ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS, III PROMOCIÓN

TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: "PROPUESTA DE UN MODELO DE ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID"

AUTOR: GUAMÁN GUANOPATÍN EDISON PATRICIO

TUTOR: ING. SOLIS FERNANDO

SANGOLQUÍ, MAYO DEL 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

CERTIFICADO

Ing. Fernando Solís MSc.
Tutor

CERTIFICO

Que el trabajo titulado “PROPUESTA DE UN MODELO DE ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID”, realizado por el Ing. Patricio Guamán Guanopatín, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento Estudiantes de la Universidad de las Fuerzas Armadas ESPE.

Debido a que el presente trabajo es una propuesta de un modelo de análisis forense a dispositivo móviles con Sistema Operativo Android y servirá como un aporte a investigaciones relacionadas a este tema, se recomienda su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf).

Autoriza a Ing. Patricio Guamán Guanopatín, entregar el mismo a la Unidad de Gestión de Postgrado.

Sangolquí, Mayo 2014

_____

Ing. Fernando Solís MSc.
Tutor

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

DECLARACIÓN DE RESPONSABILIDAD

Ing. Patricio Guamán Guanopatín

DECLARO QUE:

El proyecto de grado denominado “PROPUESTA DE UN MODELO DE ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID”, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Mayo 2014

_____

Ing. Patricio Guamán Guanopatín

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN

Yo, Ing. Patricio Guamán Guanopatín

Autorizo a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la Institución el trabajo titulado “PROPUESTA DE UN MODELO DE ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID”, cuyo contenido, ideas y criterios es de mi exclusiva responsabilidad y autoría.

Sangolquí, Mayo 2014

_____

Ing. Patricio Guamán Guanopatín

DEDICATORIA

El presente proyecto de tesis está dedicado, a mis padres que a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento; me formaron con sentimientos, inculcaron hábitos y valores.

A mi esposa, a mis hermanas y hermanos que gracias a su apoyo diario me ayudan a nunca rendirme en los momentos difíciles, ya que con todo su amor y cariño me brindan fuerzas para mantenerme constante en conseguir mis metas. Siendo mi principal fuente de inspiración en mi vida personal.

De manera especial dedico este trabajo a la eterna memoria de mi madre que desde el cielo me bendice, cuida y me da fortaleza para continuar.

Patricio Guamán Guanopatín

AGRADECIMIENTO

A Dios quien me ha dado lo más importante que es la vida y el aliento en momento difíciles. A mis padres que me formaron como una persona de bien. A mi esposa por brindarme su apoyo y confianza incondicional. A mis hermanas y hermanos por estar junto a mí en todo momento, brindándome su amor y cariño día a día. A mis sobrinos y sobrinas quienes me dan la alegría de compartir y valorar pequeñas cosas que me hacen crecer como ser humano.

Patricio Guamán Guanopatín

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

TEMA: PROPUESTA DE UN MODELO PARA ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID.

RESUMEN

El crecimiento vertiginoso que está teniendo el uso de dispositivos móviles con Sistema Operativo Android es importante, debido a la multifuncionalidad y portabilidad se han convertido en una herramienta poderosa, enfocándose en el mundo de los negocios en línea; mejorando la productividad en las organizaciones públicas y privadas; la conectividad con amigos, familiares, clientes, jefes, empleados, reuniones de negocio; las actividades con el sector financiero; las actividades laborales, académicas, diversión y entretenimiento. Debido a esto, los dispositivos móviles son vulnerables al cibercrimen por tanto pueden estar involucrados en una investigación; por otro lado la carencia de organismos locales e internacionales que regulen y controlen el uso de dispositivos móviles; la falta de parámetros, modelos, procesos y procedimientos metodológicos; la falta de conocimiento en cuanto a las vulnerabilidades que los aplicativos poseen, crea la necesidad de cumplir con un objetivo fundamental en la presente investigación que es realizar un análisis forense a dispositivos móviles con Sistema Operativo Android basándonos en lineamientos de la cadena de custodia, cumplimientos etapas y fases establecidas y así detectar hallazgos; no conformidades; localizar vulnerabilidades y determinar cuáles fueron las causas principales de los diferentes tipos de eventos o delitos realizados desde un dispositivo móvil. Además mediante un Cuadro de Mando Integral (CMI) se evalúa indicadores o métricas enfocadas desde la perspectiva del Proceso y del Cliente, brindando un seguimiento frecuente en un tablero RGY – Sistema de Semáforos.

PALABRAS CLAVE: DISPOSITIVO MÓVIL, ANDROID, ANÁLISIS FORENSE, CADENA DE CUSTODIA, CUADRO DE MANDO INTEGRAL.

ABSTRACT

The huge growth that is having to use of mobile devices with Android Operating System is important due to the multifunctionality and portability, these have become a powerful tool, focusing on the world of online business; improving the productivity in public and private organizations; the connectivity with friends, family, clients, bosses, employees, business meetings; activities with the financial sector; industrial, academic, fun and entertainment. Because of this, mobile devices are vulnerable to the cybercrime therefore they may be involved in an investigation; on the other hand the lack of local and international agencies that regulate and control the use of mobile devices; the lack of parameters, models, processes and methodological procedures; the lack of knowledge about the vulnerabilities that the applications have create the need to meet a key objective of this research that is to conduct a forensic analysis to mobile devices with Android Operating System based on guidelines of the chain of custody, compliance stages and phases and thus to detect established findings; disagreements; locate vulnerabilities and determine what were the main causes of the different types of events or crimes made from a mobile device. Using a Balanced Scorecard evaluate indicators or metrics focused from the perspective of the Process and the Client, providing frequent monitoring by Traffic System.

KEY WORDS: MOBILE DEVICE, ANDROID, FORENSIC ANALYSIS, CHAIN OF CUSTODY, SCORECARD.

CAPÍTULO I

1. Generalidades

1.1. Introducción

Los dispositivos móviles actualmente son uno de los mejores inventos que han existido en los últimos 30 años, por su demanda mundial han ido evolucionando en su funcionalidad, contenido y características de forma exponencial. El uso de dispositivos móviles se está convertido en algo esencial para la vida de las personas, permitiendo estar conectados por medio de aplicaciones a redes sociales, correo electrónico, e-learning, etc. (Melo, 2013)

Android se ha convertido en el sistema operativo dominante en dispositivos móviles, superando las 1,000 millones de activaciones, según informes de Google (Android, 2014). Si bien es utilizado en smartphones y tablets, su versatilidad y el hecho de no tener que pagar licencia para su utilización hace que nuevos dispositivos se sumen al uso de este sistema operativo. (Grupo Gowex, 2013)

Según Gartner (Empresa consultora y de investigación de las tecnologias de la información) para el 2016 por lo menos el 89% de los correos empresariales, serán consultados mediante dispositivos móviles, reemplazando a los computadores de escritorio. Para el mismo año, los usuarios que utilizarán dispositivos móviles crecerán al 90% (Gartner Inc., 2013), atado a este crecimiento las empresas de desarrollo de software lanzarán nuevas plataformas de gestión, servicios, herramientas, contenidos, video conferencias, tareas compartidas, es decir todo lo que se hace actualmente desde una computadora de escritorio se lo podrá realizar desde un dispositivo móvil (Key4Communications, 2013).

En el presente proyecto se propone elaborar un modelo de análisis forense a dispositivos móviles con sistema operativo Android, el cual se espera apoyar al auditor con una herramienta que permita detectar hallazgos; no conformidades; localizar vulnerabilidades y determinar cuáles fueron las causas principales de los diferentes tipos de eventos o delitos realizados desde el dispositivo móvil. En el capítulo 1 se describe aspectos

generales del proyecto; en el capítulo 2 se detalla la estructura del Sistema Operativo Android; en el capítulo 3 se plantea una propuesta de un modelo para análisis forense a dispositivos móviles con Sistema Operativo Android; en el capítulo 4 se establece un caso de estudio, en el cual se pretende probar el modelo propuesto para análisis forense a dispositivos móviles con Sistema Operativo Android a fin de obtener conclusiones que validen el modelo propuesto.

1.2. Justificación

El crecimiento vertiginoso que está teniendo el uso de dispositivos móviles con sistema operativo Android es importante (Gironés, 2013), gracias a la multifuncionalidad y portabilidad, hacen una herramienta poderosa, enfocándose en el mundo de los negocios en línea; mejorando la productividad en las organizaciones públicas y privadas; la conectividad con contactos (amigos, familiares, clientes, jefes, empleados); las actividades con el sector financiero; las actividades laborales, académicas, diversión y entretenimiento.

Los dispositivos móviles forman parte de la vida cotidiana de las personas, pero la carencia de organismos locales e internacionales que regulen y controlen el uso de dispositivos móviles; la falta de parámetros, modelos, procesos y procedimientos metodológicos; la falta de conocimiento en cuanto a las vulnerabilidades que los aplicativos poseen como inyección de malware en los dispositivos; la suplantación de identidad (phishing); la ingeniería social; el crecimiento de empresas que no cumplen con medidas de protección de datos como cifrado del contenido cuando desarrollan software de gestión, contenidos, servicios; no controlar puertos abiertos; el conectarse a redes públicas sin contraseña y mediante estas acceder a páginas de entidades financieras (El Comercio, 2014, p. 25); el mal uso del correo empresarial y privado; el realizar compras online en sitios inseguros los cuales pueden ser detectados fácilmente por redes propensas a MitM (Redes Man in the Middle); la existencia de vulnerabilidades en los dispositivos que incluso el atacante podría tomar el control absoluto del dispositivo para realizar llamadas, enviar mensajes o llevar a cabo cualquier

acción, sin que el usuario se percate. Y la carencia de difusión de herramientas para efectuar un análisis forense, son eventos que, justifican la necesidad de plantear una propuesta de un modelo de análisis forense a dispositivos móviles con sistema operativo Android, el cual se espera apoyar al auditor con un modelo metodológico que permita detectar hallazgos; no conformidades; localizar vulnerabilidades en textos planos, logs de aplicativos; y determinar con evidencias, cuáles fueron las causas principales de los diferentes tipos de eventos o delitos realizados desde el dispositivo móvil.

1.3. Objetivo General

- Elaborar un modelo de análisis forense a dispositivos móviles con sistema operativo Android.

1.4. Objetivos Específicos

- Analizar la estructura del sistema operativo Android.
- Desarrollar un modelo para análisis forense a dispositivos móviles con Sistema Operativo Android.
- Caso de estudio del modelo propuesto para análisis forense a dispositivos móviles con Sistema Operativo Android.

1.5. Alcance

Elaborar un modelo de análisis forense a dispositivos móviles con sistema operativo Android, el cual se espera apoyar al auditor con una herramienta que permita detectar hallazgos; no conformidades; localizar vulnerabilidades en textos planos, logs de aplicativos; y determinar con evidencias, cuáles fueron las causas principales de los diferentes tipos de eventos o delitos realizados desde el dispositivo móvil.

Espacio: Se desarrollará en Ecuador – Pichincha – Quito – ESPE (caso de estudio).

Temporalidad: Año 2014 en adelante

Base conceptual: El proyecto se sustentará en metodologías de análisis forense que se encuentran en etapa de evaluación. Aplicando la definición

de análisis forense que indica “Es una disciplina especializada que requiere un conocimiento de auditoría en general y métodos de investigación para que se lleve a cabo. Constituye una rama importante para procesos investigativos, utilizada en la reconstrucción de delitos informáticos, investigaciones de fraudes, cálculos de daños económicos y rendimientos de proyecciones financieras (Cano J. , Computacion forense, 2009, p. 14)”. El mismo que será la base en la creación del modelo de análisis forense a dispositivos móviles con sistema operativo Android.

CAPÍTULO II

2. Marco Teórico

2.1. Sistema Operativo Android

Android es una plataforma de código abierto creada por Google para todo tipo de dispositivo móvil, está basado en el kernel de Linux; a pesar de estar basado en este kernel no cuenta con un sistema nativo de ventanas de Linux, tampoco tiene soporte para glibc (libería estándar de C), tampoco es posible utilizar la mayoría de aplicaciones de GNU de Linux.

Reutilizando toda la funcionalidad que esta implementado en el kernel de Linux, Android agrega muchas funcionalidades específicas para plataformas móviles como la comunicación entre procesos, la forma de manejar la memoria compartida, la administración de energía, etc.

2.1.1. Historia de Android

El anuncio del lanzamiento del sistema operativo Android de Google, se realizó el 5 de noviembre de 2007 junto con la creación de la Open Handset Alliance, un consorcio de 78 compañías de hardware, software y telecomunicaciones dedicadas al desarrollo de estándares abiertos para dispositivos móviles.

Antes de ser presentado Google realizo acuerdos con más de 34 compañías del sector tecnológico, entre las que se encuentran Samsung, HTC, Qualcomm, Motorola, Telefónica y T-Mobile, que se comprometieron a comercializar terminales impulsados por esta plataforma. Finalmente Google liberó su sistema operativo con la mayoría del código de Android bajo la licencia Apache, una licencia libre y de código abierto (SamsungBlogspot, 2012). Dentro de la plataforma, ya aparecen todas las aplicaciones básicas de Google como: Google Maps, Google Docs, Gmail, etc.

Android nace con una filosofía basada en código abierto, ya que no sólo utiliza Linux como núcleo base, sino que muchas de sus aplicaciones base, como el navegador de Internet y otras tantas funcionalidades está basado en código libre. Con el anuncio de Google de la liberación de su sistema operativo, planificaron que se alimente de las contribuciones de

programadores de todo el mundo. En lo que Google no pareció querer transigir es en el desarrollo de las aplicaciones para su sistema operativo, forzando una homogeneización de sus máquinas virtuales Java que haga que cualquier aplicación desarrollada para Android sea ejecutable en cualquier terminal que incorpore el sistema operativo de Google. Lo cual queda claro que se trata de un sistema operativo pensado para optimizar al máximo los recursos disponibles en un dispositivo móvil, pudiendo ejecutarse en terminales no muy potentes, lo cual a su vez hace que el precio de un terminal Android pueda ser inferior al de otros smartphones (Gironés, 2013).

De acuerdo al análisis realizado del crecimiento en el mercado de Android se detalla en el Cuadro 1 por fechas más relevantes los diversos avances que ha tenido este sistema operativo.

Cuadro 1

Crecimiento en el mercado de Android

Fecha	Detalle
Julio 2005	Google adquiere Android Inc., una pequeña empresa que desarrolla software para móviles.
Noviembre 2007	Nace el consorcio de empresas unidas Open Handset Alliance con el objetivo de desarrollar estándares abiertos para móviles Texas Instruments, Broadcom CO., Google, HTC, Intel, LG, Marvel Tech, Motorola, Nvidia, Qualcomm, Samsumg Electronics, Sprint Nextel, T-Mobile. Y se anuncia su primer producto Android de plataforma soportada para móviles construida sobre el kernel de Linux 2.6
Octubre 2008	Liberación de Android, distribuida principalmente con licencia Apache 2.0. Con colaboración de otras licencias como GPL versión 2 para el núcleo. Se da apertura al Android Market HTC Dream, que fue el primer teléfono con sistema operativo Android.
Diciembre 2008	Se realiza nuevas alianzas con ARM Holdings, Athreos Communications, Asustek Computer Inc., Garmin Ltd, Softbank, Sony Ericsson, Toshiba Corp y Vodafone Group Plc.
Noviembre 2009	Motorola Droid consigue vender 1.05 millones de unidades en 74 días, superando el record establecido por el iPhone de Apple.
Diciembre 2009	A la fecha existen 16.000 aplicaciones en la tienda Android Market, 60% gratuitas, 30% de pago.
Febrero 2010	Google anuncia la masiva aceptación de Android, 60.000 teléfonos con Android vendidos al día.
Abril 2011	Android crece con un 36% de las ventas de teléfonos en el primer cuarto del 2011. Gartner anuncia que 36 millones de terminales Android se venderán en el primer trimestre del 2012. Cifras que auguran el dominio que está llevando a cabo en el mundo de los Smartphone.
Enero 2012	Google comenta que se han activado 250 millones de dispositivos. Esta cifra sorprende, dado que aumenta respecto a los datos del tercer trimestre del pasado año 2011. Son 555.000 activaciones diarias, también anunciado que desde el Android Market se han realizo 11000 millones de descargas, lo que viene a ser 1000 millones más que cuando Google anunció su llegada a los 10000 millones hace alrededor de un mes.
Mayo 2013	El mercado Android ha tenido un crecimiento de 142,4% en comparación con el mismo periodo del año pasado, con sus ventas alcanzando 49,2 millones de unidades en los primeros meses de 2013.

Android se ha convertido en una de las plataformas operativas más eficientes, los usuarios y las activaciones están dejando muy claro que Google ha alcanzado un alto grado de madurez con su plataforma.

2.1.2. Actualizaciones de Android

Android tiene numerosas actualizaciones desde su liberación inicial, como se describe en el Cuadro 2, dichas actualizaciones al sistema operativo, generalmente arreglan bugs o se añaden nuevas funcionalidades.

Cada actualización es desarrollada bajo un nombre en código de un elemento relacionado con postres como son Cupcake, Donut, Froyo, Ginebra, entre otros.

Android es criticado muchas veces por la fragmentación que sufren las terminales al no soportar las actualizaciones constantes que tienen los distintos fabricantes. Se pensaba que este entorno cambiaría tras un anuncio de Google en el que comunicó que los fabricantes se comprometerán aplicar actualizaciones al menos 18 meses desde su salida al mercado, pero esto al final nunca se concretó.

Se elabora el Cuadro 2 con las diversas actualizaciones de Android desde su primer lanzamiento basándonos en la información que contiene el portal oficial (Android, 2014).

Cuadro 2

Actualizaciones del sistema operativo Android

Versión	Fecha de liberación
1.0 Apple Pie	▪ Liberado el 23 de septiembre de 2008 ▪ El primer dispositivo Android, el HTC Dream.
1.1 Banana Bread	▪ Liberado el 9 de febrero de 2009 ▪ Resolvió fallos, cambio la API y agregó una serie de características.
1.5 Cupcake (basado en el núcleo de Linux 2.6.27)	▪ Liberado el 30 de abril de 2009 ▪ Incluye varias nuevas características y correcciones de interfaz de usuario.
1.6 Donut (basado en el núcleo de Linux 2.6.29)	▪ Liberado el 15 de septiembre de 2009 ▪ Incluye numerosas nuevas características y funcionalidades, mejoramiento del motor multilenguaje, velocidad en búsquedas, soporte resolución de pantalla WVGA, framework de gestos (GestureBuilder).
2.0/2.1 Eclair	▪ Liberado el 26 de octubre de 2009 ▪ Sincronizaciones múltiples con cuentas al dispositivo, soporte Bluetooth 2.1, funcionalidad con la cámara, renovación en la interfaz de usuario, soporte HTML5, clase MotionEvent, mejora Google Maps.
2.2 Froyo (basado en el núcleo de Linux 2.6.32)	▪ Liberado el 20 de mayo de 2010 ▪ Optimizaciones en velocidad, memoria, rendimiento e integración del motor de JavaScript v8 de Chrome, Android Cloud to Device Messaging, notificaciones push, anclaje de red por USB y WiFi, actualización del Market, soporte Adobe Flash.
2.3 Gingerbread (basado en el núcleo de Linux 2.6.35)	▪ Liberado el 6 de diciembre de 2010 ▪ Soporte para pantallas extra grandes y resoluciones WXGA, telefonía VoIP SIP, reproducción de videos WebM/VP8, audio AAC, soporte para Near Field Communication, teclado multi-táctil, soporte mejorado para desarrollo de código nativo, soporte de chat de video o voz, usando Google Talk.
3.0 Honeycomb (basado en el núcleo de Linux 2.6.36)	▪ Liberado el 22 de febrero de 2011 ▪ Soporte para tablets, escritorio 3D con widgets rediseñados, sistema multitareas, sincronización de favoritos con Google Chrome y navegación privada, soporte para video chat mediante Google Talk, mejoramiento en el soporte para redes Wi-Fi.
4.0.1 Ice Cream Sandwich (basado en el núcleo de Linux	▪ Liberado el 19 de octubre de 2011 ▪ Botones suaves Android 3.x, buzón de voz, funcionalidad de pinch-to-zoom en el calendario, captura de pantalla integrada, funcionalidad copiar-

Continúa

3.0.1)	pegar mejorada, tipografía para la interfaz de usuario Robot, aplicación People, Android Beam. ▪ Wi-Fi Direct, Android VPN Framework (AVF) and TUN (but not TAP) kernel module, soporta software tipo VPN.
4.1 Jelly Bean (basado en el núcleo de Linux 3.0.31)	▪ Liberado el 27 de junio de 2012 ▪ Actualización incremental en el enfoque primario de la funcionalidad y el rendimiento de la interfaz de usuario, triple buffer, latencia vsync extendida, velocidad de cuadros de 60 fps.
4.4 KitKat	▪ Liberado en Septiembre de 2013 ▪ Google Now es inteligente porque pretende saber en qué momento una información es más útil que otra, múltiples tarjetas, soporte a arquitecturas de 64 bits, arquitectura basado en ARM v8.

2.1.3. Características y Especificaciones

Figura 1. Características de Android (Basterra, 2012)

En el Cuadro 3 se describen las características principales del sistema operativo según análisis realizado a Android (Gironés, 2013).

Cuadro 3

Características y Especificaciones

Aplicación	Características
Diseño de dispositivo	La plataforma es adaptable a pantallas grandes, VGA, biblioteca de gráficos 2D, biblioteca de gráficos 3D basada en las especificaciones de la OpenGL ES 2.0 y diseño de teléfonos tradicionales.
Almacenamiento	SQLite, una base de datos liviana, que es usada para propósitos de almacenamiento de datos.
Conectividad	Android soporta las tecnologías de conectividad GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth, Wi-Fi, LTE y WiMAX.
Mensajería	SMS y MMS son formas de mensajería, incluyendo mensajería de texto y ahora Android Cloud to Device Messaging Framework (C2DM) es parte del servicio de Push Messaging de Android.
Navegador web	El navegador web incluido en Android está basado en el motor de renderizado de código abierto WebKit, emparejado con el motor JavaScript V8 de Google Chrome.
Soporte de Java	Las aplicaciones están escritas en código Java, sin embargo no existe una máquina virtual Java en la plataforma. El bytecode Java no es ejecutado, sino que en primera instancia se compila en un ejecutable Dalvik y corre en la Máquina Virtual Dalvik, esta es una máquina virtual especializada, diseñada específicamente para Android y optimizada para dispositivos móviles que funcionan con batería y que tienen memoria y procesador limitados. El soporte para J2ME puede ser agregado mediante aplicaciones de terceros como el J2ME MIDP Runner.
Soporte multimedia	Android soporta los siguientes formatos multimedia: WebM, H.263, H.264 (en 3GP o MP4), MPEG-4 SP, AMR, AMR-WB (en un contenedor 3GP), AAC, HE-AAC (en contenedores MP4 o 3GP), MP3, MIDI, OggVorbis, WAV, JPEG, PNG, GIF y BMP.
Soporte para streaming	Streaming RTP/RTSP (3GPP PSS, ISMA), descarga progresiva de HTML5. Adobe Flash Streaming (RTMP) es soportado mediante el Adobe Flash Player. Se planea a futuro el soporte de Microsoft Smooth Streaming con el port de Silverlight para Android. Adobe Flash HTTP Dynamic Streaming estará disponible mediante una actualización de Adobe Flash Player.

Continúa

Soporte para hardware adicional	Android soporta cámaras de fotos, de vídeo, pantallas táctiles, GPS, acelerómetros, giroscopios, magnetómetros, sensores de proximidad y de presión, termómetro, aceleración 2D y 3D.
Entorno de desarrollo	Incluye un emulador de dispositivos, herramientas para depuración de memoria y análisis del rendimiento del software. El entorno de desarrollo integrado es Eclipse usando plug-in de herramientas de desarrollo para Android (Gironés, 2013, p. 32)
Market	El Android Play es una tienda de aplicaciones gratuitas y pagadas, las cuales pueden ser descargadas e instaladas en los dispositivos Android sin la necesidad de una PC.
Multi - táctil	Android tiene soporte nativo para pantallas multi - táctiles que inicialmente hicieron su aparición en dispositivos como el HTC Hero. La funcionalidad fue originalmente desactivada a nivel de kernel (posiblemente para evitar infringir patentes de otras compañías). Más tarde, Google publicó una actualización para el Nexus One y el Motorola Droid que activa el soporte para pantallas multi - táctiles de forma nativa.
Bluetooth	El soporte para A2DF y AVRCP fue agregado en la versión 1.5; el envío de archivos (OPP) y la exploración del directorio telefónico fueron agregados en la versión 2.0; y el marcado por voz junto con el envío de contactos entre teléfonos fue en la versión 2.2.
Video llamada	Android soporta video llamada a través de Google Talk desde su versión liberada HoneyComb.
Multitarea	Multitarea real de aplicaciones está disponible, es decir, las aplicaciones que no estén ejecutándose en primer plano reciben ciclos de reloj, a diferencia de otros sistemas operativos móviles en la que la multitarea es congelada.
Características basadas en voz	La búsqueda en Google a través de voz está disponible como "Entrada de Búsqueda" desde la versión inicial del sistema operativo.
Tethering	Android soporta tethering, que permite al teléfono ser usado como un punto de acceso alámbrico o inalámbrico (todos los teléfonos desde la versión 2.2, no oficial en teléfonos con versión 1.6 o superiores mediante aplicaciones disponibles en el Google Play, como la aplicación PdaNet). Para permitir a un PC usar la conexión 3G del móvil Android se podría requerir la instalación de software adicional.

2.1.4. Arquitectura de Android

La arquitectura de Android está compuesta de aplicaciones que se ejecutan en un framework Java de aplicaciones orientadas a objetos sobre el núcleo de las bibliotecas de Java, en una máquina virtual Dalvik la compilación es en tiempo de ejecución. Las bibliotecas escritas en lenguaje C incluyen un administrador de interfaz gráfica (surface manager), un framework OpenCore, una base de datos relacional SQLite, una Interfaz de programación API gráfica OpenGL, un motor de renderizado WebKit, un motor gráfico SGL, SSL y una biblioteca estándar de C Bionic. El sistema operativo está compuesto por 12 millones de líneas de código, incluyendo 3 millones de líneas de XML, 2.8 millones de líneas de lenguaje C, 2.1 millones de líneas de Java y 1.75 millones de líneas de C++. (Gironés, 2013, p. 26)

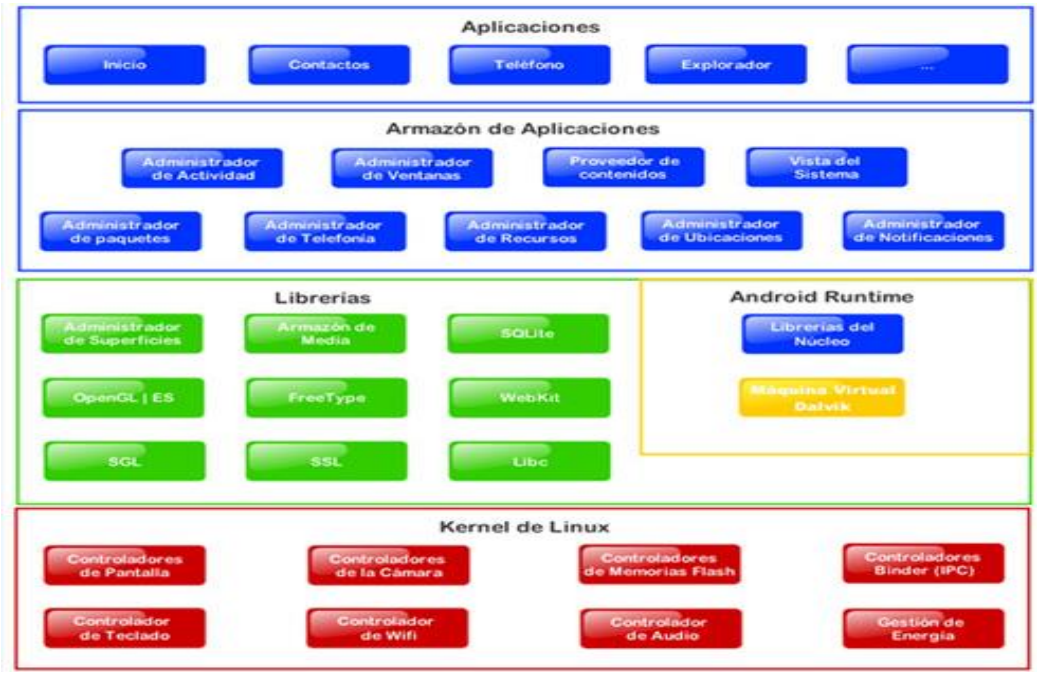


Figura 2. Arquitectura del sistema operativo Android (Android, 2013)

2.1.5. Kernel de Linux

Esta capa de la arquitectura del sistema operativo Android está formada por el kernel versión 2.6 del sistema operativo Linux; aquí se proporciona servicios como la seguridad, el manejo de la memoria, el multiproceso, la pila de protocolos y el soporte de drivers necesarios para que cualquier

componente pueda ser utilizado mediante las llamadas correspondientes. Siempre que un fabricante incluye un nuevo elemento de hardware, lo primero que se realiza para poder ser utilizado desde Android es crear las librerías de control o drivers necesarios dentro de este kernel de Linux embebido en Android.

Esta es la capa de abstracción de hardware (HAL - Hardware Abstraction Layer) y se encarga de gestionar los servicios del sistema, como la gestión de memoria y de procesos, Entrada/Salida, red, etc. El kernel es el responsable principal de facilitar a los distintos programas acceso seguro al hardware del dispositivo móvil o en forma básica es el encargado de gestionar recursos, a través de servicios de llamada al sistema. Como hay muchos programas y el acceso al hardware es limitado, también se encarga de organizar qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado. Acceder al hardware directamente puede ser realmente complejo, por lo que los núcleos suelen implementar una serie de abstracciones del hardware. Esto permite cubrir la complejidad y proporcionar una interfaz limpia y uniforme al hardware subyacente, lo que facilita el uso a la persona que desee implementar nueva funcionalidad.

Cuando se emplea una HAL, las aplicaciones no acceden directamente al hardware sino que lo hacen a la capa abstracta provista por la HAL, la cual accede al hardware a través de los drivers o controladores. Del mismo modo que las API, las HAL permiten que las aplicaciones sean independientes del hardware porque abstraen información acerca de los sistemas, como lo son las cachés, los buses de E/S y las interrupciones. Otra factor importante es la sencillez para implementar el sistema para los fabricantes, los cuales tienen que proveer a sus sistemas del kernel de Linux adecuado y siguiendo el modelado de los drivers de Linux, comunicando con los distintos periféricos del dispositivo. Una vez logrado esto, se instalan las demás capas de Android; esto implica que si se instala un núcleo Linux en un dispositivo con acceso a todas las interfaces mediante sus correspondientes drivers se podrán transformar en un dispositivo móvil con el sistema operativo de Google. (Gironés, 2013, p. 26)

El kernel se lo define como el corazón del sistema operativo y existe una serie de modelos desarrollados, así que es importante conocer la manera de numerarse los 4 dígitos (VV.RR.NR.CR) que lo conforma:

- VV: Indica la versión (o serie) del kernel.
- RR: Indica la revisión del kernel.
- NR: Indica nuevas revisiones del kernel. Estos números cambian cuando se incorporan nuevas características y drivers.
- CR: Este digito cambia cuando se corrigen fallos de programación o fallos de seguridad dentro de una revisión. (Grupo ADSL Zone, 2012)

2.1.5.1. Modificaciones en el kernel de Linux para Android

Existe varias modificaciones al kernel base de Linux para que en el sistema operativo Android funcione de acuerdo a todas las exigencias que se necesita, se cita las más importantes (Linux, 2013):

- **Goldfish.** Está diseñado específicamente para funcionar con el emulador de Android, este simula un dispositivo móvil basado en ARM (Arquitectura que contiene un conjunto de instrucciones de 32 bits). Es ejecutado bajo instrucciones ARM926T y cuenta con funciones de entrada y salida, como la lectura de las pulsaciones de teclas o mostrar la salida de vídeo en el emulador. Estas interfaces se implementan en archivos específicos para el emulador de Goldfish y no son compilados en el núcleo que se ejecuta en los dispositivos reales.
- **Yaffs2.** Es un acrónimo del sistema de archivos flash que se encuentra disponible para Linux, aunque no es parte de la norma 2.6.25 del kernel. Este sistema de archivos proporciona una interfaz de alto rendimiento entre el kernel de Linux y los dispositivos de memoria flash NAND (esta memoria combina alta densidad y es de bajo costo).
- **Bluetooth.** Google hizo varios cambios en 10 archivos de la pila de comunicación vía Bluetooth, los cuales corrigen errores relacionados

con auriculares Bluetooth y añade la depuración y funciones de control de acceso.

- **IPC Binder.** Es una comunicación entre procesos IPC, los cuales permiten la prestación de servicios a otros procesos a través de un conjunto de APIs de alto nivel que están disponibles en el estándar de Linux.
- **Depurador de baja memoria.** Android añade un depurador de poca memoria que es utilizado en el inicio de flujo de un proceso. Este es analizado en la lista de los procesos en ejecución de Linux y destruye determinado proceso que este consumiendo en exceso recursos.
- **Ashmem.** Es un sistema de memoria compartida que añade las interfaces a los procesos, estos pueden compartir bloques de la memoria. La ventaja de este sistema es, si un proceso intenta acceder a un segmento de memoria compartida del núcleo que haya liberado, recibirá un error y luego tendrá que reasignar el bloque y volver a cargar los datos.
- **Memoria RAM y dispositivo de registro.** Para solventar en la depuración, Android añade la capacidad de almacenar los mensajes del kernel de registro en un búfer de RAM. Adicional Android añade un módulo de registro independiente para que los procesos del usuario puedan leer y escribir mensajes de los usuarios de registro.
- **Android Debug Bridge.** Es una herramienta que viene junto con el SDK de Android y nos permite acceder y controlar un dispositivo desde una PC mediante un protocolo que pasa por una conexión USB entre un dispositivo de hardware con Android y un desarrollador escribe líneas de comandos para establecer la comunicación con una instancia del emulador de aplicaciones en una PC (Android, 2014).
- **Administración de energía.** La conexión se realiza por intervalos de conexión, permite una administración controlada de la ejecución de aplicaciones en segundo plano, ya que la administración pertenece a un grupo diferente de las otras piezas.

2.1.6. Librerías

La capa de librerías de la arquitectura del sistema operativo Android se coloca por encima del kernel, para proveer una interfaz de programación (API) unificada para acceder a las capacidades que el kernel provee. Siendo Android un sistema tipo Unix, hace uso de la librería C (libc) que implementa llamados al sistema para que las aplicaciones accedan a los servicios que provee el kerrnel. Además de las capacidades que provee la librería de C, Android incluye también otro conjunto de librerías escritas tanto en C, como en librerías nativas en C++. Como cita Gironés en su libro (Gironés, 2013) las librerías compiladas en código nativo del procesador utilizan proyectos de código abierto como:

- **WebKit:** Soporta un moderno navegador web utilizado en Android y en la vista webview. Se trata de la misma librería que utiliza Google Chrome y Safari de Apple.
- **System C Library:** Una derivación de las librerías BSD de C estándar, adaptados para dispositivos embebidos basados en Linux.
- **Media Framework:** Librería basada en Packet Video's Open Core, soporta codecs de reproducción y grabación de multitud de formatos de audio, video e imágenes MPEG4, H.264, MP3, AAC, AMR, JPG y PNG.
- **Surface Manager:** Maneja el acceso al subsistema de representación gráfica en 2D y 3D.
- **SGL:** Motor de gráficos 2D.
- **Librería 3D:** Implementación basada en OpenGL, las librerías utilizan el acelerador de hardware 3D si está disponible o el software altamente optimizado de proyección 3D.
- **FreeType:** Fuentes en bitmap y renderizado vectorial.
- **SQLite:** Potente y ligero motor de bases de datos relacionales disponible para todas las aplicaciones.
- **SSL:** Proporciona servicios de encriptación Secure Socket Layer.

2.1.7. Runtime – Entorno de ejecución de Android

Esta capa esta al mismo nivel que las librerías de la arquitectura del sistema operativo Android, está situada en el entorno de ejecución, lo constituyen las Libraries Core que son librerías con múltiples clases Java y la máquina virtual Dalvik que fue creada por Google por las limitaciones de los dispositivos donde se ejecuta Android. En este sistema operativo para dispositivos móviles no es posible utilizar la máquina virtual de Java estándar. Por tanto para cada aplicación Android es ejecutada en su propio proceso, en una instancia de la máquina virtual Dalvik. Se ha confirmado que un dispositivo puede ejecutar múltiples máquinas virtuales de manera eficiente.

2.1.7.1. Máquina Virtual Dalvik (Androideity, 2011)

Dalvik es una máquina virtual especialmente diseñada para Android, desarrollada por Dan Bornstein y su equipo en Google.

La máquina virtual de Java (JVM) fue diseñada para ser una solución general, y el equipo de Dalvik consideró que se podría realizar un mejor trabajo al enfocarse estrictamente en dispositivos móviles. Observando cuáles serían las posibles restricciones específicas a un ambiente móvil, que probablemente no se cambiaría en un futuro cercano. Uno de estos es la vida útil de la batería y otro es el poder de procesamiento.

En el desarrollo normal de aplicaciones Java, el código fuente es código Java, el cual es compilado en byte code usando su propio compilador, para luego sea ejecutado en la máquina virtual de java. En Android, las cosas se hacen de diferente manera, se escriben las aplicaciones en código fuente Java e igualmente se compila a byte code con el mismo compilador de java. Pero en este punto debe ser recompilado nuevamente, usando el compilador Dalvik a byte code Dalvik. Es este byte code el que será ejecutado en la máquina virtual de Android.

La arquitectura de componentes de aplicaciones de Android, es en parte un producto de la forma en que implementa un ambiente multiproceso. Para hacer ese ambiente idóneo para múltiples aplicaciones de distintos vendedores con un mínimo requerimiento de confianza entre cada vendedor,

Android ejecuta múltiples instancias de la máquina virtual Dalvik, una por cada tarea.

Como resultado de este simple y confiable enfoque a multiprocesos, Android debe dividir eficientemente la memoria en múltiples heaps. Cada heap debe ser relativamente pequeño para que muchas aplicaciones se ubiquen en memoria al mismo tiempo. En cada heap, el ciclo de vida de componentes permite que un componente que no esté en uso, especialmente componentes de interfaz actualmente inactivos, sean adoptados por el colector de basura cuando hay poco espacio y restaurado cuando sea necesario (Madrid, 2012).

El código ejecutable final de Android, como resultado de la máquina virtual de Dalvik, no se basa en el byte code de Java, sino que se basa en los archivos .dex. Esto significa que no se puede ejecutar directamente el byte code de Java, sino que hay que comenzar con los archivos .class de Java y luego convertirlos en archivos .dex.

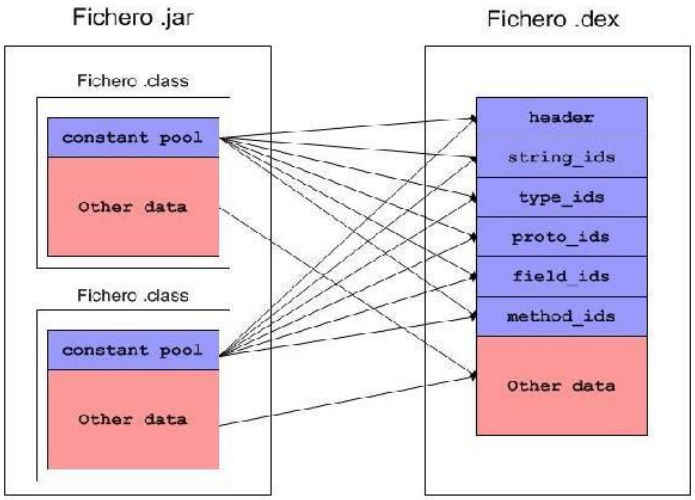


Figura 3. Formato fichero .dex (Madrid, 2012)

2.1.8. Application Framework

Esta capa de la arquitectura del sistema operativo Android, es el entorno de aplicaciones que proporcionan una plataforma de desarrollo libre para aplicaciones con gran riqueza e innovación. Esta capa ha sido diseñada para simplificar la reutilización de componentes. Las aplicaciones pueden publicar sus capacidades y otras pueden hacer uso de ellas. Este mismo mecanismo

permite a los usuarios reemplazar componentes. Una de las mayores fortalezas del entorno de aplicación de Android es que se aprovecha el lenguaje de programación Java. El SDK de Android no ofrece todo lo disponible para su estándar del entorno de ejecución JRE de Java, pero es compatible con una fracción muy significativa del sistema.

Se cita a las API más importantes que forman parte de esta capa (Android Inc, 2013):

- Activity Manager
- Window Manager
- Telephone Manager
- Content Provider
- View System
- Location Manager
- Notification Manager
- Xmpp Service
- Package Manager
- Resource Manager
- Location Manager
- Sensor Manager
- Cámara
- Multimedia
- Intent
- Broadcast Intent Receiver
- Service
- Content Provider

2.1.9. Aplicaciones

Esta capa de la arquitectura del sistema operativo Android, está formada por un conjunto de aplicaciones instaladas en la máquina virtual de Android. Todas las aplicaciones son ejecutadas en la máquina virtual Dalvik para garantizar la seguridad del sistema, normalmente las aplicaciones Android están escritas en lenguaje Java o también existen aplicaciones utilizando lenguaje C/C++.

Las aplicaciones que están incluidas por defecto en Android como aquellas que el usuario va instalando, utilizan los servicios, las API y librerías de las capas de la arquitectura de Android. 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 lenguaje C o C++) y las administradas (programadas en lenguaje Java), las que vienen preinstaladas en el dispositivo y aquellas que el usuario va instalando. En esta capa se encuentra también la aplicación principal del sistema: Inicio (Home) o lanzador (launcher), porque es la que permite ejecutar otras aplicaciones mediante una lista y mostrando diferentes escritorios donde se pueden colocar accesos directos a aplicaciones e incluso widgets, que son también aplicaciones de esta capa.

Una aplicación Android corre dentro de su propio proceso, por tanto, una característica fundamental de Android es que el tiempo y ciclo de vida de una aplicación no está controlada por la misma aplicación, sino que lo determina el sistema a partir de una combinación de estados, las cuales pueden ser, las aplicaciones que están funcionando, la prioridad que tiene el usuario y la memoria queda disponible en el sistema. (Gironés, 2013)

Una aplicación debe exponer todas sus actividades, los puntos de entrada, la comunicación, las capas, los permisos a través de AndroidManifest.xml. Es muy importante tener en consideración cómo estos componentes impactan en el tiempo de vida del proceso asociado con una aplicación, porque si no son empleados de manera apropiada, el sistema detendrá el proceso de la aplicación aun cuando se esté haciendo algo importante.

2.1.9.1. Procesos de una aplicación en Android

Cada aplicación de Android corre en su propio proceso, el cual se crea al ejecutar una aplicación, y permanece hasta que la aplicación deja de trabajar o el sistema necesita memoria para otras aplicaciones. Android sitúa cada proceso en una jerarquía de importancia basada en estado de proceso.

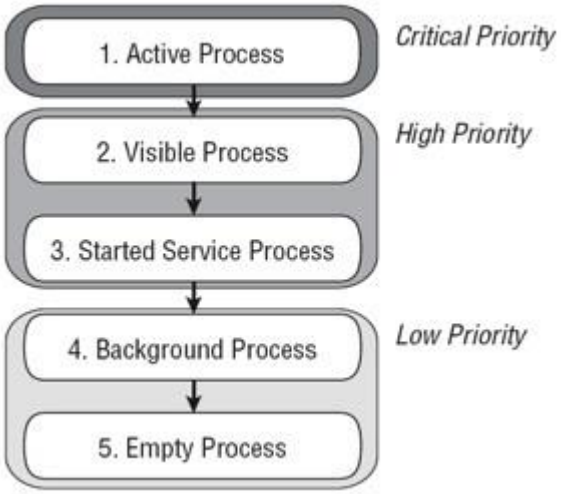


Figura 4. Procesos de una aplicación en Android (FIME-ITS, 2012)

Procesos en primer plano (ACTIVE PROCESS). Es un proceso que aloja una actividad en la pantalla y la que el usuario está interactuando (método onResume() es consumido) o que un IntentReceiver está ejecutándose. Este tipo de procesos serán eliminados como último recurso si el sistema necesita memoria.

Procesos visibles (VISIBLE PROCESS). Es un proceso que aloja una actividad pero no está en primer plano (método onPause() es consumido). Esto ocurre en situaciones dónde la aplicación muestra un cuadro de diálogo para interactuar con el usuario. Este tipo de procesos no serán eliminados en caso que sea necesaria la memoria para mantener a todos los procesos del primer plano ejecutándose.

Procesos de servicio (STARTEDSERVICE PROCESS). Es un proceso que aloja un servicio, el cual consume el método startService(). Este tipo de procesos no son visibles y suelen ser importantes para el usuario (conexión con redes, reproducción de música).

Procesos en segundo plano (BACKGROUND PROCESS). Es un proceso que aloja una actividad que no es visible para el usuario (método onStop() es consumido). Normalmente la eliminación de estos procesos no es un gran impacto para la actividad del usuario. Es muy frecuente que existan numerosos procesos de este tipo en el sistema, por lo que se mantiene en una lista LRU (LeastRecentlyUsed) la cual asegura que el último proceso

visto por el usuario sea el último en eliminarse en caso de necesitar memoria. Así el sistema mantiene vivos los procesos que son usados recientemente.

Procesos vacíos (EMPTY PROCESS). Es un proceso que no aloja ningún componente. La razón de este proceso es tener una caché disponible de la aplicación para su próxima activación. Es habitual que el sistema elimine este tipo de procesos con frecuencia para obtener memoria disponible.

Según esta jerarquía, Android prioriza los procesos existentes en el sistema y decide cuáles han de ser eliminados, con el fin de liberar recursos y poder procesar la aplicación requerida. (Madrid, 2012)

2.1.9.2. Estructura Memoria Interna

La estructura de la memoria interna se divide en varias particiones entre las que se encuentran una partición de arranque, un recovery (menú de recuperación de errores), una partición de caché y las dos más importantes que son la partición del sistema y la partición de datos de usuario, que se visualiza en la Figura 5.

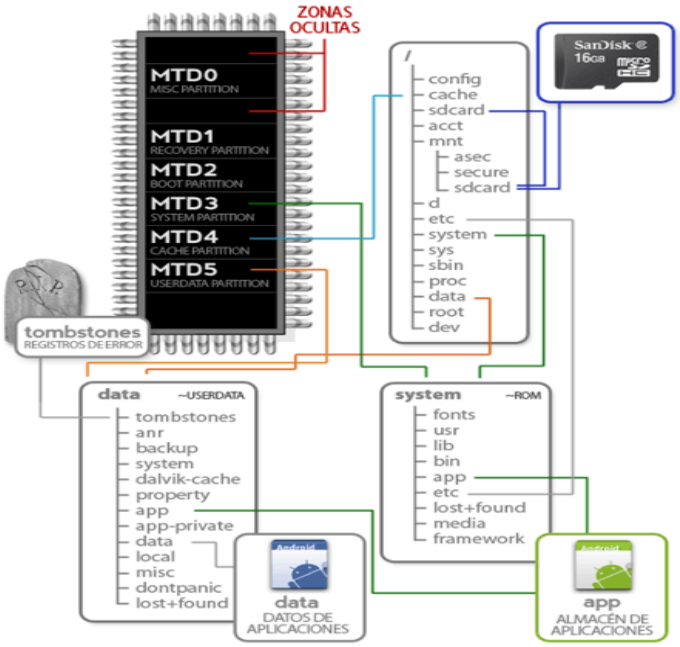


Figura 5. Estructura memoria interna (Hernandez, 2011)

2.1.9.2.1. Partición /system

En esta partición se almacena la información del sistema operativo, fuentes (tipos de letra), aplicaciones del sistema (las primarias y oficiales de Google), sonidos de notificaciones, alarmas y el framework (entorno y ventanas gráficas) del sistema operativo.

2.1.9.2.2. Partición /userdata

En esta partición se almacena los datos / información del usuario, registros de errores de programas (en la carpeta lápidas), información local, caché de la máquina virtual Dalvik y las aplicaciones descargadas del market, también la información asociada a cada aplicación del dispositivo. Esta partición utiliza un sistema de ficheros llamado YAFFS (Yet Another Flash File System), aunque en versiones superiores al Android 2.3 ha sido reemplazado por Ext4 (Fourth Extended File System).

2.1.9.2.3. Task-Killer

Uno de los errores más frecuentes en Android es el de considerar el uso de un task-killer (administrador de tareas) para liberar memoria y conseguir mayor velocidad. Esto se debe a que la mayoría de las personas asocian un modelo antiguamente utilizado y desconocen que los sistemas operativos actuales utilizan al máximo la memoria RAM, ya que memoria RAM no utilizada - memoria RAM desperdiciada. Android se encarga de cerrar y abrir las aplicaciones dependiendo de la necesidad de RAM del sistema, manteniendo abiertas las aplicaciones más utilizadas para obtener una mejor eficiencia y optimización de recursos del dispositivo.

2.2. Dispositivos móviles con Android

El uso de dispositivos móviles es cada día más común y se han convertido en herramientas casi esenciales en la vida de las personas ya que ayudan a estar conectados por medio de aplicaciones a redes sociales, correo electrónico, comunicación, geolocalización, etc.

Por medio de la conectividad en el mundo, la tendencia a masificar el uso de los dispositivos móviles es evidente. Según (Castro, 2013) describe

en la Figura 6 la distribución del uso de Internet por continente. Los porcentajes indicados con colores indican el porcentaje del total de la población de cada continente tiene conectividad a Internet y los porcentajes en negro indican el porcentaje de usuarios de Internet que el continente tiene con respecto al resto del mundo.

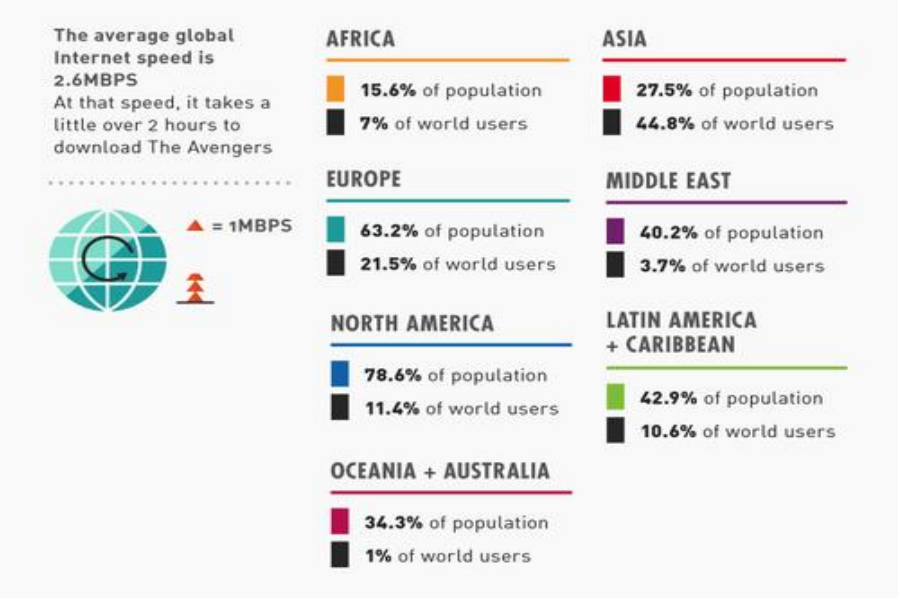


Figura 6. Distribución del uso de Internet por continente (Castro, 2013)

Según investigación realizada, la masificación de conectividad ha permitido que existan altos índices de utilización de dispositivos móviles por su característica más importante que es el concepto de movilidad, ya que por su tamaño reducido se puede portar fácilmente en las diversas actividades diarias que se realiza.

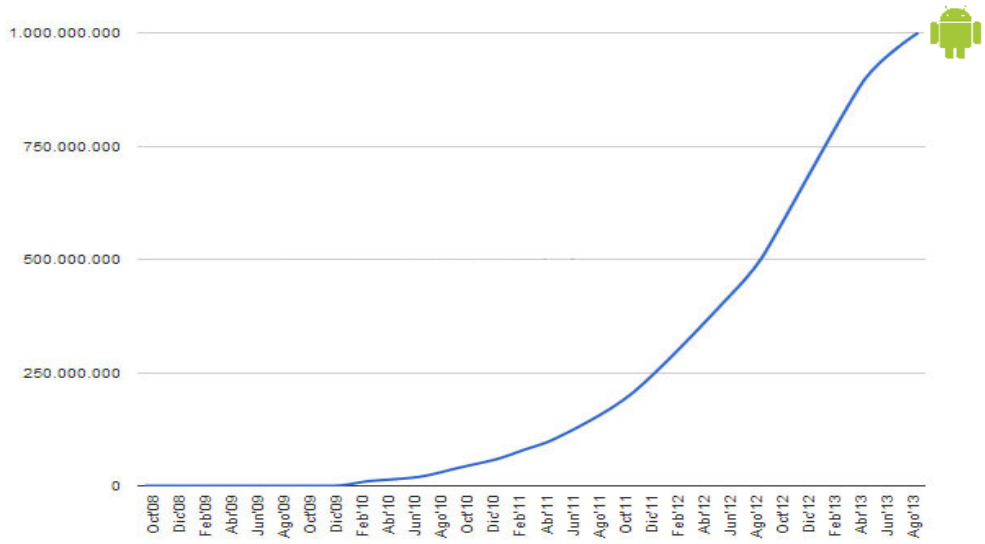


Figura 7. Activaciones de Android

Actualmente existen más de mil millones de dispositivos con sistema operativo Android activados en teléfonos inteligentes, netbooks, tablets, TV, relojes, auriculares y otros dispositivos. Se cita las empresas más importantes que producen sus dispositivos con este sistema operativo.

Teléfonos inteligentes:

- Motorola
- Huawei
- LG
- HTC
- Samsung
- Sony
- Nexus

Tablets:

- Google Nexus
- Samsung
- Sony
- Acer
- Asus
- Motorola
- Coby

- HTC
- Huawei
- LG
- Archos
- Toshiba
- ViewSonic
- Noganet

Cámaras digitales:

- Samsung

Televisores:

- Android TV, Google TV

Relojes:

- Samsung

Impresoras y reproductores multimedia

Los dispositivos Android están pensados para estar conectados a internet, apostando por un futuro inmediato en el que siempre estemos interconectados.

2.3. Malware en Android

Malware es un término que se da a todo software que tiene como propósito explícito infiltrarse o dañar un dispositivo. La palabra malware proviene del término en inglés malicious software y en español es conocido con el nombre de software malicioso. (Zhou, 2013)

Existe diversos tipos de malware producido con fines de lucro, destructivos alterando programas y archivos, otros hacen que el dispositivo sea controlado y explotado para fines ilícitos como envío de emails, almacenar datos de actividades ilegales, etc.

Según estudio realizado sobre malware a 1.85 millones de aplicaciones y vulnerabilidades, arroja dos cifras preocupantes, que desde marzo de 2012 hasta marzo de 2013 el malware en los dispositivos móviles ha subido un 61% (280.000 aplicaciones maliciosas) y Android acapara con el 92% del malware (Gartner Inc., 2013), pero Google dice que el 77% de las amenazas

de malware en Android se podría haber evitado teniendo instalada la última versión del sistema operativo (Android, 2014). Android acapara tal porcentaje de malware debido a su versatilidad y su posición como sistema de código libre, dejando infinidad de puertas a los hackers y debido al desarrollo de aplicaciones por empresas que no cumplen con ningún tipo de medidas de protección a los datos, no exista control de puertos, no posean medidas de seguridad con la información y se permita inyección de malware en los dispositivos mediante la instalación de aplicaciones hace que Android posea porcentajes muy altos en infecciones maliciosas tal como se visualiza en la Figura 8 y sigue aumentado ya que se ha convertido en el objetivo principal de los piratas informáticos.

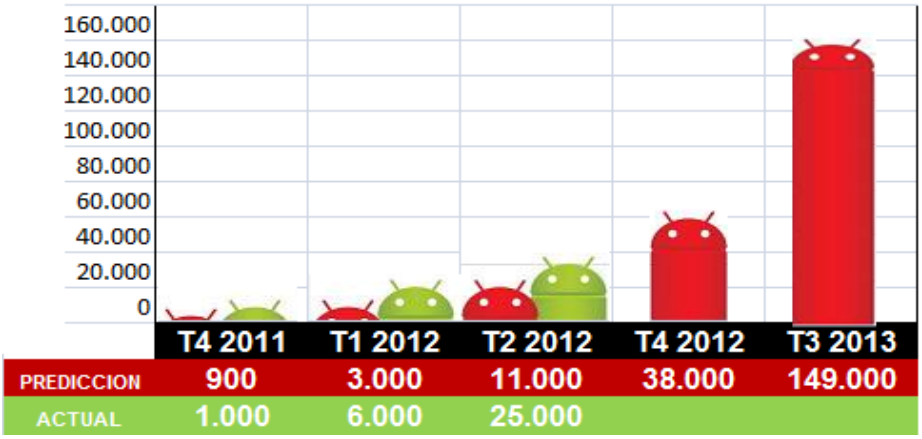


Figura 8. Crecimiento de malware en Android (Zhou, 2013)

El mayor problema se presenta cuando instalamos aplicaciones desde fuentes que no son de confianza. Por defecto, Android bloquea la instalación de este tipo de paquetes de fuentes desconocidas, sin embargo existen usuarios que deciden desactivarlo por necesidad de instalar aplicaciones que no tienen costo o son de lugares de poca seguridad ocasionando con esto un riesgo eminente.

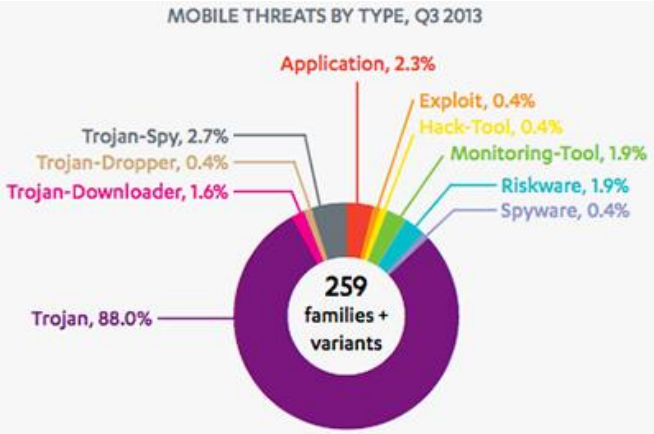


Figura 9. Malware en Android (Grupo ADSL Zone, 2012)

El malware que Android posee está directamente relacionado con su popularidad. Al igual que ocurre con otros entornos, Android es la plataforma móvil más utilizado del planeta, con una cuota de mercado que se sitúa por encima del 80% en todo el mundo (Gartner Inc., 2013). Es el precio que debe pagar por la popularidad que tiene.

En general los ámbitos atacados por malware según (Zhou, 2013) son:

- **Redes sociales**. La ingeniería social es una de las más utilizadas, ya que se encarga de engañar al usuario para que sea éste el que colabore para infectar su dispositivo y sustraer información, ya que no existen aplicaciones de seguridad que protejan al usuario de sí mismo. En este contexto el uso de redes sociales como Facebook, Twitter, Youtube, Google+, Skype, etc. Son los que permiten intercambiar información y en muchas ocasiones información personal, de esta manera los usuarios se conviertan en un blanco fácil para los delincuentes.
- **Ciberguerra / Ciberespionaje**. A lo largo de este tiempo han existido diferentes tipos de ataques contra naciones por medio del internet, cabe mencionar la guerra eminente de Oriente Medio, donde el conflicto está también presente en la red. De hecho muchos de estos ataques ya ni siquiera son llevados a cabo por gobiernos de los países, sino por ciudadanos que consideran que deben defender a su

nación atacando a otros utilizando todos los medios que tengan a su alcance.

- **Aplicaciones Financieras**. Roban contraseñas, números de cuenta, números de tarjetas para identificarse en las operaciones bancarias y así realizar fraudes financieros.
- **Publicidad**. Anuncios que llevan a páginas que distribuyen malware o webs a las que se accede directamente y pueden instalar software malicioso.
- **Crecimiento de malware**. La cantidad de malware detallada en puntos anteriores citan cifras exorbitantes de nuevos tipos de malware que aparecen cada día, divisan un crecimiento continuo que parecería estar muy lejos de llegar a su fin. A pesar de que las fuerzas del orden de los diferentes países cada vez están mejor equipadas y preparadas para luchar contra este tipo de delincuencia, existen impedimentos por la carencia de fronteras en Internet. Cada entidad policial de un país puede actuar en su territorio, mientras que un cyber delincuente puede realizar su ataque a cualquier país del mundo, mediante un dispositivo; mientras que para que actúen las fuerzas del orden de los diferentes países, es una tarea muy compleja que toma varios meses. Es por este motivo que los cyber delincuentes están viviendo su particular edad de oro.

Por todo lo anterior, actualmente existe infinidad de aplicaciones que ayudan a detectar y eliminar el malware, analizar aplicaciones, controlar el acceso no autorizado, detección de vulnerabilidades de seguridad, identificación de aplicaciones que realizan el seguimiento de ubicación para fines delictivos, etc. Por lo tanto los usuarios deben extremar precauciones y ser muy cuidadosos, cautos y conscientes del origen de las aplicaciones instaladas en sus dispositivos móviles, ya que estos son los preferidos de los delincuentes.

La ejecución de medidas de seguridad ayudará a proteger de posibles ataques, por tanto se cita las siguientes:

1. Adoptar medidas de seguridad para no poner en peligro la confidencialidad, integridad y disponibilidad de la información.
2. Evaluar la aplicación a instalar para conocer su funcionamiento.
3. Deshabilitar descargas de aplicaciones automáticamente.
4. Descargar aplicaciones de sitios oficiales.
5. Revisar detenidamente los permisos que sugiere la aplicación a instalar, estadísticamente el número promedio de peticiones debe ser entre 3 y 4 para aplicaciones legítimas, ya que para aplicaciones maliciosas se llega a pedir hasta 39.
6. Revisar el ID de la aplicación a instalar.
7. Instalar antivirus que escanee el dispositivo y las aplicaciones antes de instalarlas.
8. Bloquear llamadas, SMS, mails no deseados a través de las operadoras.
9. Protección anti-robo que permite eliminar datos remotamente del dispositivo.
10. Deshabilitar la ubicación del dispositivo si fuera el caso.
11. Ser cauto y precavido al momento de publicar información por medio de redes sociales, comunicación, etc.
12. No almacenar información sensible de la organización o personal en los dispositivos móviles.
13. No acceder a redes WiFi públicas o compartidas, como las disponibles en hoteles, cafeterías, plazas, centros comerciales ya que pueden poner en riesgo la información que ingresamos como contraseñas, coordenadas bancarias, documentos confidenciales, correos.
14. Desactivar comunicaciones inalámbricas si no se las utiliza como bluetooth, WiFi, infrarrojos.
15. Utilización de contraseña, PIN y patrón de seguridad para el dispositivo.
16. Bloqueo automático del dispositivo en un tiempo determinado de no ser utilizado.
17. Realizar actualizaciones periódicas del sistema operativo.

2.3.1. Tipos de Malware

Existen diversos métodos para obtener información de un dispositivo, este método se especifica con el tipo de aplicación maliciosa.

Spyware. Software espía, aplicación no autorizada que captura datos privados del sistema y es capaz de transmitir dichos datos a un receptor. Generalmente se tienen tres funciones principales recoger información ya sea del sistema o de otras aplicaciones, la segunda es transmitir la información y la tercera es lograr seguir permaneciendo oculto. Los tipos de información o datos que se pueden recuperar se dividen en dos datos en reposo y datos en tránsito.

Los datos en reposo son los historiales de comunicación como:

- SMS/MMS no borrados y los que fueron borrados pero continúan en la memoria y pueden ser recuperados, incluyendo todos los metadatos relacionados con estos.
- Historial de llamadas realizadas también pueden ser accedidas, también con sus respectivos metadatos, por ejemplo la posición de la celda donde se estuvo conectado al realizar la llamada.
- Mensajes de voz pueden ser recuperados de la misma manera que los mensajes SMS/MMS.
- Las aplicaciones de e-mail para Android generalmente suelen guardan el contenido de estos en texto plano incluyendo las contraseñas utilizadas.
- Mensajes instantáneos y comunicaciones con empleados.
- Historial Web en los que incluye URL, cookies y las páginas en cache.
- Historial de búsquedas de Google.
- Historial de juegos e interacciones.
- Credenciales, nombres de usuarios, contraseñas e información de dominio.
- Puntos de acceso WiFi, información y contraseñas.
- Aplicaciones financieras.
- Datos del hardware GPS - Geolocalización.
- Imágenes y videos, capturados con las cámaras del teléfono.

- Archivos corporativos que han sido almacenados en el móvil por conveniencia.

Los datos en tránsito como:

- Contraseñas
- Datos de autenticación
- Datos desplegados pero no almacenados en cache

SMS Trojans. Mediante una aplicación y sin consentimiento del usuario propietario del dispositivo se envía mensajes de texto a números Premium Rate, es decir números a los cuales tienen un costo por el envió. Generalmente estos números son anónimos y el usuario no puede recuperar su pérdida monetaria.

Worms. Los famosos gusanos que son aplicaciones que pueden auto reproducirse hasta llegar a saturar algún recurso del sistema. Generalmente tienen fin en sí mismo, es decir son diseñadas para dañar el sistema más no para obtener otros beneficios.

SMS Flooders: Envían mensajes de texto a un conjunto de números que parten del directorio del usuario, son utilizados generalmente para hacer campañas publicitarias.

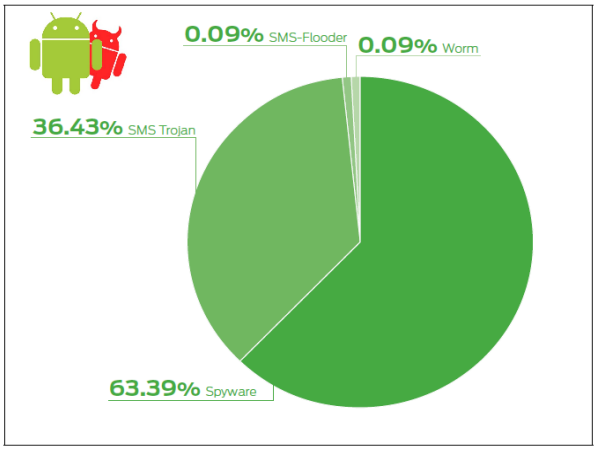


Figura 10. Tipos de Malware en Android (Networks, 2012, p. 7)

Las causas por las que existe un alto porcentaje se debe a que los dispositivos móviles están conectados todo el tiempo a la red, mucho más de lo que estaría conectado una computadora personal. Por tanto un móvil se

convierte en un dispositivo que contiene una alta cantidad de información personal y en algunos casos no posee la más mínima seguridad convirtiéndose así en una bomba de fuego para el usuario.

2.4. Aplicaciones de Android

El crecimiento exponencial que existe en cuanto a la utilización de dispositivos móviles con sistema operativo Android es importante, gracias a la portabilidad y multifuncionalidad que ofrecen, hacen una herramienta poderosa, enfocándose en negocios en línea, actividades educativas, entretenimiento, mejoramiento de la productividad en organizaciones, comunicación, actividades directas con el sector financiero, actividades laborales, etc.

Por todo esto los dispositivos móviles han venido formando parte de la vida cotidiana de las personas, y Google mediante su tienda en línea Google Play ofrece a los dispositivos Android más de un millón de aplicaciones que están publicadas allí, permitiendo a los usuarios navegar y descargar aplicaciones publicadas por los desarrolladores (Android, 2014). Los usuarios pueden instalar aplicaciones desde otras tiendas virtuales o directamente en el dispositivo si se dispone del archivo APK de la aplicación.

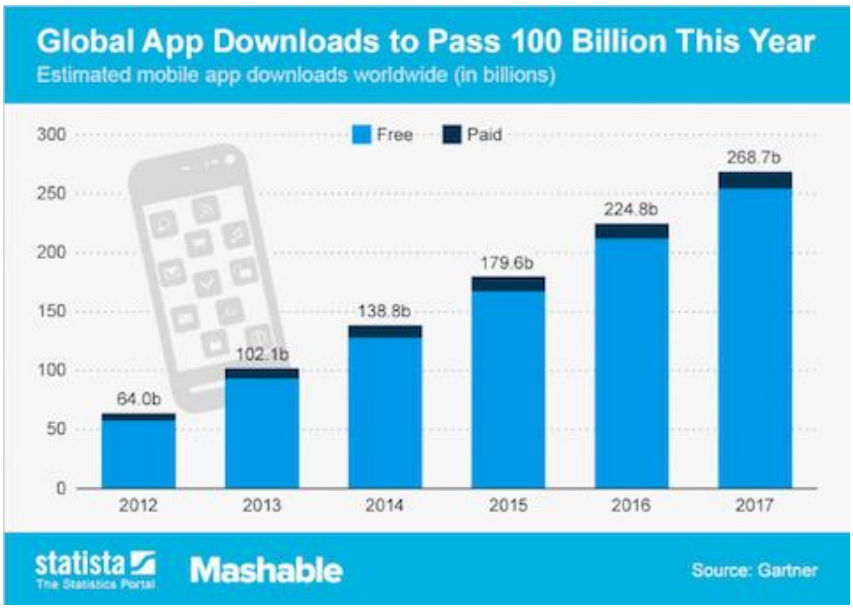


Figura 11. Aplicaciones para Android (Gartner Inc., 2013)

Google Play la tienda en línea de Google tiene un acceso fácil y rápido a sus aplicaciones. Las aplicaciones son creadas por desarrolladores y son diseñadas especialmente para dispositivos móviles. Estas pueden ser gratuitas o de pago. Inicialmente las aplicaciones tenían una función puramente recreativa, sin embargo han ido evolucionando en aplicaciones más útiles, como son las aplicaciones para el registro de gastos, información deportiva, guías de restaurantes, callejeros, canales transacciones, comunicación, etc. Actualmente las nuevas aplicaciones más innovadoras son las llamadas de realidad aumentada que combinan elementos reales y virtuales.

El tipo de aplicaciones Android se clasifican de la siguiente manera: Compras, comunicación, cómics, deportes, estilo de vida, finanzas, herramientas, variedades, multimedia, noticias y meteorología, ocio, productividad, referencia, salud, sociedad, temas, viajes, demostración y bibliotecas de software.

Unas de las aplicaciones más importantes para dispositivos móviles son los juegos y estos reciben un trato especial dentro de las aplicaciones su clasificación es la siguiente: Arcade y acción, casuales, juegos de cartas, casino, puzzle y juegos para ejercitar la mente.

2.5. Auditoria Informática

El concepto de auditoría informática ha estado siempre ligado al de auditoría en general, unido al de contabilidad y control de los registros y operaciones. Si analizamos la auditoría informática desde un punto de vista empresarial, tendremos que empezar visualizando el contexto organizativo y ambiental en el que se mueve dentro de un contexto estratégico, tecnológico y operativo de las organizaciones, los sistemas de información y la arquitectura tecnológica que los soporta, desempeñan un papel importante como uno de los soportes básicos para la gestión y el control del negocio. Para el cumplimiento de objetivos las organizaciones necesitan validar que sus procesos cumplan las metodologías de calidad, normas de seguridad las mismas que se realizan por medio de auditorías permanentes (Gironés, 2013).

La auditoría se desarrolla con base a normas, procedimientos y técnicas definidas formalmente por institutos nacionales e internacionales. Con frecuencia la palabra auditoría se ha empleado incorrectamente y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. El concepto de auditoría es más amplio, no sólo detecta errores, sino que es un examen crítico que se realiza con el único objeto de evaluar la eficiencia y eficacia de una sección o de un organismo con el objetivo de detectar oportunidades de mejora.

La palabra auditoría viene del latín auditorius que significa auditor, que tiene la virtud de oír, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando. Por medio del señalamiento de procesos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación. (Dominguez, 2007)

La auditoría no es una actividad enteramente mecánica, la auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos.

De la misma manera que existen normas y procedimientos específicos para la realización de auditorías contables, existen normas y procedimientos para la realización de auditorías informáticas. Las cuales están basadas en las experiencias de otras profesiones pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, además la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer nuevas alternativas de solución ante los errores, es decir aplicar la constante mejora continua como se observa en la Figura 12.

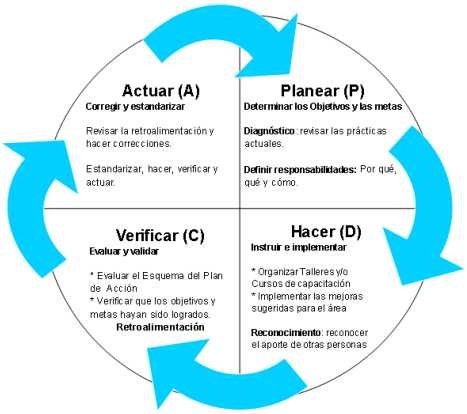


Figura 12. Mejora Continua (Chang, 1996)

2.6. Informática Forense

Es una disciplina especializada que requiere un conocimiento de auditoría en general y métodos de investigación para que se lleve a cabo. Constituye una rama importante para procesos investigativos, utilizada en la reconstrucción de delitos informáticos, investigaciones de fraudes, cálculos de daños económicos y rendimientos de proyecciones financieras. (Cano J. , Computacion forense, 2009, p. 14)

La informática forense se aplica en la investigación de fraudes, considerándose un verdadero apoyo a la tradicional auditoria, en especial ante delitos informáticos. Sin embargo, el análisis forense no se ha limitado a los fraudes propios de la corrupción administrativa, sino también se ha diversificado su portafolio de servicios para participar en investigaciones relacionadas como delitos informáticos, investigación de fraudes, suplantación de identidad, enriquecimiento ilícito, peculado, cohecho, soborno, malversación de fondos, corrupción administrativa, lavado de dinero, crímenes fiscales, crímenes corporativos y terrorismo.

La auditoría de informática forense es reconocida internacionalmente como un conjunto de técnicas efectivas para la prevención e identificación de actos irregulares de fraude y corrupción. Se enfoca en los vínculos más débiles en los controles internos. Se cita las principales actividades:

- **Prevención de Fraudes**. Orientada a proporcionar aseguramiento o asesoría a las organizaciones respecto de su capacidad para disuadir, prevenir (evitar), detectar y reaccionar ante fraudes, puede incluir

trabajos de consultoría para implementar programas y controles anti fraude, esquemas de alerta temprana de irregularidades, sistemas de administración de denuncias. Este enfoque es proactivo por cuanto implica tomar acciones y decisiones en el presente para evitar fraudes en el futuro.

- **Detección de Fraudes.** Orientada a identificar la existencia de fraudes mediante la investigación profunda, establecer entre otros aspectos la cuantía del fraude, efectos directos e indirectos, posible tipificación, presuntos autores, cómplices y encubridores, en muchas ocasiones los resultados de un trabajo de auditoría de informática forense detectiva son puestos a consideración de la justicia que se encargará de analizar, juzgar y dictar la sentencia respectiva. Este enfoque es reactivo por cuanto implica tomar decisiones y acciones en el presente respecto de fraudes sucedidos en el pasado.

2.6.1. Evidencia Digital

Según (Cano J. , 2006) se puede considerar a la evidencia como cualquier información, que sujeta a la intervención humana u otra semejante, ha sido extraída de un medio informático. La evidencia digital tiene como características principales de ser anónima, volátil, duplicable, modificable y eliminable, por tal razón a diferencia de la evidencia física en un crimen clásico, la evidencia digital es un reto para aquellas personas que la identifican, localizan y analizan debido a que se encuentran en un ambiente dinámico.

La evidencia digital puede ser divida en tres categorías (Cano J. , 2006):

1. Registros almacenados en el equipo de tecnología informática como correos electrónicos, imágenes, música, archivos de aplicaciones de ofimática, etc.
2. Registros generados por los equipos de tecnología informática como registros de auditoría, registros de transacciones, registros de eventos, etc.
3. Registro generados y almacenados parcialmente en los equipos de tecnología informática como hojas de cálculo financieras, consultas

especializadas en bases de datos, vistas parciales de datos, documentos, etc.

2.6.1.1. Administración de evidencia digital

La administración de evidencia digital sigue un ciclo de vida de seis fases como lo establece la Handbook guidelines for the management of TI evidencie (Ghosh, 2004), se visualiza en la Figura 13.

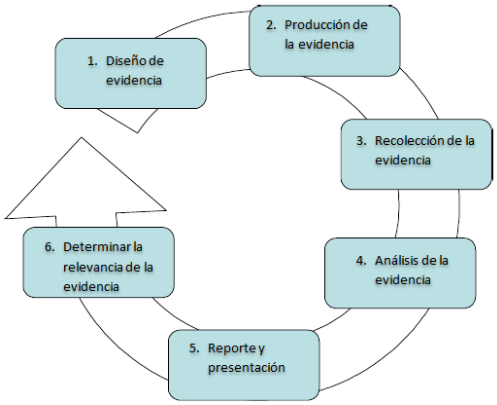


Figura 13. Ciclo de vida administración de la evidencia (Cano J. , Buenas prácticas en la administración de la evidencia digital, 2006)

(Cano J. , Buenas prácticas en la administración de la evidencia digital, 2006) Describe las fases del ciclo de vida para la administración de evidencia digital de la siguiente manera:

1. **Diseño de la evidencia**

   Esta fase se encarga de fortalecer la admisibilidad y relevancia de la evidencia producida por TI, existen cinco prácticas que deben ser consideradas para el diseño de la evidencia digital:

   a) Asegurar la relevancia de los registros electrónicos, que sean identificados, estén disponibles y sean utilizables.
   b) Los registros electrónicos deben tener un autor claramente identificado.
   c) Los registros electrónicos cuentan con una hora y fecha de creación o modificación.
   d) Los registros electrónicos cuentan con elementos que permiten validar su autenticidad.

e) Verificar la confiabilidad de la producción o generación de los registros electrónicos por parte del sistema de información.

2. Producción de la evidencia

Esta fase se encarga de producir la mayor cantidad de información posible con el fin de aumentar las probabilidades de identificar y extraer la evidencia digital relacionada con el incidente. Por lo tanto, es necesario que el sistema de información produzca los registros electrónicos e identificar el autor de estos, identificar la fecha y hora de creación de estos, verificar que la aplicación esté operando correctamente al momento de generar o modificar registros y finalmente verificar la completitud de los registros generados.

En esta fase existen cinco prácticas importantes:

a) Desarrollar y documentar un plan de pruebas formal para validar la correcta generación de registros electrónicos.
b) Diseñar mecanismos de seguridad basados en certificados digitales para validar que es la aplicación en cuestión la que genera los registros electrónicos.
c) Establecer un servidor contra los cuales se pueda verificar la fecha y hora de creación de los registros electrónicos.
d) Contar con pruebas y auditorias frecuentes alrededor de confiabilidad de los registros.
e) Diseñar y mantener el control de integridad de los registros electrónicos, que permita identificar cambios que hayan sido realizado sobre ellos.

3. Recolección de la evidencia

Esta fase se encarga de localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales no han sido alterados. Para dicha recolección se debe aplicar las siguientes cinco prácticas importantes:

a) Establecer un criterio de recolección de evidencia digital según lo más volátil hasta la menos volátil.
b) Al momento de realizar la inspección de los equipos se evite alterar cualquier variable, ya que al manipular el dispositivo se

podría alterar los registros y esto podría invalidar todo el proceso de investigación en un proceso judicial.

c) La recolección debe ser realizada mediante herramientas especializadas y certificadas con el objetivo de evitar modificaciones en las fechas de acceso y en la información de registro del sistema.
d) Documentar todas las actividades que el personal autorizado realice.
e) Asegurar el área donde ocurrió el siniestro, con el fin de custodiar el área o escena del delito y así fortalecer la cadena de custodia y recolección de la evidencia.

4. Análisis de la evidencia

Esta fase se encarga de identificar como fue efectuado el ataque, cual fue la vulnerabilidad explotada y en lo posible identificar al atacante, para lograr esto es necesario reconstruir la secuencia temporal del ataque, para lo cual se debe recolectar la información de los archivos asociados, marcas de tiempo, permisos de acceso y estado de los archivos.

Para esta fase se debe aplicar las siguientes cinco prácticas importantes:

a) Realizar copias autenticadas de los registros electrónicos originales sobre medios forenses estériles.
b) Capacitar y formar en aspectos técnicos y legales a los profesionales que adelantarán las labores de análisis de datos.
c) Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para adelantar los análisis de los datos.
d) Establecer el rango de tiempo de análisis y correlacionar los eventos en el contexto de los registros electrónicos recolectados y validados previamente.
e) Mantener la perspectiva de los análisis efectuados sin descartar lo obvio, desentrañar lo escondido y validando las

limitaciones de las tecnologías o aplicaciones que generaron los registros electrónicos.

5. **Reporte y presentación**

   Esta fase se encarga de presentar los resultados por parte del investigador sobre su búsqueda y análisis de los medios, lo que se localizó en la fase de análisis de la evidencia, así como información puntual de los hechos y posibles responsables. Debido al rigor que requiere una investigación de este tipo, cada movimiento por parte del investigador o su equipo de trabajo se debe documentar hasta que se resuelva o se dé por finalizado el caso. Esta documentación se debe llevar a cabo por formularios que hacen parte del proceso estándar de investigación, entre los cuales se encuentran el documento de custodia de la evidencia, formulario de identificación de equipos y componentes, formulario de incidencias tipificadas, formulario de recolección de evidencias y formulario de medios de almacenamiento.

6. **Determinar la relevancia de la evidencia**

   El objetivo de esta fase es valorar las evidencias de tal manera que se identifiquen aquellas que sean relevantes y que permitan presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve a cabo.

   Para esta fase se debe aplicar los siguientes criterios:

   a) Valor probatorio. Establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación y confiabilidad del sistema.
   b) Reglas de la evidencia. Establece que se han seguido los procedimientos y reglas establecidas para la adecuada recolección y manejo de la evidencia.

2.7. Metodologías Forenses

Actualmente existen metodologías para análisis forense que están sujetas a análisis y estudio, las cuales se cita para conocer las fases que cada una de estas realiza. Las mencionadas metodologías son:

- Instituto SANS
- Laboratorio de cibercrimen del departamento de justicia de Estados Unidos.
- Kevin Mandia y Chris Prosise

2.7.1. Metodología del Instituto SANS (SANS, 2014)

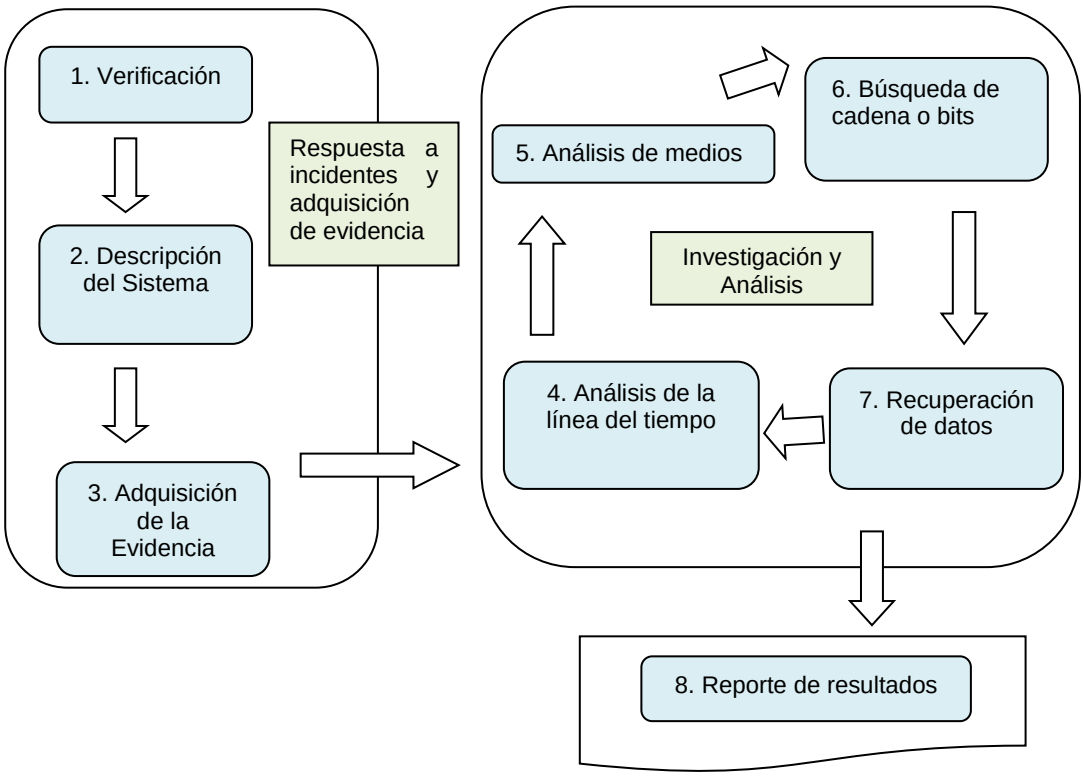


Figura 14. Metodología del Instituto SANS (SANS, 2014)

En el Cuadro 4 se describe las ventajas y desventajas de la metodología según el Instituto SANS.

Cuadro 4

Ventajas y desventajas de la Metodología del Instituto SANS

Particularidades	Ventajas	Desventajas
▪ Posee formato para establecer la cadena de custodia. ▪ Define lugares donde se puede localizar información oculta dentro de los sistemas operativos Windows y Linux.	▪ Toma en cuenta el cuidado de la cadena de custodia ▪ Cubre con todas las etapas para hacer una investigación forense.	▪ Es específicamente para análisis de dispositivos que cuenten con sistema operativo Windows o Linux ▪ No se puede aplicar esta metodología para dispositivos móviles. ▪ No propone métodos para realizar la adquisición de evidencia de grandes volúmenes de datos

2.7.2. Metodología del laboratorio de cibercrimen del departamento de justicia de E.U.A. (USDOJ, 2013)

El laboratorio de crimen digital del departamento de justica de los Estados Unidos desarrollo un diagrama de flujo en el cual se describe una metodología para análisis forenses que cubre sus necesidades de operatividad. En la Figura 15 se visualiza la secuencia de las fases que propone el autor.

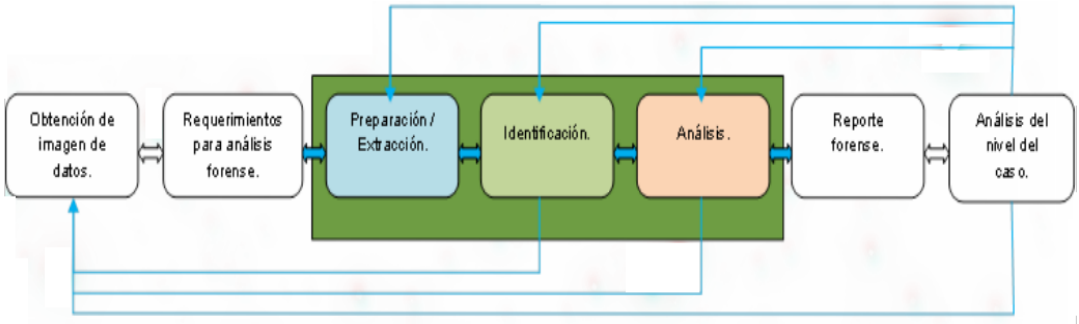


Figura 15. Metodología del departamento de justicia de E.U.A. (USDOJ, 2013)

Siendo para esta metodología el núcleo que está formado principalmente por tres de sus seis etapas para el análisis forense, las cuales son: preparación, extracción, identificación y análisis.

En el Cuadro 5 se describe las ventajas y desventajas de la metodología según el departamento de justicia de los Estados Unidos.

Cuadro 5

Ventajas y desventajas de la Metodología del departamento de justicia de Estados Unidos.

Particularidades	Ventajas	Desventajas
▪ Especifica un flujo bien definido para la realización de cada una de las etapas que propone.	▪ Es muy claro el procedimiento que se debe seguir gracias al diagrama de flujo que proporciona para cada una de las etapas.	▪ Se enfocada a la investigación de computadoras que tengan un sistema operativo Windows. ▪ No se establece una cadena de custodia. ▪ La metodología no propone para la realización de análisis en grandes volúmenes de información. ▪ No da resultados de mejora en el sistema. ▪ No cubre todas etapas generales necesarias para realizar una investigación forense

2.7.3. Metodología de Kevin Mandia y Chris Prosise (Prosise, 2003)

Kevin Mandia y Chris Prosise proponen un modelo para análisis forense compuesto por las fases que se detallan a continuación:

- **Preparación al incidente**. Esta fase involucra la preparación de la organización y del personal de investigación, para dar inicio a la respuesta ante el incidente suscitado.
- **Detección del incidente**: Esta fase es uno de los aspectos más importantes en la respuesta a incidentes, normalmente los incidentes de seguridad se identifican cuando alguien sospecha que un evento no autorizado, inaceptable o ilegal, se ha producido y la participación

de redes informáticas de la organización o equipo de procesamiento de datos se ve involucrada.

- **Respuesta inicial**: Esta fase implica la recolección de datos de la red, la determinación del tipo de incidente que ha ocurrido y evaluar el impacto del incidente. La idea principal es reunir suficiente información para corroborar en la siguiente fase.
- **Formular estrategia de respuesta**: En esta fase se determina la estrategia de respuesta más adecuada, dadas las circunstancias del incidente. La estrategia, debe tener en cuenta aspectos políticos, técnicos, jurídicos, comerciales y factores que rodean el incidente. La solución final depende de los objetivos del grupo o individuo con la responsabilidad de la selección de la estrategia.
- **Investigar el incidente**: Esta fase consiste en determinar, quién, qué, cuándo, dónde, cómo y el por qué, alrededor de un incidente. Se llevará a cabo la recolección de datos y se realizará la investigación de la evidencia recolectada.
- **Presentación de informes**: Esta fase es la más compleja del proceso de respuesta a incidentes. El desafío es crear los informes que describen con precisión los detalles de un incidente, de forma tal, que sean comprensibles para el personal que toma decisiones, que puedan soportar la barrera del análisis y escrutinio jurídico, y que se produzca en el momento oportuno.
- **Resolución**: Esta fase es poner en práctica las medidas y procedimientos determinados, para evitar que un incidente cause más daños. De forma tal, que se retorne a una situación estable, operativa y saludable. Es decir se resuelve el problema o dudas y se toman medidas para evitar que el problema ocurra de nuevo.

En la Figura 16 se visualiza la secuencia de las fases que (Prosise, 2003) describe.

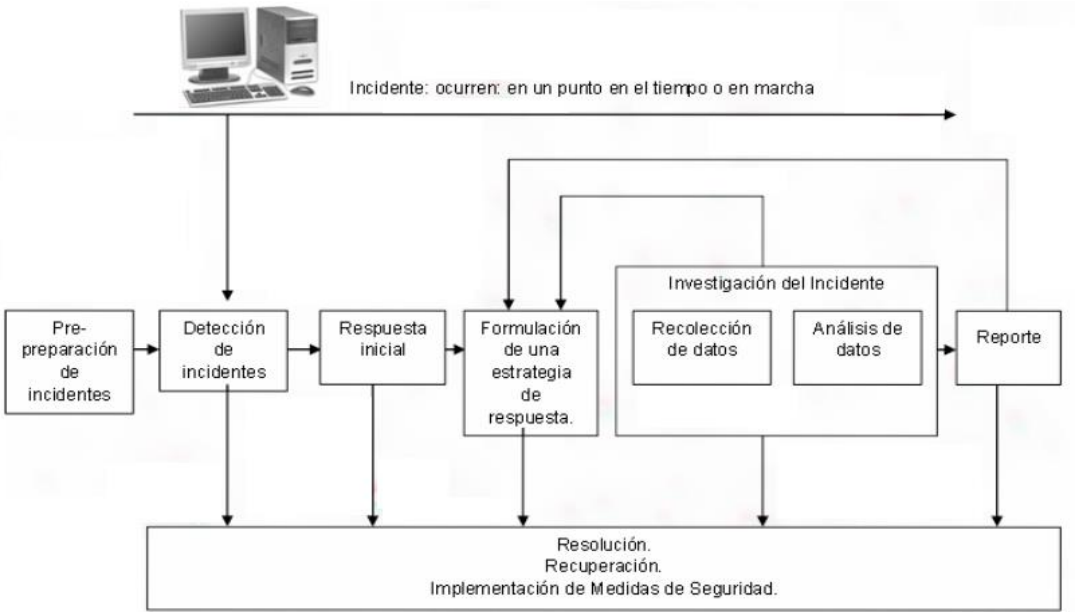


Figura 16. Metodología de Kevin Mandia y Chris Prosise

En el Cuadro 6 se describe las ventajas y desventajas de la metodología según (Prosise, 2003)

Cuadro 6

Ventajas y desventajas Metodología Mandia y Prosise

Particularidades	Ventajas	Desventajas
▪ Propone un paso llamado pre-preparación en el cual el grupo encargado de reaccionar ante un incidente se anticipa a ellos preparando las herramientas necesarias y conocimientos de la infraestructura. ▪ Proporciona una lista de los principales ataques que se presentan hacia una computadora y recomienda una pronta estrategia de respuesta.	▪ Cumple con todas las etapas generales de una investigación forense. ▪ Proporciona métodos para realizar un análisis de datos.	▪ Está enfocada principalmente en la investigación de plataformas Windows, Unix y routers Cisco. Dejando fuera a dispositivos que utilicen una plataforma diferente. ▪ No propone métodos para el análisis de grandes volúmenes de información.

2.8. Roles y funciones para un análisis forense

En un proceso de análisis forense existen diversos tipos de roles ya que es fundamental definirlos con el objetivo de asignar responsabilidades al personal que va encargarse de realizar el análisis. Además es importante para mantener la cadena de custodia de la evidencia, debido a que dependiendo del rol asignado, la persona puede o no tener acceso a la evidencia asegurando de esta manera la admisibilidad de la evidencia y su preservación. El NIST (NIST, 2014) hace distinción de una serie de roles genéricos, para identificar responsabilidades asociadas y asegurar que el alcance de las actividades sea completo y suficiente (NIST, 2008):

- **Personal de primera respuesta**. Personal profesional entrenado para llegar en primera instancia al lugar de los hechos, proveer una evaluación inicial y empezar con el primer nivel de respuesta del incidente. Las responsabilidades de este rol son identificar y asegurar la escena del incidente, acudir al personal de apoyo adecuado y asistir en la recolección y preservación de evidencia.
- **Investigadores**. Personal profesional encargado de planear y manejar la preservación, adquisición, examinación, análisis y reporte de la evidencia digital. El investigador líder está a cargo de asegurar que las actividades que se llevan a cabo en la escena del crimen se ejecuten de acuerdo al cronograma establecido. Su responsabilidad es establecer la cadena de mando, la realización de la búsqueda en la escena del crimen, desplegar la evidencia, preparar el reporte del caso e informar los hallazgos localizados.
- **Técnicos**. Personal profesional encargado de llevar a cabo tareas y actividades bajo la supervisión del investigador líder. Son responsables de identificar y recolectar evidencia, así como de documentar la escena del incidente. Son las personas que realizan la incautación de los equipos electrónicos y encargados de obtener imágenes digitales de ellos y preservar los datos volátiles, por tal motivo deben ser expertos en computación forense o simplemente se cuenta con técnicos expertos en diferentes áreas. Además son los responsables de identificar, registrar, aislar, transportar y procesar la evidencia.

- **Custodios de la evidencia**. Personal profesional encargado de proteger toda la evidencia y almacenada en un lugar centralizado. Ellos acceden a la evidencia recolectada por los técnicos, se aseguran que esté correctamente identificada y mantienen una estricta cadena de custodia.
- **Examinadores forenses.** Personal profesional encargado de generar las imágenes digitales de los dispositivos incautados y recuperar datos digitales.
- **Analistas forenses.** Personal profesional encargado de evaluar el resultado obtenido por el examinador forense, de acuerdo a su significancia y valor probatorio.

CAPÍTULO III

3. Elaboración del modelo para análisis forense a dispositivos móviles con Sistema Operativo Android

El objetivo principal de la investigación es proponer un modelo metodológico para realizar análisis forense a dispositivos móviles con sistema operativo Android. Para la elaboración de dicho modelo se fundamenta en las metodologías citadas en el capítulo 2 sección Metodologías Forenses.

La propuesta metodológica mencionada está formada de cinco etapas y doce fases.

Figura 17. Modelo propuesto para análisis forense

3.1. Etapa de Identificación y Preparación

En esta etapa se receptará la solicitud firmada por las partes involucradas con las respectivas autorizaciones para llevar a cabo el análisis forense de los dispositivos, asignando roles y funciones al personal que formará el grupo de investigadores. Recopilando información de los procesos de la organización que fueron afectados, así como información del personal relacionado con el incidente. Finalmente identificando y documentando todos los componentes electrónicos facilitados para la investigación.

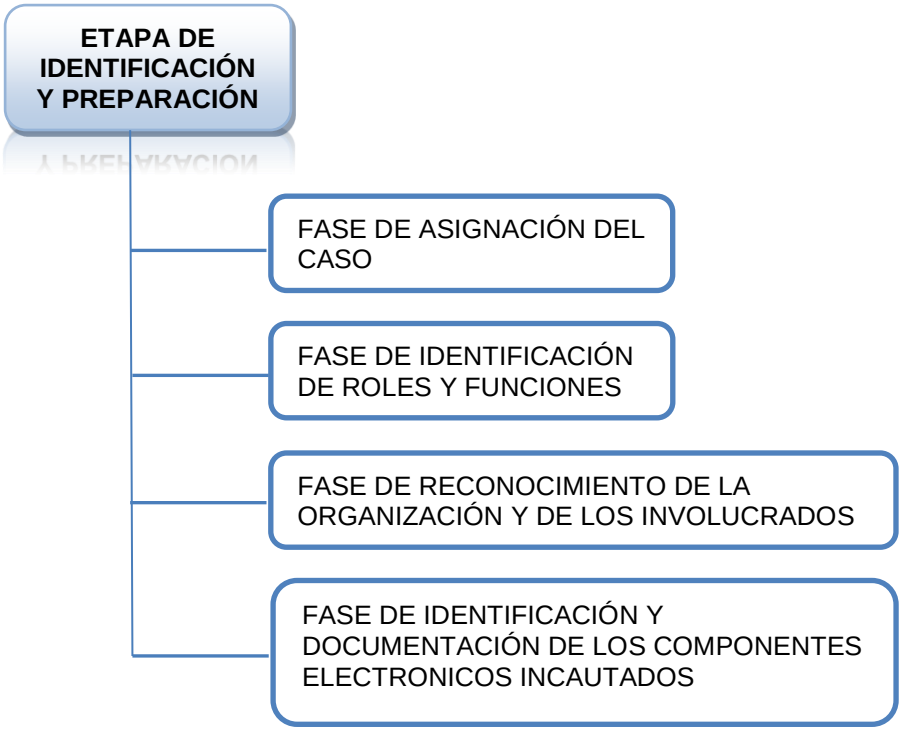


Figura 18. Etapa 1 de identificación y preparación

3.1.1. Fase de asignación del caso

En esta fase se receptará de la solicitud para la ejecución del análisis forense la cual deberá estar debidamente firmada por las partes involucradas, con las respectivas autorizaciones por escrito para la continuidad del proceso. En el caso de no existir dichas autorizaciones el análisis no tendrá ninguna validez legal y por lo contrario se estaría cometiendo un delito. Es de suma importancia conocer sobre las políticas y legislación vigente para la relación del análisis forense y manejo de evidencias, además saber las acciones y antecedentes que preceden la investigación para lo cual se recomienda asesorarse con juristas que posean experiencia en este tipo de temas.

3.1.2. Fase de identificación de roles y funciones

En esta fase se definirá el equipo de investigadores forenses, siguiendo lineamientos establecidos según (NIST, 2014) (Ver sección, Roles y funciones para un análisis forense). (Ver Anexo 1, Roles y Funciones)

3.1.3. Fase de reconocimiento de la organización y de los involucrados

En esta fase se identificarán los procesos implicados de la organización en el incidente para localizar e identificar los posibles involucrados en lo suscitado, y así poder recabar información que ayude con certeza aclarar los hechos. (Ver Anexo 2, Información personal).

3.1.4. Fase de identificación y documentación de los componentes electrónicos incautados

En esta fase se procederá a identificar y documentar todos y cada uno de los dispositivos móviles con sistema operativo Android y accesorios que se incautó, con el fin de realizar el análisis forenses. (Ver Anexo 3 – Componentes electrónicos y Anexo 4 - Información del dispositivo).

3.2. Etapa de Preservación y Adquisición

En esta etapa se definirá el hardware y las aplicaciones a utilizar para la realización de la investigación, teniendo en mente que los dispositivos facilitados para el análisis forense no deben ser manipulados ya que se deberá generar copias de la evidencia que se genere y así poder recrear la escena del evento suscitado.

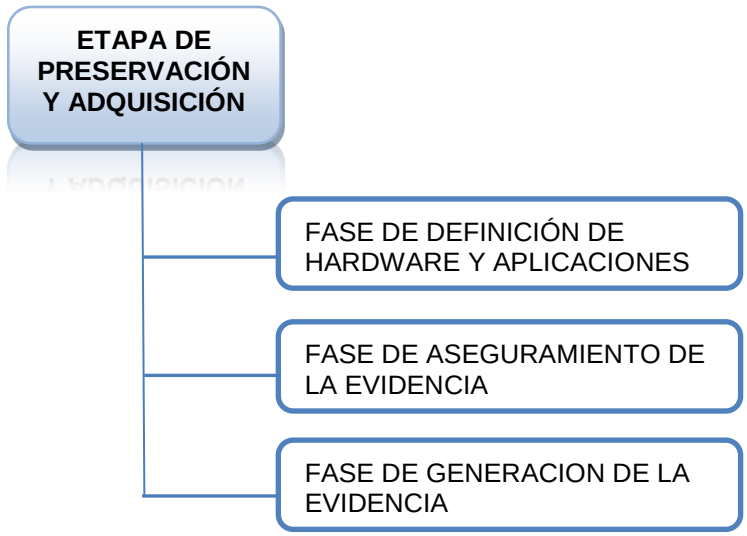


Figura 19. Etapa 2 de preservación y adquisición

3.2.1. Fase de definición de hardware y aplicaciones

En esta fase se describirá el hardware y seleccionará las aplicaciones a utilizar en el proceso de análisis mediante la Matriz DAR (Ver Anexo 5, Matriz DAR - Análisis de Decisión y Resolución).

3.2.2. Fase de aseguramiento de la evidencia

En esta fase, con el fin de asegurar la evidencia se deberá aislar los dispositivos de cualquier tipo de red (WiFi, Edge, 3G, GPRS, Bluetooth) con lo cual se evitará que exista algún tipo de acceso vía remota a los dispositivos.

3.2.3. Fase de generación de la evidencia

En esta fase se deberá bloquear los puertos USB en modo solo lectura hacia el dispositivo que se va generar la imagen digital; esta generación consiste en tomar la imagen binaria bit a bit mediante herramientas adecuadas para el dispositivo. Adicional se deberá generar un código hash MD5 para conservar la integridad de la evidencia durante todo el análisis. El código hash MD5 deberá ser generado para cada imagen digital realizada, etiquetando fecha de la creación y nombre del archivo de la imagen digital (Ver Anexo 6, Acta de entrega código MD5). Esta documentación servirá también en la etapa de presentación.

Todas estas actividades ayudarán para que el acceso a la evidencia sea restrictivo, quedando documentado y posibilitando detectar manipulaciones incorrectas, intentos de acceso indebidos o no autorizados.

3.3. Etapa de Análisis

En esta etapa se llevará a cabo la búsqueda, localización y análisis de la evidencia digital obtenida en la etapa anterior; diligenciando el acta de entrega código MD5 de la evidencia digital. Se deberá poner hincapié en la preservación, integridad y admisibilidad de la evidencia digital.

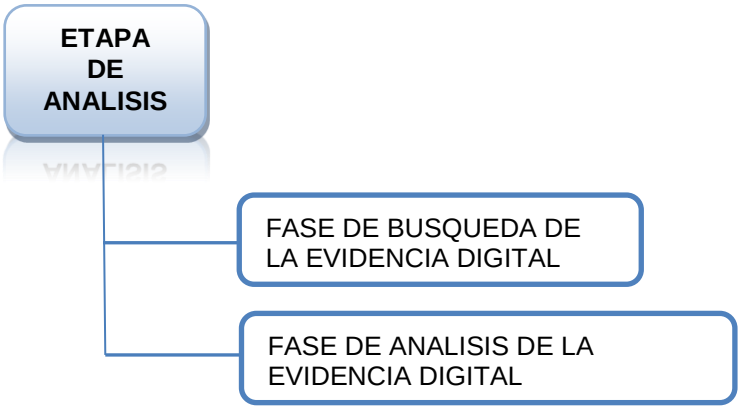


Figura 20. Etapa 3 de análisis

3.3.1. Fase de búsqueda de la evidencia digital

En esta fase se realiza la búsqueda profunda de fuentes de información, la cual servirá como evidencia digital para esclarecer eventos suscitados que se han llevado a cabo durante un tiempo determinado; así como las aplicaciones, herramientas utilizadas, los involucrados y sus posibles motivaciones. Esta búsqueda se debe realizar de una manera adecuada y confiable la cual garantice una correcta localización de las fuentes de evidencia digital. Además se generará un documento con las ubicaciones (Ver Anexo 7, Fuente de información), para posterior ser analizada y así esclarecer los eventos suscitados que se han llevado a cabo durante un tiempo determinado, así como las personas involucradas y sus posibles motivaciones.

Para realizar esta fase es necesario seguir los siguientes pasos:

1. Rootear dispositivo mediante software especializado
2. Descargar drivers necesarios para el dispositivo
3. Configurar dispositivo en modo depuración
4. Encender dispositivo en modo download
5. Conectar el cable USB a la PC
6. Ejecutar aplicación Root Checker para iniciar como súper usuario
7. Ubicación (path) de fuentes de información

3.3.2. Fase de análisis de la evidencia digital

En esta fase se realiza el análisis de las fuentes de información localizadas en la fase anterior mediante el software especializado (Ver Fase de definición de hardware y aplicaciones), identificando cada uno de los datos para construir una línea de tiempo, de tal forma que los eventos suscitados se puedan correlacionar y a partir de esto reconstruir la escena del incidente y obtener detalles del mismo.

3.4. Etapa de Presentación

En esta etapa se genera un informe con los hallazgos localizados; adicional se indicará posibles sugerencias de cierre y explicación del impacto de las fuentes de información analizadas.

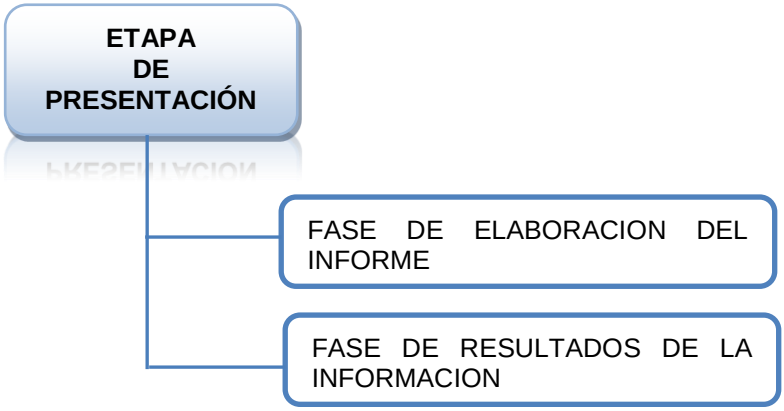


Figura 21. Etapa 4 de presentación

3.4.1. Fase de elaboración del informe

En esta fase se recopila toda la documentación como los respectivos hallazgos adquiridos en cada fase del modelo de análisis forense. Todo el personal profesional que fue participe en las diversas etapas deberán aportar, ya que es vital para asegurar la cadena de custodia de la evidencia. La adquisición del reporte de los resultados del análisis forense habitualmente es generada por la herramienta.

3.4.2. Fase de resultados de la información

En esta fase se realizará una reunión con el personal que solicito la realización del análisis forense, donde se mostrará en el informe todos los

hallazgos localizados durante el análisis. Además se indicará sugerencias de cierre y explicación del impacto de los hallazgos localizados (Ver Anexo 8, Análisis fuente de información).

3.5. Etapa de Entrega de Evidencia

En esta etapa se debe realizar la entrega de cada uno los componentes eléctricos, manuales, informes y toda la documentación facilita para la realización del análisis del incidente suscitado.

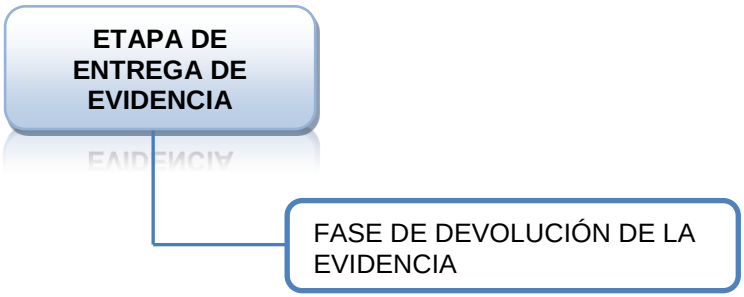


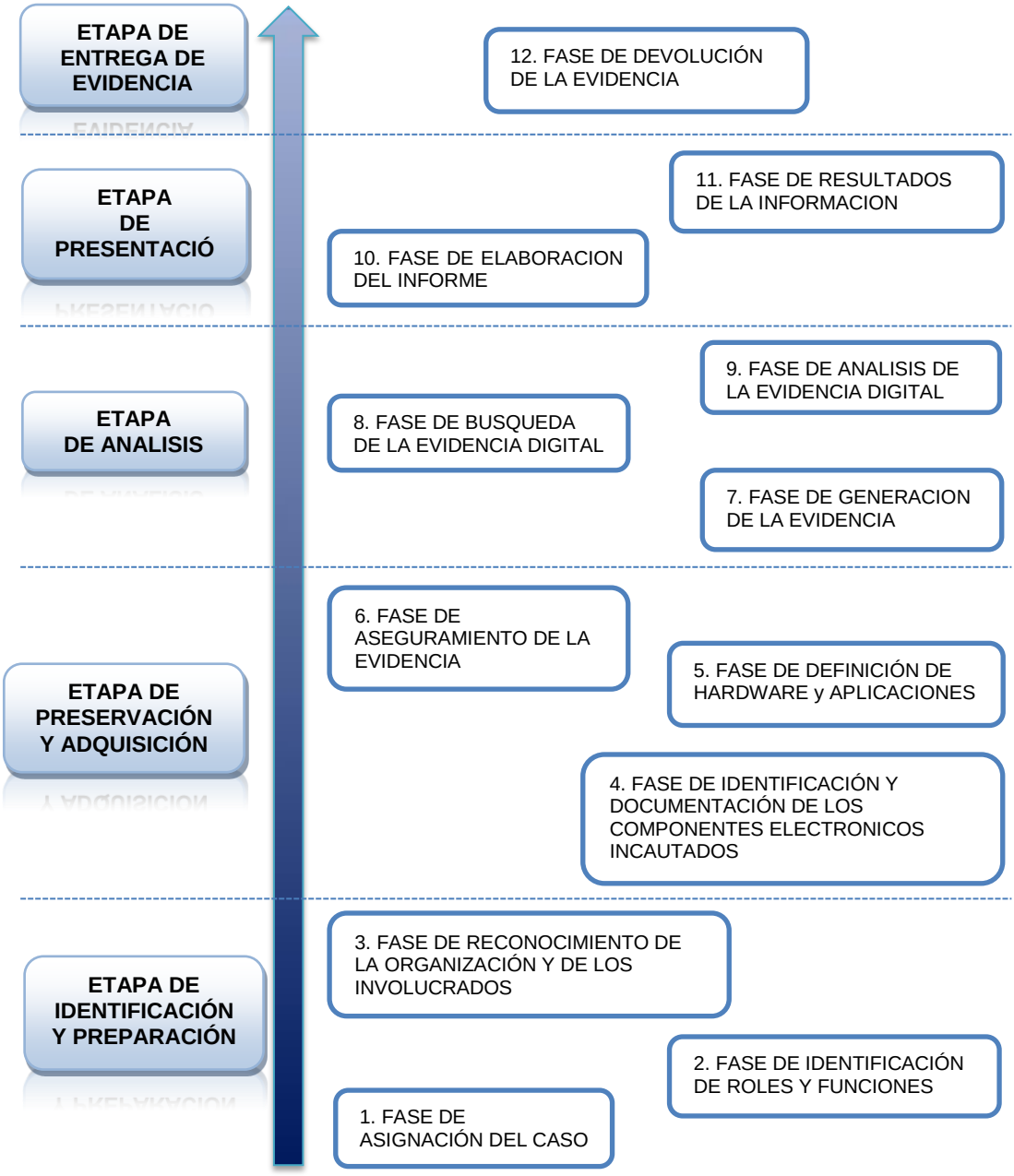
Figura 22. Etapa 5 de devolución

3.5.1. Fase de devolución de la evidencia

En esta fase se realizará la devolución de los componentes electrónicos, manuales, informes y toda la documentación que fue sujeto de análisis. Para así cumplir con la cadena de custodia en cuanto a los implementos que contienen información confidencial; debiendo esta ser manejada bajo estrictas normas de seguridad y protección.

En general toda la información generada y adquirida será entregada para que esta sea añadida en una bitácora de la organización. (Ver Anexo 9, Devolución de evidencia).

3.6. Diagrama - Modelo metodológico propuesto



3.7. Comparación modelo metodológico propuesto y metodologías forenses existentes.

Se debe tener en cuenta que un modelo metodológico debe ser aplicable para cualquier dispositivo y/o plataforma que para la presente investigación se plantea únicamente para dispositivos con plataforma Android, también debe contener procedimientos suficientes para realizar una investigación forense y estar dentro de un proceso de implementación y monitoreo continuo.

La comparativa de aplicación de fases entre los modelos existentes versus el modelo metodológico propuesto se lo realiza en el Cuadro 7.

Cuadro 7

Comparativa entre modelo propuesto vs modelos existentes

Etapa modelo metodológico	Modelo: Instituto SANS	Modelo: USDOJ	Modelo: Mandia y Prosise	Modelo propuesto
Identificación	✓	✓	✓	✓
Preparación		✓	✓	✓
Preservación	✓		✓	✓
Adquisición	✓	✓	✓	✓
Análisis	✓	✓	✓	✓
Presentación	✓		✓	✓
Entrega de evidencia				✓

CAPÍTULO IV

4. Caso de estudio del modelo propuesto para análisis forense a dispositivos móviles con Sistema Operativo Android

El caso de estudio del modelo metodológico propuesto ayudará en primera instancia a probar y dar seguimiento al modelo. El mismo que apoyará a la obtención de hallazgos, los mismos serán utilizados como evidencia digital en un proceso legal, permitiendo así reconstruir escenas, actos delictivos, explorar, analizar información digital. Pero siempre teniendo en consideración la integridad y conservación de los datos y el procesamiento de los mismos.

Un análisis forense no solo abarca la aplicación de herramientas forenses sino también la aplicación de conocimiento en software, hardware, redes, seguridad, hacking, cracking, recuperación de datos informáticos, etc. Para así detectar pistas sobre los ataques informáticos suscitados, robo de información, conversaciones o pistas de correos electrónicos, chats, historial de navegación, videos, ubicación de lugares visitados. Por tanto hay que tener en cuenta que la evidencia digital que se va manejar es sumamente frágil, ya que con el simple hecho de ingresar a ciertos archivos se modificará la última fecha de acceso del mismo, por tanto es importante seguir lineamiento adecuados o un modelo aproximado para no cometer errores o en su defecto los minimicé y así se garantice la admisibilidad de la misma en procedimientos judiciales.

El modelo metodológico propuesto (Ver capítulo 3, Modelo propuesto para análisis forense) a seguir consta de cinco etapas y doce fases que para implementarlo se crea un escenario de prueba donde se realice un ataque a un dispositivo móvil (Samsumg Galaxy Tab3) destinado para la realización de dicho caso de estudio. Es importante resaltar que no se busca solucionar exhaustamente el caso, sino mostrar cómo se aplica el modelo metodológico propuesto.

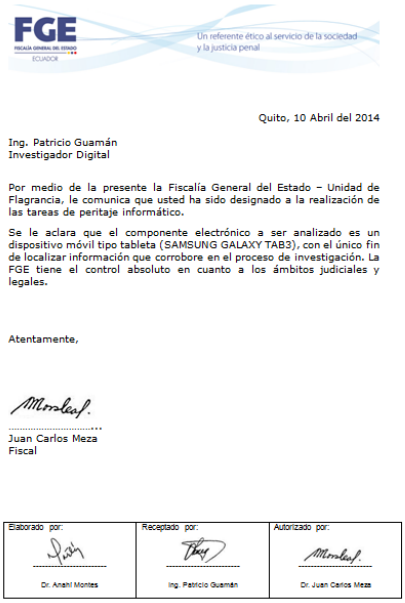
En aspectos generales, el caso se plantea en una situación de venta de sustancias estupefacientes en la cual el implicado es Juan Pérez Juárez,

quien aparentemente es el traficante. El caso requiere el análisis del dispositivo móvil incautado para identificar archivos que incriminen a este personaje con el tráfico de drogas en establecimientos educativos.

4.1. Etapa de Identificación y Preparación

4.1.1. Fase de asignación del caso

Se recepta la solicitud emitida por la Fiscalía General del Estado – Unidad de Flagrancia, para dar el inicio al proceso de análisis forense.



FGE

Un referente ético al servicio de la sociedad y la justicia penal

Quito, 10 Abril del 2014

Ing. Patricio Guamán
Investigador Digital

Por medio de la presente la Fiscalía General del Estado – Unidad de Flagrancia, le comunica que usted ha sido designado a la realización de las tareas de peritaje informático.

Se le aclara que el componente electrónico a ser analizado es un dispositivo móvil tipo tableta (SAMSUNG GALAXY TAB3), con el único fin de localizar información que corrobore en el proceso de investigación. La FGE tiene el control absoluto en cuanto a los ámbitos judiciales y legales.

Atentamente,

Juan Carlos Meza
Fiscal

Elaborado por:	Receptado por:	Autorizado por:
Dr. Anahí Montes	Ing. Patricio Guamán	Dr. Juan Carlos Meza

Figura 23. Solicitud de asignación de caso (Anexo 10)

4.1.2. Fase de identificación de roles y funciones

Se asigna roles y funciones al personal que colabora en la investigación.

DEPARTAMENTO DE INVESTIGACION
MEVAST - ESPE
QUITO - ECUADOR

FECHA: 10/04/2014	HORA: 2:27 (PM)	FORMULARIO: E1F2
		CODIGO CASO: INC-001

ROLES Y FUNCIONES

Rol	Nombre	# Identificación
Personal de primera respuesta	Investigador 1	1712430076
Investigador	Investigador 2	1712430077
Técnico	Investigador 3	1712430078
Custodio de la evidencia	Investigador 4	1712430079
Examinador forense	Patricio Guamán	0502733686
Analista forense	Patricio Guamán	0502733686

Observaciones:
Los roles son asignados de acuerdo a sus conocimientos en las diversas fases de análisis forense. Se indica que el líder del grupo de investigadores es Ing. Patricio Guamán

Figura 24. Roles y Funciones (Anexo 11)

4.1.3. Fase de reconocimiento de la organización y de los involucrados

El incidente fue localizado en el domicilio del Sr. Juan Pérez Juárez dueño del dispositivo móvil incautado, que al tratarse de un asunto judicial no es posible recabar más información al respecto. Al momento se obtiene la información facilitada por la fiscalía.

[Para el caso en que el incidente fuese realizado en una organización se deberá solicitar documentación pertinente de la administración de infraestructura y se ejecute entrevistas con los administradores; esto dependiendo el caso]

Se recepta información de las personas involucradas en el presente incidente.

DEPARTAMENTO DE INVESTIGACION
MEVAST - ESPE
QUITO - ECUADOR

FECHA: 10/04/2014	HORA: 3:30 (PM)	FORMULARIO: E1F3 CODIGO CASO: INC-001

INFORMACION PERSONAL

Apellidos: PEREZ JUAREZ		Nombres: JUAN	
Lugar de nacimiento: UIO	Edad: 38	Estado civil: SOLTERO	# Identificación: 1712540069
Dirección del lugar donde vive: AV. AMAZON y JAPON, SECTOR IÑAQUITO			
Nombre de empresa en la que trabaja: BANCO DEL IESS		Lugar de la empresa: QUITO	
Correo electrónico de la empresa: JUAN.PEREZ@BIESS.FIN.EC		Correo electrónico personal: JPEREZ@GMAIL.COM	
Departamento: TECNOLOGIA	Area: INFRAESTRUCTURA		Cargo: TECNICO 4
Tiempo de trabajo en la empresa: 3 AÑOS		Número telefónico del domicilio: 02340441	
Breve descripcion de sus tareas: -ADMINISTRADOR DE REDES Y CANALES -SERVICIOS DE BALANCEADOR PARA CONEXION A INSTANCIAS JBOSS -CONTROL DE ACCESO (PUERTOS, PC)			
Observaciones: -LA INFORMACION ES RECEPTADA SIN NINGUN TIPO DE COMPLICACION -MANIFIESTA QUE EL DISPOSITIVO MOVIL INCAUTADO QUE SE ENCONTRABA EN SU DEPARTAMENTO ES DE UN AMIGO -EXISTEN VARIAS REDES INALÁMBRICAS PÚBLICAS POR SU DOMICILIO			
Investigador:		Colaborador:	

Figura 25. Información del involucrado (Anexo 12)

4.1.4. Fase de identificación y documentación de los componentes electrónicos incautados

Se recepta todos los componentes electrónicos para la realización del proceso de análisis.

DEPARTAMENTO DE INVESTIGACION MEVAST - ESPE QUITO - ECUADOR				
FECHA: dd/MM/YYYY	HORA: hh:mm (AM/PM)		FORMULARIO: E1F4A CODIGO CASO: INC-001	
COMPONENTES ELECTRÓNICOS PARA LA INVESTIGACIÓN				
Tipo accesorio	Color	Marca	Número Serial	Descripcion
Tablet	Blanco	Samsung	41000740554CA9000	Dispositivo utilizado para efecto del incidente
Cable USB	Blanco	Samsung	N/A	Cable USB es usado para cargar el dispositivo y para sincronización con la PC
Cargador	Blanco	Samsung	RT4D906PS/B-E	
Manos libres	Blanco	Samsung	N/A	
Observaciones: Los componentes recibidos se encuentran en buenas condiciones fisicas				
Receptado por:	Revisado por:		Autorizado por:	

Figura 26. Componentes electrónicos (Anexo 13)

Se obtiene información del dispositivo móvil incautado para la realización del análisis de su contenido.

DEPARTAMENTO DE INVESTIGACION MEVAST - ESPE QUITO - ECUADOR		
FECHA: 11/04/2014	HORA: 12:45 (PM)	FORMULARIO: E1F4B CODIGO CASO: INC-001
INFORMACION DEL ESTADO DEL DISPOSITIVO		
Estado (Encendido/Apagado)		ENCENDIDO
Estado de protección PIN (Activado/Desactivado)		DESACTIVADO
Estado de protección código de seguridad (Activado/Desactivado)		ACTIVADO
INFORMACION DEL DISPOSITIVO		
Tipo de dispositivo (Tablet, Teléfono celular)		TABLET
Tamano pantalla		600x1024
Fabricante		SAMSUNG
Marca		SAMSUNG
Modelo		SM-T210
Sistema Operativo		ANDROID
Version de SO		JELLY BEAN 4.1.2
Procesador		ARMv7 Processor rev 0
Capacidad de almacenamiento		8G
Número de serie		41000740554CA9000
Número ICCID		N/A
IMEI		N/A
Operadora telefónica (CNT, Claro, Movistar)		N/A
Número telefónico asignado al dispositivo		N/A
Dirección MAC WiFi		00-1A-73-F5-0E-8C
Dirección IP		192.168.1.6
Dirección MAC Bluetooth		00-1E-37-B9-27-DB
Número de canciones		11
Número de videos		5
Número de fotografías		77
Número de aplicaciones		29
Observaciones: -DISPOSITIVO APARENTEMENTE SE ENCUENTRA EN BUENAS CONDICIONES -DISPOSITIVO SE ENCUENTRA ENCENDIDO Y NO POSEE PATRON DE INGRESO		
Receptado por:	Revisado por:	Autorizado por:

Figura 27. Información del dispositivo (Anexo 14)

4.2. Etapa de Preservación y Adquisición

4.2.1. Fase de definición de hardware y aplicaciones

Para la investigación se utilizará una computadora portátil HP modelo Pavilion serie dv2000, propiedad del líder del grupo de investigación. Dicho equipo contiene el aplicativo Oxygen Forensic Suite que fue analizada mediante la Matriz DAR (Ver Anexo 15, Matriz DAR - Análisis de Decisión y Resolución).

4.2.2. Fase de aseguramiento de la evidencia

Como primera instancia al dispositivo móvil se aísla de redes 3G, WiFi; ingresando en una bolsa antiestática.

Figura 28. Bolsa antiestática

Es importante tener en cuenta que la información que se obtiene es delicada y frágil, la misma debe ser manejada con mucho cuidado para así no tener errores o en su defecto estos sean mínimos.

Para garantizar la admisibilidad de la información se procede a realizar el bloque de puerto USB en solo lectura, con el fin de mantener toda la evidencia intacta del dispositivo móvil, es decir al conectar el dispositivo móvil se podrá acceder al contenido pero no se podrá copiar absolutamente nada a este por medio del puerto USB, y así garantizando que el dispositivo móvil no tenga ningún tipo de alteración en cuanto a su contenido.

1. Ingresar a inicio/ejecutar y escribir “regedit”, se abrirá una ventana.

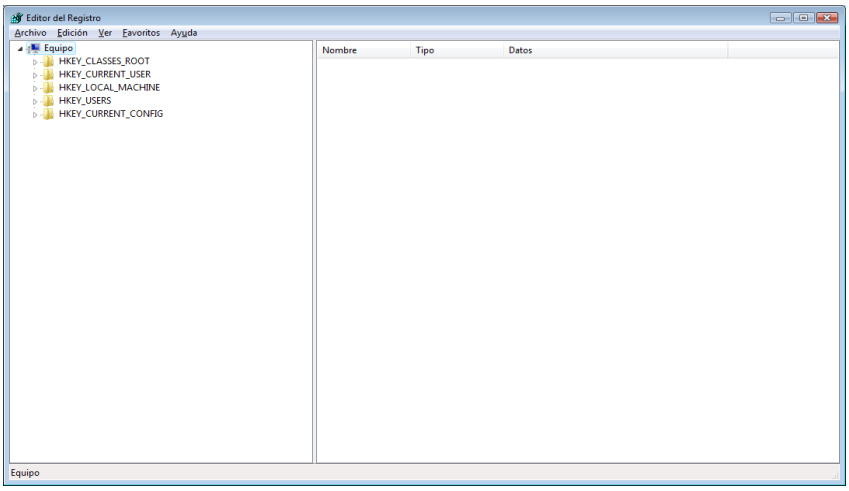


Figura 29. Editor de Registro

2. Ubicar la ruta:

   HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/StorageDevicesPolicies

   En el caso de no existir la llave “StorageDevicesPolicies” debemos crearla. Posterior en la llave crear la clave “DWORD” con el nombre “WriteProtect” con el valor “1”.

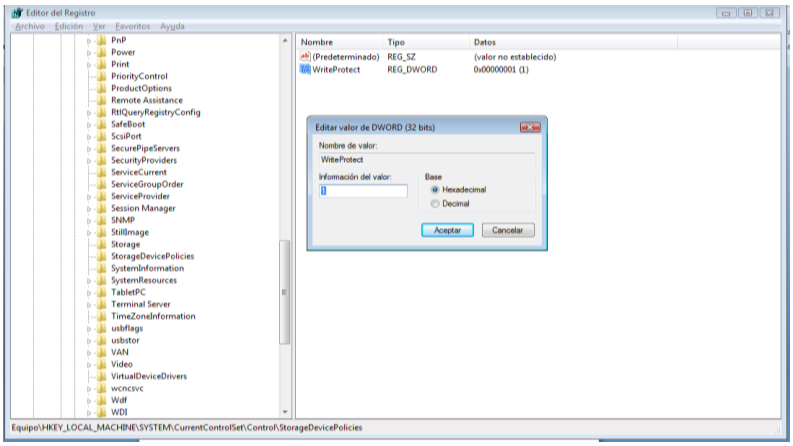


Figura 30. Clave DWORD en StorageDevicesPolicies

3. Al ingresar un dispositivo en el puerto USB, se podrá acceder al contenido pero no se podrá crear, modificar nada ya que hace referencia a las políticas del dispositivo configuradas.

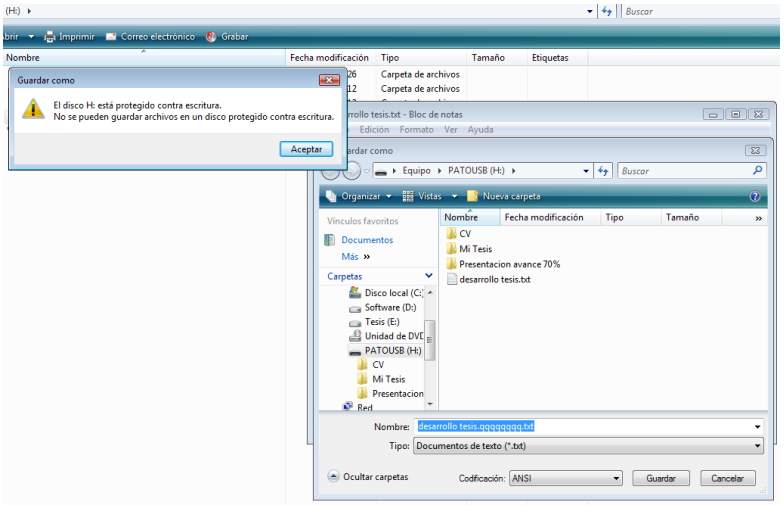


Figura 31. Protección contra escritura

4.2.3. Fase de generación de la evidencia

Para conservar intacta la evidencia digital del dispositivo móvil y no sufra ningún tipo de alteración al momento de realizar el análisis de la información de la siguiente etapa, se realizar una copia de seguridad mediante software especializado para esta actividad. Para ello se descarga el software e instala en la PC, dicho software servirá como administrador del contenido digital que posea.

Posterior a la instalación del software y una vez realizado el procedimiento para bloqueo de puertos USB y la configuración del dispositivo en modo depuración USB para desarrollador (Ver, Figura 47 Configuración perfil desarrollador). Se procede a conectar y sincronizar el dispositivo móvil con la PC mediante el cable USB. Para el reconocimiento por parte del software de las distintas aplicaciones, videos, música, contactos, imágenes, fotos, SMS, archivos, etc.

Procedimiento de generación de copia de seguridad mediante software MobileGo for Android versión 4.3.0.

Figura 32. Instalación MobileGo for Android

Figura 33. Sincronización mediante ModileGo for Android

Figura 34. Visualización de conexión en el dispositivo móvil

Mediante MobileGo se obtiene detalles y características del dispositivo.

Figura 35. Información dispositivo Samsung Galaxy Tab3

Mediante el software se realiza una copia de seguridad, la cual permita obtener respaldo integro de todo el contenido digital del dispositivo.

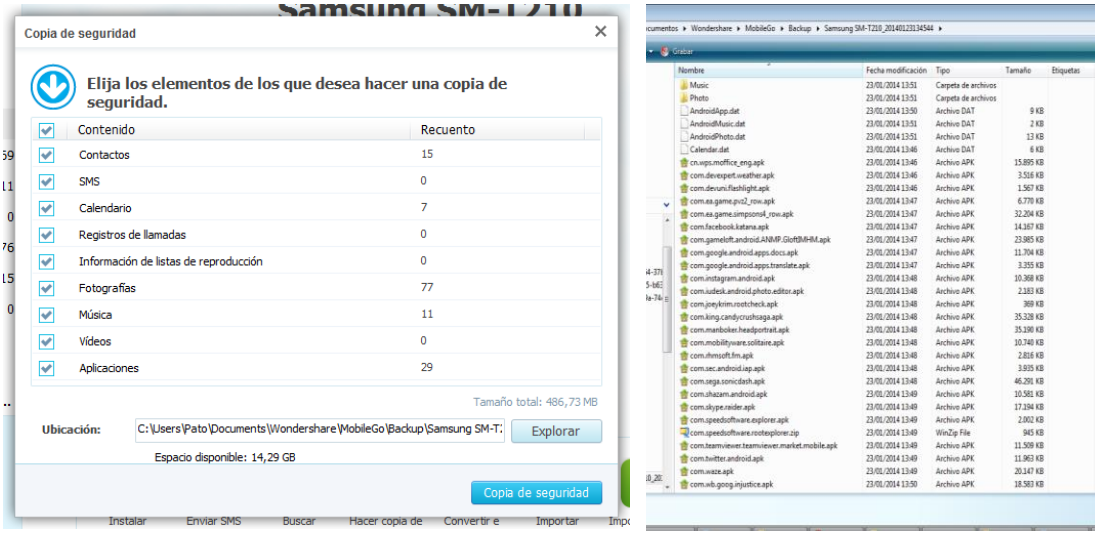


Figura 36. Copia de seguridad y ubicación

Como otra alternativa para la generación de la copia de seguridad se puede utilizar Samsung Kies versión 2.6.1; este software es producto original del fabricante del dispositivo móvil analizar.

Figura 37. Instalación Samsung Kies

Figura 38. Sincronización mediante Samsung Kies

En la opción dispositivo conectado se obtiene información básica.

Figura 39. Información del dispositivo móvil

Para la realización de la copia de seguridad de datos se escoge las secciones: información personal, contenido y configuración de la cuenta. Esta copia se almacenada en la directorio establecido por el aplicativo.

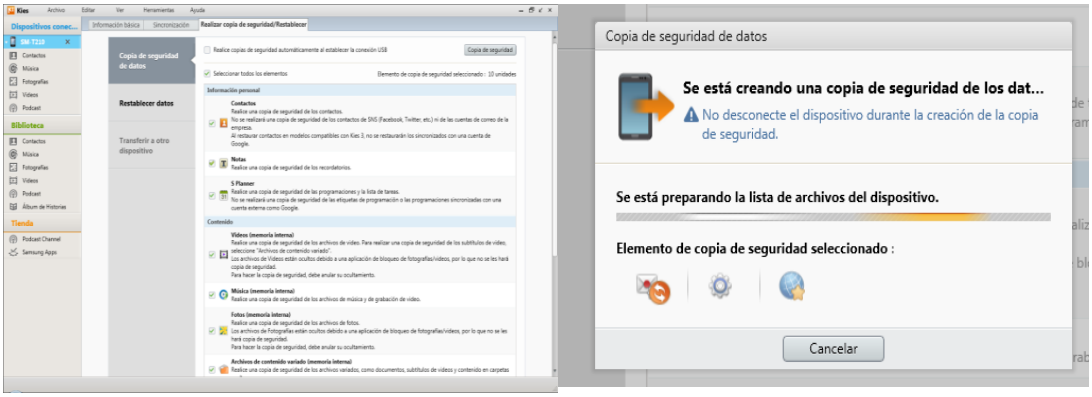


Figura 40. Creación copia de seguridad

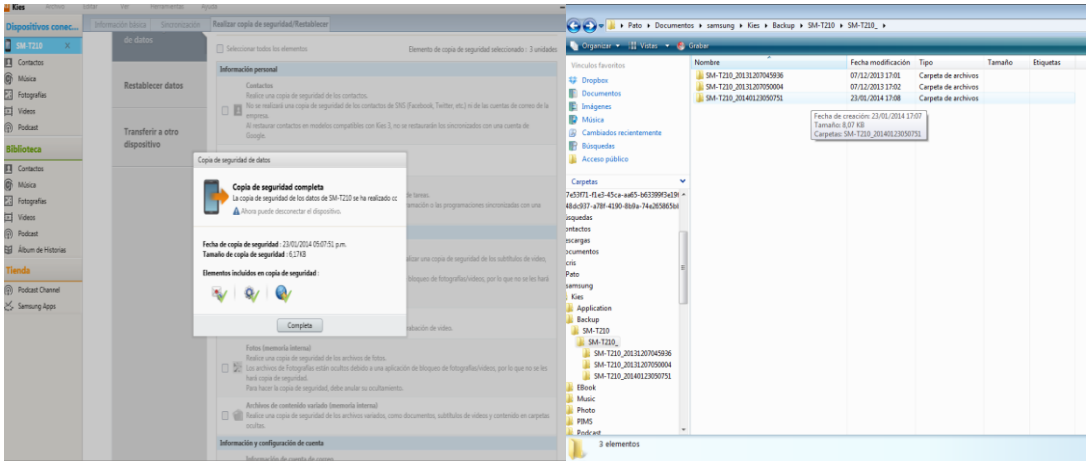


Figura 41. Copia de seguridad y ubicación

Posterior se procede con la herramienta UltraISO a generar una imagen digital de la copia de seguridad, para luego sobre esta realizar la indagación e investigación de su contenido. Se obtiene un código de seguridad de la imagen digital generada utilizando la herramienta WinMD5 versión 2.07, de tal manera el código de seguridad sirva para validar que la evidencia no ha sufrido algún tipo de modificación o alteración.

1. Para la generación de la imagen digital tipo ISO de la copia de seguridad de los datos del dispositivo móvil, se utiliza la herramienta

UltraISO versión 8.6. Ubicamos el directorio y seleccionamos el archivo generado por la herramienta MobileGo o Kiess.

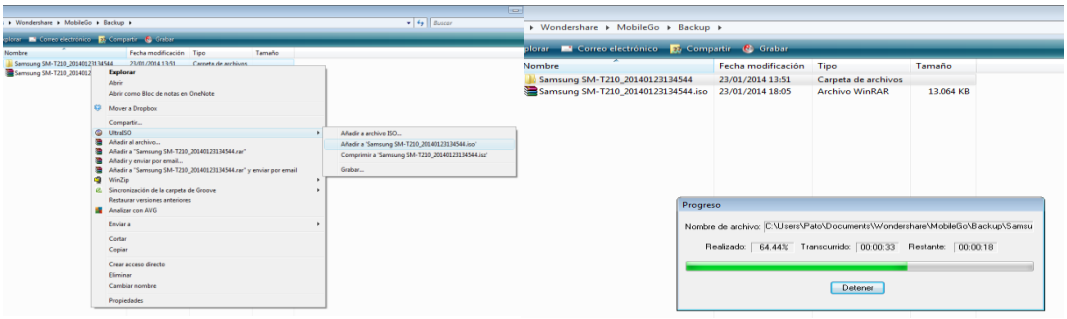


Figura 42. Generación imagen digital (.iso)

2. Con la creación de la imagen digital (.iso) de la copia de seguridad de los datos del dispositivo móvil se procede a generar el código Hash MD5 (Algoritmo de codificación de 128 bits que genera un hash hexadecimal de 32 caracteres) utilizando la herramienta WinMD5 versión 2.07.

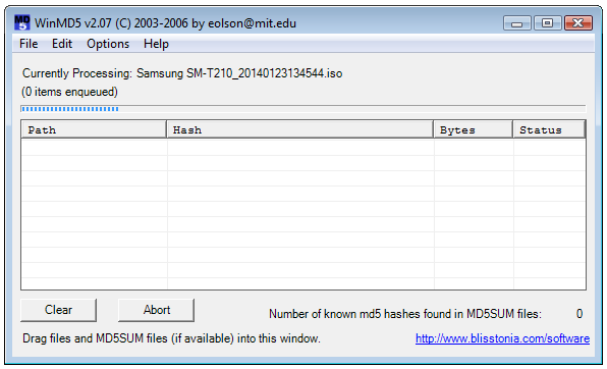
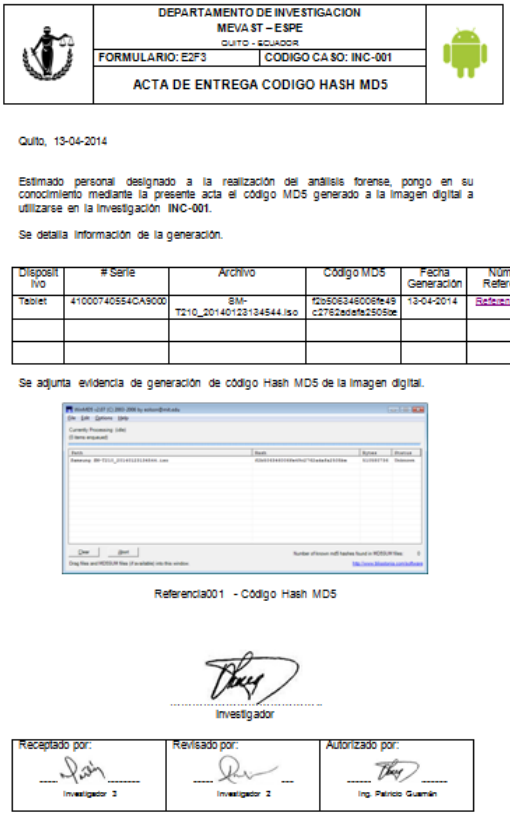


Figura 43. Generación código Hash MD5

Con la generación de código Hash MD5 se emite un acta de entrega. La cual sirva para verificar en un momento determinado si el archivo proporcionado inicial para el análisis forense ha sufrido algún tipo de alteración o modificación por las partes encargadas.



DEPARTAMENTO DE INVESTIGACION
MEVAST – ESPE
QUITO - ECUADOR

FORMULARIO: E2F3 | CODIGO CASO: INC-001

ACTA DE ENTREGA CODIGO HASH MD5

Quito, 13-04-2014

Estimado personal designado a la realización del análisis forense, pongo en su conocimiento mediante la presente acta el código MD5 generado a la Imagen digital a utilizarse en la investigación **INC-001**.

Se detalla información de la generación.

Dispositivo	# Serie	Archivo	Código MD5	Fecha Generación	Número Referencia
Tablet	410007405S4CA9000	SM-T210_20140123134544.iso	f2b506346006fe49c2762adafa2505be	13-04-2014	Referencia001

Se adjunta evidencia de generación de código Hash MD5 de la Imagen digital.

Referencia001 - Código Hash MD5

Investigador

Receptado por:	Revisado por:	Autorizado por:
Investigador 3	Investigador 2	Ing. Patricio Guamán

Figura 44. Generación código Hash MD5 (Anexo 16)

4.3. Etapa de Análisis

4.3.1. Fase de búsqueda de la evidencia digital

Para la búsqueda y localización de las fuentes de información se utiliza un gestor de archivos para usuarios raíz o súper usuario (root), el cual permita acceder a todo el sistema de archivos de Android como textos planos, logs, archivos, cuentas, imágenes, acceso a redes, repositorios en la nube, etc. La visualización de los mencionados archivos en la mayoría de dispositivos no es visible porque está protegida u oculta, por este motivo se debe rootear el dispositivo Android instalando un código dentro para poder acceder al sistema con todos los permisos (lectura, escritura), sin restricciones, ingresando con una cuenta de súper usuario o administrador (root).

Se describe los pasos para rootear el dispositivo móvil del fabricante Samsung modelo Galaxy Tab 3 modelo SM-T210 con sistema operativo Android versión Jelly Bean 4.1.2 y Kernel versión 3.4.5-1256430 KST 2013.

1. Descargar software libre disponible en la web: Odin_v1.85 y prerooted.tar.md5 (http://d-h.st/leL) los cuales permitirán realizar las actividades.
2. Descomprimir y ejecutar el software Odin3 v1.85.

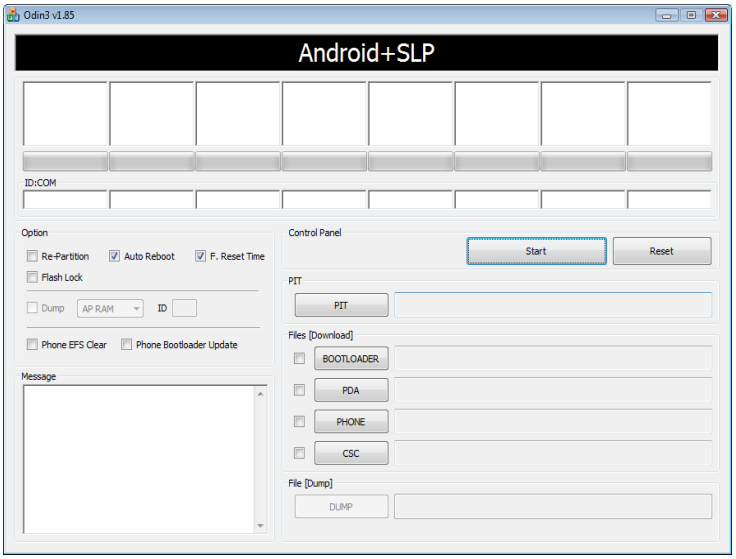


Figura 45. Software Odin3 v1.85

3. Descargar drivers necesarios para la PC del dispositivo a rootear.

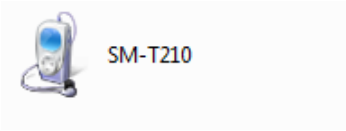


Figura 46. Drivers Samsung Galaxy Tab3

4. Ubicar en la configuración del dispositivo móvil en modo depuración USB para desarrollador.

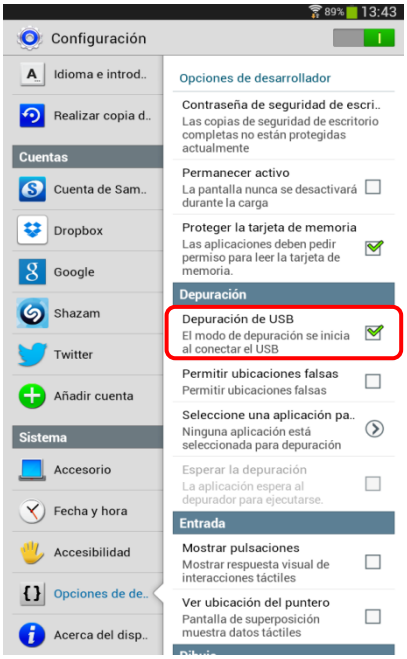


Figura 47. Configuración perfil desarrollador

5. Encender el dispositivo en modo download, presionando el botón de menú con el botón de bajar volumen y el botón de encendido.

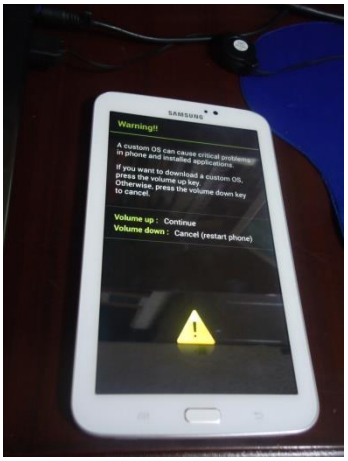


Figura 48. Inicio modo download

6. Presionar botón subir volumen para continuar en modo download.

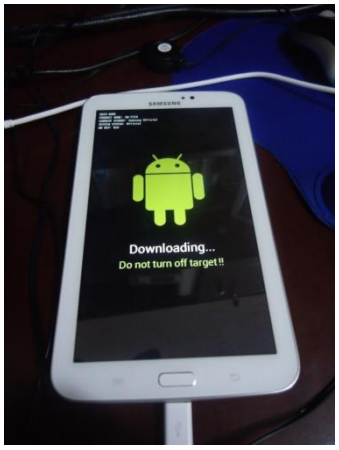


Figura 49. Modo downloading

7. Conectar el cable USB al dispositivo y a la PC.
8. Ejecutar software Odin3 v1.85, debe reconocer el puerto COM en el que fue conectado el dispositivo móvil caso contrario no existirá enlace.

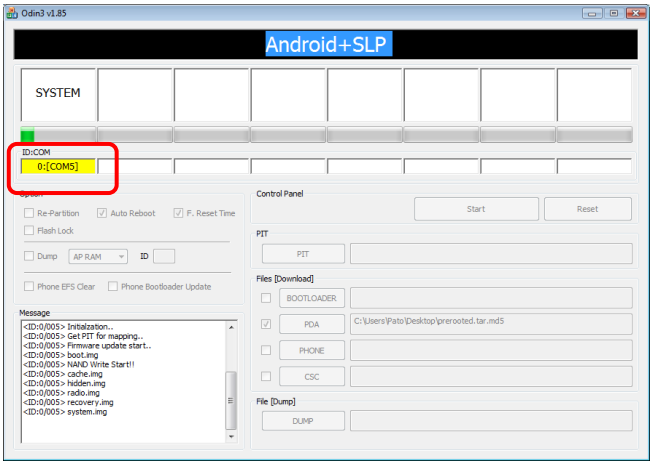


Figura 50. Conexión dispositivo

9. Seleccionar el archivo prerooted.tar.md5 y tener en cuenta que la opción Re-Partition debe estar deshabilitada.

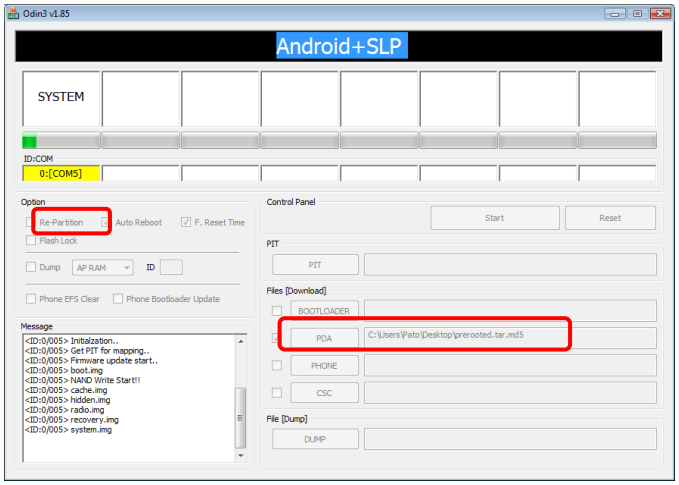


Figura 51. Selección archivo para root

10. Presionar el botón Start para dar inicio al proceso.
11. Durante la ejecución del proceso no se debe desconectar el cable USB del dispositivo móvil, ni tampoco apagar la PC.
12. Al culminar con el proceso se presentara mensajes de ejecución correcta.

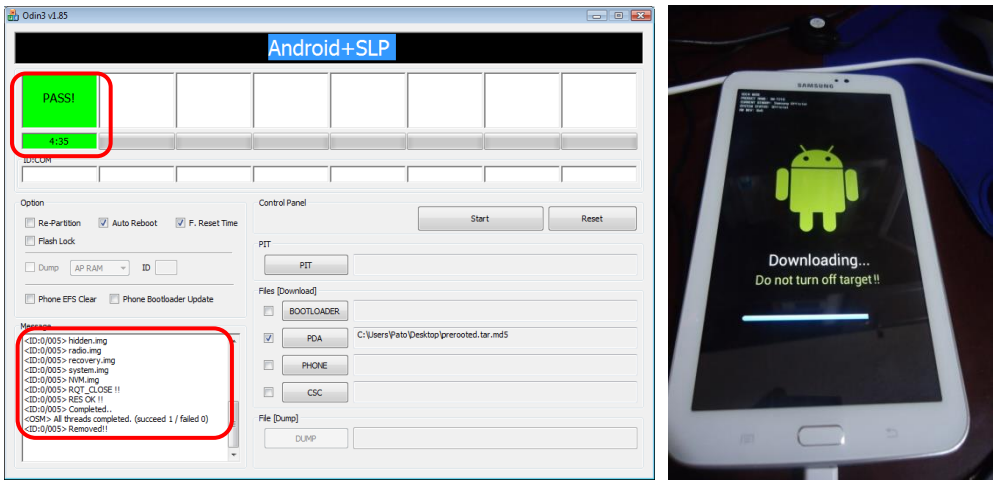


Figura 52. Ejecución correcta de root

13. Reinicio automático del sistema operativo Android.

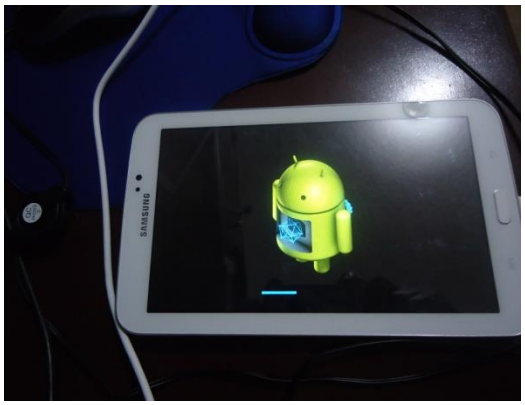


Figura 53. Reinicio de sistema Android

14. Finalmente para verificar que el dispositivo móvil inicie como súper usuario o administrador (root), ejecutamos la aplicación Root Checker, la cual fue descargada desde el store Google Play de Android.

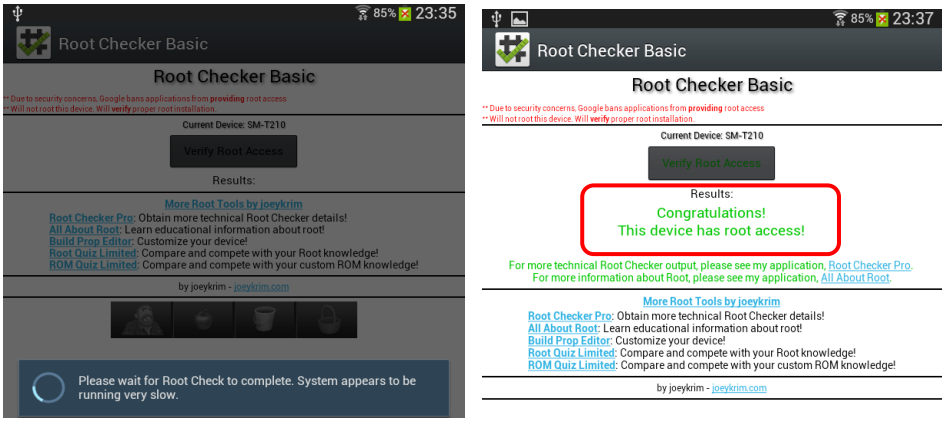


Figura 54. Ejecución como súper usuario

Una vez rooteado el dispositivo móvil y con los accesos necesarios para visualizar los archivos del sistema, utilizamos el aplicativo Root Explorer el cual permitirá navegar y gestionar los archivos raíz. Al ejecutar el aplicativo por primera vez solicita permisos de ejecución como súper usuario (root).

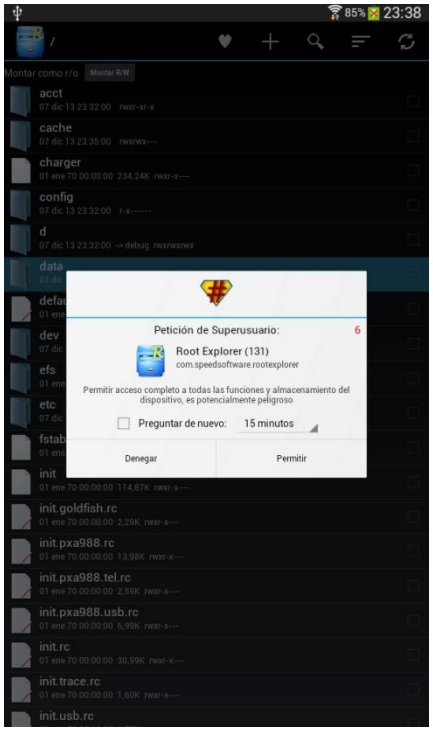


Figura 55. Petición de ejecución como súper usuario (root)

Con el dispositivo rooteado se procede a localizar los archivos del sistema que se ubican en los path que se describen.

/acct: Almacena archivos ocultos del sistema.

/cache: Almacena la memoria caché.

/d: Contiene drivers, controladores de hardware del dispositivo móvil.

/data: Almacena datos de las aplicaciones instaladas en el dispositivo móvil.

/dev: Contiene archivos del dispositivo, los cuales permiten la comunicación con los distintos elementos hardware que tiene instalado en el sistema.

/efs: Contiene información importante de la terminal (por ejemplo IMEI o PRODUCT CODE), es recomendable realizar un respaldo de esta información en el caso de querer realizar modificaciones al ROM, Kernel.

/etc: Contiene archivos propios de la configuración del sistema**.**

/factory: Contiene enlace a EFS y datos importantes como MAC Wifi, MAC Bluetooth, IMEI.

/lib: Contiene bibliotecas, librerías del sistema que son necesarias durante el inicio del mismo. Estas librerías son necesarias para integrar mediante código con los programas, ya que cuando un programa necesita alguna de

sus funciones, se carga la biblioteca en la memoria y puede ser usada por cualquier otro programa que la necesite, sin necesidad de volver a cargarla en memoria. **/lib/modules:** Contiene módulos del núcleo (normalmente se trata de controladores de dispositivos) que se cargan únicamente en caso de que falte utilizar un determinado dispositivo, por lo que no estará permanentemente en utilización de la memoria.

/mnt: Este directorio se agrupa los puntos de montaje de diversas particiones externas, como por ejemplo: sdcard, extSdcard, usb, secure, etc. Este directorio contiene un subdirectorio adicional para cada una de estas particiones (/mnt/sdcard, /mnt/UsbDriveA, etc). Si se accede a estos subdirectorios se está accediendo a las particiones.

/proc: Contiene archivos del sistema que se encuentran en proceso. Para cada proceso en ejecución existe un subdirectorio /proc/<número de proceso> con información sobre él.

/root: Directorio personal del usuario root o súper usuario. Contiene la información de los directorios personales de los distintos usuarios del sistema, pero orientada al usuario root.

/sbin: Contienen programas ejecutables (programas binarios) que forman parte del sistema operativo GNU/Linux.

/sdcard: Contiene información de la tarjeta interna**.**

/storage: Directorio donde se monta la tarjeta externa, interna y las conexiones usb como storage del dispositivo.

/sys: Contiene información sobre los dispositivos conectados al dispositivo.

/system: Contiene los apk de todo el software del sistema operativo en el subdirectorio /system/app.

/vendor: Contiene librerías, información de versión firmware, sistema, etc.

4.3.1.1. Ubicación de fuentes de evidencia digital en Android

La ubicación y localización de fuentes de información de aplicaciones de comunicación, redes sociales, etc. Se encuentra en las siguientes rutas.

- Las fuentes de información de los dispositivos enlazados mediante bluetooth, detallan claves de transmisión, información y contenido de los archivos enviados se localiza en la ruta:

/data/data/com.android.bluetooth, estas bases son pre-instaladas con el sistema operativo.

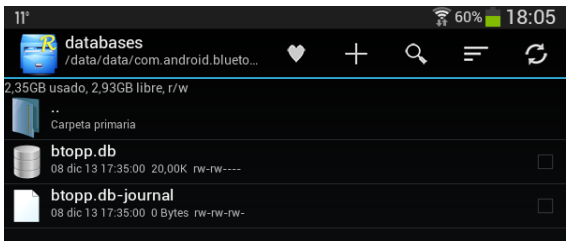


Figura 56. Archivo dispositivos enlazados vía bluetooth

- Las fuentes de información de datos de navegación e historial de búsquedas realizadas por medio del navegador se localiza en la ruta: /data/data/com.android.browser/databases/webview.db, estas bases son pre-instaladas con el sistema operativo.

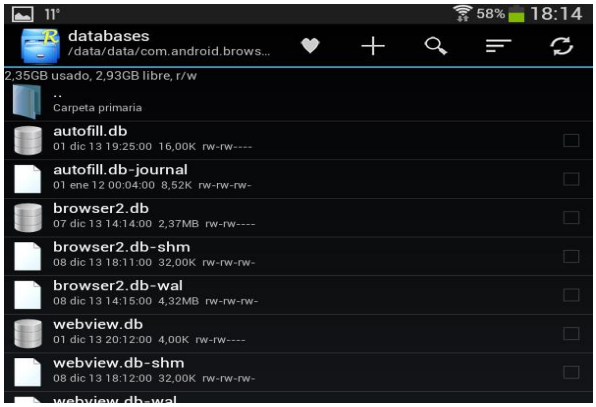


Figura 57. Archivo del navegador

- Las fuentes de información de eventos agendados, programados y calendario (recordatorios, tareas, reuniones) se localiza en la ruta: /data/data/com.android.calendar/shared_prefs, estas fuentes son generadas por el sistema operativo.

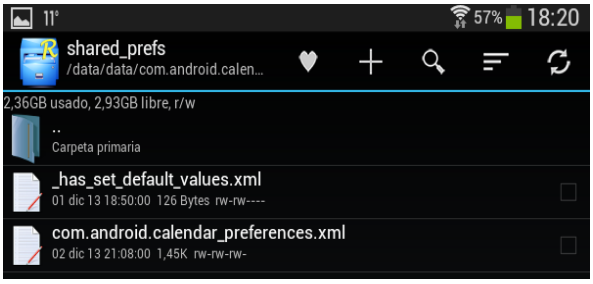


Figura 58. Archivo del calendario

- Las fuentes de información como sincronización de cuentas google, datos e historial de negación por medio de la aplicación Google Chrome se localiza en la ruta: /data/data/com.android.chrome/app_chrome/Default/. Estas fuentes son generadas por el aplicativo por tanto se las obtiene previa instalación del mismo.

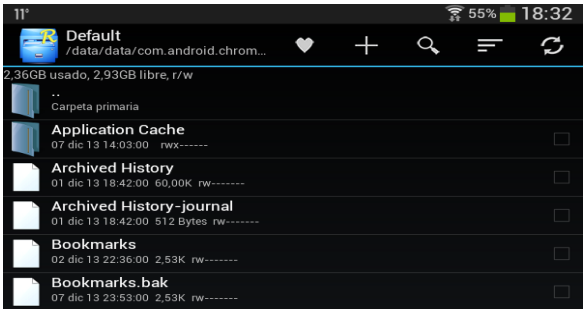


Figura 59. Archivos de Chrome

- Las fuentes de información de Google Calendar se localiza en la ruta: /data/data/com.android.providers.calendar/databases/, estas bases son pre-instaladas con el sistema operativo.

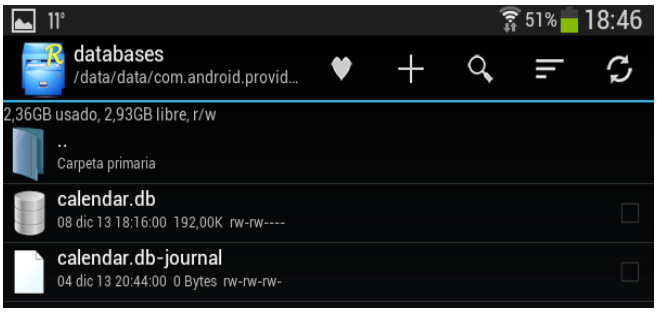


Figura 60. Archivos de calendario de Google

- Las fuentes de información de contactos registrados en el dispositivo se localiza en la ruta: /data/data/com.android.providers.contacts/databases/, estas bases son pre-instaladas con el sistema operativo.

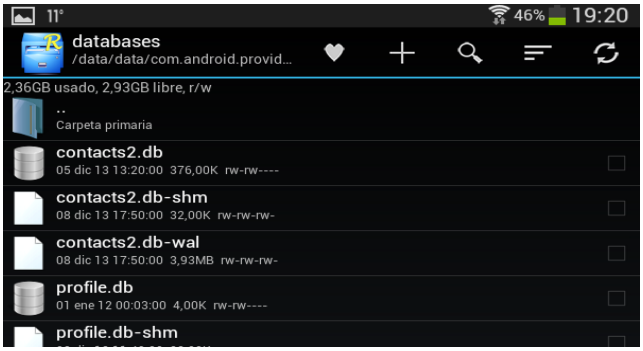


Figura 61. Archivos de contactos

- Las fuentes de información de descargas realizadas por medio del dispositivo móvil se localiza en la ruta: /data/data/com.android.providers.downloads/databases/, las cuales son bases pre-instaladas con el sistema operativo.

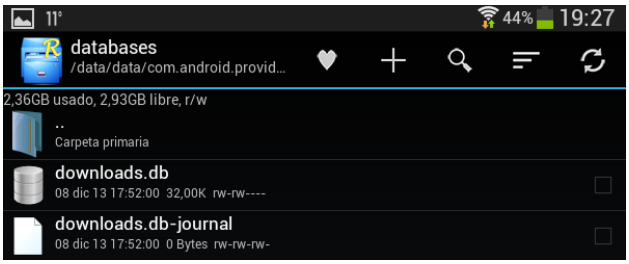


Figura 62. Archivos de descargas

- Las fuentes de información de social media se localiza en la ruta: /data/data/com.android.providers.media/databases/, las cuales son bases pre-instaladas con el sistema operativo.

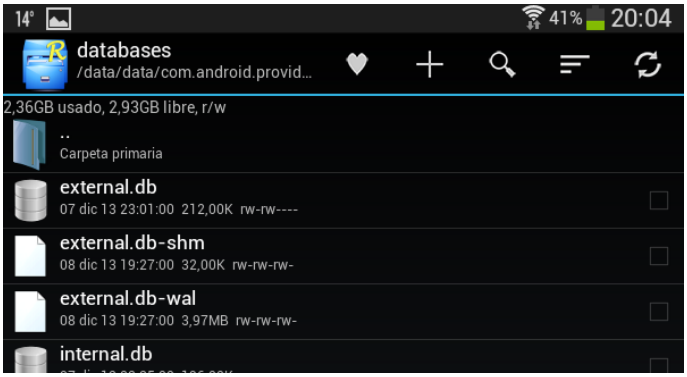


Figura 63. Archivos de social media

- Las fuentes de información del localizador de ubicación de Google, que contiene un historial de sitios ubicados por la aplicación se encuentra en la ruta: /data/data/com.google.android.location/, las cuales son bases pre-instaladas con el sistema operativo.

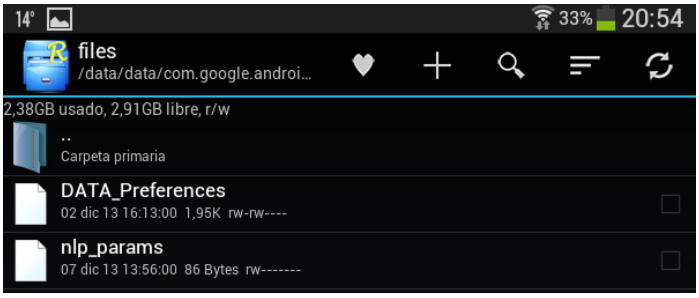


Figura 64. Archivo de localización

- Las fuentes de información de la aplicación youtube se localiza en la ruta: /data/data/com.google.android.youtube, estas fuentes se obtienen previa instalación de la aplicación en el dispositivo.

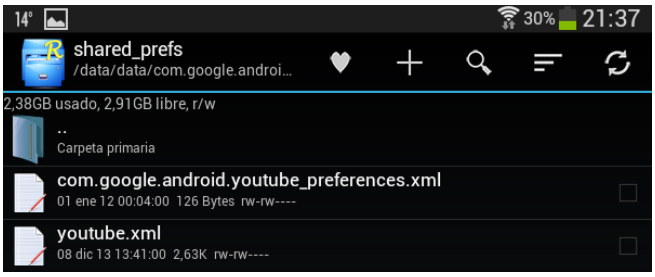


Figura 65. Archivo de youtube

- Las fuentes de información de redes WiFi, que contiene usuario y contraseña se localiza en la ruta: /data/misc/wifi/wpa_supplicant/, estas bases son pre-instaladas con el sistema operativo.

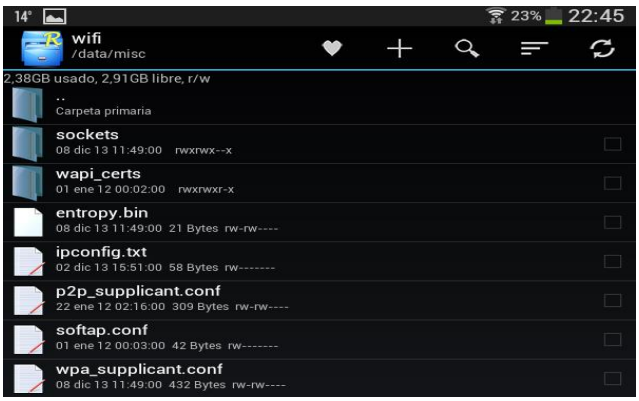


Figura 66. Archivos de redes wifi

- Las fuentes de información de la aplicación shazam que contiene historial de descargas, búsquedas se localiza en la ruta: /data/data/com.shazam.android/databases/, estas fuentes se obtienen previa instalación de la aplicación en el dispositivo.

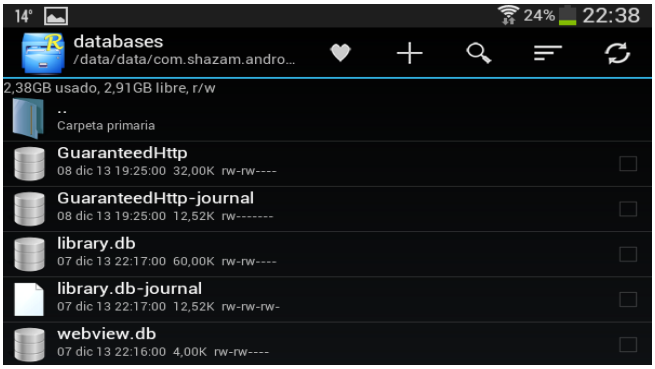


Figura 67. Archivos de shazam

- Las fuentes de información de la aplicación Skype que contiene información de contactos, llamadas realizadas, chat, información de archivos compartidos se localiza en la ruta: /data/data/com.skype.raider/files, estas fuentes se obtienen previa instalación del aplicativo en el dispositivo.

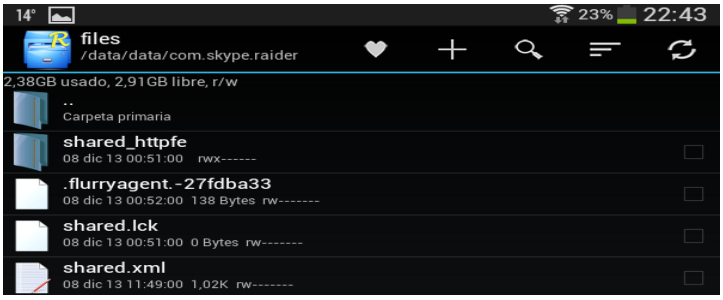


Figura 68. Archivos de skype

- Las fuentes de información del correo Gmail que contiene usuario, contraseña, correo sincronizado, direcciones electrónicas se localiza en la ruta:
  /data/data/com.google.android.providers.gmail/, estas fuentes se obtienen previa instalación del aplicativo en el dispositivo.
- Las fuentes de información del aplicativo Facebook que contiene usuario, contraseña, contactos, direcciones electrónicas, publicaciones, archivos compartidos se localiza en la ruta: /data/data/com.sec.android.app.sns3/databases/snsFacebookDB.db/journal, estas bases se obtienen previa instalación del aplicativo en el dispositivo.

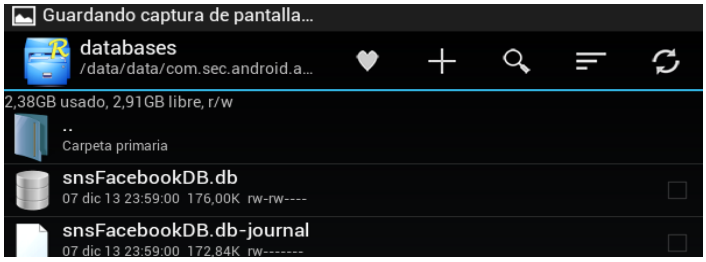


Figura 69. Archivos de facebook

- Las fuentes de información del aplicativo de Twitter que contiene usuario, contraseña, contactos, direcciones electrónicas, publicaciones se localiza en la ruta: /data/data/com.twitter/databases, estas bases se obtienen previa instalación del aplicativo en el dispositivo.

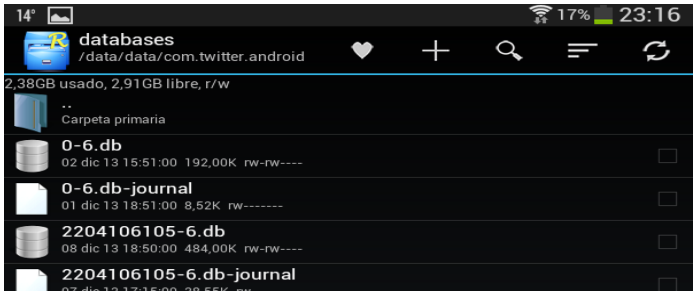


Figura 70. Archivos de twitter

- Las fuentes de información del patrón de ingreso hacia el dispositivo se localiza en la ruta: /data/system/gesture.key, este archivo es autogenerado por el sistema ya que este componente de seguridad es pre-instalado con el sistema operativo.

Figura 71. Archivos de patrón de claves

- Las fuentes de información del aplicativo DropBox que contiene usuario, contraseña, archivos, documentos, imágenes cargadas al repositorio en la nube se localiza en la ruta:

/data/data/com.dropbox.android/databases, estas bases se obtienen previa instalación del aplicativo en el dispositivo.

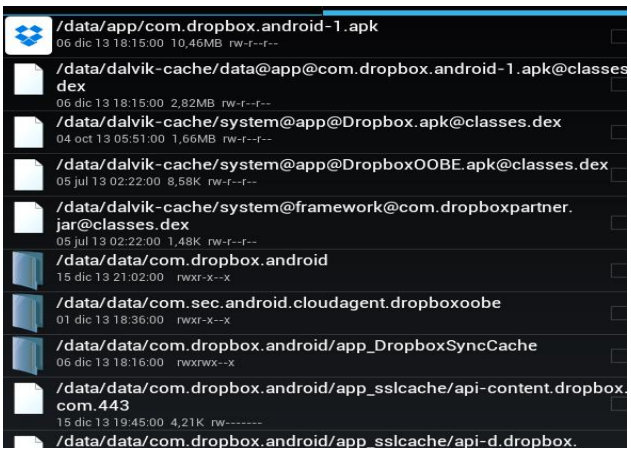


Figura 72. Archivos de DropBox

- Las fuentes de información del aplicativo Instagram que contiene usuario, contraseña, imágenes publicadas y compartidas, etiquetas se localiza en la ruta: /data/data/com.instagram.android/databases/, estas bases se obtienen previa instalación del aplicativo en el dispositivo.

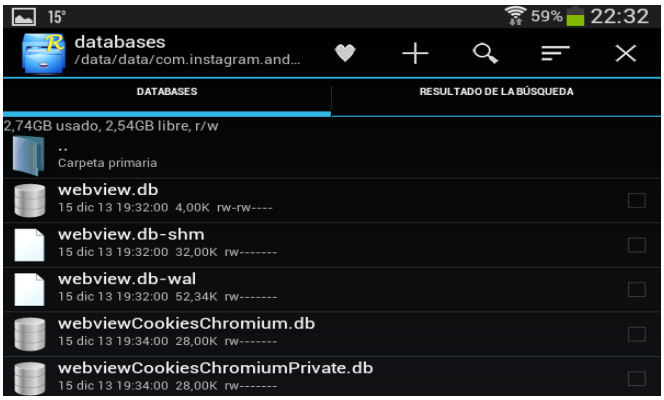


Figura 73. Archivos de Instagram

En la búsqueda de evidencia se emite un formulario, el cual contiene el tipo de fuente, la ruta y el nombre del archivo localizado.

DEPARTAMENTO DE INVESTIGACION MEVAST - ESPE QUITO - ECUADOR		
FECHA: 15/04/2014	HORA: 10:15 (AM)	FORMULARIO: E3 F1 CODIGO CASO: INC-001
FUENTE DE INFORMACION		
Tipo fuente de información (db, xml, txt, log, etc)	**Ruta**	**Nombre fuente de información (file)**
.db	/data/data/com.android.bluetooth/	btopps.db
.xml	/data/data/com.android.calendar/shared_prefs/	preferences.xml
.db	/data/data/com.android.providers.contacts/databases/	contacts.db
.xml	/data/data/com.skype.raider/files/	shared.xml
.db	/data/data/com.sec.android.app.sns3/databases/snsFacebookDB.db/jd	snsFacebookDB.db
.db	/data/data/com.twitter/databases/	twitter.db
.key	/data/system/	gesture.key
.db	/data/data/com.dropbox.android/databases/	dropbox.db
.db	/data/data/com.instagram.android/databases/	instagram.db
...	...	...
Receptado por:	Revisado por:	Autorizado por:

Figura 74. Formulario de fuente de información (Ver Anexo 17)

4.3.2. Fase de análisis de la evidencia digital

En esta fase con la utilización de software especializado se analiza las fuentes de evidencia localizadas, que para el caso se utiliza Oxygen Forensic Suite 2014. (Ver Anexo 15, Matriz DAR – Análisis de Decisión y resolución).

Como fase inicial se procede a la instalación del software especializado para el análisis.

Figura 75. Instalación Oxygen Forensic Suite 2014

A continuación, se procede a conectar el dispositivo móvil mediante el software para la extracción de la evidencia y análisis de la misma.

Figura 76. Conexión del dispositivo mediante Oxygen Forensic

Ingreso de información referente al caso y selección de data.

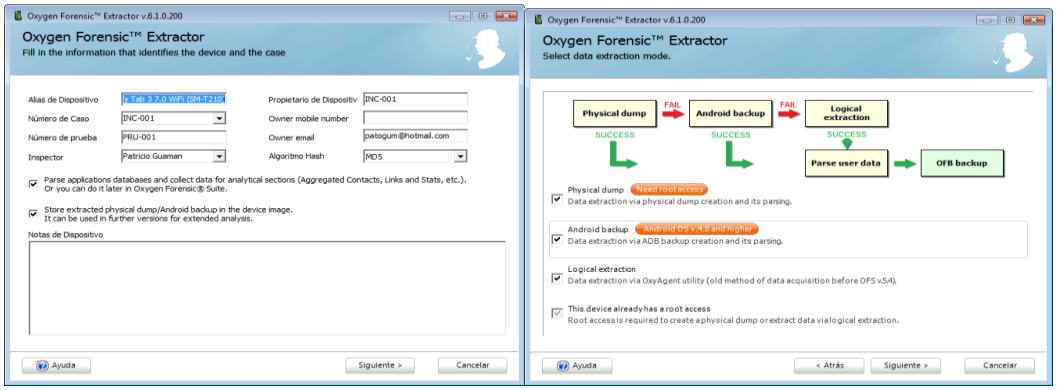


Figura 77. Obtención de evidencia

Información detallada del caso y extracción de evidencia.

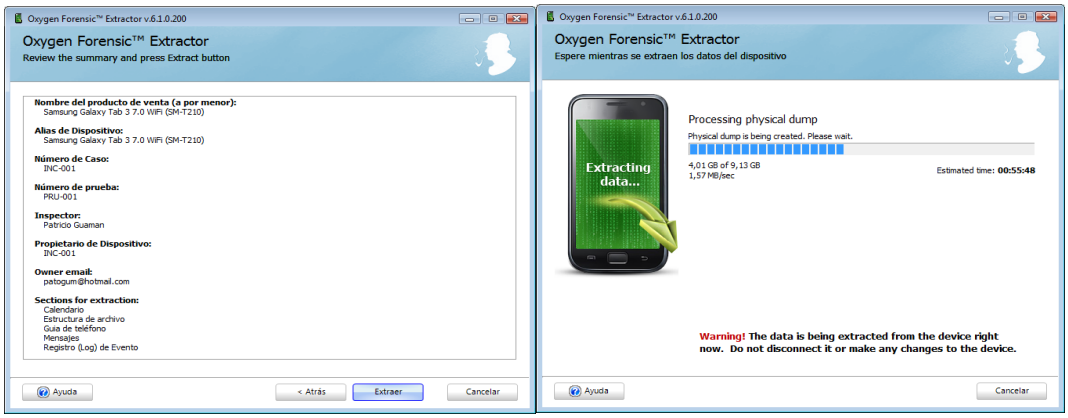


Figura 78. Información del caso analizar

Finalizada la extracción de la información se procede a recabar información. Se visualiza información detalla del dispositivo móvil.

Figura 79. Información del dispositivo móvil

Se puede explorar los archivos de imágenes, audio, videos, documentos, archivos de base de datos.

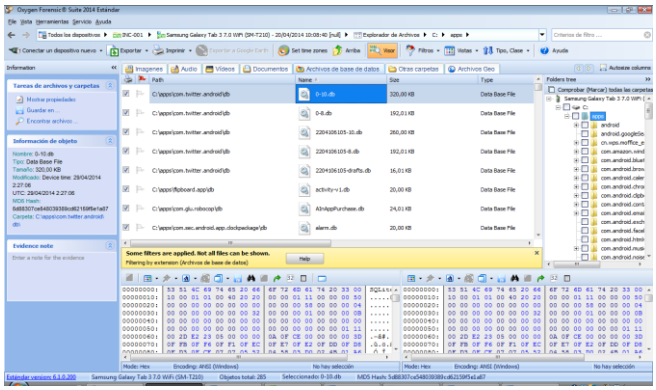


Figura 80. Información de archivos

Información de la guía telefónica del dispositivo.

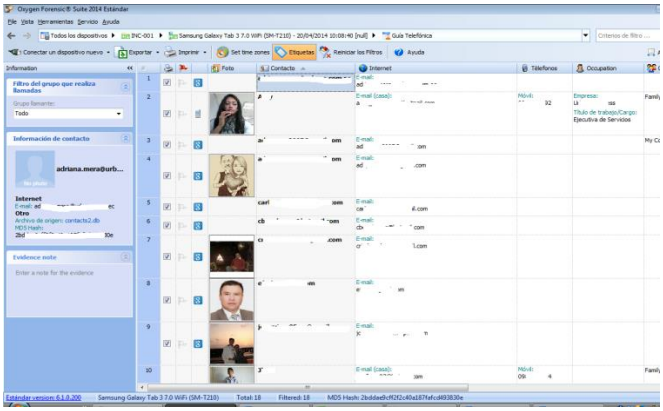


Figura 81. Información guía telefónica

Información de la agenda, calendario del dispositivo.

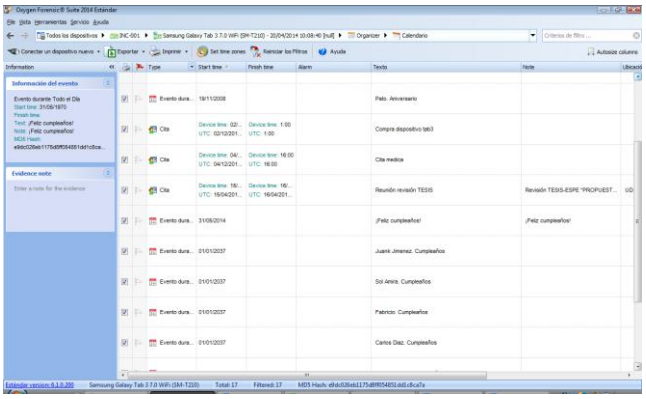


Figura 82. Información agenda, calendario

Información de llamadas efectuadas, recibidas y perdidas

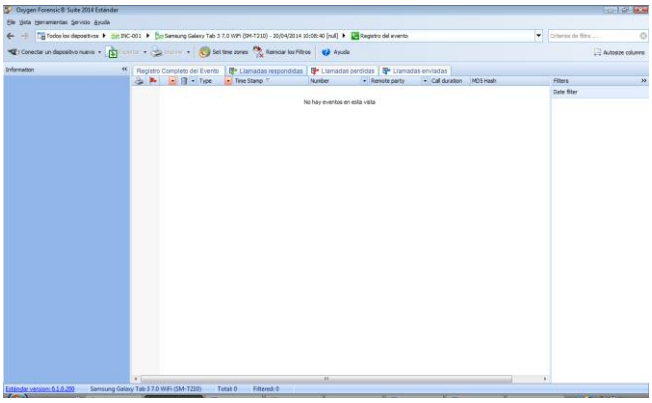


Figura 83. Registro de llamadas

Información de mensajes realizados.

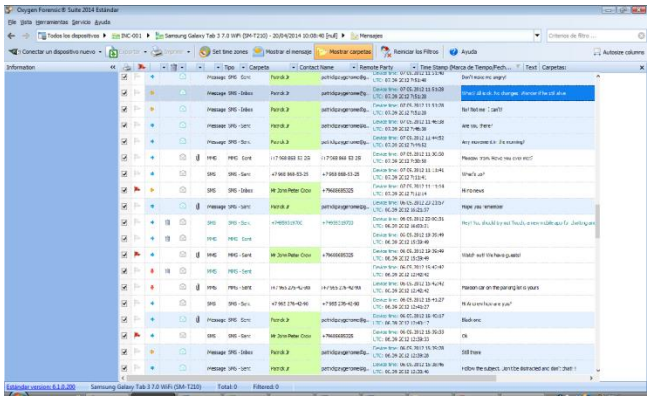


Figura 84. Información de mensajes

Información de geo locación.

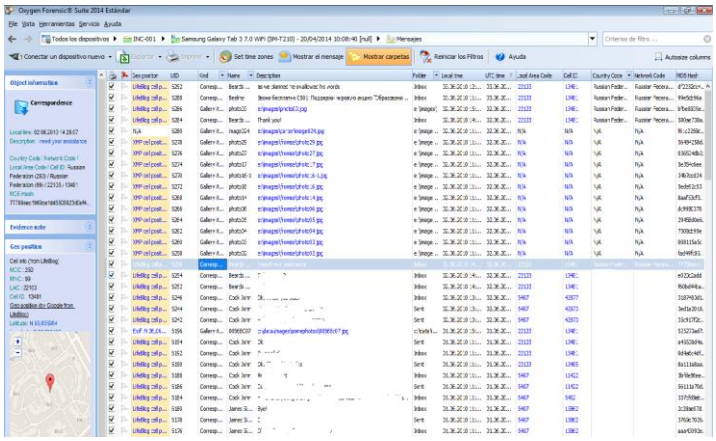


Figura 85. Información de ubicación

Información de aplicaciones de redes sociales y comunicación.

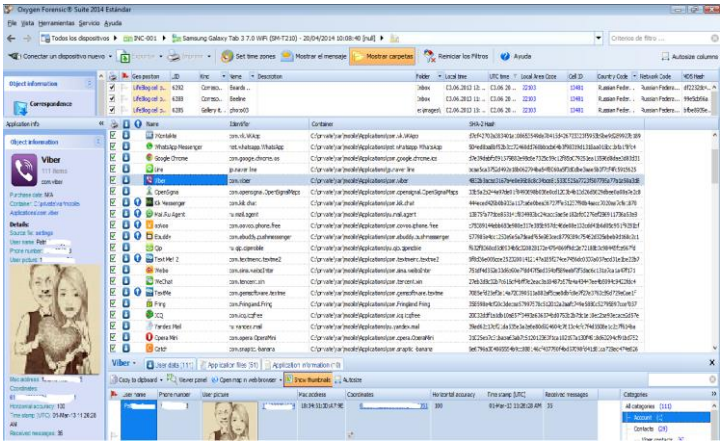


Figura 86. Información de aplicaciones

El software Oxygen Forensic Suite 2014 ofrece gran variedad de opciones para obtener información, la cual sirva para indagar y llegar a una conclusión de los hechos suscitados en el dispositivo móvil.

Finalmente Oxygen Forensic Suite genera un reporte en formato PDF con todo el contenido localizado.

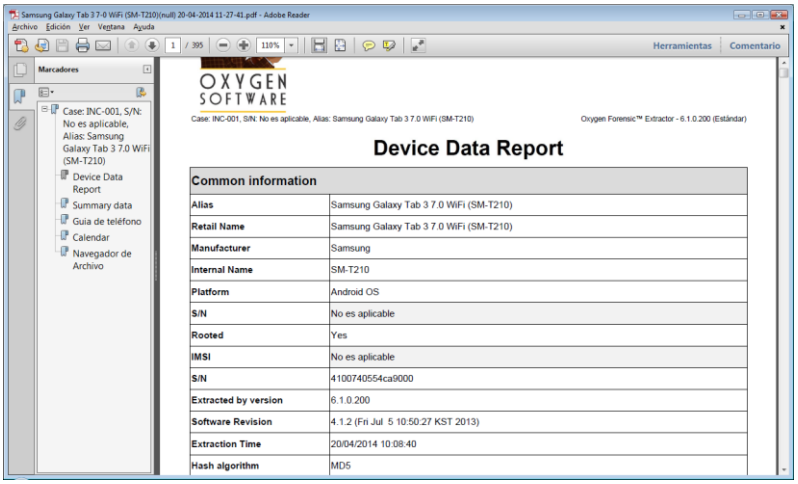


Figura 87. Generación de reporte (Anexo 18)

4.4. Etapa de Presentación

4.4.1. Fase de elaboración del informe

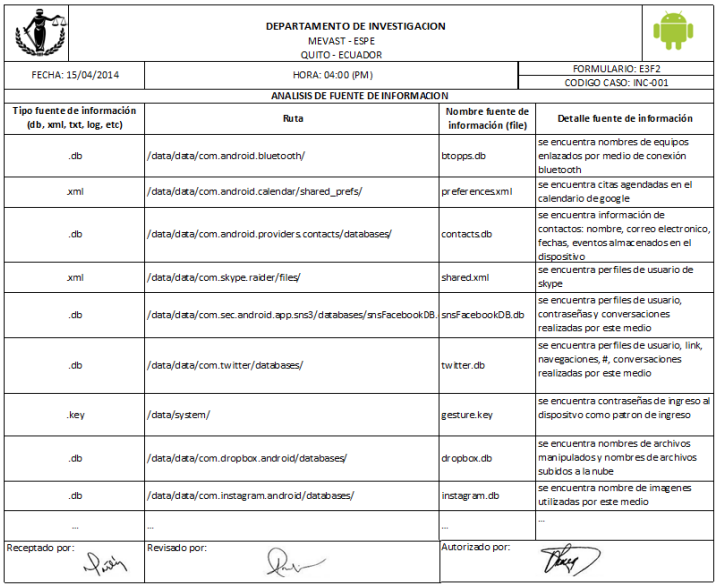
Para proceder con la elaboración del informe, se recopila toda la información obtenida y generada en la primera, segunda y tercera etapa.

- Solicitud de asignación de caso (Ver, Anexo 10)
- Roles y funciones (Ver, Anexo 11)
- Información del involucrado (Ver, Anexo 12)
- Componentes electrónicos incautados (Ver, Anexo 13)
- Información del dispositivo (Ver, Anexo 14)
- Software especializado para análisis forense (Ver, Anexo 15)
- Generación código Hash MD5 (Ver, Anexo 16)
- Formulario de fuente de información (Ver, Anexo 17)
- Reporte generado por Oxygen Forensic Suite (Ver, Anexo 18)

4.4.2. Fase de resultados de la información

Mediante la visualización del contenido se determina las causas, motivaciones, lugares, personas de contacto, imágenes, documentos compartidos, archivos comprometidos, geo localizaciones, conexiones WiFi, conexiones IP, direcciones web, rutas visitadas por el sospechoso.

Toda esta información sirve para solventar el incidente y la línea de tiempo para la ejecución del mismo.



DEPARTAMENTO DE INVESTIGACION
MEVAST - ESPE
QUITO - ECUADOR

FECHA: 15/04/2014	HORA: 04:00 (PM)	FORMULARIO: E3F2 CODIGO CASO: INC-001

ANALISIS DE FUENTE DE INFORMACION

Tipo fuente de información (db, xml, txt, log, etc)	Ruta	Nombre fuente de información (file)	Detalle fuente de información
.db	/data/data/com.android.bluetooth/	btopps.db	se encuentra nombres de equipos enlazados por medio de conexión bluetooth
.xml	/data/data/com.android.calendar/shared_prefs/	preferences.xml	se encuentra citas agendadas en el calendario de google
.db	/data/data/com.android.providers.contacts/databases/	contacts.db	se encuentra información de contactos: nombre, correo electronico, fechas, eventos almacenados en el dispositivo
.xml	/data/data/com.skype.raider/files/	shared.xml	se encuentra perfiles de usuario de skype
.db	/data/data/com.sec.android.app.sns3/databases/snsFacebookDB.	snsFacebookDB.db	se encuentra perfiles de usuario, contraseñas y conversaciones realizadas por este medio
.db	/data/data/com.twitter/databases/	twitter.db	se encuentra perfiles de usuario, link, navegaciones, #, conversaciones realizadas por este medio
.key	/data/system/	gesture.key	se encuentra contraseñas de ingreso al dispositivo como patron de ingreso
.db	/data/data/com.dropbox.android/databases/	dropbox.db	se encuentra nombres de archivos manipulados y nombres de archivos subidos a la nube
.db	/data/data/com.instagram.android/databases/	instagram.db	se encuentra nombre de imagenes utilizadas por este medio
...	...	...	...

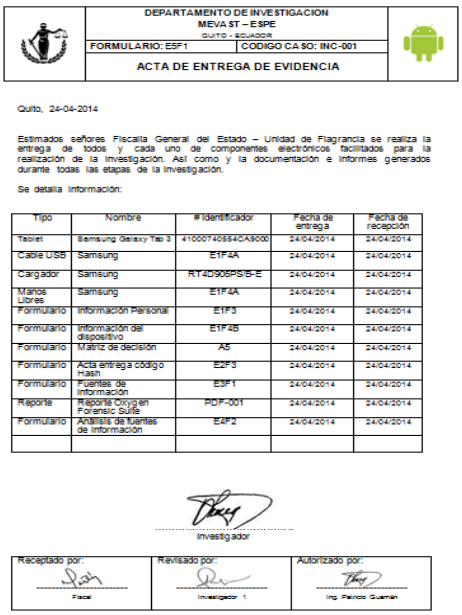
Receptado por: Revisado por: Autorizado por:

Figura 88. Formulario de análisis de fuente de información (Anexo 19)

4.5. Etapa de Entrega de Evidencia

4.5.1. Fase de devolución de la evidencia

La devolución y entrega de la evidencia con sus respectivos informes adjuntos se detalla en el formulario.



DEPARTAMENTO DE INVESTIGACION
MEVAST – ESPE
QUITO - ECUADOR

FORMULARIO: ESF1 | CODIGO CASO: INC-001

ACTA DE ENTREGA DE EVIDENCIA

Quito, 24-04-2014

Estimados señores Fiscalía General del Estado – Unidad de Flagrancia se realiza la entrega de todos y cada uno de componentes electrónicos facilitados para la realización de la investigación. Así como y la documentación e informes generados durante todas las etapas de la investigación.

Se detalla información:

Tipo	Nombre	# Identificador	Fecha de entrega	Fecha de recepción
Tablet	Samsung Galaxy Tab 3	4100074088ACA9000	24/04/2014	24/04/2014
Cable USB	Samsung	E1F4A	24/04/2014	24/04/2014
Cargador	Samsung	RT4D908PSIB-E	24/04/2014	24/04/2014
Manos Libres	Samsung	E1F4A	24/04/2014	24/04/2014
Formulario	Información Personal	E1F3	24/04/2014	24/04/2014
Formulario	Información del dispositivo	E1F4B	24/04/2014	24/04/2014
Formulario	Matriz de decisión	A5	24/04/2014	24/04/2014
Formulario	Acta entrega código Hash	E2F3	24/04/2014	24/04/2014
Formulario	Fuentes de información	E3F1	24/04/2014	24/04/2014
Reporte	Reporte Oxygen Forensic Suite	PDF-001	24/04/2014	24/04/2014
Formulario	Analisis de fuentes de información	E4F2	24/04/2014	24/04/2014

Investigador

Receptado por:	Revisado por:	Autorizado por:
Fiscal	Investigador 1	Ing. Patricio Guamán

Figura 89. Formulario devolución de evidencia (Anexo 20)

Finalizado la ejecución del modelo metodológico se puede concluir que del análisis forense efectuado, se obtuvo información relevante la cual servirá de apoyo en el caso de investigación. También destacar que durante todo el proceso se garantizó la cadena de custodia de la información.

Se recomienda que durante la obtención de pruebas y evidencia digital localizada sea totalmente aislada de personas que no tienen ningún tipo de autorización para su acceso, ya que se está manejando información extremamente confidencia que solo sirve para las personas pertinentes o la fiscalía.

4.6. Cuadro de Mando Integral (Norton, 1992)

Cuadro de Mando Integral (CMI) fue presentado en 1992 en la revista Harvard Business Review, sus autores, Robert Kaplan y David Norton, plantean que el CMI es un sistema de administración, que va más allá de la perspectiva financiera con la que los gerentes acostumbran evaluar la marcha de una empresa, sino que proponen generar indicadores o métricas no-financiera enfocadas desde la perspectiva del Desarrollo y Aprendizaje, Interna del Negocio, del Proceso, del Cliente y Financiera. (Norton, 1992, p. 15)

4.6.1. Inventario de Indicadores / Métricas

Se utiliza una serie de indicadores los cuales permiten validar la efectividad de la utilización del modelo metodológico. A estos indicadores se darán seguimiento mes a mes mediante un tablero RGY (Red, Green, Yellow - Sistema de Semáforos), ver Anexo 21.

Se describe el inventario de indicadores para el modelo metodológico propuesto desde la perspectiva del cliente y del proceso.

Cuadro 8

Inventario de indicadores

Perspectiva Cliente	
Nombre	% encuestas de satisfacción
Objetivo	Validar la satisfacción del cliente (Fiscalía, otras entidades)
Forma de cálculo	Media aritmética de todas las encuestas Ẋ= ∑Xi / n
Responsable	Investigador Forense
Frecuencia de Levantamiento y Reportaje	Trimestral
Fuente de Información	Encuestas
Niveles de reporte	Gerencia
Acciones a tomar	Cada tres meses se enviará encuestas de satisfacción en formato Excel a todos los clientes (internos / externos)

Perspectiva Cliente	
Nombre	# casos cerrados en el mes
Objetivo	Validar la oportunidad de atención al cliente
Forma de Cálculo	#casos cerrados / # total de casos abiertos
Responsable	Investigador Forense
Frecuencia de Levantamiento y Reportaje	Mensual
Fuente de Información	Investigador Forense
Niveles de reporte	Gerencia
Acciones a tomar	Establecer reuniones mensuales con todos los involucrados en el proceso forense

Continúa

Perspectiva Cliente	
Nombre	# acuerdo de nivel de servicios (SLA)
Objetivo	Número de casos cerrados en las fechas acordadas
Forma de Cálculo	# casos fuera del acuerdo de nivel de servicio
Responsable	Investigador Forense
Frecuencia de Levantamiento y Reportaje	Mensual
Fuente de Información	Investigador Forense
Niveles de reporte	Gerencia
Acciones a tomar	Establecer reuniones mensuales con todos los involucrados en el proceso forense

Perspectiva Cliente	
Nombre	% efectividad por cliente
Objetivo	Validar efectividad del proceso
Forma de Cálculo	# casos realizados / # casos recibidos
Responsable	Investigador Forense
Frecuencia de Levantamiento y Reportaje	Trimestral
Fuente de Información	Investigador Forense
Niveles de reporte	Gerencia
Acciones a tomar	Establecer reuniones mensuales con todos los involucrados en el proceso forense

Perspectiva Proceso	
Nombre	# hallazgos promedio
Objetivo	Número de hallazgos promedio localizados
Forma de cálculo	# hallazgos / # casos cerrados
Responsable	Investigador Forense
Frecuencia de Levantamiento y Reportaje	Mensual
Fuente de Información	Investigador Forense
Niveles de reporte	Gerencia
Acciones a tomar	Establecer reuniones mensuales con todos los involucrados en el proceso forense

Perspectiva Proceso	
Nombre	# horas de análisis forense
Objetivo	Número de horas promedio de análisis forense
Forma de Cálculo	# horas de análisis forense / # casos cerrados
Responsable	Investigador Forense
Frecuencia de Levantamiento y Reportaje	Mensual
Fuente de Información	Investigador Forense
Niveles de reporte	Gerencia
Acciones a tomar	Establecer reuniones mensuales con todos los involucrados en el proceso forense

CAPÍTULO V

5. Conclusiones y recomendaciones

5.1. Conclusiones

- El modelo de análisis forense a dispositivos móviles con sistema operativo Android propuesto cubre diversas etapas de la investigación: la etapa de identificación y preparación, etapa de preservación y adquisición, etapa de análisis, etapa de presentación y etapa de entrega de evidencia; las cuales conjuntamente apoyan a la búsqueda y al análisis de la evidencia digital.
- Se utilizarán plantillas genéricas en las diversas etapas del proceso, las mismas que buscan un orden durante el proceso de análisis forense a dispositivos móviles con sistema operativo Android.
- Como conclusión del caso de estudio del modelo propuesto para análisis forense a dispositivos móviles con sistema operativo Android; se localizó evidencias digitales, las cuales serán entregadas a los estamentos judiciales y servirán como una variable en el proceso judicial.
- Android es un sistema operativo de código fuente abierto, en este sentido existen vulnerabilidades en cuanto a la seguridad de la información. Teniendo en cuenta también que la seguridad de la información en el País aún no alcanza un nivel de madurez que garantice y de confianza a los clientes sobre el resguardo de la información, la cual hoy en día constituye uno de los activos más importantes en las organizaciones.
- El modelo de análisis forense a dispositivos móviles con sistema operativo Android propuesto es aplicable para dispositivos móviles Android, sin embargo por las características generales del modelo metodológico podría ser ampliado a otras plataformas como iOS, BlackBerry, Symbian.
- Se logró demostrar que el modelo de análisis forense a dispositivos móviles con sistema operativo Android propuesto cumple con lineamientos de la cadena de custodia en todo el proceso de investigación, basándose desde el punto de vista científico y técnico.

5.2. Recomendaciones

- El análisis de la evidencia digital se debe realizar sobre una copia de la imagen digital generada o facilitada por las partes y que no haya sido manipulada.
- El modelo de análisis forense está basado sobre la ejecución de sistemas operativo Android, en caso de requerir su aplicación en otra plataforma como iOS, BlackBerry, Symbian; se deberá evaluar las herramientas y software a utilizar, mediante matrices de decisión que ayuden a seleccionar adecuadamente y no por percepción.
- Involucrar a organizaciones tanto públicas como privadas para el mejoramiento de la investigación sobre el análisis forense a dispositivos móviles.
- El avance tecnológico y el incremento de transacciones electrónicas en el País, hace que los usuarios estén más expuestos a ser víctimas del cibercrimen e ingeniería social, en este sentido se requiere que se continúe realizando investigaciones en el área de informática forense orientada a dispositivos móviles.
- Los dispositivos móviles siguen aumentando sus capacidades con nuevas versiones, por tanto seguirán presentándose nuevos retos para el análisis forense. Es este sentido se requiere de aportes e investigación continua.

BIBLIOGRAFÍA

Andrea Ariza Díaz - Juan Camilo Ruíz. (2009). *Un protocolo de análisis forense para dispositivos móviles inteligentes.* Bogotá, Colombia: Pontificia Universidad Javeriana de Colombia.

Android. (2013, 6 29). *Android Developers*. Retrieved 10 20, 203, from http://developer.android.com

Android. (2014, 3 1). *Android*. Retrieved 3 15, 2014, from www.android.com

Android. (2014, 1 30). *Developer Android*. Retrieved 2 22, 2014, from http://developer.android.com/intl/es/tools/help/adb.html

Android Inc. (2013, 8 15). *Android - Jelly Bean*. Retrieved 12 20, 2013, from http://developer.android.com/intl/es/about/versions/jelly-bean.html

Androideity. (2011, 7 7). *Androideity*. Retrieved 12 17, 2013, from http://androideity.com/2011/07/07/la-maquina-virtual-dalvik/

Basterra, B. B. (2012). Android OS. *Readthedocs*.

Cano, J. (2006). *Buenas prácticas en la administración de la evidencia digital.* Bogota: GECTI - Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática.

Cano, J. (2006). Introducción a la informática forense. *ACIS - Asociación Colombiana de Ingenieros de Sistemas*, 64-73.

Cano, J. (2009). *Computacion forense.* Mexico: Alfaomega.

Carlos Andrés Castillo Londoño, R. A. (2008). *Guía Metodológica para el Análisis Forense Orientado a Incidentes en Dispositivos Móviles GSM.* Bogotá, Colombia: Pontificia Universidad Javeriana.

Castro, L. (2013, 6 30). *Conectividad de Internet.* Retrieved 1 5, 2014, from http://aprenderinternet.about.com/od/ConceptosBasico/ig/Conectividad-de-Internet-en-el-2013/Qui-n-usa-m-s-Internet-en-el-mundo.htm

Chang, R. Y. (1996). *Mejora Continua de Procesos.* Granica: Ilustrada.

Daniel, L. E., & Daniel, L. E. (2012). *Digital forensics for legal professionals, understanding digital evidence from the warrant to the courtroom.* Syngress.

Dominguez, L. (2007, 1 20). *Monografias.* Retrieved 1 15, 2014, from http://www.monografias.com/trabajos44/informatizacion-auditoria/informatizacion-auditoria2.shtml

El Comercio. (2014, 4 11). Tecnología. *Víctimas de robos informáticos piden respuestas*, pp. 25-26.

FIME-ITS. (2012, 3 2). *Tipos de aplicaciones en Android*. Retrieved 12 20, 2013, from http://danimtzc.blogspot.com/2012/03/tipos-de-aplicaciones-en-android.html

Gartner Inc. (2013, 9 29). *TI*. Retrieved 2 3, 2014, from http://www.gartner.com/technology/home.jsp

Ghosh, A. (2004). *Guidlines for the management of TI.* Hong Kong: APEC Telecommunications and Information Working Group.

Gironés, J. T. (2013). *El gran libro de Android* (Tercera ed.). Barcelona: Marcombo.

Grupo ADSL Zone. (2012, 2 19). *Linux Zone.* Retrieved 11 18, 2013, from http://linuxzone.es/que-es-el-kernel/

Grupo Gowex. (2013, 10 25). *Internet y telecomunicaciones*. Retrieved 11 15, 2013, from http://www.telcommunity.com/category/internet-y-telecomunicaciones/page/75/

Hernandez, R. (2011, 10 20). *Entendiendo Android.* Retrieved 10 12, 2013, from Tenerife LAN Party 2k11: http://www.emezeta.com/articulos/conferencia-entendiendo-android

Hoog, A. (2011). *Android forensics : investigation, analysis, and mobile security for Google Android.* Waltham, MA : Syngress.

Key4Communications. (2013, 7 23). *9 datos sobre el comer móvil*. Retrieved 12 15, 2013, from http://www.key4communications.com/es/key4/tendencias/9-datos-sobre-el-comercio-movil_221.html

Lillard T, G. C. (2010). *Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data.* Syngress.

Linux. (2013, 11 10). *Linux*. Retrieved 2 17, 2014, from http://elinux.org/Android_Kernel_Features

Madrid, U. C. (2012, 3 5). *Software de comunicaciones*. Retrieved 12 20, 2013, from https://sites.google.com/site/swcuc3m/home/android/generalidades/dalvikvm-1

Melo, J. (2013, 6 2). *Historia para dispositivos móviles*. Retrieved 11 1, 2013, from www.memoriadigital.historiaabierta.org/historia-para-dispositivos-moviles

Networks, J. (2012). Mobile threats report. *Jupiter Networks*, 7.

NIST. (2008, 8 30). *National Institute of Standards and Technology.* Retrieved 3 27, 2014, from Forensic Filtering of Cell Phone Protocols: www.nist.gov

NIST. (2014, 4 3). *National Institute of Standards and Technology*. Retrieved 4 6, 2014, from http://www.nist.gov/

Norton, K. . (1992). *Cuadro de Mando Integral.* Barcelona: Gestión 2000.

Pino, D. S. (2009). *PERFIL SOBRE LOS DELITOS INFORMÁTICOS EN EL ECUADOR.* Quito, Ecuador: Fiscalía General del Estado.

PMI. (2008). *A Guide to the Project Management Body of Knowledge Fourth Edition.* Atlanta, E.E.U.U.: Project Management Institute.

Prosise, K. M. (2003). *Incident Response & Computer Forensics* (Segunda Edición ed.). California: Mc Graw Hill.

Rick Ayers, W. J. (2005). *Cell Phone Forensic Tools: An Overview and Analysis, NISTIR 7250,.* Washington, E.E.U.U.: NIST is an Agency of the U.S. Department of Commerce.

SamsungBlogspot. (2012, 11 3). *Sistema Android*. Retrieved 12 9, 2013, from http://samsungmonica.blogspot.com/

SANS. (2014, 2 20). *SANS Forensics*. Retrieved 3 27, 2014, from http://digital-forensics.sans.org/

USDOJ. (2013, 9 14). *U.S. Department of Justice*. Retrieved 3 15, 2014, from http://www.doj.state.wi.us/

Wayne Jansen, R. A. (2007). *Guidelines on Cell Phone Forensics, SP 800-101.* Washington, E.E.U.U.: NIST is an Agency of the U.S. Department of Commerce.

Zhou, X. J.-Y. (2013). *Android Malware.* North Carolina State: Material Springer.