tipo auditorías. Su página web es https://digital-forensics.sans.org/

5.3.2 Recolección y análisis de evidencia:

La recolección de evidencia y análisis es otra de las actividades primordiales del investigador forense informático. Una vez el investigador garantice la integridad de la evidencia principal por medio de los bloqueadores, procede a tomar por lo menos tres copias digitales bit a bit con la siguiente finalidad:

1. La primera imagen forense, será la copia de seguridad principal de la imagen obtenida de la fuente principal. Sobre esta imagen no se realiza ningún tipo de trabajo y solo se utiliza si es solicitada por un juez, o para generar nuevas copias de la imagen forense en caso de que las demás copias hayan sido alteradas. **Nota**. Estas copias se deben realizar con equipos especializados para garantizar que la primera copia no se vea alterada bajo ningún motivo.
2. Las demás copias se utilizan para hacer el análisis correspondiente por el investigador o investigadores.

Con el fin de mantener la integridad de la evidencia digital es necesario que al momento de realizar la copia bit a bit, se realice la extracción de la huella digital por medio del algoritmo SHA-2 256 o superior. De este modo podemos validar la autenticidad de la copia de la fuente digital.

Algunas de las herramientas que nos puede ayudar con este proceso de recolección y análisis de evidencia, sin limitarse a ellas son: Encase, Autopsy, FTK Access data, Santoku, CAIN y DEFT. Todas ellas tienen la capacidad de realizar una imagen forense bit a bit, procesarla y ayudar al investigador con el análisis para lograr reconstruir la secuencia de eventos que ocurrieron para que se materializara un incidente de seguridad de la información.

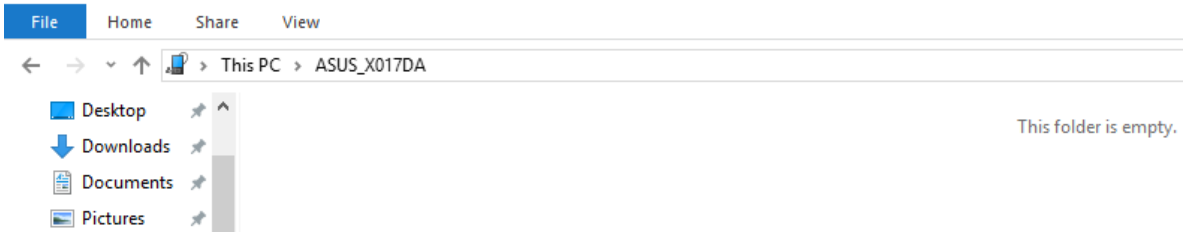
5.4 CAPITULO 4. EJECUTAR UN PROCESO DE ANÁLISIS FORENSE A UN DISPOSITIVO MÓVIL CON SISTEMA OPERATIVO ANDROID EN SU VERSIÓN 7.1 O SUPERIOR

Para el desarrollo de este capítulo se realizará bajo las siguientes premisas:

- El dispositivo móvil utilizado es:
  - Marca: Asus
  - Modelo: Asus_X017DA
  - Versión de Android: 7.1.1
- El dispositivo se encuentra en modo de fábrica, lo cual indica que no esta modificado con permisos root.
- El dispositivo móvil tiene patrón de desbloqueo.
- El dispositivo móvil viene con la adecuada cadena de custodia en la cual se garantiza que el equipo no ha sido alterado de manera directa o remota por ningún individuo o programa informativo.

Lo primero que debemos tener en consideración es que el dispositivo móvil si esta bloqueado y lo conectamos a un pc, no se visualizara la información contenida en el móvil debido a la seguridad que estable la versión de Android. Para poder tener acceso a la información es necesario que el usuario habilite la opción desde el móvil como se visualiza en la imagen 8.

Imagen 7. Dispositivo conectado sin transferencia de información.



Fuente: Autor

Cuando conectamos el dispositivo móvil por medio de cable a la computadora, el dispositivo nos pregunta la opción que deseamos habilitar. En estas opciones tenemos:

Solo Cargar el dispositivo: Con esta opción el dispositivo móvil solo permitirá la carga más no permitirá acceso a la información que este contenga.

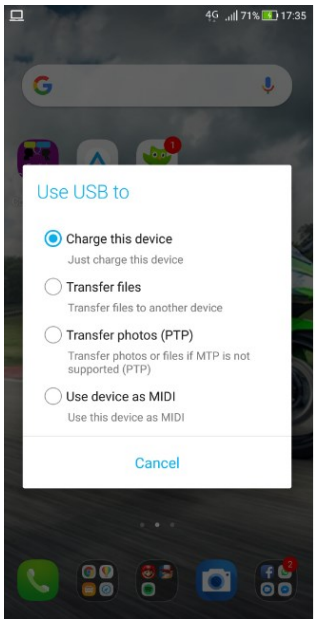
Transferencia de datos: Esta opción permite que el dispositivo móvil se comporte como un dispositivo de almacenamiento masivo. De esta manera se obtienen acceso completo a la memoria interna y externa del móvil.

Transferencia de fotos (PTP): Picture Transfer Protocol, es un mecanismo de transferencia limitada a fotografías desde el dispositivo móvil al computador. Es poco utilizado debido a la limitante de tipos de archivos que puede transferir.

Usar como MIDI: Musical Instrument Digital Interface, es un estándar que permite conectar varios dispositivos, entre ellos instrumentos musicales. Este protocolo esta muy asociado a archivos digitales de música.

En la imagen 8 podemos ver las opciones que nos brinda el dispositivo, para el caso de este ejercicio damos la opción de transferencia de archivos para tener acceso completo a la memoria interna del equipo y a la memoria externa.

Imagen 8. Asignación de permiso de lectura/escritura en el dispositivo móvil.



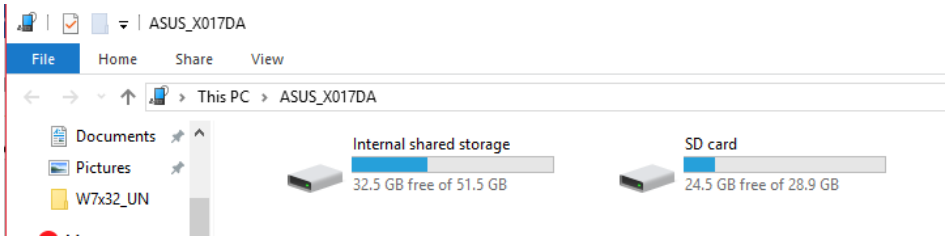
Fuente: Autor

Cuando seleccionamos la opción transferencia de datos, el almacenamiento, tanto interno como externos, el móvil se comporta como un dispositivo de

almacenamiento masivos conectado por USB. De esta manera tenemos control total sobre este recurso.

En la Imagen 9 se visualiza cómo en el equipo de cómputo se tiene acceso al almacenamiento interno del móvil.

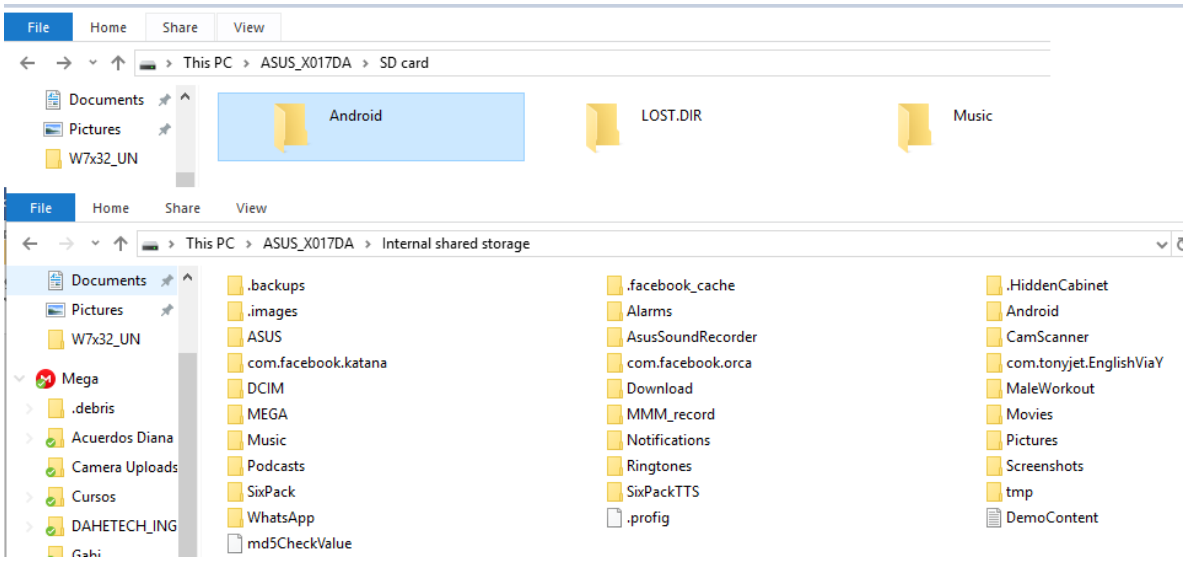
Imagen 9. Dispositivo conectado con transferencia de información.



Fuente: Autor

En la Imagen 10 se visualiza el contenido interno del equipo móvil.

Imagen 10. Contenido del Dispositivo móvil.

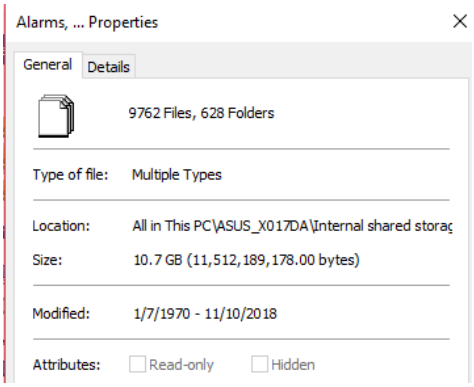


Fuente: Autor

Teniendo acceso a la información del dispositivo móvil podemos realizar una copia de espacio alojado de las unidades donde se encuentra la información en el dispositivo móvil. Se debe aclarar que debido a que el dispositivo no está con permisos root no es posible realizar una copia forense del dispositivo.

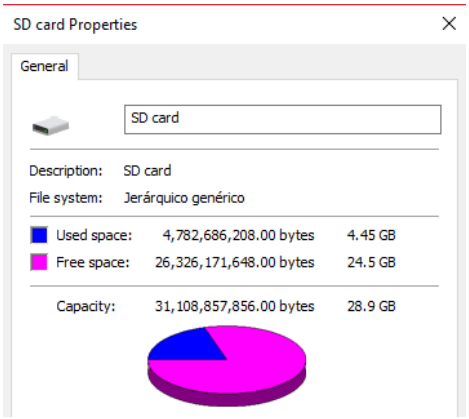
En la imagen 11 y 12 podemos visualizar cuanto serian los archivos y el tamaño total en cada uno de ellos al momento de realizar la copia.

Imagen 11. Archivo y almacenamiento de la unidad interna.



Fuente: Autor

Imagen 12. Archivo y almacenamiento de la unidad externa.



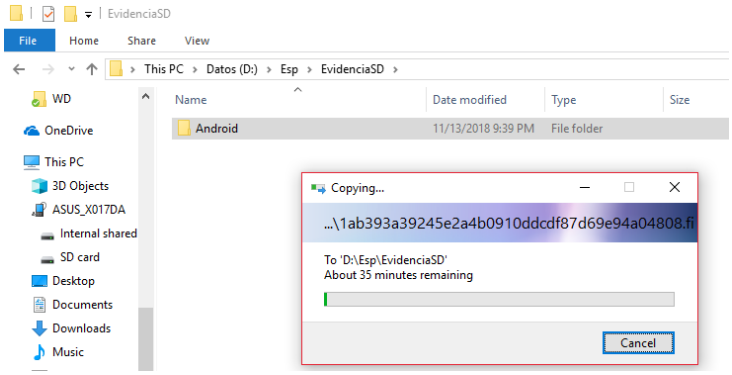
Fuente: Autor

Para el proceso de copiar el contenido del dispositivo móvil se realiza el siguiente proceso:

- Se copia la información y se almacena en una unidad distinta a la del móvil en una carpeta.
- Luego se realiza una imagen forense del contenido copiado.
- Se obtiene el Hash de la imagen forense para poder validar la integridad en caso de que un juez la requiera.
- Se almacena las evidencias en una unidad de almacenamiento masivo, la cual será suministrada a un juez como evidencia.

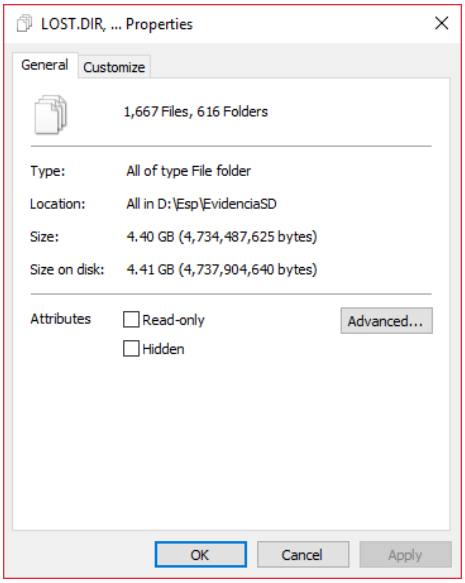
Se realizará la copia de la información contenida en el almacenamiento externo del dispositivo. En las imágenes de la 12 a la 18 se puede visualizar el proceso de copiado y de generación de imagen forense.

Imagen 12. Archivo y almacenamiento de la unidad externa.



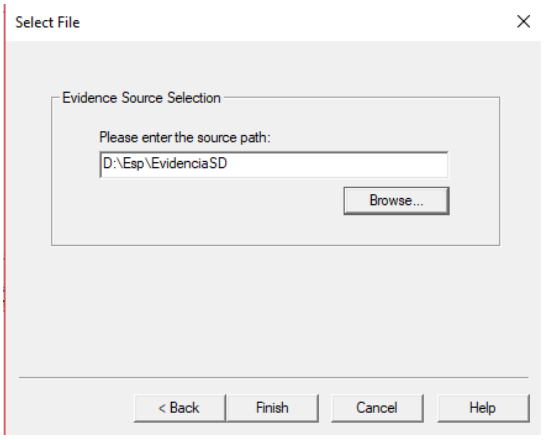
Fuente: Autor

Imagen 13. Información de la unidad externa copiada.



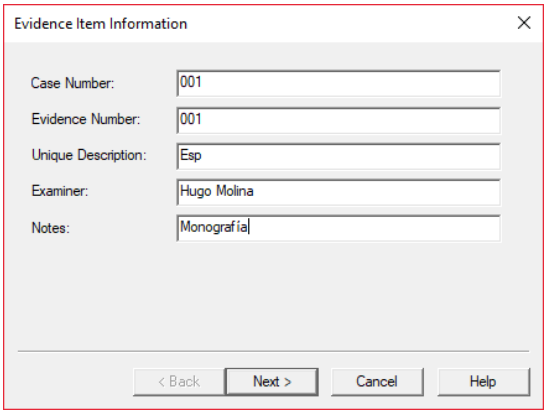
Fuente: Autor

Imagen 14. fuente de imagen forense de la información copiada.



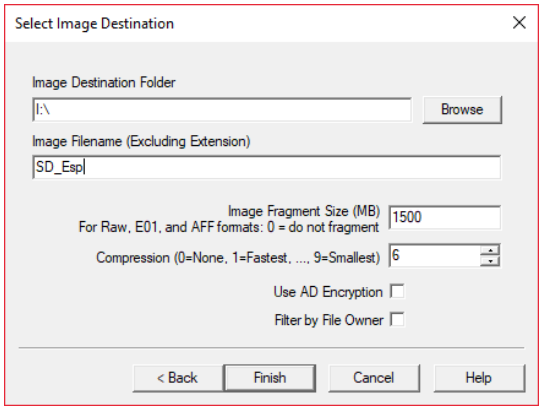
Fuente: Autor

Imagen 15. Creación de la imagen forense.



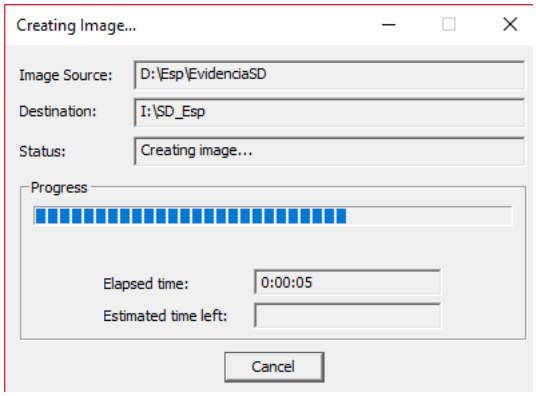
Fuente: Autor

Imagen 16. Destino de la imagen forense.



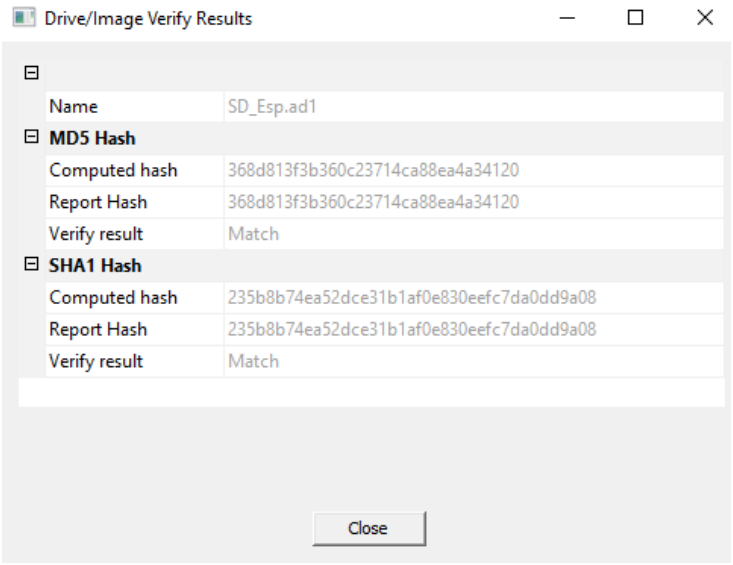
Fuente: Autor

Imagen 16. Proceso de la imagen forense.



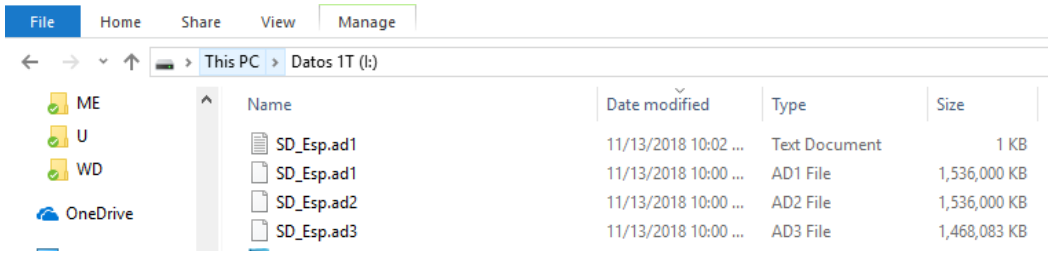
Fuente: Autor

Imagen 17. Resultado de la imagen forense.



Fuente: Autor

Imagen 18. Resultado en archivos de la imagen forense.



Fuente: Autor

Con el sistema operativo Santoku, realizaremos una extracción de la información que contiene el dispositivo móvil como:

- Registro de llamadas.
- Teléfonos de contactos.
- MMS. Multimedia Messaging Service.
- MMSParts.
- SMS. Short Message Service.

El dispositivo móvil no requiere tener permisos de root para ejecutar esta actividad, pero si en necesario que tenga habilitada las opciones de desarrollador en el dispositivo móvil. Para esto debemos ir a configuración – acerca del dispositivo – información del software y presionamos en varias ocasiones en número de

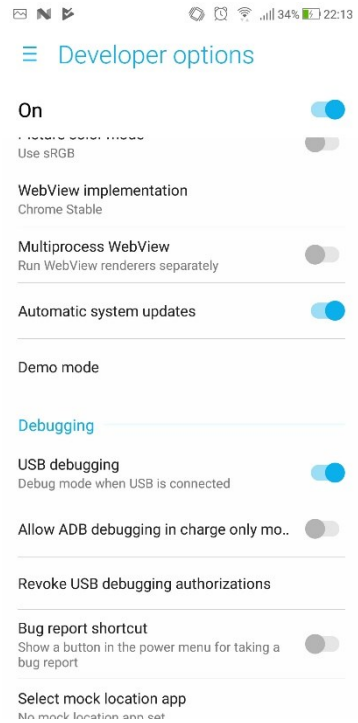
compilación hasta el sistema nos indique que ya somos desarrolladores. En la imagen 19 vemos el mensaje que genera el dispositivo móvil cuando realizamos esta operación y ya somo administradores.

Imagen 19. Permisos de desarrollador habilitados.

Fuente: Autor

Luego tenemos que buscas las nuevas opciones que tenemos en el dispositivo móvil que se llama opciones de desarrollador. Ingresamos a estas opciones y habilitamos la opción USB debugging. En la imagen 20 se visualiza la habilitación de esta opción.

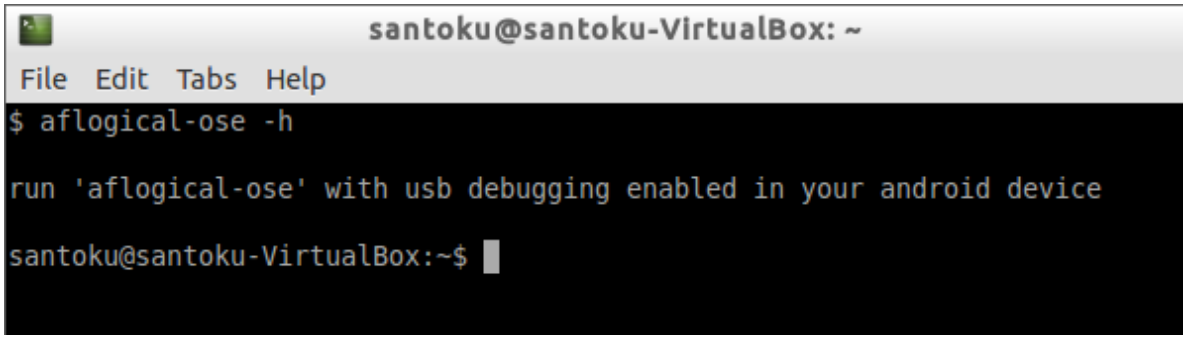
Imagen 20. Habilitación USB Debugging.



Fuente: Autor

Luego, ejecutamos el programa aflogical-ose en santoku donde nos solicita que conectemos el dispositivo móvil con la opción USB debugging habilitada.

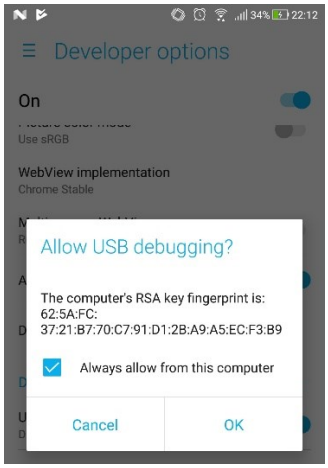
Imagen 21. Inicio del programa en Santoku.



Fuente: Autor

Cuando conectamos el dispositivo móvil nos genera un mensaje donde non indica que se queremos permitir conexión por medio de USB debugging y nos referencia la huella digital. En la imagen 22 observamos el mensaje que nos genera el dispositivo.

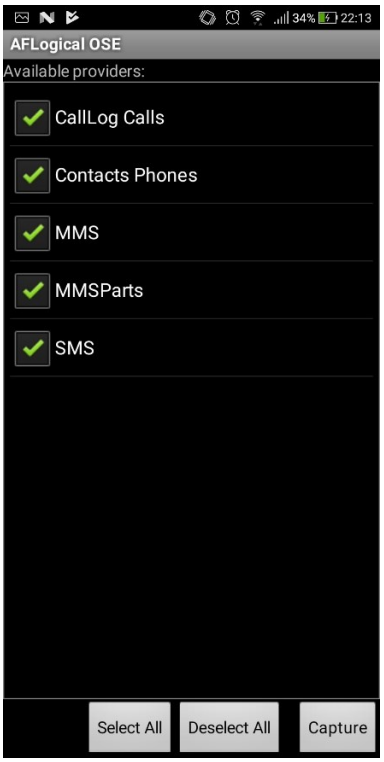
Imagen 22. Autorización del móvil para conexión USB Debugging.



Fuente: Autor

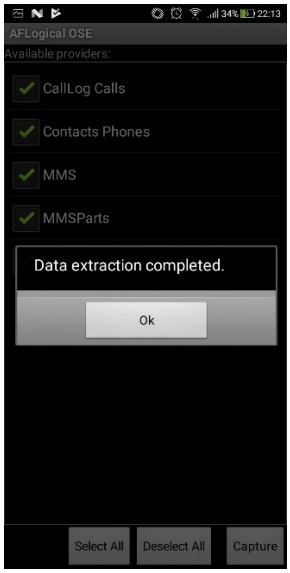
Cuando damos la opción OK, automáticamente se instala en el dispositivo móvil una aplicación de AFLogical OSE, la cual hace la extracción de la información y la envía al almacenamiento interno del dispositivo móvil.

Imagen 23. Ejecución AFLogical OSE.



Fuente: Autor

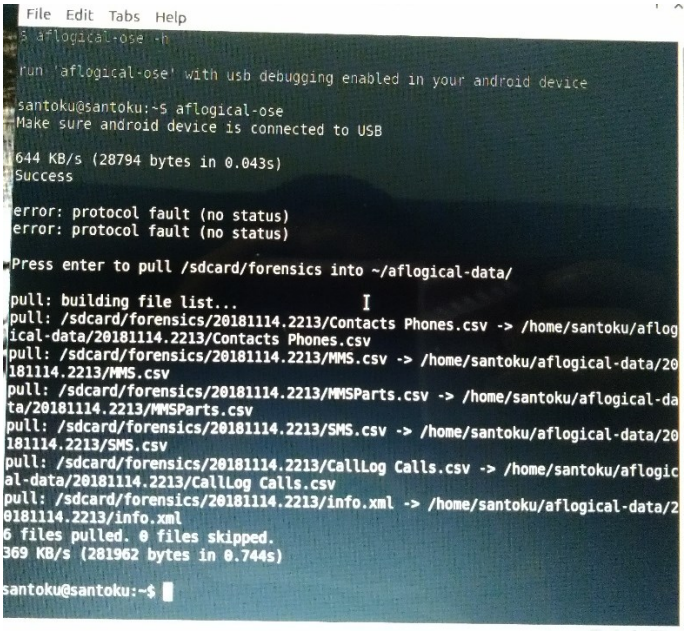
Imagen 24. Ejecución exitosa de AFLogical OSE en el móvil.



Fuente: Autor

Cuando el proceso se ejecuta de manera exitosa en la ventana del terminal de santoku no aparece lo que se visualiza en la imagen 25.

Imagen 25. Ejecución exitosa de AFLogical OSE en santoku.

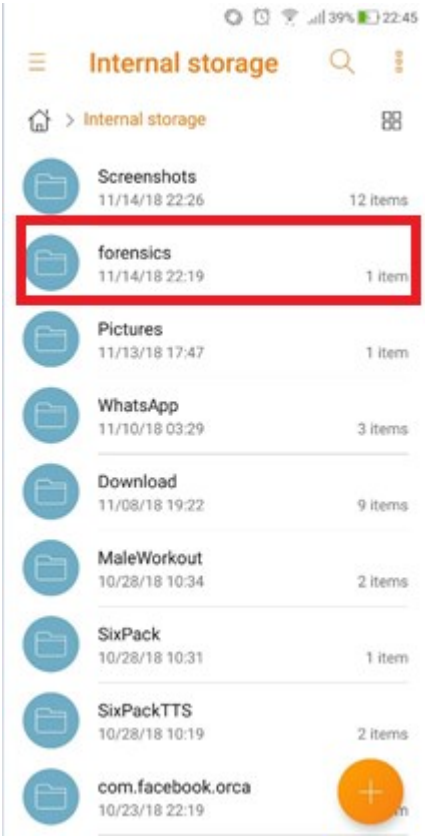


Fuente: Autor

En la imagen 26 se puede ver que la aplicación AFlogic OSE crea una carpeta en el almacenamiento interno del dispositivo móvil para posterior mente sea tomada y analizada por el investigador forense que esté llevando el caso.

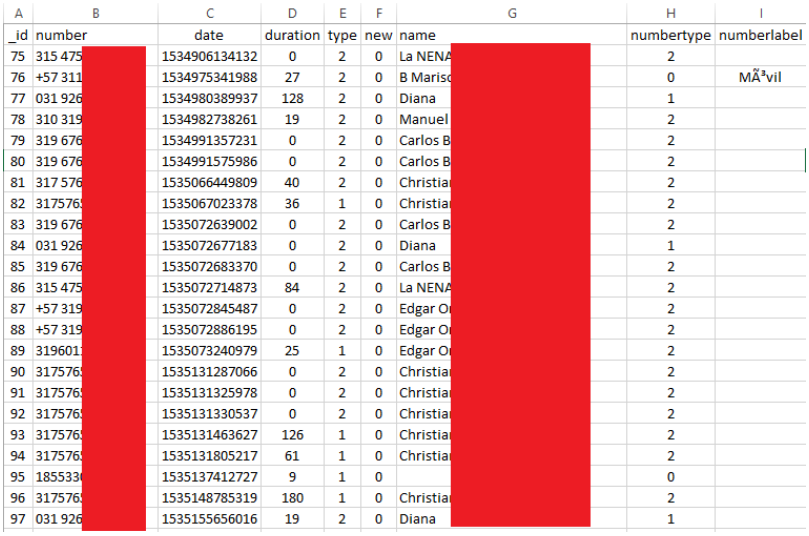
En las imágenes 27 y 28 podemos ver el log del registro de llamas y SMS respectivamente, no se visualiza el log de MMS o MMSParts debido a que el dispositivo móvil no contaba con este tipo de información y el log se genero en blanco.

Imagen 26. Información extraída de AFLogical OSE.



Fuente: Autor

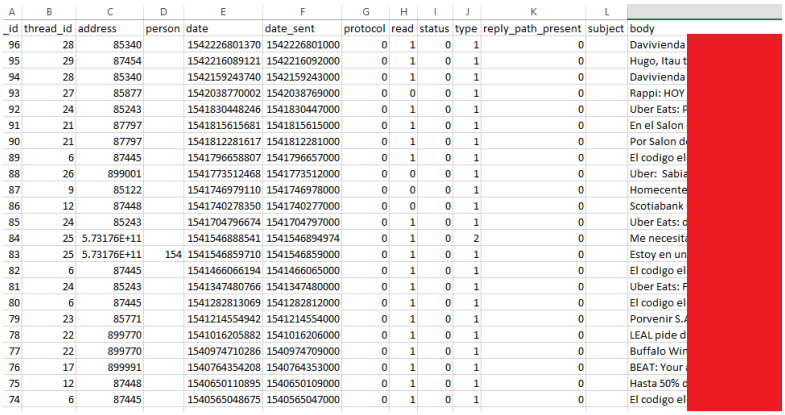
Imagen 27. Registro de llamadas.



_id	number	date	duration	type	new	name	numbertype	numberlabel
75	315 475	1534906134132	0	2	0	La NENA	2	
76	+57 311	1534975341988	27	2	0	B Marisc	0	MÃ³vil
77	031 926	1534980389937	128	2	0	Diana	1	
78	310 319	1534982738261	19	2	0	Manuel	2	
79	319 676	1534991357231	0	2	0	Carlos B	2	
80	319 676	1534991575986	0	2	0	Carlos B	2	
81	317 576	1535066449809	40	2	0	Christia	2	
82	317576	1535067023378	36	1	0	Christia	2	
83	319 676	1535072639002	0	2	0	Carlos B	2	
84	031 926	1535072677183	0	2	0	Diana	1	
85	319 676	1535072683370	0	2	0	Carlos B	2	
86	315 475	1535072714873	84	2	0	La NENA	2	
87	+57 319	1535072845487	0	2	0	Edgar O	2	
88	+57 319	1535072886195	0	2	0	Edgar O	2	
89	319601	1535073240979	25	1	0	Edgar O	2	
90	317576	1535131287066	0	2	0	Christia	2	
91	317576	1535131325978	0	2	0	Christia	2	
92	317576	1535131330537	0	2	0	Christia	2	
93	317576	1535131463627	126	1	0	Christia	2	
94	317576	1535131805217	61	1	0	Christia	2	
95	185533	1535137412727	9	1	0		0	
96	317576	1535148785319	180	1	0	Christia	2	
97	031 926	1535155656016	19	2	0	Diana	1	

Fuente: Autor

Imagen 28. Registro de SMS.



_id	thread_id	address	person	date	date_sent	protocol	read	status	type	reply_path_present	subject	body
96	28	85340		1542226801370	1542226801000	0	1	0	1	0		Davivienda
95	29	87454		1542216089121	1542216092000	0	1	0	1	0		Hugo, Itau t
94	28	85340		1542159243740	1542159243000	0	1	0	1	0		Davivienda
93	27	85877		1542038770002	1542038769000	0	0	0	1	0		Rappi: HOY
92	24	85243		1541830448246	1541830447000	0	1	0	1	0		Uber Eats: P
91	21	87797		1541815615681	1541815615000	0	1	0	1	0		En el Salon
90	21	87797		1541812281617	1541812281000	0	1	0	1	0		Por Salon d
89	6	87445		1541796658807	1541796657000	0	1	0	1	0		El codigo el
88	26	899001		1541773512468	1541773512000	0	0	0	1	0		Uber: Sabia
87	9	85122		1541746979110	1541746978000	0	0	0	1	0		Homecente
86	12	87448		1541740278350	1541740277000	0	0	0	1	0		Scotiabank
85	24	85243		1541704796674	1541704797000	0	1	0	1	0		Uber Eats: d
84	25	5.73176E+11		1541546888541	1541546894974	0	1	0	2	0		Me necesita
83	25	5.73176E+11	154	1541546859710	1541546859000	0	1	0	1	0		Estoy en un
82	6	87445		1541466066194	1541466065000	0	1	0	1	0		El codigo el
81	24	85243		1541347480766	1541347480000	0	1	0	1	0		Uber Eats: F
80	6	87445		1541282813069	1541282812000	0	1	0	1	0		El codigo el
79	23	85771		1541214554942	1541214554000	0	1	0	1	0		Porvenir S.A
78	22	899770		1541016205882	1541016206000	0	1	0	1	0		LEAL pide d
77	22	899770		1540974710286	1540974709000	0	1	0	1	0		Buffalo Wir
76	17	899991		1540764354208	1540764353000	0	1	0	1	0		BEAT: Your
75	12	87448		1540650110895	1540650109000	0	1	0	1	0		Hasta 50% d
74	6	87445		1540565048675	1540565047000	0	1	0	1	0		El codigo el

Fuente: Autor

Para realizar una copia forense es necesario que el dispositivo móvil cuente con permisos root. Si e dispositivo no cuneta con esta funcionalidad activada, entonces, no es posible realizar la copia forense.

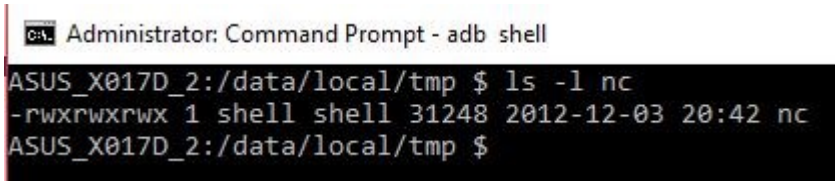
A continuación, se realizará un proceso de extracción de información forense del dispositivo móvil Asus, modelo X017DA y con sistema operativo Andorid 7.1.1. Los prerequisitos para ejecutar este proceso son:

- Tener instalada las herramientas ADB para tener conexión con el dispositivo móvil.
- El dispositivo debe tener la opción USB Debugging habilitada.
- El dispositivo debe tener permisos root sobre el sistema operativo Android.
- Brindar permisos root a la aplicación ADB Shell desde el dispositivo móvil.

En primera instancia, se debe realizar una copia del programa netcat desde el equipo de computo del investigador hacia el dispositivo móvil al cual deseamos realizar la copia forense.

El comando que podemos utilizar es **adb push nc /data/local/tmp**. Se debe tener en cuenta que el programa nc debe estar en la misma ubicación donde se encuentra ejecutando el programa adb. En la imagen 29 podemos visualizar la comprobación de la transferencia del programa nc hacia el dispositivo móvil y que este cuenta con permisos de ejecución.

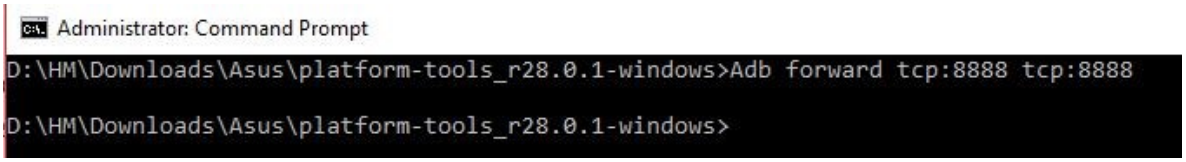
Imagen 29. Transferencia de nc al dispositivo móvil.



Fuente: Autor

Seguido de este paso, se procede a realizar la apertura de puertos del host local y del host remoto, para este caso vamos a trabajar con el mismo número de puerto, 8888, para cada uno de los extremos. Esta apertura de puestos se realizar con el comando **adb forward tcp:8888 tcp:8888.** En la imagen 30 podemos ver la ejecución exitosa de este comando.

Imagen 30.

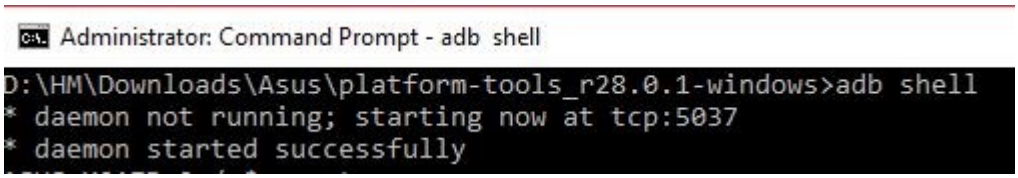


Fuente: Autor

Teniendo los requisitos listos del lado del equipo del investigador, procedemos con el alistamiento y copia forense del dispositivo móvil.

En la imagen 31 observamos como nos conectamos con el dispositivo móvil por medio del comando **adb Shell**.

Imagen 31.



Fuente: Autor

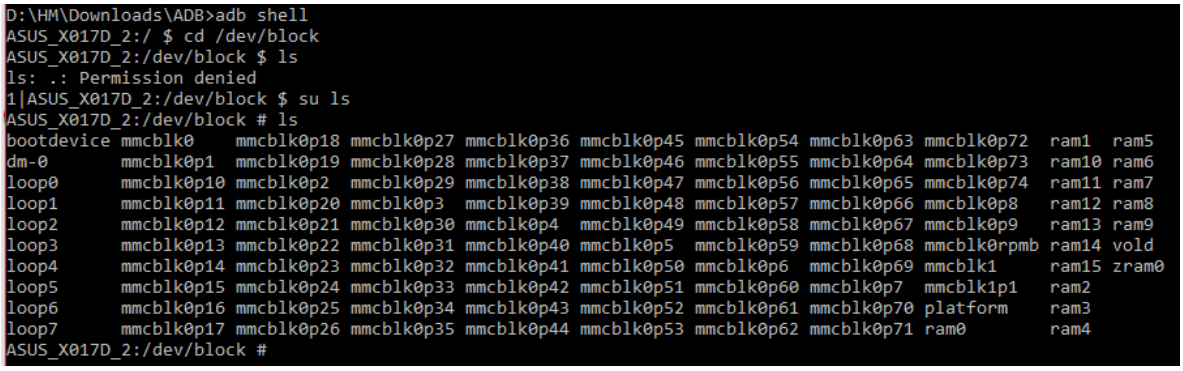
Una vez conectados al dispositivo móvil se debe identificar cuales son las particiones con las que cuenta el dispositivo móvil y cuales son de nuestro interés.

Estando conectados al móvil, navegamos hasta la ruta /dev/block, y listamos el contenido que tiene esta carpeta, allí se visualizan las particiones con las que dispone el móvil.

Para el caso de este análisis podemos observar que tenemos 2 particiones principales que son: mmcblk0 y mmcblk1; donde, mmcblk0 corresponde al almacenamiento interno y mmcblk1 corresponde al almacenamiento de la microSD.

En la imagen 32 podemos ver todas las particiones con la que cuenta el dispositivo móvil.

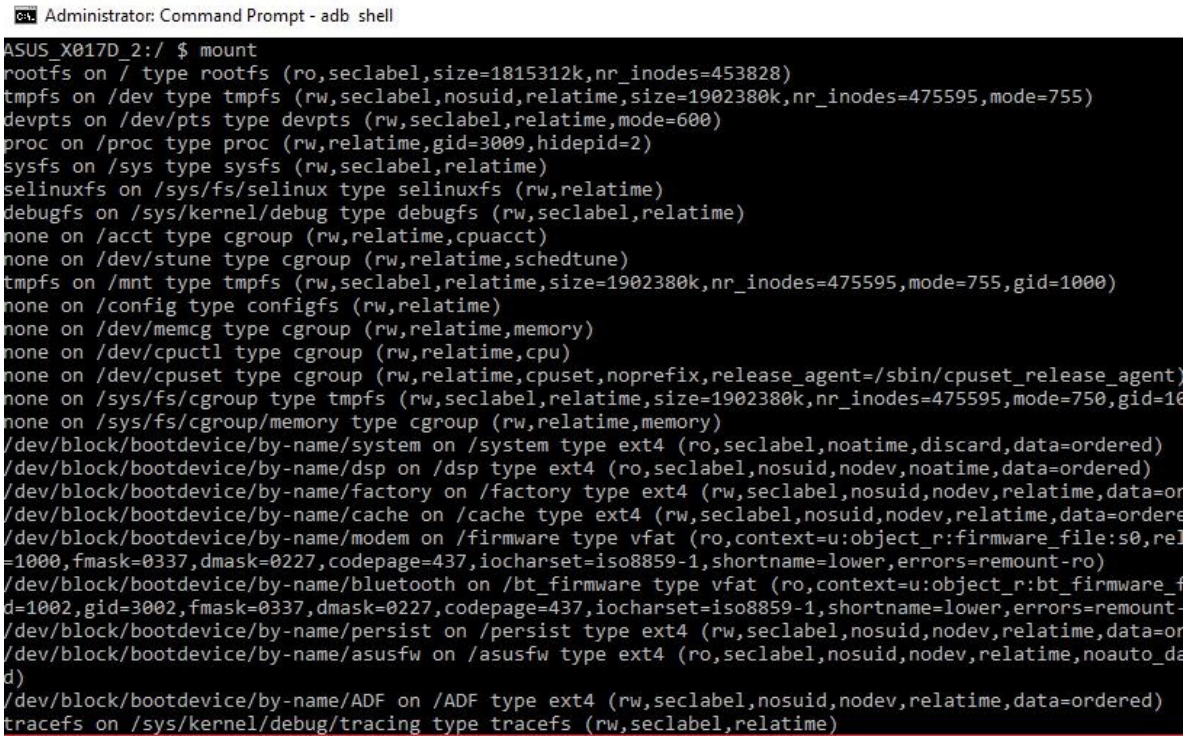
Imagen 32. Particiones del dispositivo móvil.



Fuente: Autor

Luego se procede a montar el almacenamiento del dispositivo móvil con el comando **mount**. En la imagen 33 se visualiza la ejecución exitosa de este comando.

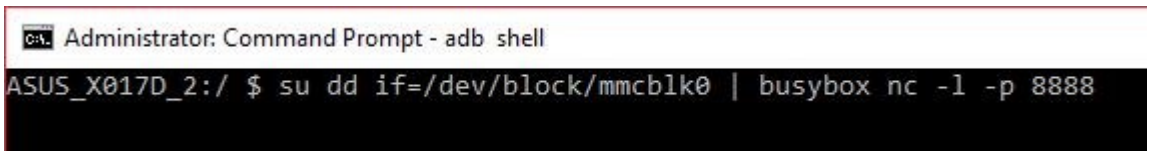
Imagen 33. Montaje del almacenamiento del dispositivo móvil.



Fuente: Autor

Finalmente, se procede a realizar la copia forense con el comando dd. Con este comando y teniendo identificada la partición a la cual deseamos realizar la copia forense podemos realizar este proceso con el comando **dd if=/dev/block/ mmcblk0 | busybox nc –l –p 8888**. En la imagen 34 podemos visualizar la ejecución exitosa del comando.

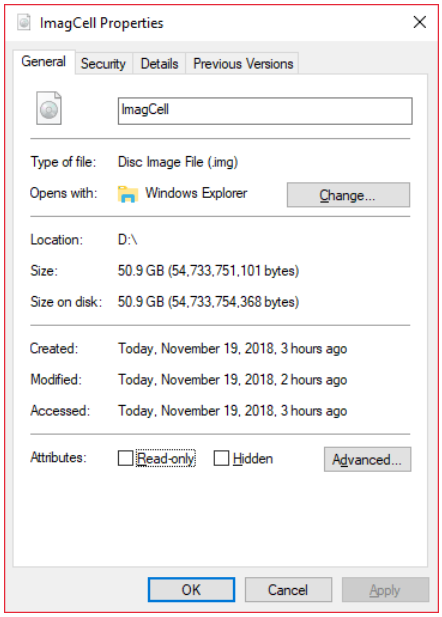
Imagen 34.



Fuente: Autor

Finalmente, se puede ver el resultado en un archivo obtenido despues de realizar la copia forense.

Imagen 35. Imagen forense.



Fuente: Autor

6 IMPACTOS

A nivel mundial y local en Colombia tenemos referentes de manejo de evidencias digitales, tales como: ISO/IEC 27042 - Guía con directrices para el análisis e interpretación de las evidencias digitales, ISO/IEC 27043 - Desarrolla principios de investigación para la recopilación de evidencias digitales, the best practices for seizing electronic evidence, versión 3.0, US of the Department of Home Land Security, and the United States Secret Service, Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la OEA, Evidencia Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, entre otras. Estas guías proporcionas metodologías o marcos de referencia para hacer un adecuado tratamiento de evidencia de las pruebas.

Colombia ha dado pasos importantes en términos legislativos para luchar contra la ciber delincuencia, es así, que en Colombia tenemos la ley 1273 del 2008 – ley de delitos informáticos, Ley estatutaria 1266 de 2008 – Hábeas Data o la ley estatutaria 1581 de 2012 – Protección de Datos Personales y todas estas leyes en común que buscar proteger la información personal o de entidades contra actos mal intencionados de personas inescrupulosas que buscar hacer un daño u obtener un beneficio de manera ilegal.

El proceso de recolección de evidencia es bastante importante y delicado debido a que puede inducirse a la culpabilidad de un hecho a una persona inocente o inducir la inocencia de una persona culpable. Una inadecuada cadena de custodia o manejo de evidencias digitales pueden llegar a anular un caso judicial contra un individuo o grupo de individuos.

De acuerdo con lo anterior, el impacto generado en este trabajo es la generación conocimiento a la sociedad en general para realizar una toma de imagen forense en un dispositivo móvil Android, reduciendo la probabilidad de un inadecuado proceso de recolección de evidencias digitales. Por otro lado, la reducción de la probabilidad de una inadecuada toma de evidencias digitales que puede llegar a anular un caso

jurídico y dañar la reputación del equipo de investigación forense que participó en el caso.

7 CONCLUSIONES

En todo proceso informático es necesario conocer como funciona los componentes para lograr identificar mejoras o vulnerabilidades del sistema. La identificación de la arquitectura del sistema operativo de dispositivos móviles Android permite comprender el funcionamiento del sistema con el fin de que el investigador forense conozca la interacción en cada una de las capas referenciadas en el capítulo 1 con el fin de que el investigador sea más eficiente al momento de encontrar evidencias en el dispositivo.

Google como propietario del sistema operativo Android ha demostrado preocuparse por tres características fundamentales, la primera de ellas es la seguridad del usuario, la segunda es mantener su producto como un software abierto que permita su evolución y la última de ellas es la innovación en su sistema operativo. Estas características han conllevado a dos particularidades al momento de realizar un análisis forense en un dispositivo con sistema operativo Android.

El primer lugar tenemos que no es posible realizar un análisis forense a un dispositivo Android si este no se encuentra en modo root y no se encuentra desbloqueado en la sesión del usuario. Dentro de las características de seguridad de Nougat o superior es que cuando un usuario coloca un patrón de seguridad para el desbloqueo del dispositivo el sistema operativo lo toma como clave de cifrado, adicional, si el teléfono no esta desbloqueado no es posible ver la información contenida en el almacenamiento externos como la microSD. Si el dispositivo móvil no está en modo root pero se encuentra desbloqueado es posible extrae alguna información del sistema como lo

contenido en el almacenamiento externo y interno, extraer la libreta de contactos, mensajes de multimedia o SMS.

Cuando el dispositivo ya se encuentra en modo root, se puede extraer una imagen forense del dispositivo, adicional a la información que podemos extraer en modo no root, podemos hacer una copia de los archivos del sistema, unidades de almacenamiento y particiones.

Finalmente, Un investigador forense no puede iniciar un proceso de rooteo sobre el dispositivo móvil sin la autorización de un juez debido a que esta actividad modifica archivos del sistema operativo de tal manera que pierde la integridad de la información frente al momento en que el dispositivo fue tomado en custodia. En el evento que sea una investigación privada, es deber del investigador forense notificar al cliente que si se realiza un proceso de rooteo en el dispositivo móvil este equipo ya no podrá ser utilizado como evidencia ante una instancia legal que el cliente desee llevar.

Se identificaron herramientas tecnológicas que son funcionales y confiables para el análisis forense de dispositivos móviles bajo el sistema operativo Android en su versión 7.1 o superior. Algunas de ellas son open source y otras no, pero en cualquiera de los dos casos están completamente habilitadas para iniciar un proceso forense sin afectar su calidad de evidencia ante un juez. Para brindar la transparencia sobre la calidad de las herramientas, la confiabilidad se establece cuando el investigador forense relaciona en el informe final las herramientas y versiones del software o hardware con el que trabajo para realizar la ejecución de la investigación. De esta manera, la contra parte deberá demostrar cualquier anomalía o falla en el software para apelar el informe presentado por el perito informático.

En este proceso se identificó tres aspectos fundamentales:

a. Obtener información de un dispositivo móvil en modo root es bastante limitado, podemos llegar a obtener información de las unidades de almacenamiento interno o externo o la información de contactos, registro de llamadas, SMS o MMC.
b. El proceso de asignar permisos root a un dispositivo móvil cambia de acuerdo con el fabricante y al modelo, esto conlleva que lo debe realizar una persona experta de tal manera que no dañe el kernel del dispositivo móvil dejándolo inservible. Así mismo, en algunos casos es necesario reinstalar el sistema operativo de tal manera que la información que contiene el dispositivo móvil es eliminada.
c. Realizar el proceso forense a un dispositivo en modo root es sencillo siempre y cuando se tenga conocimiento en comandos Unix, y en la arquitectura del sistema operativo Android. De igual manera se encontró que el alcance de toma de evidencia es mucho mayor que un dispositivo en modo no root.

   Con este modo podemos tomar una imagen forense bit a bit del dispositivo móvil y obtener toda la información que este contenga. Esto incluye, archivos temporales, archivos ocultos, archivo protegidos por el sistema, archivos de configuración, adicional de la misma información que podemos obtener si el dispositivo estuviera en modo no root.

8 RECOMENDACIONES

La recomendación principal para el lector de este trabajo de grado es realizar un estudio sobre los marcos de referencia y legales frente a la recolecta, custodia y análisis de evidencias digitales.

Como hemos mencionado en este trabajo, un mal proceso realizado por parte del equipo forense puede inducir a la culpabilidad de un hecho a un inocente, inducir a la inocencia de un culpable o invalidar todas las pruebas ante un caso judicial por falta de garantías en la integridad de las evidencias.

Ante un proceso mal realizado también se genera otro impacto para el equipo investigador y es la pérdida de credibilidad en su trabajo.

9 BIBLIOGRÁFIA

ACURIO DEL PINO, Santiago. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0. [En línea]. Bogotá: Organización De Estados Americanos. Disponible en https://www.oas.org/juridico/english/cyb_pan_manual.pdf

androidcurso.com. Arquitectura de Android. [En línea]. Bogotá: Android Curso. Disponible http://www.androidcurso.com/index.php/tutoriales-android-fundamentos/31-unidad-1-vision-general-y-entorno-de-desarrollo/99-arquitectura-de-android

BERESFORD Alastair. Security Metrics for the Android Ecosystem. [En línea]. Bogotá: University of Cambridge. Disponible en https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

CHICKOWSKI Ericka. Mobile Malware Makes Mobile Banking Treacherous. [En línea]. Bogotá: Dark Reading. Disponible en https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

CHSOSUNAL20161912551. Capa de Abstracción de Hardware (HAL). [En línea]. Bogotá: CHSOSUNAL20161912551. Disponible en https://chsosunal20161912551.wordpress.com/2016/03/15/capa-de-abstraccion-de-hardware-hal/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1564 DE 2012 (12, julio, 2012). Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. CONGRESO DE LA REPÚBLICA. Bogotá D. C., 2012. 109 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 DE 1999 (121, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las

entidades de certificación y se dictan otras disposiciones. CONGRESO DE LA REPÚBLICA. Bogotá D. C., 1999. 1-3 p.

Deloitte. Consumo móvil en Colombia. [En línea]. Bogotá: Deloitte. Disponible en https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil(VF1).pdf

Derechopenalonline.com. El perito informático y la prueba pericial. [En línea]. Bogotá: Andrés Eduardo Bassini. Disponible en http://derechopenalonline.com/el-perito-informatico-y-la-prueba-pericial/

Developer.android.com. Arquitectura de la plataforma. [En línea]. Bogotá: Developers. Disponible https://developer.android.com/guide/platform/?hl=es-419

Ley 1564 DE 2012 Código de Procedimiento Civil. [En línea]. Bogotá: Defensoría. Disponible en http://defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1564_2012.pdf

Ministerio de Tecnologías de la Información y Comunicaciones. Seguridad y privacidad de la información. Guia No. 13. [En línea]. Bogotá: Mintic. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Nokia Threat Intelligence Laboratories. Nokia Threat Intelligence Report. [En línea]. Bogotá: Nokia Threat Intelligence Laboratories. Disponible en https://onestore.nokia.com/asset/201094

Norma ISO/IEC 27000:2014(E). Information technology — Security techniques — Information security management systems — Overview and vocabulary. 15 de enero de 2014. p. 3.

Pcmag Noticias. El 99.6% del mercado móvil le pertenece a Android y iOS. [En línea]. Bogotá: pcmag. Disponible en http://latam.pcmag.com/sistemas-operativos-moviles/18490/news/el-996-del-mercado-movil-le-pertenece-a-android-y-ios

Ramírez Iván. Historia y evolución de Android: cómo un sistema operativo para cámaras digitales acabó conquistando los móviles. [En línea]. Bogotá: xatakandroid. Disponible en https://www.xatakandroid.com/sistema-operativo/historia-y-evolucion-de-android-como-un-sistema-operativo-para-camaras-digitales-acabo-conquistando-los-moviles

Tech Crunch. 6.1B Smartphone Users Globally By 2020, Overtaking Basic Fixed Phone Subscriptions. [En línea]. Bogotá: Tech Crunch. Disponible en https://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/#.n7ibu3d:RPIH