UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

Metodología de Análisis Forense en Smartphones y sus Implicaciones en el Cómputo en la Nube

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JUAN MEZA CASTRO

ASESOR:

M.C. Leobardo Hernández Audelo

CIUDAD NEZAHUALCÓYOTL, ESTADO DE MÉXICO, 2019

Índice Temático

Índice de Figuras

Índice de Tablas

Agradecimientos

El presente trabajo est. dedicado a mi familia por haber sido mi apoyo a lo largo de toda mi carrera universitaria y a lo largo de mi vida. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

Agradezco a mi familia, por haberme dado la oportunidad de formarme en esta prestigiosa universidad y haber sido mi apoyo durante todo este tiempo.

De manera especial a mi tutor de tesis, por haberme guiado, no solo en la elaboración de este trabajo de titulación, sino a lo largo de mi carrera universitaria y haberme brindado el apoyo para desarrollarme profesionalmente y seguir cultivando mis valores.

A la Facultad de Estudios Superiores Aragón lugar donde el proyecto se llevó a cabo con el apoyo del “Laboratorio de Seguridad Informática” espacio donde realicé mi estancia académica la cual me permitió introducirme en actividades de investigación y colaboración en temas de Ciberseguridad.

Prólogo

La base de esta investigación surge de los desafíos que presenta la Computación en la Nube mezclado con el Cómputo Móvil que ha sido motivada en base diversos hechos que han resaltado la necesidad de expertis y generación de nuevas metodologías orientadas a la investigación en dispositivos móviles.

Este trabajo ha sido escrito como parte de los requisitos de graduación para la licenciatura de Ingeniería en Computación. El periodo de investigación y redacción de este trabajo de fin de grado ha durado desde septiembre hasta noviembre de 2018.

Se trata de un trabajo que pretende dar una visión completa del panorama actual que ha surgido de la rápida evolución y adaptación de los Smartphones en nuestra vida diaria, sin darnos cuenta que estamos dejando a un lado temas tan importantes como lo es la seguridad y protección de nuestros datos personales, lo que evita la sana convivencia entre nuestras sociedades y este nuevo paradigma.

Para desarrollar esta tesis se han utilizado disciplinas científicas con un sustento sólido como lo son las ciencias del cómputo, también la investigación se ha apoyado en estándares e institutos que son altamente reconocidos por su apoyo en la regulación de las tecnologías de la Información.

Este trabajo está dividido en 5 capítulos, el primer capítulo es una revisión de las bases del Cómputo Móvil las cuales le han permitido adaptarse a los dispositivos móviles, tres capítulos más que resaltan como la tecnología de la Nube ha influido en el desarrollo de entornos para cómputo móvil, posteriormente de comprender la relación de los primero temas, se abre la puerta al contenido del Cómputo forense tanto tradicional como en Smartphones, y los capítulos finales están dedicados al estudio y desarrollo de nuevas propuestas que puedan hacer frente a la temática de este trabajo.

Esta tesis contiene en su parte final una bibliográfica de los libros y artículos utilizados, así como referencias, un índice de figuras y tablas, junto con anexos donde se puede encontrar la información generada por la implementación de los escenarios ficticios.

En la actualidad el Smartphone se puede traducir como una minicomputadora con capacidades de telecomunicaciones, lo que ha provocado que sea vendido globalmente a millones de personas. Las cuales lo han adoptado por su flexibilidad para el trabajo y el entretenimiento

Una de las razones del éxito del Smartphone es en parte a las aplicaciones desarrolladas por terceras partes y el papel que juega el Cómputo en la nube de impulsar el crecimiento de estas aplicaciones.

La combinación de la tecnología del Cómputo en la Nube y el Smartphone ha llevado a que se realicen diversas predicciones. Forrester Research predice que para finales del 2018 el mercado global de la Nube será de 178 billones de dólares, más de 146 billones de dólares que en el 2017 y seguirá creciendo a una tasa de crecimiento anual del 22%. Las plataformas de Nube Pública seguirán siendo el segmento de mayor crecimiento y generarán más 44 mil millones de dólares en ventas en el 2018.

Sin embargo, Gartner por su parte tiene una predicción menos conservadora, que asegura que el mercado mundial de la Nube alcanzará los 260 billones de dólares este año, para el 2021 más del 40% del software se venderá como servicio a lo que Gartner llama Business Process Services.

No obstante, es importante recordar que entre más popular es la tecnología, causa que sea muy atractiva para un uso indebido que un su mayoría hay motivaciones económicas. Por lo que se ha visto un aumento en la utilización de la nube para la propagación de virus con el fin de causar grandes daños económicos a nivel global.

Por lo que debe haber un mejor entendimiento de cómo llevar a cabo análisis forense en dispositivos móviles. Por otra parte, hay muy poco expertis al momento de aplicar metodologías forenses en la Nube, e incluso escases de preparación para poder conducir investigaciones en la Nube.

El objetivo de este trabajo es identificar las implicaciones que tiene el Cómputo en la Nube al conducir una investigación forense en algún Smartphone y probar el software actual para análisis forense en móviles con el fin de resaltar los desafíos que presenta la incorporación de esta nueva tecnología. Además poder proporcionar recomendaciones que puedan ser incorporadas en los procedimientos actuales de investigación forense.

1. Cómputo Móvil

1.1. Introducción al Capítulo

El aspecto más familiar del *Cómputo Móvil* es que lo podemos portar prácticamente en el bolsillo. Hace aproximadamente 4 décadas los teléfonos eran fijos y bastante voluminosos y usados únicamente para llamadas de voz, fue solamente una extensión del cable telefónico que permitió mantenerse en contacto y compartir información con colegas. Actualmente los teléfonos ya no son fijos ni pesados debido al avance tecnológico en la miniaturización del hardware y la necesidad de que fueran a cualquier parte como si fuera un órgano más de nuestro cuerpo, además son usados para enviar mensajes con multimedia, realizar videoconferencias y acceder a grandes bancos de información, adicionalmente son capaces de procesar y transferir información a altas velocidades.

Información es poder, no solamente es un conjunto de datos organizados como ha sido definida por diferentes autores.

> ***La oportunidad de incrementar la productividad, de acceder a la información y a las aplicaciones corporativas en todo momento y desde cualquier lugar, ha llevado a las organizaciones a implementar soluciones de movilidad.***

"*Consiste en datos seleccionados y ordenados con un propósito específico*" [1]

Por mucho tiempo la humanidad no sabía cómo resguardar información y conocimiento de tal forma que fuere fácilmente recuperable y accesible.

Prontamente surgió la necesidad de que la información y las tecnologías de comunicación convergieran para abordar los desafíos en cuanto al almacenamiento y accesibilidad. Hoy en día aun estando en movimiento podemos acceder a grandes recursos de información desde cualquier parte y a cualquier hora.

En las últimas décadas la *movilidad* ha sido redefinida. Debido a que objetos virtuales y físicos ahora están en constante movimiento.

Diferentes hechos y avances tecnológicos surgieron para dar paso a este nuevo paradigma:

1831	Joseph Henry quien demostró el potencial del uso de fenómenos electromagnéticos para comunicaciones de larga distancia.
1837	Samuel F.B. Morse utilizo las propiedades de la electricidad para desarrollar el telégrafo.
1976	Alexander Graham Bell realiza la primera llamada de voz sobre cableado telefónico

Tabla 1 Avances tecnológicos que impulsaron la movilidad

El 4 de octubre a finales de los 50´s la antes llamada Unión Soviética lanzó el primer satélite artificial alrededor del globo terráqueo "Sputnik". En respuesta a estas acciones los Estados Unidos ponen en marcha el proyecto "*ARPA*" (Agencia de Proyectos de Investigación Avanzado) incorporada al Departamento de Defensa con la estricta finalidad de posicionar a los E.U.A como líder en ciencia y tecnología.

Su misión de ARPA incito a iniciar diferentes proyectos de investigación para ayudar a conducir nuevos estudios en el campo de "*Computadoras en Red*". Dando como origen a la conmutación de paquetes. Con la evolución de las computadoras y la conmutación de paquetes en red, el movimiento de bits y bytes avanzaron a un nuevo estado. En las últimas décadas de nuestra realidad se ha visto la evolución del "*ring telefónico*" al Cómputo Móvil.

El primero echo hacia la intersección entre las telecomunicaciones y TI se dio alrededor de los 1965 cuando AT&T uso computadoras para realizar conmutación en (SCE). Por otro lado, la red de conmutación de paquetes permitió acercarse al desarrollo de la idea de comunicación entre computadoras. La World Wide Web (WWW), que empezó en los 1989 como un programa de procesamiento de texto, trajo las facilidades la Telecomunicaciones y TI estableciendo al internet como una herramienta poderosa de medio de comunicación.

Internet satisface 4 necesidades principales de la sociedad: comunicación, compartir el conocimiento, entretenimiento y comercio. Esta convergencia es llamada "Tecnologías de la Información y Comunicación". Gracias a las TIC´s se dio paso a un nuevo paradigma conocido como "*Sociedades basadas en la información*".

Las TIC´s permitieron abordar el problema de la necesidad de acceder a datos, información y conocimiento desde cualquier lugar y a cualquier hora.

El Cómputo Móvil describe la funcionalidad de dispositivos de comunicación compactos, portables e inalámbricos con capacidades de cómputo, que son usados cuando hay una variación respecto a su localización. Requieren de una red inalámbrica para ofrecer movilidad al aire libre y transferencia de una red a otra red.

Los desafíos del Cómputo Móvil son movilidad, aplicaciones, localización, ruteo de datos y mensajes, confiablidad ante desconexión, administración de datos, modelos de transacción, seguridad y movilidad sin preocupaciones.

1.2. Cómputo Móvil

Se han preguntado qué es el Cómputo Móvil o cuáles son las diferencias entre el cómputo con el cual trabajamos diariamente. Básicamente, los sistemas de cómputo móvil son sistemas distribuidos con una red de comunicaciones para comunicarse entre diferentes dispositivos. Bastante sencilla y muy hueca la explicación de esta nueva tecnología que nos está envolviendo rápidamente sin darnos cuenta, e incluso es atrevido decir que hasta cierto punto ha sido muy penetrante y persuasiva en nuestras actividades cotidianas.

Pero en realidad como podemos entender este concepto sin explicaciones vacías y que reflejen sus características y propiedades las cuales le han permitido tener una ventaja enorme la cual le ha hecho posible abrirse paso en la sociedad y en los sectores de mercado más exclusivos.

Pues bien, contextualizando y acotando un poco más el concepto y definiendo al ámbito académico podemos hacer mención de algunas conceptualizaciones más serias y acordes a un panorama de investigación en el cual estamos, por lo cual hare menciones de las que considero más afines y competentes.

"*Una forma de interacción entre el hombre y el dispositivo, en el cual el dispositivo se espera que sea transportado durante un uso normal" [2].*

La conceptualización que más me gusta en lo personal debido a que engloba la esencia de la tecnología es la siguiente.

"*Una tecnología que permite la trasmisión de datos, vía una computadora sin tener que estar conectado a un enlace físico*" [3]

La cual está basando en una recopilación de 3 mayores aspectos; hardware, software y comunicaciones. El concepto de hardware engloba los dispositivos móviles como los teléfonos inteligentes, laptops y sus componentes móviles.

Software son las numerosas aplicaciones móviles que se desarrollan como lo son los motores de búsqueda, procesadores de texto, juegos, etc.

Las comunicaciones incluyen la infraestructura de las redes de comunicación, protocolos y la entrega de datos durante su uso sin importar que el dispositivo se encuentre en movimiento.

El término de “Cómputo Móvil” es usado para describir el uso de dispositivos de cómputo con los cuales se interactúa de alguna manera con sistemas de información central mientras se encuentra lejos de un lugar de trabajo fijo como una oficina. La tecnología del Cómputo Móvil da a sus usuarios la capacidad de crear, acceder, procesar, guardar y comunicar información sin estar preocupados de permanecer en una única localización. Debido al aumento de los sistemas de información en las organizaciones, esta tecnología logra abrirse paso ya que da la oportunidad a que los empleados de dicha organización puedan seguir realizando sus tareas y proyectos sin la necesidad de estar en el centro de datos, y aquellos que antes se encontraban desconectados de los sistemas de información hoy es totalmente opuesto [AWE01].

El Cómputo Móvil es la disciplina de crear plataformas de administración de información, las cuales son libres de las restricciones espaciales y temporales.

La libertad de estas restricciones permite a los usuarios procesar y acceder a información deseada desde cualquier lugar en el planeta. La condición del usuario ya sea estático o en movimiento, no afecta la capacidad de obtener información de las plataformas móviles obligándolas a estar limitadas a una única localización [SAT02].

En plataformas de Cómputo Móvil la información fluye entre unidades de procesamiento a través de canales inalámbricos.

Las unidades de procesamiento (El cliente en un paradigma cliente/servidor) son libres de restricciones temporales y espaciales. Esto quiere decir que las unidades de procesamiento (El cliente) son libres de moverse sobre su entorno mientras se está conectado al servidor.

Esta libertad espacial y temporal provee una poderosa facilidad de permitir a sus usuarios de recuperar o alcanzar cualquier sitio de datos (sito donde el dato deseado es almacenado) y procesar en el mismo sitio (la posición geográfica donde el procesamiento debe ser realizado) desde cualquier lugar. Esta maravilla permite a las organizaciones establecer sus oficinas en cualquier localización.

Este nuevo paradigma tiene sus raíces en los SCP. Servicios de comunicación personal se refiere a una amplia variedad de accesos inalámbricos y servicios de movilidad personal provistos a través de terminales (Cell phones), con el objetivo de habilitar comunicaciones en cualquier momento en cualquier lugar y de cualquier forma. Los SCP están conectados a switches públicos de redes telefónicas para proporcionar acceso a teléfonos móviles.

Hasta aquí se ha presentado el panorama y esencia de esta nueva tecnología, pero ¿Tendrá alguna diferencia con las comunicaciones móviles? Las comunicaciones son necesarias para el Cómputo distribuido.

Las tareas que realiza el Cómputo Móvil requieren comunicaciones Móviles. Pero eso no es todo. Las comunicaciones móviles no resuelven todo el problema que hay de fondo, algunas cuestiones necesitan ser resueltas desde una perspectiva de alto nivel.

Lo que más nos interesa del Cómputo Móvil es lo que podemos hacer con estas facilidades de las comunicaciones móviles. ¿Qué nuevas aplicaciones y funciones pueden ser posibles? Por un momento pensemos en las aplicaciones que frecuentemente usamos.

Si somos sinceros la mayoría de las apps no se adaptan a nuestras necesidades. Por ejemplo, imaginemos que estamos navegando en internet desde nuestro Smartphone y estamos interesados en ir a una tienda de bicicletas de montaña.

¿Qué información obtendremos cuando realicemos la búsqueda "*Bicicletas de Montaña*" a través de un motor de búsqueda como Google? Usualmente obtendremos un sinfín de información que en realidad no nos interesa. En sus orígenes los motores de búsqueda no les importaba quien estaba invocando la búsqueda o la localización desde el lugar en cual se hacía la petición de búsqueda.

Al realizar la búsqueda usted puede escribir "Bicicletas de montaña en CDMX" con la finalidad de hacer su consulta más especifica si fuere posible. En esta primera etapa de los motores de búsqueda de los Smartphones no era agradable que no estuvieran conscientes de su ubicación, o más general que no entendiera contexto de su búsqueda ¿Por lo tanto los resultados arrojados de realizar la búsqueda serian acordes a su contexto? Seguramente estas observaciones han hecho que el Cómputo Móvil sea más productivo.

Consideremos otra aplicación como ejemplo, tomemos algo peculiar y novedoso que en estos días es muy popular como la transmisión de video sobre internet, supongamos que se encuentra viajando en el metro tranquilamente mientras ve una película desde su Smartphone. Las conexiones inalámbricas son muy diferentes de las conexiones alámbricas. Cuando usted dispone de internet por medio de una conexión cableada tendrá un ancho de banda estable disponible para usted y la

aplicación de la cual hace uso. Cuando la película comienza, usted la puede visualizar en una excelente calidad dependiendo el formato de la misma.

Sin embargo, en conexiones inalámbricas el ancho de banda es compartido entre varios usuarios de una forma dinámica. Esto quiere decir que el ancho de banda ya no es dedicado y disponible exclusivamente para usted. Incluso si su Smartphone tiene la capacidad de reservar cierto ancho de banda, el uso de la banda ancha tendrá fluctuaciones debido a la misma naturaleza del medio inalámbrico. Cabe destacar que hay dos tipos de fluctuaciones las cortas y largas. La pregunta interesante aquí es ¿Cómo debería la aplicación y el dispositivo responder a estas fluctuaciones? Un modo es que la aplicación pueda responder de una forma constante, esto quiere decir que no considerara lo que usted está viendo.

El otro enfoque y el más conveniente es que responda acorde al tipo de película y contenido que está visualizando. Por ejemplo, acotemos más lo que queremos dar entender. Usted está viendo una película de acción. La aplicación puede reducir los requerimientos de ancho de banda al cambiar la luminosidad de la aplicación o bajar la calidad del video. Por otro lado, si lo que está visualizando es una conferencia de cualquier tema de su interés, la aplicación puede simplemente centrarse en el audio.

Hasta aquí tenemos distintos puntos importantes a destacar. Las decisiones están basadas en el contenido del video y las decisiones echas pueden envolver al cliente y al servidor [NOB03]. (El cliente necesita informar al servidor que ya no quiere el video, sino solamente el audio).

En esta sección como se darán cuenta estamos examinando el diseño de los sistemas de los dispositivos móviles (software) para darnos cuenta como han ido cambiando y como necesitan seguir evolucionando para adaptarse mejor a nuestras necesidades y adaptarse mejor a este nuevo paradigma móvil.

Como veremos varias de estas mejoras son resultado de la preocupación de proveer mecanismos más sólidos que permitan adaptarse al cambio de entorno y las condiciones del sistema, así como la localización y los recursos disponibles del sistema.

El Cómputo Móvil trata de proporcionar información en cualquier lugar a cualquier hora, o más brevemente hacer cómputo donde sea en el momento que uno lo desee.

Además, esta disciplina trata de lidiar con las limitaciones propias de los dispositivos (hardware). Por ejemplo, las tabletas y Smartphones en su gran mayoría tienen interfaces (pantalla) y teclados lo cuales son alimentados por la batería. Uno de los mayores problemas es como realizar computaciones de una manera energéticamente eficiente. La tecnología de las baterías no está avanzando al mismo ritmo que lo hacen los procesadores, por lo cual no es de esperarse que la capacidad de la batería doble su tasa de rendimiento como lo hacen los

procesadores (Ley de Moore). Uno no tiene que lidiar con estos problemas cuando desarrolla sistemas autónomos o distribuidos, otra cuestión con la que tenemos que tratar es la tolerancia a fallos. Sin embargo, la energía usualmente no es una preocupación tan grande. En dispositivos móviles la energía se convierte en un recurso como lo es el tiempo de procesador o espacio de memoria. Por lo tanto, los fabricantes se ven en la necesidad de desarrollar e implementar técnicas de administración de energía, exactamente como lo hacen los sistemas operativos para gestionar el procesador y la memoria.

Diferentes dispositivos en el Cómputo Móvil tienen distintas capacidades, cualquier actividad colaborativa entre estos dispositivos necesita de una configuración de una entidad de software para tratar con esta heterogeneidad de los dispositivos. Esta entidad es llamada middleware el cual permite que los dispositivos puedan interactuar sin importar el modelo. Cuando un cliente (cliente/servidor) se mueve de un dominio a otro necesita saber que nuevos servicios están disponibles.

1.2.1. Características del Cómputo Móvil

El Cómputo Móvil es realizado mediante el uso del hardware de cómputo tradicional, sistemas, aplicaciones y redes de comunicación. Poderosas soluciones móviles se han hecho recientemente debido al rápido avance de la miniaturización de dispositivos de cómputo, software especializado y la mejora de las comunicaciones.

- **Hardware:** Software y telecomunicaciones que son comúnmente integradas para crear soluciones de Cómputo Móvil están definidas en lo siguiente. Las propiedades del hardware del Cómputo Móvil están acotadas por:

  (1) Tamaño
  (2) Peso
  (3) Microprocesador
  (4) Almacenamiento primario y secundario
  (5) Pantalla
  (6) Batería
  (7) Comunicaciones
  (8) Durabilidad

- **Software:** Dispositivos de Cómputo Móvil hacen uso de una gran variedad de sistemas y software. Los S.O más comúnmente usados son (Windows Mobile, Unix, Android, Google). Estos S.O tienen capacidad de levantar gráficos como si fueran computadoras de escritorio permitiéndole a si a sus usuarios desarrollar sus tareas.

- **Comunicaciones:** La habilidad de los dispositivos móviles de comunicarte con sistemas fijos establecidos es una de las características principales del Cómputo Móvil.

  El tipo y capacidad de comunicaciones impacta significativamente en el tipo de aplicaciones que pueden ser desarrolladas.

  La forma en que un dispositivo de Cómputo Móvil se comunica con otro sistema se puede categorizar de la siguiente formar: (a) conectado, (b) débilmente conectado, (c) lote y (d) desconectado.

  La categoría conectado implica disponibilidad de conexión de alta velocidad continuamente. La capacidad de comunicarse continuamente, pero a baja velocidad, permite a dispositivos móviles conectarse débilmente a un sistema de información fijo. En lote quiere decir que el dispositivo no está continuamente disponible para comunicarse con sistema de información. En este tipo de conexión la comunicación es establecida periódicamente o aleatoriamente para intercambiar o actualizar datos con el sistema de información. Dispositivos móviles pueden operar en modo lote sobre medios de comunicación que son capaces de operación continua, reduciendo el tiempo inalámbrico y tarifas asociadas.

  El estado de desconexión da a los usuarios la oportunidad de mejorar la eficiencia, realizando cálculos, almacenando contactos y otras tareas no orientadas a conexión. Este último modo de conexión es un poco menos interesante debido a que el móvil se encuentra incapaz electrónicamente de interactuar e intercambiar información con sistemas de información en organizaciones o corporativos. Intercambiar información desde un equipo desconectado solo se puede realizar manualmente, es decir transfiriendo la información deseada o copiándola al sistema de interés.

Sin embargo, las características técnicas y físicas que describimos no es lo único que les ha dado a estos dispositivos la capacidad de trascender en nuestra sociedad y ser bien aceptados entre nosotros, quizás hay una relación muy estrecha que compartimos los seres humanos y los Smartphones, lo cual nos ha hecho permanecer constantes en el día a día en este entorno. Pero ¿Cuál es esta estrecha relación, si es que la hay?

Los seres humanos hemos destacado en reino animal por tener la capacidad de evolucionar y posicionarnos en la cima de la cadena alimenticia. Casi podemos afirmar que es innegable que hemos tenido la oportunidad de adaptarnos rápidamente a distintas situaciones ¿Cuáles son esas técnicas mediante las cuales hemos sido capaces de adaptarnos a diferentes ambientes? ¿Podemos incorporar estas técnicas a nuestros sistemas de cómputo? Cualquiera que haya ocupado una computadora o un dispositivo móvil de forma seria, le gustaría que estos fueran más resistentes a fallos, adaptativo a nuestras necesidades y circunstancias.

Los sistemas y aplicaciones fallan por diversas razones. Lo más frustrante es cuando fallan sin ninguna razón aparente. Usted instala una aplicación y otra aparentemente no relacionada deja de funcionar. En algunas ocasiones quisiéramos que nuestros equipos aprendieran de nuestro pasado para que actúen proactivamente y apropiadamente. Hacer que los sistemas móviles sean resistentes a fallos y adaptables no es un trabajo sencillo. A los seres humanos nos tomó millones de años colocarnos en la cumbre de cadena alimenticia. Las computadoras como las conocemos actualmente no llevan ni siquiera 100 años.

La visión del Cómputo Móvil es ser capaz de desempeñarse sin problemas con su dispositivo móvil mientras continuamente realiza procesos de computación y mantiene comunicaciones simultáneamente sin interrupciones. Varios avances tecnológicos en distintas fronteras como lo es la seguridad, privacidad, asignación de recursos, recarga de batería han hecho esto posible. Otra característica que podemos destacar a soluciones de problemas de Cómputo Móvil es la habilidad de adaptarse a cambios dinámicos en ambientes de cómputo y comunicaciones. La agilidad de los dispositivos de reaccionar a cambios en el entorno computacional y continuar realizando sus tareas de cómputo interrumpidamente es una nueva medida de rendimiento en sistemas de Cómputo Móvil [SAT04].

Alguna de las características más importantes del Cómputo Móvil que podemos resaltar y resumir son las siguientes:

1. **Movilidad:** Nodos móviles en redes de cómputo móvil pueden establecer conexión con otros, incluso en nodos fijos en la red cableada a través ESM mientras se está en movimiento.

2. **Transparencia:** Es la habilidad del sistema de esconder ciertas características de su configuración e implementación de los usuarios.

3. **Diversidad en condiciones de red:** Normalmente las redes usadas por los nodos móviles no son únicas, cada red puede ser una red cableada con banda ancha o una inalámbrica WAN, o incluso en un estado de desconexión.

4. **Frecuentes desconexiones y consistencia:** Como la limitación del rendimiento de la batería, afecta y recae a la comunicación inalámbrica, sin olvidar las condiciones de la red. Los nodos móviles no siempre mantendrán la conexión, por cual a pesar de las desconexiones debe mantener una consistencia con las redes inalámbricas.

5. **Redes de comunicación Asimétrica:** Servidores, puntos de acceso y otros ESM habilitan una fuerte capacidad de enviar/recibir información, a comparación de los nodos móviles que es un poco más débil comparativamente, por eso el ancho de banda en la comunicación y la sobrecarga entre el enlace ascendente y el descendente son discrepantes.

6. **Baja Confiabilidad:** Debido a que la recepción de señal es susceptible a la interferencia y monitoreo en la transmisión de datos, se debe considerar en los sistemas de red de Cómputo Móvil, las bases de datos, terminales, aplicaciones, abordar temas de seguridad y privacidad con la finalidad de lograr desarrollar estándares que apoyen a cumplir estos problemas de seguridad.

7. **Desafíos:** Comparado con las redes telefónicas cableadas, el Cómputo Móvil encara varios problemas y desafíos en diferentes aspectos, así como la distorsión de la señal, cuestiones de seguridad, limitación de la batería, baja capacidad de cómputo y mucho más la calidad del servicio en algunas redes de Cómputo Móvil es más fácil que sea afectada por el clima, relieves naturales y construcciones realizadas por el hombre.

1.3. Redes Móviles

Los dispositivos móviles pueden conectarse a una red de comunicaciones a través de un proveedor telefónico o mediante una red inalámbrica. Los sistemas celulares 1G tuvieron muchas deficiencias, como una pésima calidad en llamadas, insuficiencia de señal y fuga de comunicaciones cifradas.

Para sobrepasar dichos obstáculos se introdujo 2G lo cual abrió las puertas al desarrollo de nuevas aplicaciones desde funciones como video conferencias, motores de búsqueda, correo electrónico, pero cómo había de esperarse 2G comenzó hacer ineficiente debido a que el uso de estas nuevas funciones demandaba un gran uso de ancho de banda.

A pesar de que los sistemas 2G fueron un gran excito en términos de aceptación de mercado, estaban limitados por la máxima velocidad de transferencia de datos. Por ejemplo, si consideramos una transferencia de 2MB podía tomar hasta 28 minutos.

Por consecuente hubo la necesidad de brincar a 3G la cual haría frente a las necesidades de ese entonces y tendencias futuras del mercado. Smartphones como el iPhone y Google-Phone fueron diseñados especialmente para comunicaciones 3G y estos dispositivos son los más populares en el mercado hasta hoy en día. A pesar de que 3G permitió la trasmisión de multimedia y roaming global a través diferentes telefónicas, actualmente se encuentra fuera de cobertura.

Similar a las comunicaciones cableadas, comunicación inalámbrica también necesitan de un trasmisor de señales que puedan ser propiamente recibidas y descifradas por un receptor. Comunicaciones bidireccionales requiere un par de transceptores – cada transceptor consiste de un trasmisor y un receptor. A pesar de que es posible para un transceptor ser diseñado para poder trasmitir y recibir al mismo tiempo, por varias razones como el costo por unidad, el peso, un transceptor es diseñado con componentes compartidos (antenas). Por lo tanto, comunicaciones bidireccionales en redes inalámbricas son usualmente half-duplex. Dependiendo de varios factores como la potencia utilizada para la amplificación de señales inalámbricas, propiedades del medio, sensibilidad del receptor y la interferencia de la señal de otras fuentes, una señal de transceptor inalámbrica puede ser recibida a cierta distancia de este.

Los transceptores inalámbricos están diseñados para generar y percibir señales dentro un cierto rango de frecuencia, llamado banda de frecuencia [DAV05].

Las propiedades de propagación de la señal varían con la frecuencia. A medida que la frecuencia de la señal aumenta, su penetración disminuye y la distancia con la cual se puede propagar dentro del medio disminuye.

Por lo tanto, frecuencias más altas (como el infrarrojo) el transceptor tiene que estar en la línea de la señal de cada dispositivo. A frecuencias bajas (como la radio

frecuencia) la línea de la señal no es requerida, debido a que la señal puede ser reflejada por varios objetos y llegar al transceptor desde varias rutas.

No olvidemos que las señales inalámbricas presentan desvanecimientos. Hay dos tipos de desvanecimiento: de corto plazo y largo plazo. Esto resulta en una severa variabilidad en la disponibilidad de banda ancha del enlace inalámbrico.

Desvanecimiento en un medio inalámbrico resulta en una mayor proporción de error de bit que en medios de comunicación cableada.

1.3.1. Redes de Área local y direcciones IP móviles

Un punto de acceso (AP) es usualmente un transceptor conectado a una red alámbrica. Un dispositivo móvil puede establecer conexión mediante un enlace bidireccional en un punto de acceso utilizando protocolos comunes como IEEE 802.11. Por supuesto que el dispositivo debe tener el protocolo indicado y hardware que le permita realizar dichas conexiones. LANs inalámbricas están comenzado a usarse para proporcionar conexiones inalámbricas en sitios públicos como aeropuerto, cafeterías, escuelas, centros comerciales, hospitales y hogares.

Las redes LAN permiten movilidad, lo cual restringen los puntos de acceso por su área de cobertura. Para tecnologías de corto alcance el radio de cobertura pueden ser unos pocos metros (bluetooth), mientras que para tecnologías de largo alcance esto puede variar desde varios cientos hasta varios miles de kilómetros como por ejemplo celulares satelitales. Protocolo como IP móviles proporcionan una amplia movilidad. IP móviles es una extensión del protocolo de internet para soportar sin problemas movilidad a través de distintas redes [RAJ06].

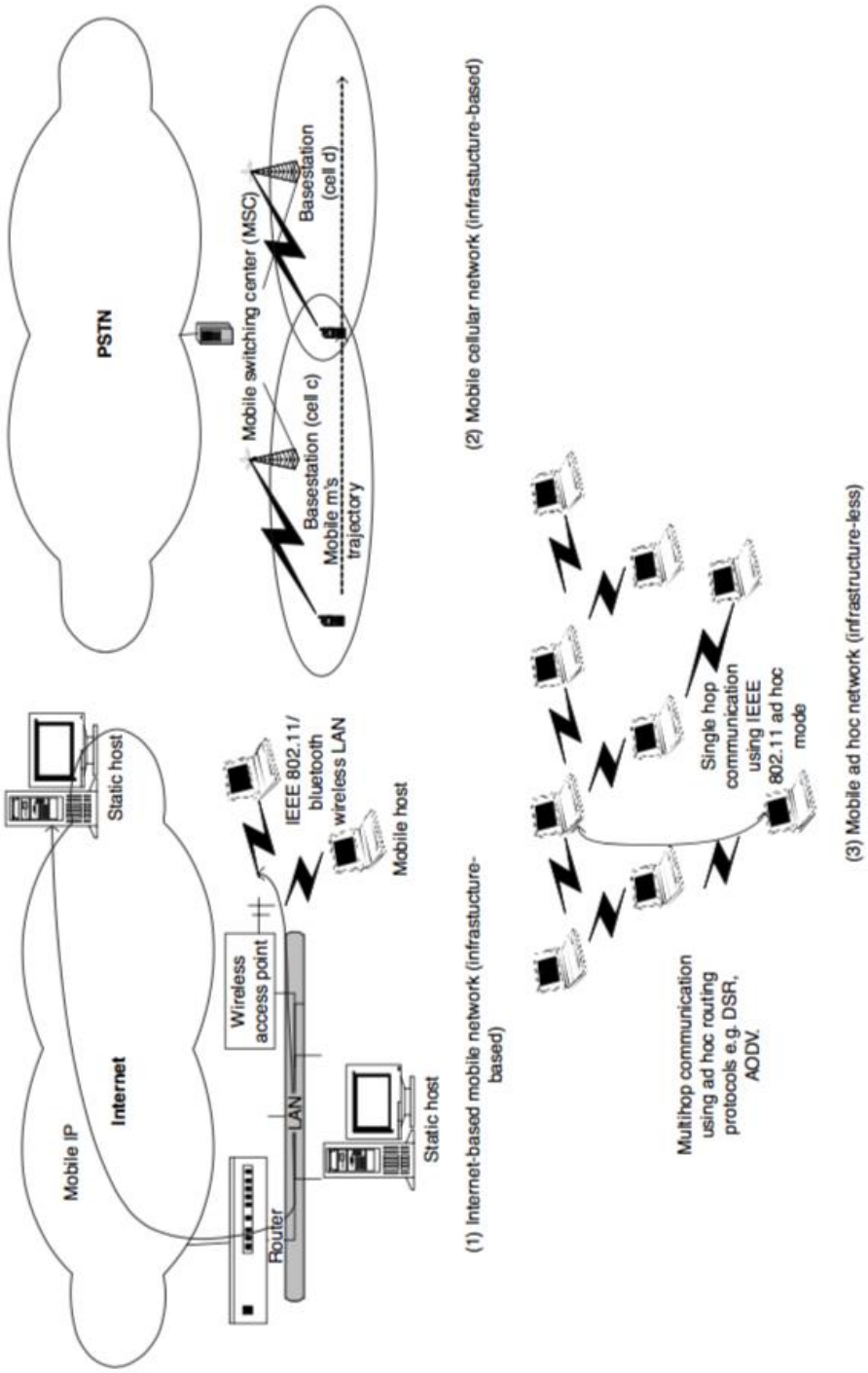


Figura 1 Redes de Área Local y direcciones IP Móviles

Frank. A. (2004). Ilustración de los diferentes tipos de redes inalámbricas. Obtenido de Fundamentals Of Mobile and Pervasive Computing: 2004 McGraw-Hill.

1.3.2. Redes celulares inalámbricas

En redes celulares inalámbricas, varias estaciones base están desplegadas, en cada una de las localizaciones de servicio que cubra las distintas regiones establecidas por el proveedor. Estas estaciones se pueden comunicar con otras y computadoras estáticas mediante un cable.

El área de cobertura es nombrada célula. Cuando un dispositivo móvil activo (activo se entiende por aquel dispositivo que se encuentra envuelto en una comunicación) se mueve fuera del área de cobertura de la estación base, dicha estación intenta entregarlo a otra estación base para continuar la comunicación [IMI07]. En redes celulares, células de estaciones bases contiguas se superponen para permitir una transferencia de un dispositivo móvil de una estación a otra sin problemas. Además, en telefonía inalámbrica la disponibilidad del rango de frecuencia es dividida en canales. Un canal es lo suficiente amplio cuando puede acomodar un circuito de voz (mínimo 64 kbps). Adicionalmente células utilizan diferentes canales para reducir la interferencia.

2. Cloud Computing (Cómputo en la Nube)

2.1. Introducción al capitulo

La promesa revolucionaria del Cómputo en la Nube de transformar el cómputo en una quinta utilidad, después del agua, gas, electricidad y telefonía tiene el potencial de cambiar la cara de las Tecnologías de la información. Especialmente en el aspecto de la entrega del servicio y administración del servicio. Aunque hay numerosas formas de definir el fenómeno del Cómputo en la Nube, se presenta la que fue dada por el NIST que se enuncia de la siguiente manera

"Es un modelo que permite el acceso a recursos de cómputo en la red bajo demanda que pueden ser rápidamente aprovisionados y entregados con un mínimo de esfuerzo administrativo o interacción del prestador de servicios" [4]

Es una agrupación de redes, servidores, almacenamiento, aplicaciones y servicios. Vagamente hablando, Cómputo en la Nube representa una nueva forma de desplegar tecnología de cómputo, para darle al usuario la habilidad de acceder a recursos, e información compartida usando internet. La nube por sí misma es una red de centros de datos, cada una compuesta de varios cientos de computadoras trabajando juntamente que pueden desempeñar funciones de software en una computadora personal, proporcionando al usuario poderosas aplicaciones, plataformas, y servicios entregados a través de internet. Es en esencia un conjunto de servicios habilitados en red que son capaces de ofrecer computación escalable, personalizable y de bajo costo en demanda, la cual puede ser accedida en una forma simple y penetrante por una amplia variedad de usuarios dispersos geográficamente.

La nube además asegura la aplicación de la calidad del servicio garantizada a sus usuarios. Por eso la computación en la nube ofrece a sus usuarios un gran grupo de recursos de manera transparente a través de mecanismos para la administración de recursos por eso el usuario puede acceder ubicuamente, sin afectar la calidad del desempeño. La forma ideal de describir Cómputo en la Nube puede ser con la siguiente frase "*Todo como servicio*".

Sin embargo, la computación en la nube no implica que solo consista de una sola nube. El término acuñado nube hace referencia a internet, la cual en sí misma es una red de redes, Además no todas las formas cómputo remoto es Cómputo en la Nube, no es más que servicios ofrecidos por un proveedor que podría tener sus propios sistemas en algún lugar determinado.

Cientos de años atrás, las industrias dejaron de generar su propia energía con las máquinas de vapor y el carbón como elemento principal, para conectarse a la nueva red eléctrica.

El económico despliegue de energía eléctrica de ciertas utilidades no solo cambio la forma en que operaban los negocios, sí no que dio pasó a una reacción en cadena de una transformación económica y social que trajo la existencia del mundo moderno. Hoy en día estamos viviendo una revolución.

La conexión a internet global de redes de computadoras, centros de procesamiento de información masiva han comenzado a llevar, aplicaciones, software y código hasta nuestras casas y oficinas. Es el momento del cómputo en lugar de electricidad el cual se está convirtiendo en una nueva utilidad.

La computación en la nube ha integrado varios aspectos positivos de diferentes paradigmas de cómputo, resultando en un modelo hibrido que ha evolucionado a través de los años teniendo sus orígenes en los años 1990 cuando John McCarthy declaro que “Computar podía ser algo organizado como una utilidad pública”.

Comenzó su evolución con la concepción del cómputo en malla que es un paradigma del cómputo distribuido. Cómputo en malla es diferente, comparado con el Cómputo en la Nube ya que ofrece una recopilación virtual de recursos de cómputo. El cómputo en malla particularmente se refiere a controlar muchas computadoras como una sola. Dando como resultado la administración de muchas computadoras con la finalidad de ejecutar una tarea específica o alguna aplicación.

Por otra parte, el Cómputo en la Nube se refiere a controlar múltiples recursos, incluyendo los recursos del sistema, para distribuir un servicio integral al cliente.

En el cómputo en malla la concentración de algún trabajo se trata de trasladar a una computadora deseada que generalmente está aislada. En pocas palabras en este tipo de cómputo hay una aglomeración de servidores en los cuales una tarea muy grande puede ser dividida en piezas más pequeñas y ser ejecutadas simultáneamente. Desde esta perspectiva, una malla puede visualizarse como un único servidor virtual. Las mallas involucran aplicaciones para acomodar las interfaces del software de la malla, mientras que dentro del entorno de la nube junto con las extensivas TI involucra recursos de negocio, como aplicaciones, servidores, y almacenamiento.

En los 1990, la teoría de la virtualización se extendió más allá de los servidores virtuales aun nivel más avanzado de abstracción. Presentando clusters como plataformas de virtualización para propósitos de cómputo hacía modelos de negocios medidos. Actualmente el software como servicio (SaaS) ha aumentado la intensidad de la virtualización de las aplicaciones con un modelo de negocios comercial, pero no por el consumo de recursos. La idea del Cómputo en la Nube tuvo que evolucionar de las mallas a la SaaS

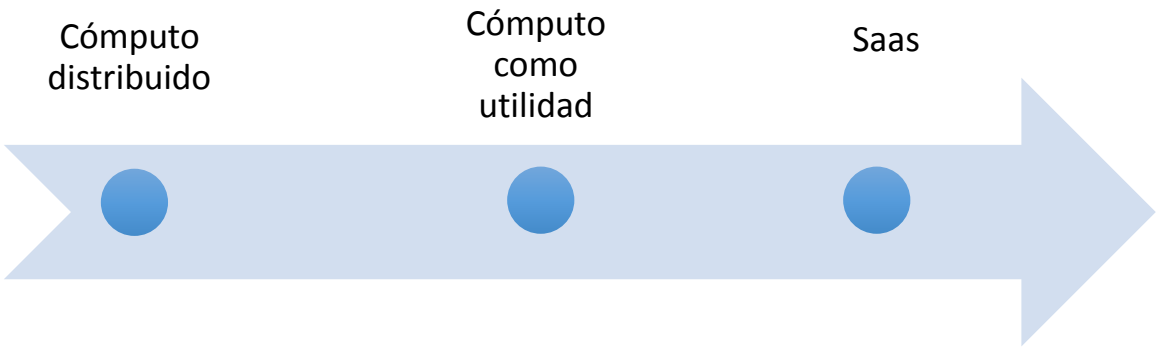


Figura 2 Evolución del Cómputo en la Nube

El esquema anterior muestra la evolución del Cómputo en la Nube. La evolución de la computación distribuida, a cómputo como utilidad, posteriormente a Saas, y finalmente Cómputo en la Nube.

Las empresas prefieren distribuir sus recursos entre Nubes privadas y públicas, basadas en sus especificaciones. Nubes públicas representan servicios a los consumidores, y negocios con sus consumidores en internet.

El poder de la Nube es la administración de su infraestructura, la cual es promovida por el progreso de las tecnologías de la virtualización, para supervisar un mejor consumo de los recursos básicos, mediante un aprovisionamiento automático, supervisado y reequilibrado. Muchas empresas como Google, IBM, Amazon, y Microsoft han fabricado centros de datos gigantes basados en capacidades de cómputo para mantener la asistencia de su servicio web en todo el mundo.

Aplicaciones de ERP son enormes soluciones de software empresariales, los cuales son convencionalmente razonables para empresas muy grandes con mucho presupuesto de T.I.

Por el contrario, las empresas que venden estos servicios están esperanzados en que puedan alcanzar pequeños a medianos negocios al desarrollar aplicaciones complicadas haciéndolas disponibles como servicios de software basados en internet. Las capacidades de la SaaS como lo es distribuir aplicaciones muy costosas a precios accesibles continuara expandiéndose.

La nube está basada en la idea de generar facilidad de cómputo en demanda.

Equivalente al hecho de ir a un auto servicio y ordenar una comida, o conectar tu teléfono a la corriente para recargar su batería, similarmente la computación en la nube intenta crear un nuevo paradigma donde la mayoría de las funciones y características de computadoras individuales puedan ser compartidas sobre internet. Por eso si profundizamos en la filosofía del Cómputo en la Nube nos daremos cuenta que el concepto data de la era de los "*Mainframes*" donde recurso como la (memoria y capacidades de cómputo) de poderosas computadoras centralizadas que eran propiedad de grandes organizaciones para ser usadas y compartidas en una pequeña área geográfica.

Hoy en día el Cómputo en la Nube presume de una arquitectura que amenaza con remplazar a las súper computadoras y quizás hasta las redes de súper computadoras al ofrecer la facilidad de acceder a recursos de cómputo a través de internet. En el pasado, cuestiones como escases de banda ancha, pérdida de control, confianza y factibilidad probaron ser los mayores obstáculos en el camino para hacer posible el concepto de Nube.

Actualmente la mayoría de esas limitaciones han sido superadas, también se están tomando contramedidas para resolver dichas cuestiones. Rápido ancho de banda, virtualización y mayormente habilidades que rodean a la Nube han ayudado en la realización de este paradigma.

La primera generación de Cómputo en la Nube la cual se involucró a lo largo de la "*Era del internet*" fue principalmente orientada para servicio de comercio en línea.

La actual generación de servicios en la Nube ha progresado escalando a nuevos peldaños que ahora incluye "Servicios de TI" que pueden ser considerados y visualizados como consumo de servicios de internet. El uso estandarizado de alta infraestructura virtualizada y aplicaciones, hace que las TI puedan ser manejadas a altos grados de automatización y consolidación, reduciendo a si el costo de mantenimiento de soluciones existentes.

En estos días la red es el cómputo, las capacidades de la nube como recurso centralizado puede coincidir con escalas industriales. Esto implica que el poder de procesamiento involucra miles de computadoras incrustadas en la red incluso hasta ha superado las capacidades de súper computadoras de alto rendimiento. Al hacer

esta tecnología disponible a través de la red sobre las bases de la demanda y el servicio.

La Nube mantiene la promesa de darle a individuales, organizaciones, empresas y gobiernos alrededor del mundo de ofrecer acceso a poder de cómputo extraordinario desde cualquier localización y cualquier dispositivo. Es un hecho que los datos y la información están creciendo a un paso vertiginoso.

A si la siguiente generación de Cómputo en la Nube permitirá acceder a la información a través de servicios que están establecidos en el contexto de la experiencia del consumidor. Esto es significativamente diferente – lo que significa que los datos podrán ser separados de las aplicaciones – un paradigma donde el procesamiento puede ser roto en piezas más pequeñas y automatizado a través de una recopilación de servicios, entrelazados con el acceso masivo a datos.

Eliminará la necesidad de grandes escalas, aplicaciones complejas construidas alrededor de procesos monolíticos. Los cambios pueden venir acompañados con el replanteamiento de los modelos de servicio, y la integración lograda al subscribirse a nuevas fuentes de información. Esto creara nuevas conexiones, nuevas capacidades y nuevas innovaciones que serán incomparables con lo actualmente existente. A continuación, mostramos una tabla desplegando los servicios que actualmente se pueden acceder.

	Cloud 1 E-business como servicio	Cloud 2 TI como servicio	Cloud 3 Todo como servicio
Fuerza primaria	1990 1995 2000	2005 2010	2015 2020
	Cadena de suministro basada en e-comerce	Consumo de servicios de TI Costos bajos de TI	Penetrante consumo de servicios y negocio
Orientación tecnológica	Diseño de aplicaciones basadas en web Protocolos internos 3 nivel de arquitectura	WEB 2 Virtualización Tecnología de plataformas basadas en clousters	Concientización de datos orientados a servicios Ecosistemas horizontales y verticales de Nube
Diseño organizacional de TI	Organización entorno a dominios de TI	Organización basada en consumo de suministros de ti Servicio céntrico	Organización en torno al valor de la red Servicio céntrico

Tabla 2 Segmentación del Cómputo en la Nube

Las estimaciones que se muestran en la tabla indican que la mayoría de personas accederán a aplicaciones en línea y compartirán información a través de servidores remotos en la red, en lugar de depender primariamente de herramientas e información guardada en sus computadoras. Se predice que el Cómputo en la Nube se vuelva más dominante que el cómputo tradicional en la próxima década.

En otras palabras, la mayoría de los usuarios realizará la mayoría de sus tareas y necesidades de procesamiento a través de conexiones a un servidor que será operado por el proveedor de servicios. Más expertos en estos temas y organizaciones creen que el Cómputo en la Nube continuara expandiéndose cada vez más y se volverá dominante en transacciones de información, debido a que ofrece muchas ventajas, permitiéndole a usuarios tener fácil acceso instantáneo e individualizado a herramientas que necesitan sin importar donde estén y desde que dispositivo lo soliciten.

Para validar esta información, PEW INTERNET, & AMERICAN LIFE PROJECT ha llevado a cabo una encuesta con una gran diversidad de poblaciones, que muestra que el 71% de los encuestados creen que para el 2020 la mayoría de las personas no desearan trabajar en sus oficinas con un software ejecutándose en su computadora de escritorio. En lugar de eso trabajaran en alguna aplicación basada en internet como Google DOCS, y en aplicaciones desde su Smartphone. Sin embargo, la calidad del servicio garantizara la inter operatividad entre plataformas existentes, y concientización acerca de la seguridad son de las cuestiones que seguirán abrumando el crecimiento de la Nube.

2.2. Características del Cómputo en la Nube

El Cómputo en la nube está basado en 2 técnicas principales, 1) Arquitectura orientada a servicio y 2) Virtualización.

Arquitectura Orientada a Servicio (AOS): Desde que comenzó el paradigma de la Nube todas las tareas son ejecutadas como "*Servicio*" prestado al usuario. Esta arquitectura comprende un conjunto de diseño flexible usados durante la fase de desarrollo e integración del sistema [STR08]. El despliegue basado en AOS proporcionara un paquete de servicios ligeramente integrado que podrán ser usados dentro de múltiples dominios de negocios. Habilitar tecnologías en AOS permitirá que servicios sean descubiertos, compuestos y ejecutados. Por ejemplo, cuando un usuario final desee realizar una cierta tarea, se hará un despliegue de servicios para conocer que recursos son necesarios para completar dicha tarea. Esto será seguido por una composición de servicios los cuales planearan la ruta para proporcionar la calidad y funcionalidad deseada del usuario final.

Virtualización: El concepto de la virtualización es para aliviar al usuario de la compra de recursos e instalaciones. La nube trae los recursos al usuario. La virtualización se refiere al hardware (La ejecución de un software en un ambiente separado de la configuración de los recursos del hardware), memoria (Dando la impresión de que se cuenta con la memoria suficiente para ejecutar aplicaciones), almacenamiento (El proceso es completamente abstracto, almacenamiento lógico desde un almacenamiento físico), software (El hospedaje de múltiples entornos virtualizados dentro de un único S.O.), datos (La presentación de los datos en una capa abstracta, independiente de la configuración de la base de datos, almacenamiento y estructuras). La virtualización se ha convertido en un ingrediente indispensable en todas las nubes; la razón más obvia es la fácil encapsulación y abstracción [ROC09]. Entre otras razones importantes por las cuales la nube tiende a utilizar virtualización son:

- **Consolidación de aplicación y servidor:** Como muchas aplicaciones pueden ser ejecutadas en el mismo servidor los recursos pueden utilizarse más eficientemente.

- **Configuración:** Como los recursos para varias aplicaciones pueden variar significativamente, la virtualización es la única solución para la personalización y agregación de recursos que no son logrados a nivel de hardware.

- **Aumento en la disponibilidad de aplicaciones:** La Virtualización permite una rápida recuperación ante interrupciones no planeadas, debido a que el ambiente virtual puede ser fácilmente restaurado o migrado sin interrupciones en el servicio.

- **Responsivas mejoradas:** Suministro de recursos, monitorización y mantenimiento pueden ser automatizados, y algunos recursos pueden ser recuperados y re usados.

Adicionalmente los beneficios de la virtualización tienden a facilitarle a la Nube el cumplimiento estricto de los Acuerdos de Nivel de Servicio, requerimientos de negocio establecidos que de otra manera no pueden ser logrados de una forma económicamente eficiente [GSC10].

Las cinco características esenciales de la sube son amplio acceso a la red, rápida elasticidad, servicio medido, auto servicio en demanda y agrupamiento de recursos.

Estas cinco características esenciales demuestran como la Nube se diferencia de los otros enfoques del cómputo.

- **Agrupamiento de recursos:** Recursos de cómputo como, almacenamiento, procesamiento, memoria, ancho de banda y máquinas virtuales son agrupadas juntas para ofrecer un modelo de servicio de multi-tenencia. Diferentes recursos físicos y virtuales son asignados al usuario de acuerdo a sus necesidades. Los clientes no tienen conocimiento preciso de la ubicación de los recursos proporcionados. Sin embargo, los usuarios podrían ser informados a un alto nivel de abstracción como, el país o el lugar donde los datos son almacenados en el centro de datos.

- **Amplio acceso a red:** Permite a dispositivos como, computadoras, Smartphones acceder a los servicios de la Nube vía red. El servicio de la

Nube incluye mecanismos estandarizados y otros servicios basados en software tradicionales de este paradigma.

- **Rápida elasticidad:** La rápida elasticidad proporciona recursos flexibles, fácilmente escalables (Aplicaciones, almacenamiento y servidores). Dicha característica le permite a los usuarios escalar hacía arriba y hacia abajo los recursos en demanda, rápidamente y elásticamente en cualquier momento.

- **Servicio medido:** El uso de los recursos de la Nube son constantemente monitorizados aprovechando las capacidades de medición. La medida del servicio, puede controlar y optimizar el uso de recursos y luego informar al usuario, este modelo se conoce como “Pague a medida que avanza”.

- **Auto servicio bajo demanda:** Esta característica permite al usuario ordenar y administrar servicio a través de un portal web o interfaces de administración sin interacción humana con el proveedor de servicios.

Figura 3 Características del Cómputo en la Nube
Imagen obtenida de: http://www.magazcitum.com.mx/?p=866#.WsVsVGbmF-U

2.3. Modelos de servicio en la nube

El Cómputo en la Nube es un modelo que permite a los usuarios finales acceder a un grupo de recursos compartidos, como cómputo, redes, almacenamiento, base de datos y aplicaciones como un servicio bajo demanda sin la necesidad de tener que comprarlos. Los servicios proporcionados y administrados por el proveedor de servicios, reduciendo la fatiga del usuario al tener que gestionarlos de su parte.

El NIST define 3 modelos básicos de servicio llamados IaaS, PaaS, SaaS [LIU11].

- **IaaS:** La habilidad dada a los arquitectos de infraestructuras de desplegar o ejecutar cualquier software sobre los recursos de cómputo proporcionados por el proveedor de servicios. Por lo tanto, los arquitectos de infraestructura están exentos de mantener el centro de datos o la infraestructura subyacente.

  Los usuarios son responsables de administrar las aplicaciones que están siendo ejecutadas en lo más alto de la pirámide de la infraestructura del proveedor de servicios. Generalmente, los servicios IaaS proporcionados desde el centro de datos de la Nube del proveedor de servicios. Los usuarios finales pueden acceder a los servicios desde sus dispositivos a través interfaces de línea de comando o interfaces de aplicación programada proporcionadas por el proveedor de servicios. Algunos proveedores de servicios populares son Amazon Web Services, Google Compute Engine, OpenStack y Eucalyptus.

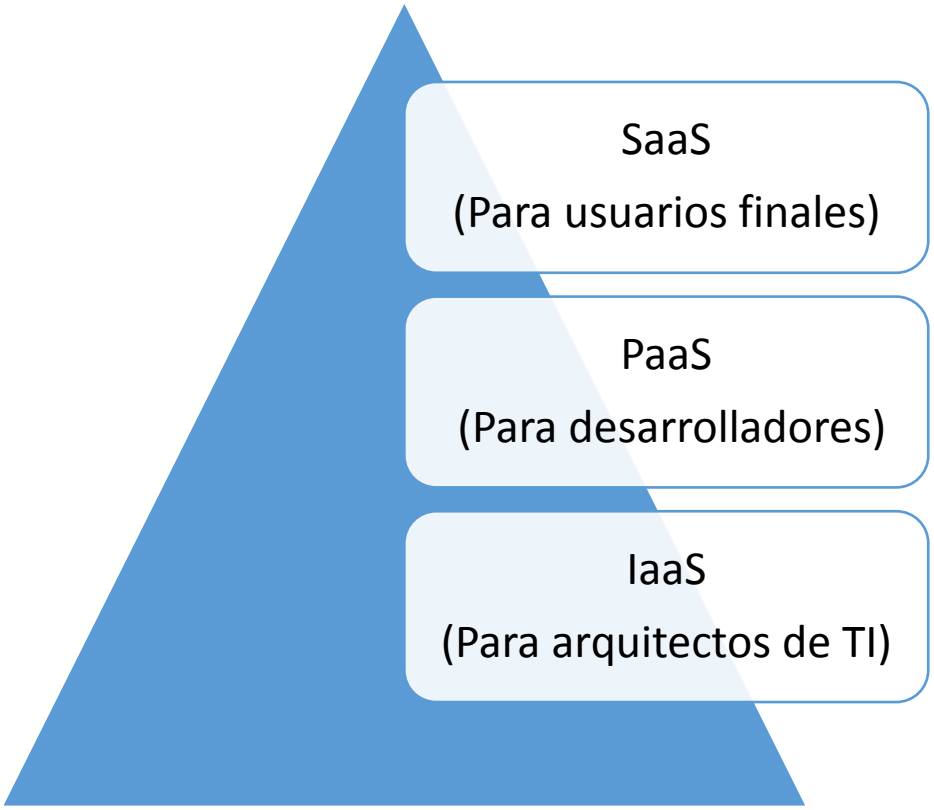


Figura 4 Modelos de Servicio

- **PaaS:** La facilidad dada a los desarrolladores para crear cualquier aplicación sobre la plataforma de desarrollo proporcionada por el proveedor de servicios. Es por eso, que los desarrolladores están exentos de gestionar la plataforma de desarrollo y la infraestructura subyacente. Aquí, los desarrolladores son responsables de administrar sus aplicaciones desarrolladas y configurar el ambiente de desarrollo. Generalmente los servicios como PaaS son proporcionados por el proveedor de servicios en instalaciones e infraestructuras dedicadas. Los programadores pueden acceder a la plataforma de desarrollo mediante internet a través de la WEB. Algunos ejemplos populares son Google App Engine, Forece.com, Red Hat OpenShift, Heroku y Engine Yard.

- **SaaS:** La capacidad dada a los usuarios finales de acceder a las aplicaciones sobre internet que son hospedadas y administradas por el proveedor de servicios. Los usuarios finales pueden acceder a los recursos desde

cualquier navegador. Algunas populares son Saleforce.com, Google Apps y Microsoft office 365.

Los diferentes modelos de servicio de la Nube están dirigidas a diferentes objetivos de audiencia. Por ejemplo, el modelo de servicio IaaS su objetivo son los arquitectos de las Tecnologías de la Información. PaaS está dirigido a desarrolladores y SaaS abarca los usuarios finales. Basándose en la subscripción del servicio la responsabilidad de las de las audiencias específicas puede variar como se muestra en la siguiente figura.

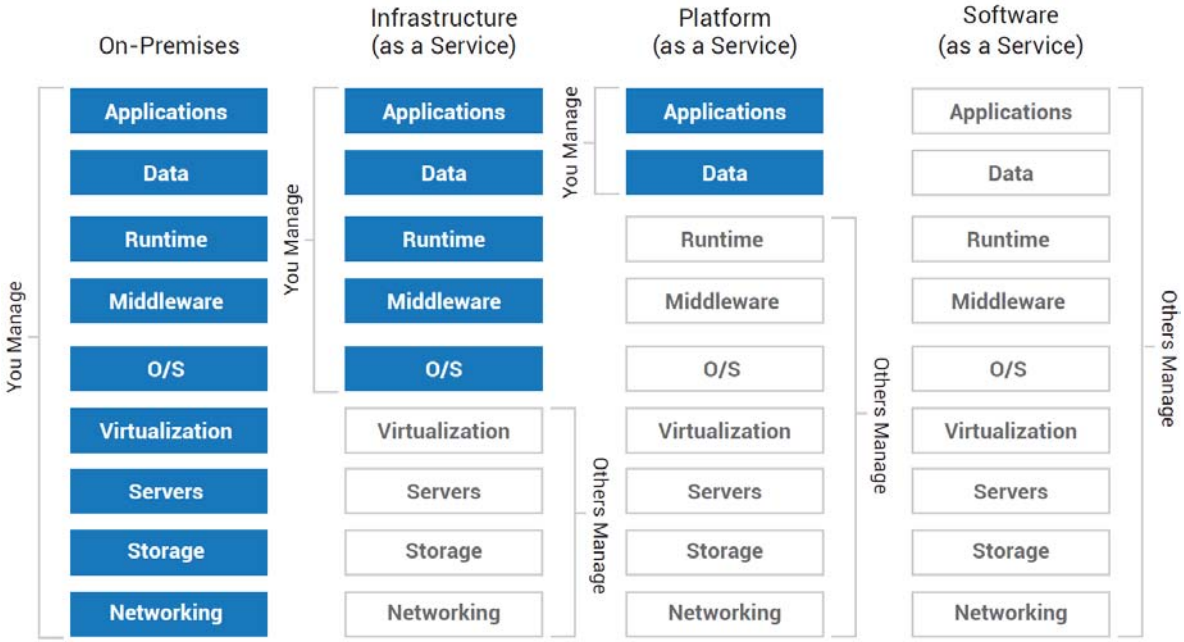


Figura 5 Objetivo de los diferentes modelos de despliegue

Imagen obtenida de: https://mycloudblog7.wordpress.com/2013/06/19/who-manages-cloud-iaas-paas-and-saas-services/

En IaaS, los usuarios finales son responsables de mantener la plataforma de desarrollo y las aplicaciones ejecutándose en lo más alto de la infraestructura subyacente.

Los proveedores de IaaS son responsables de mantener el hardware subyacente como se muestra en la figura anterior. En PaaS los usuarios finales son responsables de administrar las aplicaciones que ellos han desarrollados. La Infraestructura subyacente será sostenida por el proveedor de servicios. En SaaS, los usuarios finales son libres del mantenimiento de la infraestructura, plataforma de desarrollo y aplicaciones que ellos están usando. Todo el mantenimiento será llevado a cabo por el proveedor de SaaS como se muestra en la figura anterior.

Los diferentes modelos de servicio del Cómputo en la Nube pueden ser desplegados y entregados mediante cualquier modelo de despliegue. El NIST define 4 tipos diferentes de modelos de despliegue, llamados Nube pública, Nube privada, Nube comunitaria y Nube hibrida. El servicio entregado por la Nube puede ser a través de cualquiera de los modelos de despliegue.

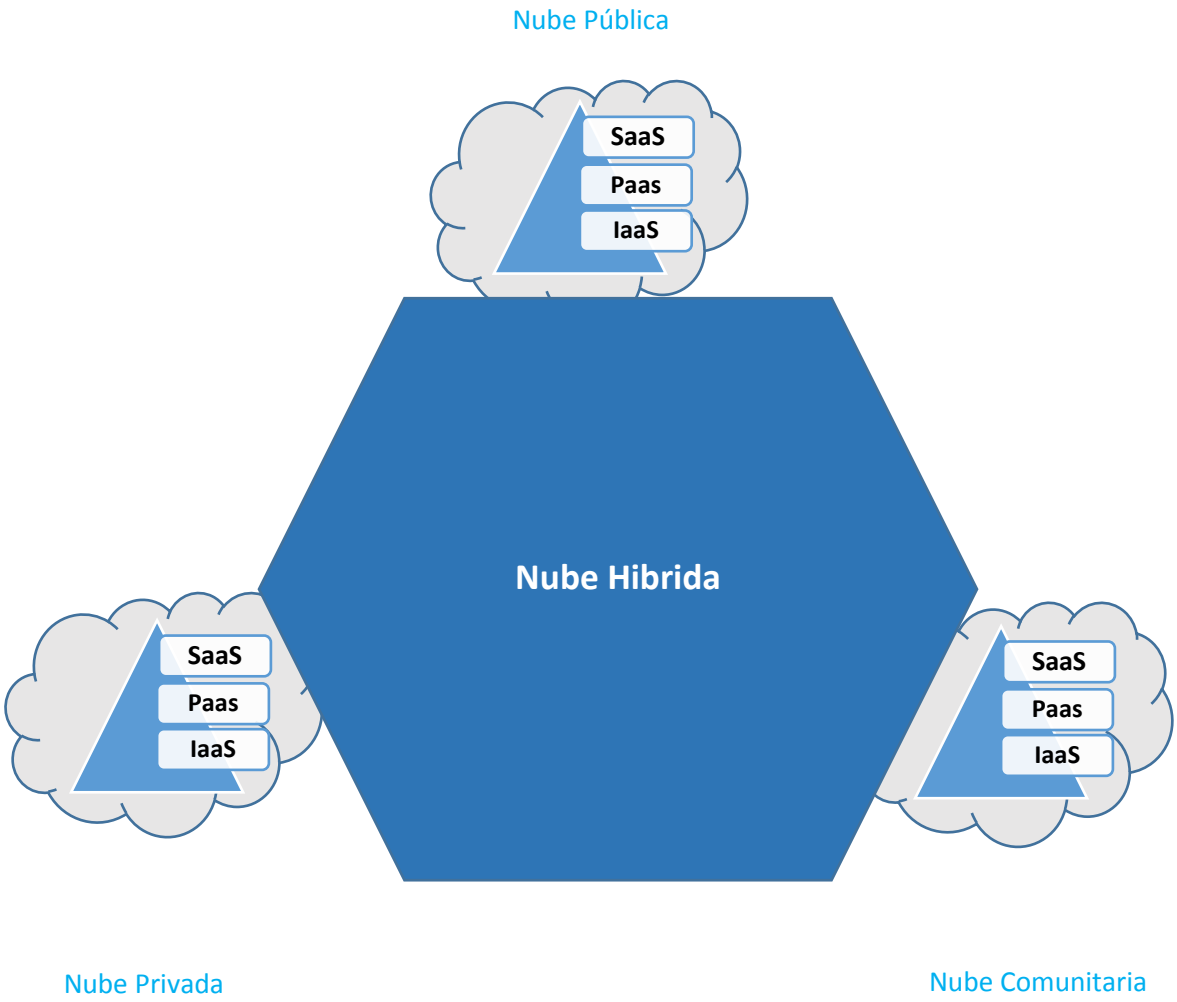


Figura 6 Conceptualización de los modelos de Despliegue

2.3.1.PaaS (Plataforma como servicio)

Plataforma como servicio cambia la manera en como el software se desarrolla y se despliega. En el desarrollo tradicional de aplicaciones, la aplicación será desarrollada localmente y será alojada en una ubicación central. En el desarrollo de aplicaciones automática, las aplicaciones serán desarrolladas y entregadas como ejecutables.

La mayoría de aplicaciones desarrolladas en plataformas de desarrollo tradicional resultan en un software basado en licencia. Mientras que PaaS cambia el desarrollo de aplicaciones de una máquina local a en línea [ORL12]. Proveedores de servicios PaaS proporcionan el desarrollo desde sus centros de datos. Los desarrolladores pueden adquirir el servicio a través de internet como se muestra en la figura siguiente.

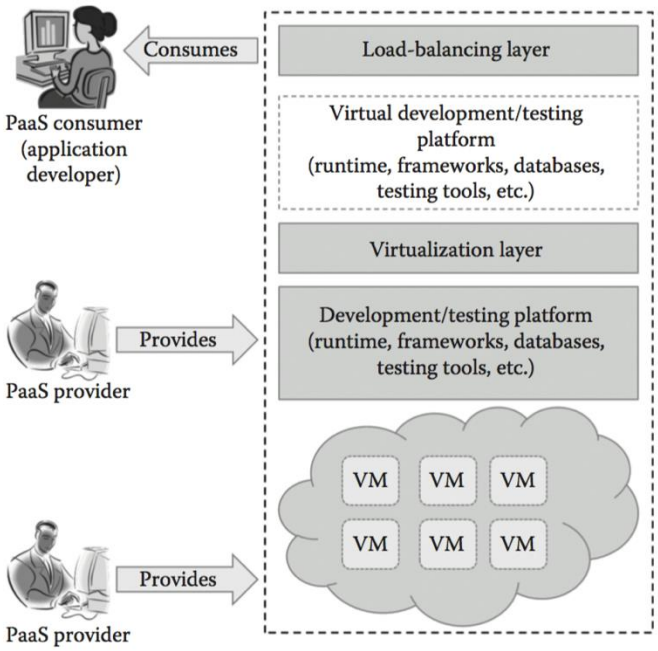


Figura 7 Plataforma como Servicio

PaaS permite a sus usuarios desarrollar sus aplicaciones en línea y además les permite desplegarlas en la misma plataforma. Los desarrolladores y consumidores de PaaS pueden consumir tiempos de ejecución de lenguaje, frameworks, base de datos, mensajería, herramientas de prueba y desplegar herramientas como servicio sobre internet.

Por lo tanto, reduce la complejidad de comprar y mantener diferentes herramientas para el desarrollo de aplicaciones. Los proveedores de servicios PaaS pueden proporcionar lenguajes de programación, aplicaciones, framework, etc. Algunos de estos proveedores además proporcionan herramientas de compilación, herramientas de despliegue y balanceadores de carga de software como servicio.

1. **Lenguajes de programación:** Los proveedores PaaS proporcionan una amplia variedad de lenguajes de programación a los desarrolladores para desarrollo de sus aplicaciones. Algunos de los lenguajes de programación populares que ofrece son Java, Perl, PHP, Python, Ruby, Scala, Clojure y Go.

2. **Frameworks:** Proporcionan frameworks que simplifican el desarrollo de la aplicación. Algunos de los frameworks proporcionados por los proveedores de servicios PaaS incluye Node.js, Rails, Drupal, Joomla, WordPress, Django, EE6, Spring, Play, Sintara, Rack y Zend.

3. **Base de datos:** Desde que cada aplicación necesita comunicarse con una base de datos, se ha convertido en una herramienta que se debe tener para cada aplicación. Proveedores de servicios PaaS están proporcionando bases de datos con las plataformas de desarrollo. Algunos ejemplos son ClearDB, PostgreSQl, Cloudant, Membase, MongoDB, and Redis.

4. **Otras herramientas:** También se proporcionan otras herramientas que son requeridas para desarrollar, probar y desplegar aplicaciones.

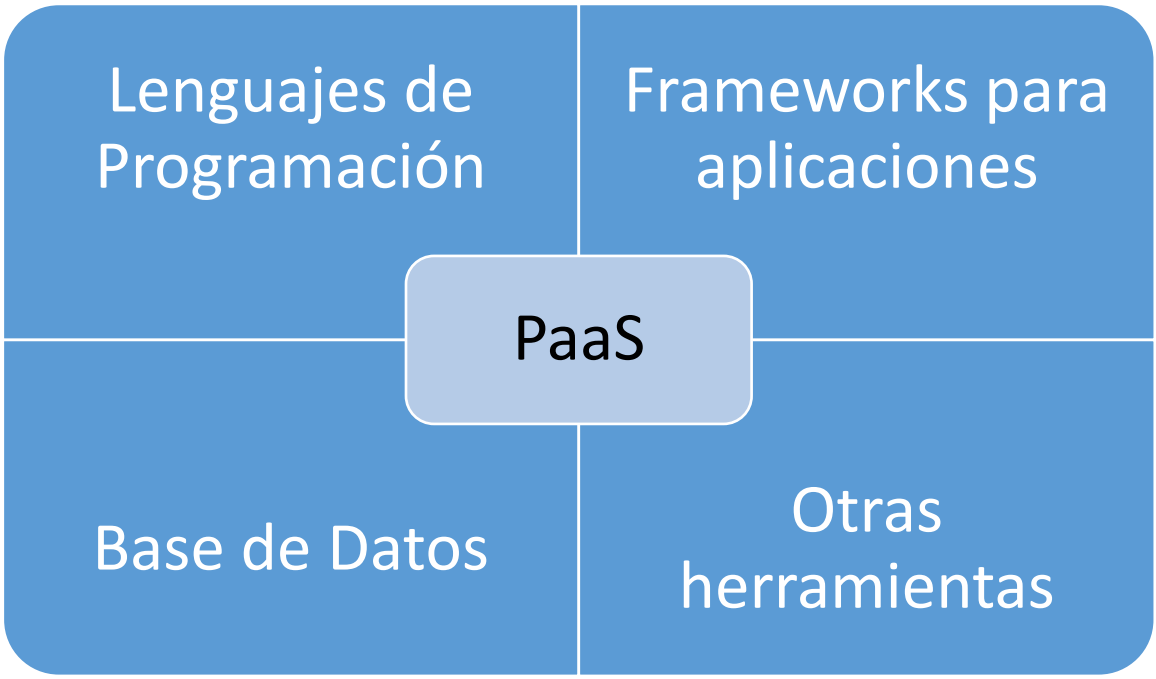


Figura 8 Herramientas desplegadas dentro de PaaS

Las plataformas de desarrollo PaaS son diferentes de las plataformas de desarrollo tradicionales. Lo siguiente son características esenciales que hacen única a PaaS a comparación de otras plataformas.

- **Todo en uno:** La mayoría de los proveedores PaaS ofrecen servicios de desarrollo, prueba, despliegue, alojamiento y mantenimiento de aplicaciones en el mismo IDE. Adicionalmente, varios proveedores proporcionan todos los lenguajes de programación relacionados, haciendo que el programador tenga una amplia variedad de elección.

- **Acceso web a las plataformas de desarrollo:** Una típica plataforma de desarrollo usa cualquier IDE para desarrollar aplicaciones. Típicamente el IDE será instalado en la máquina del programador. Sin embargo, PaaS proporciona acceso web a la plataforma de desarrollo. Usando web UI, cualquier programador puede acceder a la plataforma de desarrollo. UI ayuda a los desarrolladores a crear, modificar, probar y desplegar diferentes aplicaciones en la misma plataforma.

- **Acceso fuera de línea:** Cualquier desarrollador se puede encontrar en la situación de no poderse conectar a internet en todo un día. Cuando no haya conectividad a internet, al desarrollador se le debe permitir trabajar

sin conexión. Para habilitar desarrollo offline, algunos de los proveedores PaaS permiten al usuario sincronizar su IDE local con los servicios PaaS. El programador puede desarrollar su aplicación localmente y desplegarla cuando esté conectado a internet.

- **Construido en escalabilidad:** La Escalabilidad es un importante requerimiento para las nuevas generaciones de aplicaciones. Es muy complicado habilitar escalabilidad dinámica para cualquier aplicación desarrollada usando plataformas de desarrollo tradicional. Sin embargo, PaaS proporciona construcción escalable para cualquier aplicación que está siendo desarrollada usando PaaS. Esto garantiza que la aplicación sea capaz de manejar variaciones de carga eficientemente.

- **Plataforma colaborativa:** Hoy en día, los equipos de desarrollo consisten en programadores que están trabajando desde diferentes lugares. Hay una necesidad de plataforma común donde los desarrolladores puedan trabajar colaborativamente juntos en el mismo proyecto. La mayoría de los servicios PaaS proporcionan soporte para desarrollo colaborativo. Para habilitar colaboración entre desarrolladores, la mayoría de los proveedores PaaS proporcionan herramientas para planeación de proyectos y comunicación.

- **Diversidad en herramientas de clientes:** Para facilitar el desarrollo de aplicaciones, los proveedores PaaS proporcionan una amplia variedad de herramientas a sus clientes para ayudar en el desarrollo. Las herramientas de clientes incluyen CLI, web CLI, web UI, REST API e IDE. Los desarrolladores pueden elegir cualquier herramienta de su elección. Estas herramientas además son capaces de manejar facturación y administración de subscripciones.

La mayoría de los nuevos desarrolladores, empresas emergentes y vendedores de software independientes usan ampliamente PaaS en el desarrollo de sus aplicaciones. La tecnología PaaS está teniendo atención desde otras empresas de desarrollo de software tradicional. PaaS es una opción adecuada para las siguientes situaciones:

1. **Desarrollo colaborativo:** Para incrementar la eficiencia en el desarrollo y a la hora de comprar, hay una necesidad de un lugar común donde los equipos de desarrollo y otras partes interesadas puedan colaborar con cada uno de ellos. Desde que los proveedores de servicio PaaS proporcionan un entorno colaborativo, es una opción adecuada para aplicaciones que necesitan colaboración entre desarrolladores y otros terceros para llevar a cabo el proceso de desarrollo.

2. **Despliegue y pruebas automatizadas:** Pruebas y construcción automatizadas son muy útiles mientras se desarrolla la aplicación en periodos de tiempo muy cortos. Las herramientas de prueba automatizadas reducen el tiempo invertido en realizar pruebas manuales. La mayoría de los proveedores de servicio PaaS ofrecen herramientas de prueba automatizadas. Los equipos de programadores necesitan concentrarse más en el desarrollo que en el despliegue y las pruebas. Por lo tanto, servicios PaaS son la mejor opción donde hay una mayor necesidad de despliegue y pruebas automatizadas de las aplicaciones.

3. **Hora de comprar:** Los servicios PaaS siguen un interactivo e incremental desarrollo metodológico que garantiza que la aplicación esté en el mercado por un periodo de tiempo dado. Por ejemplo, PaaS son las mejores opciones para desarrollo de aplicaciones que usan metodologías agiles de desarrollo. Si el vendedor de software quiere que la aplicación este en el mercado tan pronto como sea posible, PaaS es opción más adecuada para estos casos.

2.3.2.IaaS (Infraestructura como servicio)

IaaS cambia la manera en que el cómputo, el almacenamiento y recursos de red son consumidos. En centros de datos tradicionales, el poder de cómputo es consumido teniendo acceso físico a la infraestructura. IaaS cambia la forma de hacer computación de una infraestructura física a una infraestructura virtual [ORL13]. IaaS proporciona cómputo virtual, almacenamiento y recursos de redes, al hacer una abstracción de los recursos físicos.

La tecnología de virtualización es utilizada para ofrecer los recursos virtuales. Todos los recursos son dados por máquinas virtuales que son configuradas por el proveedor de servicio. Los usuarios finales o los arquitectos de infraestructura de T.I usarán los recursos de infraestructura en forma de máquinas virtuales.

Al público que está orientado IaaS son los arquitectos de infraestructura de TI.

Ellos pueden diseñar la infraestructura virtual, redes, equilibradores de carga, etc. Basándose en sus necesidades.

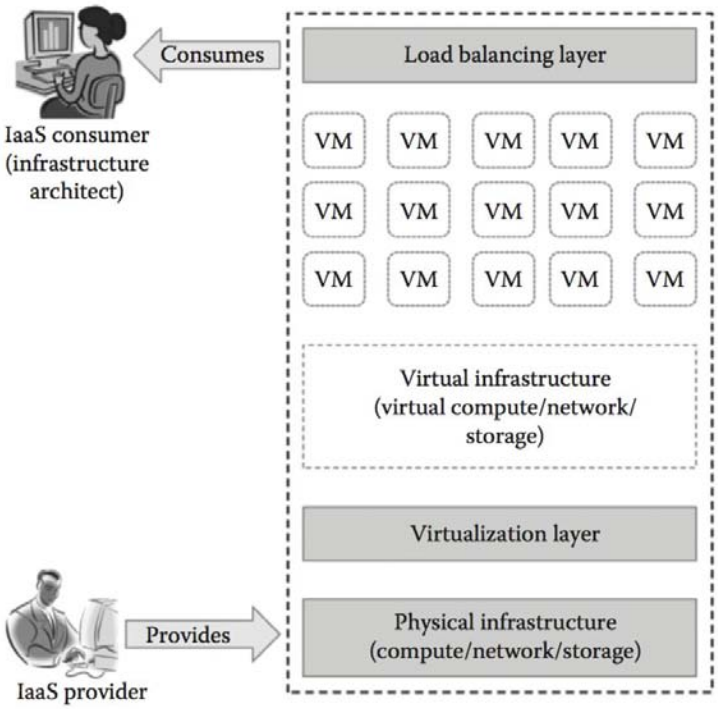


Figura 9 Infraestructura como Servicio

No es necesario que los arquitectos de TI mantengan los servidores físicos, así como lo hace el proveedor de servicios. La infraestructura física puede ser mantenida por el proveedor de servicios. Un típico proveedor de servicios puede proporcionar los siguientes servicios que se muestran a continuación en la figura.

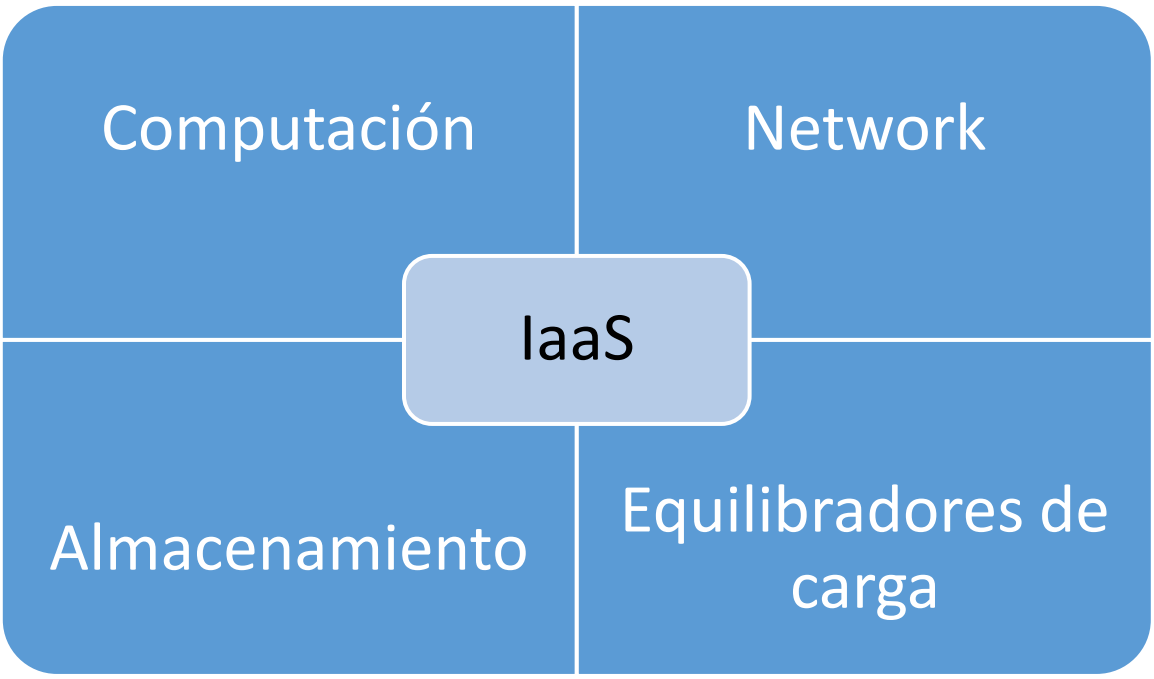


Figura 10 Servicios Provistos por IaaS

1. **Computación:** El Cómputo como servicio incluye las unidades de procesamiento central virtuales y memoria principal que son proporcionados a los usuarios finales.

2. **Almacenamiento:** Proporciona un almacenamiento de back-end para las imágenes de las máquinas virtuales. Algunas de los proveedores de IaaS además proporcionan un back-end para archivos almacenados.

3. **Network:** El Networking como servicio proporciona componentes networking virtual como routers virtuales, switch y bridges para las máquinas virtuales.

4. **Equilibradores de carga:** Los equilibradores de carga como servicio pueden proporcionar capacidades de balanceamiento a la infraestructura subyacente.

Los proveedores de IaaS ofrecen recursos de cómputo virtual a los consumidores en una base de pago por uso. IaaS contiene las características del cómputo en la nube como auto servicio en demanda, amplio acceso a la red,

agrupación de recursos, rápida elasticidad y servicio medido. Aparte de todos estos IaaS tiene sus propias características.

- **Acceso web a los recursos:** El modelo de IaaS habilita a los usuarios de TI acceder a los recursos de la infraestructura sobre internet. Cuando se accede a una gran capacidad de cómputo, los usuarios de TI no necesitan tener un acceso físico a los servidores. Si no por el contrario a través de cualquier motor de búsqueda, o una consola de administración pueden acceder a la infraestructura requerida.

- **Administración centralizada:** Aunque los recursos físicos están distribuidos, la administración será de un solo lugar. Los recursos distribuidos a lo largo de diferentes lugares pueden ser controlados desde cualquier consola de administración. Esto garantiza la administración de recursos efectiva y eficiente utilización de recursos.

- **Elasticidad y escalamiento dinámico:** IaaS proporciona servicio elástico, lo que quiere decir es que los recursos pueden ser incrementados o disminuidos de acuerdo a los requerimientos. La infraestructura depende de la carga de la aplicación. Conforme a la carga, los servicios de IaaS pueden proporcionar recursos. La carga en cualquier aplicación es dinámica y los servicios de IaaS son capaces de proporcionar los recursos requeridos dinámicamente.

- **Infraestructura compartida:** IaaS sigue un modelo de entrega de uno a muchos y permite a distintos usuarios de TI compartir la misma infraestructura. Cada uno de los usuarios de TI recibirán diferentes máquinas virtuales. Por lo tanto, de esta manera IaaS asegura una alta utilización de recursos.

- **MVs preconfiguradas:** IaaS proporciona máquinas virtuales preconfiguradas con el S.O, configuraciones de red, etc. Los usuarios de TI pueden escoger cualquier máquina virtual a su disposición. A si mismo los clientes son libres de configurar sus máquinas virtuales desde cero. Los usuarios pueden comenzar a usar los VMs tan pronto como se suscriban a los servicios.

- **Servicio medido:** IaaS permite a los usuarios de TI rentar los recursos de cómputo en lugar de comprarlos. Los servicios consumidos por los

usuarios serán medidos y serán facturados en base a la cantidad proporcionado por el proveedor de servicios.

IaaS reduce el costo total de tener la propiedad e incrementa el retorno de inversiones, para empresas nacientes que no pueden invertir en comprar infraestructura. IaaS puede ser usada en las siguientes situaciones.

- **Picos de uso impredecibles:** Cuando hay un aumento significativo en los recursos de cómputo IaaS en la mejor opción para las industrias de TI. Cuando la demanda es demasiada volátil, no podemos predecir los picos y valles en términos de demanda de la infraestructura. En estas situaciones no podemos agregar o quitar infraestructura inmediatamente en la demanda de recursos en una infraestructura tradicional. Si hay una demanda impredecible de la infraestructura, es recomendado usar el servicio de IaaS.

- **Inversión de capital limitada:** Las empresas recién creadas no pueden invertir demasiando en infraestructura para cubrir las necesidades de su negocio. Por lo tanto, usando IaaS pueden reducir la inversión de capital en la adquisición de hardware. IaaS es una opción adecuada para empresas de este tipo con menos posibilidades de inversión de capital en la compra de hardware.

- **Infraestructura en demanda:** Algunas organizaciones pueden requerir una grande infraestructura un periodo muy corto de tiempo. Por esta situación las organizaciones no pueden permitirse comprar recursos y administrarlos ellos mismos por su propia cuenta. En cambio, pueden rentar infraestructura requerida por un periodo de tiempo necesario. IaaS se adecua mejor a organizaciones que están buscando una infraestructura en demanda por un periodo de tiempo muy corto.

IaaS ayuda a las empresas recién iniciadas a limitar su gasto en capital. Si bien es ampliamente utilizado por este tipo de organizaciones, hay algunas situaciones en las cuales IaaS no es la mejor opción. En los siguientes casos, los usuarios de TI pueden evitar su uso.

- **Cuando el cumplimiento regulatorio no permite el alojamiento fuera de las instalaciones:** Para algunas empresas en las cuales su normatividad no permite que sus aplicaciones y datos sean alojados en una infraestructura externa de terceros.

- **Cuando hay mínimo uso:** Cuando el uso es mínimo, y la infraestructura disponible en las instalaciones es capaz por si misma de satisfacer las necesidades del negocio.

- **Cuando se requiere un mejor rendimiento:** Dado que se accede a los servicios de IaaS a través de internet, a veces el desempeño puede no ser el esperado debido a las latencias de la red.

- **Cuando hay una necesidad de mayor control en la infraestructura física:** Algunas organizaciones pueden requerir mayor control sobre la infraestructura subyacente. Como los servicios de IaaS son abstractos dados que son recursos virtuales, no es posible tener más control de la infraestructura física subyacente.

Actualmente hay distintos proveedores de servicios IaaS públicos y privados en el mercado, los cuales proveen infraestructura a usuarios finales. La siguiente tabla muestra un panorama general.

Proveedor	Licencia	Modelo de despliegue	S.O. Host	S.O. Host	Hypervisor soportado
Amazon Web Services	Propietarios	Pública	No disponible	Red Hat Linux, Windows Server, Suse Linux, Ubuntu Fedora, Debian, CentOS	
Google Compute Engine	Propietarios	Pública	No disponible	Red Hat Linux, Windows Server, Suse Linux, Ubuntu Fedora, Debian, CentOS	KVM
Microsoft Windows Azure	Propietarios	Pública	No disponible	Red Hat Linux, Windows Server, Suse Linux, Ubuntu Fedora, Debian, CentOS	Windows Azure hypervisor
Eucalyptus	GPLv3	Pública, Privada e Hibrida	linux	Linux y Windows	KVM, vSphere, XenServer y XCP
Apache Cloud Stack	Apache 2	Pública, Privada e Hibrida	linux	Windows, Linux y Open BSD	Xen, KVM y VMware
Open Nebula	Apache 2	Pública, Privada e Hibrida	CentOS, Debian y Open Suse	Windows y Linux	Libvirt, Hiper-V, VMware, Xen Server
OpenStack	Apache 2	Pública, Privada e Hibrida	CentOS, Debian, Open Suse, Fedora, REHEL y Ubuntu	CentOS, Ubuntu y FreeBSD	LXC libvirt

Tabla 3 Panorama actual de los proveedores de Nube

2.3.3.SaaS (Software como Servicio)

SaaS cambia la forma en que el software es entregado a los clientes. En un modelo tradicional de software, el software es entregado como un producto basado en licencia que necesita ser instalado en el dispositivo del cliente.

Desde que SaaS es entregado como un servicio en demanda sobre internet, no hay necesidad de instalar el software en los dispositivos de los usuarios finales.

Los servicios de SaaS pueden ser accedidos o desconectados en cualquier momento dependiendo en las necesidades del usuario [ORL14]. Se puede acceder a los recursos de SaaS mediante cualquier motor de búsqueda y cualquier dispositivo como laptops, tablets y Smartphones.

Algunos de los servicios SaaS pueden ser accedidos por un cliente que no tiene mucho espacio de almacenamiento y que no puede ejecutar distintos softwares como una computadora de escritorio tradicional. Los beneficios importantes de utilizar estos tipos de clientes para acceder a las aplicaciones SaaS son las siguientes:

- Menos vulnerables a ataques
- Tiene mayor ciclo de vida
- Consume menos recursos
- Más económico

Un proveedor de servicio SaaS puede proporcionar servicios de negocio, social Network, administración de documentos y servicios de mail como se muestra en la figura siguiente.

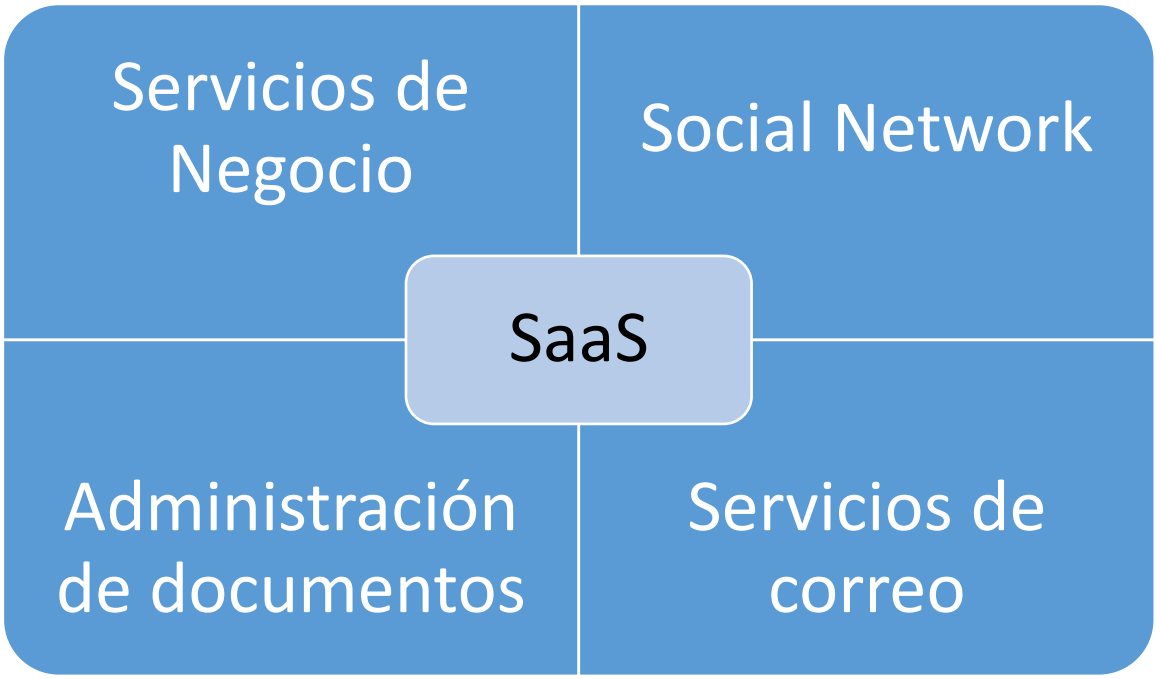


Figura 11 Servicios Provistos en SaaS

1. **Servicios de Negocio:** La mayoría de los proveedores SaaS empezaron proporcionando una variedad de servicios empresariales que atrajeron a las empresas emergentes. Los servicios de negocio SaaS incluidos son ERP, CRM, facturación, ventas y recursos humanos.

2. **Social Networks:** Desde que los sitios de las redes sociales son extensivamente usados por el público en general, diferentes proveedores de servicios de redes sociales tuvieron que adoptar SaaS para su sustentabilidad. A partir de que el número de usuarios de redes sociales incremento exponencialmente, el Cómputo en la Nube es la combinación perfecta para manejar la carga de trabajo variable.

3. **Administración de documentos:** Desde que la mayoría de las empresas usan extensivamente documentos electrónicos, la mayoría de los proveedores de SaaS comenzaron a ofrecer servicios que son usados para crear, administrar y rastrear documentos electrónicos

4. **Servicios de mail:** El correo electrónico es usado actualmente por muchas personas. El futuro crecimiento en el uso del e-mail es impredecible. Para manejar el número impredecible de usuarios y la carga

en los servicios de e-mail, la mayoría de los proveedores de servicios de e-mail comenzaron a ofrecer SaaS.

Los servicios de SaaS son diferentes y dan más beneficios a usuarios finales que el software tradicional. Las siguientes son características esenciales de los servicios SaaS que lo hacen único a comparación del software tradicional.

- **Uno a muchos:** Servicios de SaaS son entregados en un modelo de un a muchos donde una única instancia de una aplicación puede ser compartida por muchos clientes.

- **Administración centralizada:** Desde que los servicios SaaS están hospedados y administrados desde una ubicación central, la administración de las aplicaciones SaaS se vuelve más fácil. Normalmente, los proveedores de SaaS realizaran las actualizaciones automáticamente que aseguraran que cada cliente está accediendo a la versión más reciente de la aplicación sin ninguna actualización del lado del cliente.

- **Acceso web:** SaaS proporciona acceso web al software. Esto permite a los usuarios acceder a las aplicaciones desde cualquier lugar siempre y cuando el dispositivo esté conectado a internet.

- **Soporte de multi dispositivos:** Se puede acceder a los servicios desde cualquier dispositivo de los usuarios finales como computadoras de escritorio, laptops, tablets y Smartphone.

- **Mejor escalabilidad:** Desde que la mayoría de los servicios SaaS aprovechan IaaS y PaaS para su desarrollo y despliegue, han logrado una mejor escalabilidad que el software tradicional. El escalamiento dinámico de los recursos subyacentes de la Nube hace que las aplicaciones de SaaS trabajen eficientemente incluso con las variaciones de demanda.

- **Alta disponibilidad:** SaaS asegura el 99.999% de la disponibilidad de los datos con respaldos propios y mecanismos de recuperación son implementados.

- **Integración de API:** Los servicios SaaS tienen la capacidad de integración con otros softwares o servicios a través de APIs estandarizadas.

SaaS es popular entre particulares y empresas emergentes dado a los beneficios que otorga. La mayoría de los usuarios tradicionales están buscando versiones de software como servicio que tienen varias ventajas por encima de las aplicaciones tradicionales. Aplicaciones SaaS son más adecuadas en las siguientes situaciones:

- **Software en demanda:** El modelo de software basado en licencia requiere la compra de paquetes completos e incrementa el gasto en la compra de estos softwares. Algunos del software que se usa ocasionalmente no genera ningún retorno o recuperación. Por este motivo muchos usuarios se encuentran buscando software que puedan usar cuando necesiten. Si los usuarios finales buscan software en demanda en lugar de software basado en licencia entonces el modelo SaaS es su mejor opción.

- **Software para empresas emergentes:** Cuando se usa software tradicional, generalmente los usuarios finales compran hardware con los mínimos requerimientos necesarios para la aplicación. Esto aumenta la inversión de capital en la compra de hardware para empresas emergentes. Dado que SaaS no requiere una gran infraestructura para acceder a sus servicios es la mejor opción para este tipo de organizaciones, en las cuales puede reducir el gasto inicial en la compra de hardware específico.

- **Compatibilidad de software:** Algunas aplicaciones como los procesadores de texto o servicios de correo electrónico necesitan mejor accesibilidad desde cualquier dispositivo. Las aplicaciones SaaS se adaptan con la mayoría de los dispositivos.

- **Software con variaciones de carga:** No podemos predecir la carga en aplicaciones populares como los sitios de redes sociales. Los usuarios se puedes conectar y desconectar en cualquier momento. Es muy complicado manejar las variaciones de carga con infraestructuras tradicionales. Con las capacidades de escalamiento dinámico, las aplicaciones SaaS pueden manejar las variaciones de carga eficientemente sin ninguna afectación en el comportamiento normal de la aplicación.

La mayoría de los vendedores de software tradicional se están moviendo a SaaS como un modelo de entrega de software emergente que atrae a usuarios finales.

Pero aún muchas aplicaciones tradicionales no tienen sus versiones para SaaS.

Esto implica que el modelo SaaS no sea adecuado para todos los tipos de software. El modelo de entrega SaaS no es la mejor opción para los siguientes ámbitos de uso.

- Aplicaciones de tiempo real
- Aplicaciones con datos confidenciales

2.4. Modelos de Despliegue de la Nube

Los modelos de despliegue pueden ser definidos de diferentes formas en las cuales la Nube puede ser desplegada. Estos modelos están completamente centrados en los usuarios, esto quiere decir que depende de los requerimientos del usuario y necesidades. Un usuario puede seleccionar un modelo de acuerdo a sus requerimientos. Básicamente, tenemos 4 modelos de despliegue en la Nube:

1. Nube Privada.
2. Nube Pública.
3. Nube Comunitaria.
4. Nube Hibrida.

La clasificación de la Nube está basada en varios parámetros como el tamaño de la nube (número de recursos), tipo de proveedor de servicios, localización, tipo de usuarios, seguridad y otras cuestiones [MEL15]. La Nube más pequeña es la que denominamos privada.

La Nube privada es el modelo de despliegue más básico que puede ser desplegada por una singular organización para su uso personal. No es compartida con otras organizaciones y no es permitido su uso público. La Nube privada sirve para empleados de una organización.

Usualmente se encuentra en la empresa, pero también puede ser externa. La siguiente que tenemos es la nube comunitaria, la cual es una extensión de la Nube privada. Aquí este modelo es el mismo que el privado, pero es compartida por muchas organizaciones. La nube comunitaria está establecida para un uso común.

La Nube pública es la opuesta a la Nube privada. La cual permite el acceso desde cualquier lugar en el mundo y es abierta a todo público. Esta nube es la más grande en tamaño entre los otros modelos de despliegue.

La Nube pública es uno de los modelos de despliegue más populares. También tenemos la Nube hibrida, la cual es una combinación de otros modelos. Típicamente consiste de una combinación dela Nube pública y privada. Muchas propiedades la Nube privada son usadas con las propiedades de la Nube pública. Este modelo es uno los próximos modelos que tendrá más impacto en la industria.

2.4.1.Nube Privada

De acuerdo con el NIST, la Nube privada puede ser definida como la infraestructura de la nube que es aprovisionada para uso exclusivo de una organización que comprende múltiples consumidores. Esta será administrada, operada y es propiedad de la organización, o de una tercera parte.

En términos simples la Nube privada es un ambiente creado para una sola organización. Es usualmente privada, porque solo es para la organización, pero puede ser manejada por la organización o una tercera parte. La Nube privada puede ser desplegada usando herramientas de código libre como OpenStack y Eucalyptus.

Figura 12 Nube Privada

Imagen obtenida de: https://www.lynda.com/IT-Infrastructure-tutorials/Cloud-Computing-Private-Cloud-Platforms/555797-2.html

La Nube privada es de tamaño pequeño a comparación con los otros modeles, en este caso la nube es desplegada y mantenida por la misma organización [EUC16]. Ciertas características de la Nube son las siguientes:

- **Segura:** La nube privada es segura. Esto debido a que usualmente la Nube privada es desplegada y administrada por la organización en sí misma, por lo tanto, disminuye la posibilidad de que sean filtrados los datos fuera de la Nube. En caso de que la Nube sea subcontratada, el proveedor de servicios puede apoyarse a través de lineamientos de gobernanza, pero no hay ningún otro riesgo ni de un externo ni de los empleados de la misma organización.

- **Control centralizado:** La organización mayormente tiene control completo sobre la Nube dado que es manejada por la organización misma. Por lo tanto, cuando, cuando es administrada por la misma organización, no hay necesidad de confiar en alguna otra entidad.

Nos referimos a que este modelo es idóneo para instancias que la pueden usar en ciertas condiciones. Además, significa que las condiciones más adecuadas y el ambiente donde este modelo de nube puede ser usado son las siguientes:

- Las organizaciones o empresas que requieren separar la nube de su personal o uso oficial.

- Las organizaciones o empresas que tienen una cantidad suficiente de fondos y recursos para administrar.

- Para las organizaciones que consideran que la seguridad de sus datos es importante.

- Para las organizaciones o empresas que quieren autonomía y control sobre la Nube.

- Para las organizaciones o empresas que tienen menor número de empleados.

- Para las organizaciones que tienen una infraestructura pre construida para el despliegue de la nube y están listas momentáneamente para mantenimiento eficiente de la nube.

- Se debe tener especial cuidado y los recursos deben estar disponibles para la resolución de problemas.

La Nube privada no es adecuada en los siguientes casos:

- Para las organizaciones que tienen gran cantidad de usuarios.
- Para las organizaciones que tienen restricciones financieras.

2.4.2. Nube Pública

De acuerdo con NIST, la Nube pública es la infraestructura de la Nube que es provisionada para un uso abierto al público en general. Puede ser administrada, operada y propiedad de un negocio, académicos u organización de gobierno o alguna combinación de estos. Existe en las instalaciones del proveedor de servicios.

La Nube pública consiste de usuarios alrededor del mundo. Un usuario simplemente puede comprar recursos por hora y trabajar con los recursos. No hay ninguna necesidad de una infraestructura preconstruida para usar este tipo de modelo [BAD17]. Estos recursos están disponibles en las instalaciones del proveedor de servicios de la Nube. Usualmente los proveedores de servicios aceptan todas las solicitudes, y por lo tanto, los recursos en extremos del proveedor de servicios dan la sensación de ser infinitos. Un buen ejemplo de estos casos en la Nube de Amazon (AWS). Sus características son las siguientes:

- **Alto escalamiento:** La Nube pública es altamente escalable, los recursos en la Nube pública son grandes en números y el proveedor de servicios se asegura que todas las solicitudes estén garantizadas. Por lo tanto, la Nube pública se considera escalable.
- **Económica:** La Nube pública es ofrecida al público en un modelo de pago por uso; por lo tanto, el usuario tiene que pagar solamente por lo que está usando.
- **Menor seguridad:** La Nube pública es menos segura de los 4 modelos de despliegue. Esto es porque es ofrecida por una tercera parte y esta tiene control total sobre la Nube. A través de acuerdos de nivel de servicio puede mejorar la privacidad, hasta si hay un alto riesgo de filtración.

- **Alta disponibilidad:** La Nube pública tiene alta disponibilidad porque cualquier persona desde el lugar que sea puede acceder a la Nube con los permisos adecuados, y esto no es posible en otros modelos.

- **Estrictos Acuerdos de nivel de servicio:** Estos acuerdos son muy estrictos en el caso de la Nube pública. Como la reputación del proveedor de servicios depende totalmente de la calidad de servicios que ofrezca, debe apegarse a los acuerdos hechos y evitar violaciones. Los acuerdos son muy competitivos.

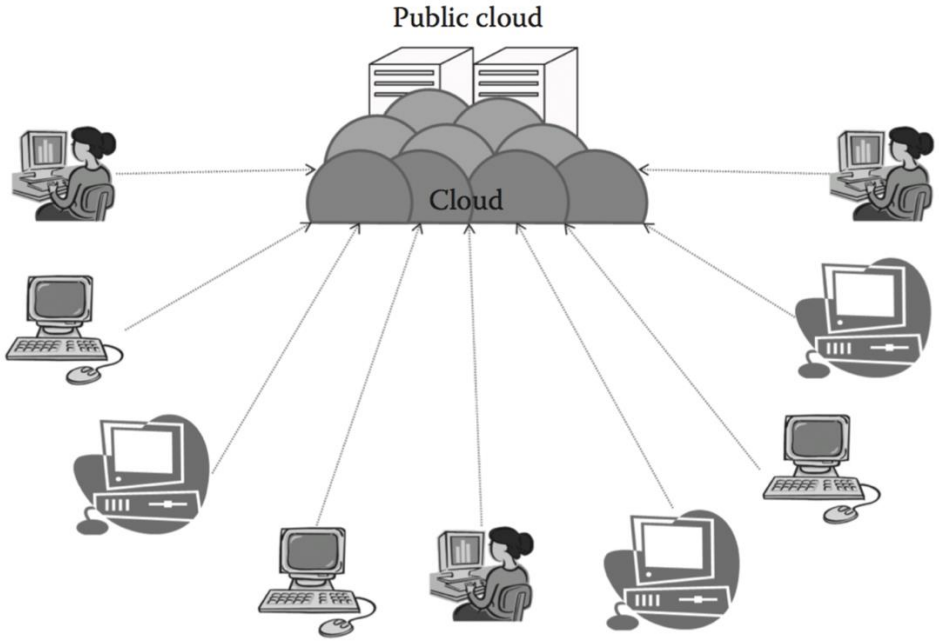


Figura 13 Nube Pública

Hay varias situaciones y ambientes donde la Nube pública es adecuada. La Nube pública puede ser usada donde sea que aplique lo siguiente:

- Los requerimientos de los recursos sean grandes, y haya gran cantidad de empleados.

- Los requerimientos de recursos son variantes.

- Donde no hay infraestructura física disponible.

- Donde se encuentren con restricciones económicas.

La Nube pública no es adecuada en los siguientes casos:

- Los requerimientos de seguridad son muy importantes.
- Donde la organización espera autonomía.
- La confianza en terceras partes no es una opción

2.4.3. Nube Comunitaria

De acuerdo con el NIST, la Nube comunitaria es la infraestructura de la Nube que aprovisiona exclusivamente a una comunidad de consumidores específicos de varias organizaciones que tiene preocupaciones compartidas (misión, requerimientos de seguridad, políticas y cumplimientos). Puede ser propiedad, administrada, operada por una o más organizaciones. Se considera una extensión más de la Nube privada. Por lo tanto, podemos decir que la Nube privada es compartida entre varias organizaciones. Ya sea que una organización que haga cargo de la Nube o varias entre sí.

La principal ventaja de la Nube comunitaria es que las organizaciones son capaces de compartir recursos entre ellas en base a preocupaciones específicas. Por eso en este escenario las organizaciones son capaces de usar el poder la nube, el cual es más grande que el de Nube privada y al mismo tiempo son capaces de usarla a menor costo [OPE18]. La comunidad es formada en base a una causa en común, pero eventualmente, todos los miembros de la comunidad son beneficiados. El modelo es perfecto para organizaciones que no pueden costear una Nube privada y no pueden confiar en una Nube pública. La imagen siguiente describe la Nube comunitaria.

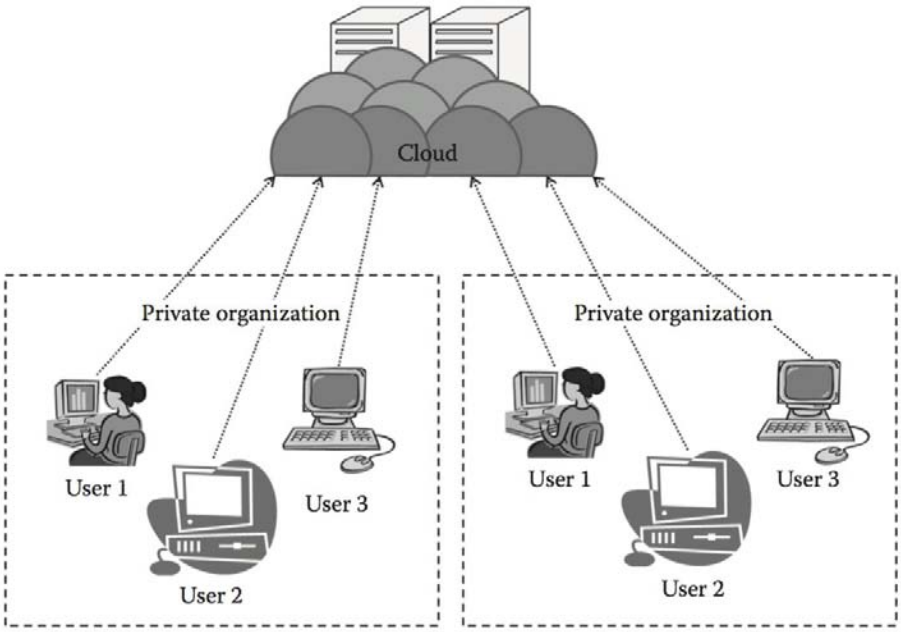


Figura 14 Nube Comunitaria

Las características de la Nube comunitaria son las siguientes:

- **Colaborativa y mantenimiento distribuido:** La Nube comunitaria es completamente colaborativa, y generalmente todas las partes tienen control total de la Nube, en algunos casos lo puede tener solo una parte. Por esto es que usualmente es distribuida y por lo tanto, una mejor cooperación da mejores resultados. Incluso puede ser contratada.

- **Parcialmente segura:** Parcialmente segura se refiere a la propiedad de la Nube de ser comunitaria, debido a que puede ocurrir filtración de información pocas organizaciones comparten la Nube.

- **Económica:** La Nube pública es efectiva en este aspecto dado que es compartida por varias organizaciones o comunidades. Usualmente no solo la renta se divide, si no también otras responsabilidades entre los participantes.

Este tipo de Nube es adecuada para organizaciones que:

- Desean establecer una Nube privada, pero tienen restricciones económicas.
- No quieren la responsabilidad completa del mantenimiento de la Nube.
- Desean establecer la Nube con el fin de tener colaboración con otros.
- Quieren tener una Nube colaborativa con mayores características de seguridad que la Nube pública.

En cambio, no es adecuada en los siguientes casos:

- Se prefiere mayor autonomía y control sobre la Nube.
- No desean colaborar con otras organizaciones.

2.4.4. Nube Hibrida

De acuerdo con el NIST, la Nube hibrida puede ser descrita como la infraestructura de la Nube que es compuesta por 2 o más distintas infraestructuras (Privada, comunitaria, pública) y aun a si siguen siendo entidades únicas, pero están unidas juntas por un propietario de tecnología estandarizado que habilita datos y portabilidad de aplicaciones.

La Nube hibrida es generalmente una combinación de la Nube pública y privada con el objetivo de combinar las ventajas de la Nube pública y privada. La razón principal de usar una Nube hibrida es inicialmente para tener privacidad, y después para tener más recursos adicionales. Hay muchas ventajas en la Nube Hibrida.

La Nube hibrida puede considerarse como una Nube privada extendida a la Nube pública. Esto conduce a utilizar el poder de la Nube Pública, pero reteniendo las propiedades de la Nube privada. Uno de los ejemplos populares es Eucalyptus.

Eucalyptus fue inicialmente diseñada para ser Nube privada, pero actualmente ya soporta la Nube hibrida [HYB19]. La Nube hibrida puede ser extendida más allá, en vastas áreas de Nubes federadas como se muestra en la siguiente imagen.

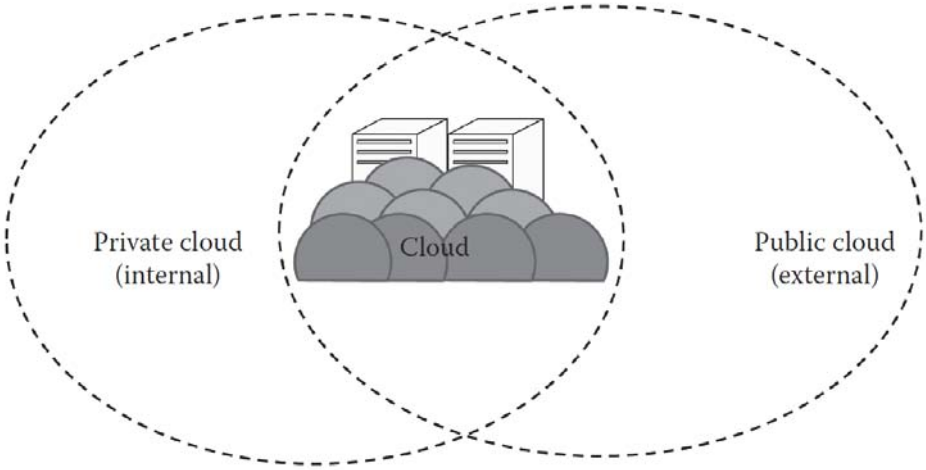


Figura 15 Nube Hibrida

La Nube hibrida presenta las siguientes características:

- **Escalable:** La Nube hibrida es una combinación 1 o más modelos de despliegue. Usualmente es el resultado de combina la privada con la pública. La razón principal de tener una Nube hibrida es para usar las propiedades de la Nube pública con el entorno de la Nube privada. La Nube pública es usada cuando sea necesaria; sin embargo, como la Nube pública es escalable, la Nube hibrida con la ayuda de la Nube pública es escalable también.

- **Parcialmente segura:** La Nube hibrida es una combinación de la privada y la pública. La Nube privada es considerada por tener seguridad, pero como la Nube hibrida además usa la Nube pública, hay un alto riesgo de tener brechas de seguridad. Por eso no puede ser denominada completamente segura, por eso se dice que es parcialmente segura.

- **Acuerdos estrictos:** Como la Nube pública está envuelta en un ambiente de Nube pública, los acuerdos son estrictos y lo pueden ser tanto como el cliente y proveedor de servicios lo determinen.

- **Administración compleja:** La administración de la Nube es completa y es una tarea más difícil en la Nube Hibrida como envuelve más de un modelo de despliegue y generalmente el número de usuarios son muy altos.

La Nube hibrida es adecuada en los siguientes casos:

- Para las organizaciones que requieren un entorno de Nube privada con la escalabilidad de la Nube pública.

- Para las organizaciones mayor seguridad que la que ofrece la Nube pública.

La Nube hibrida no es adecuada en:

- En organizaciones que consideran la seguridad como objetivo primordial.

- En organizaciones que no serán capaces de manejar la administración de la Nube hibrida.

2.5. Cómputo en la Nube Móvil

En el foro de la Computación en la Nube Móvil se define al Cómputo en la Nube Móvil de la siguiente manera:

> "Cómputo en la Nube Móvil en su forma más simple, se refiere a una infraestructura donde el almacenamiento y procesamiento de datos ocurren fuera del dispositivo móvil. Las aplicaciones de móviles en la Nube alejan la capacidad de cómputo y almacenamiento de datos de los teléfonos móviles hacía la Nube" [8].

Cómputo en la Nube Móvil es básicamente la interacción de los campos de las redes móviles y el Cómputo en la Nube. Redes Móviles son básicamente redes que conectan usuarios móviles.

El rápido surgimiento de las Redes Móviles hizo necesario traer el dominio de la Nube a las redes Móviles. Este campo aún está en su fase primaria de desarrollo.

Cómputo en la Nube Móvil básicamente habilita la construcción y organización de aplicaciones sobre la Nube. Hay varios problemas que deben ser resueltos como es la virtualización, seguridad, privacidad, preservación y la tolerancia a fallos.

Desafortunadamente los dispositivos móviles están limitados por sus recursos y poder de cómputo. Las limitaciones del Cómputo Móvil pueden ser superadas por el Cómputo en la Nube Móvil [MAR20].

Permitirá a usuarios acceder a plataformas y aplicaciones proporcionados por la Nube a través de sus dispositivos móviles. En este escenario, los usuarios no volverán a verse restringidos por los recursos computacionales de sus dispositivos.

Por esto cuando se requiera de un procesamiento de cómputo más demandante más dispositivos móviles serán capaces de realizarlo a través de las aplicaciones en la nube.

Actualmente hay diversas aplicaciones basadas en la Nube, las más comunes son iCloud de Apple y Gmail.

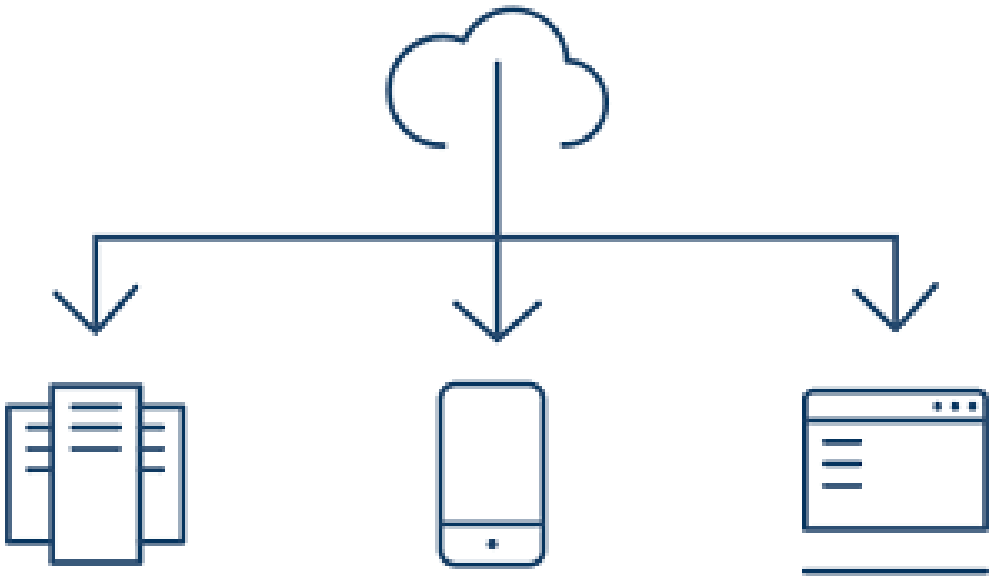


Figura 16 Cómputo en la Nube Móvil.

En aplicaciones móviles que involucran el procesamiento de imágenes, el procesamiento de lenguaje natural, la búsqueda de multimedia y más son la fuga de recursos en el dispositivo móvil, la cual puede ser conllevada por servicios de Nube ofrecidos. En la siguiente imagen se muestra un servidor remoto de Nube ofreciendo servicios a un dispositivo móvil.

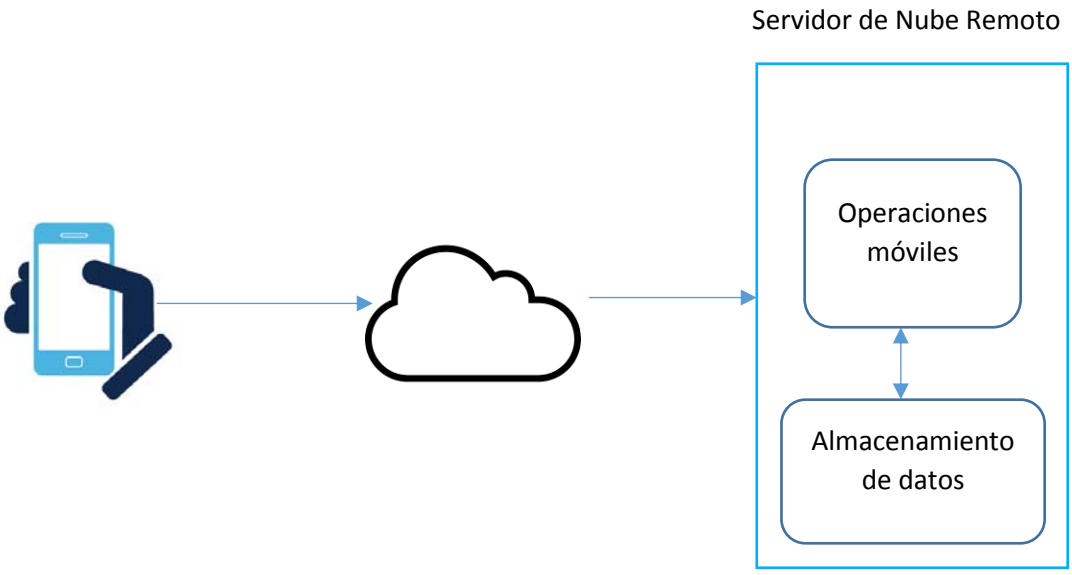


Figura 17 Servidor de Nube remoto ofreciendo servicio a un dispositivo móvil

Otro escenario puede ser descrito cuando un dispositivo móvil por sí mismo puede ser parte de la nube y ofrecer sus recursos en una forma de renta para otro dispositivo móvil.

A si la recopilación de recursos puede estar disponible siempre que se encuentren dentro de la misma plataforma. Otro escenario común es el uso de Cloudlets.

Cloudlets son básicamente una recopilación de multiprocesadores de computadoras conectadas a un servidor de Nube remoto. Es este caso los dispositivos móviles actúan como clientes ante el Cloudlets [HON21].

Un problema importante en el Cómputo en la Nube Móvil es el proceso de entregar los trabajos a la nube. Depende grandemente en la distancia física que separa la Nube y el dispositivo móvil. Este proceso puede incurrir en costos adicionales. Por su puesto que el costo debe de tomarse en consideración. Actualmente hay muchos libros dedicados al análisis del costo beneficio del Cómputo en la Nube Móvil.

Otro de los mayores problemas es que el Cómputo en la Nube tradicional es que no soporta la movilidad del usuario. Debe de tener mecanismos apropiados para identificar la localización correcta del cliente móvil. La movilidad del usuario no debe de afectar la conectividad hacía la nube.

La eficiencia de la batería es otro aspecto que requiere ser tomado en cuenta para la evolución de este campo. Ciertas arquitecturas han sido propuestas para la Computación en la Nube Móvil, las cuales toman en consideración la privacidad, seguridad, entre otros problemas.

2.5.1. Fundamentos claves del Cómputo en la Nube Móvil

Las aplicaciones de Cómputo en la Nube Móvil están usualmente diseñadas para proporcionar a los usuarios de la Nube servicios basados en la Nube, pero desde sus dispositivos móviles. Se alcanzó este objetivo gracias a tres factores claves, los cuales son los siguientes.

1. Cómputo Móvil
2. Internet Móvil
3. Cómputo en la nube

La combinación de estos tres aspectos es un requerimiento fundamental para la generación de soluciones de Cómputo en la Nube Móvil [CHE22].

En la siguiente figura se muestra la estructura técnica del Cómputo en la Nube Móvil e ilustra los mecanismos usados en cada dominio principal. Hay más técnicas siendo implementadas en la práctica.

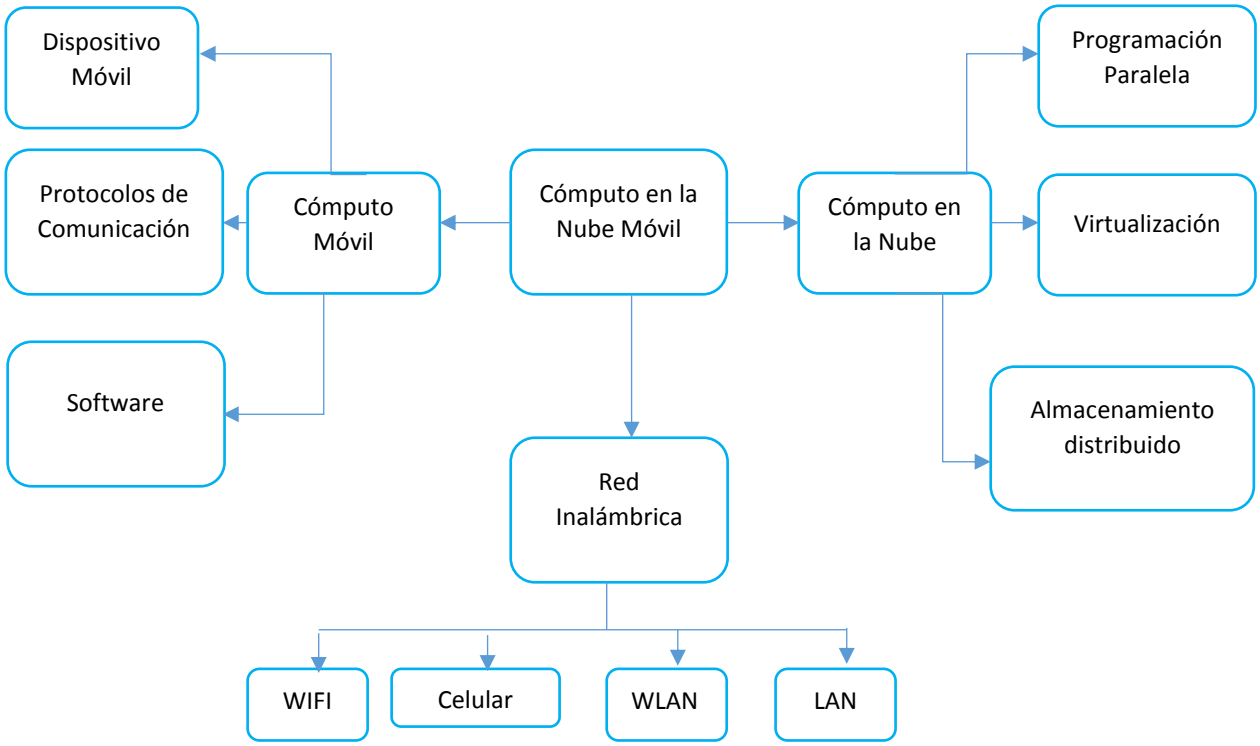


Figura 18 Estructura del Cómputo en la Nube Móvil

2.5.2. Beneficios del Cómputo en la Nube Móvil

1. ***Aumento de la vida de la batería:*** En cuanto los usuarios de Smartphones están conectados, la duración de la batería es una de las mayores preocupaciones. A pesar que los Smartphones tienen una amplia gama de funcionalidades, la duración de la batería drásticamente disminuye cuando se le asignan tareas al dispositivo. Al implementar la ejecución de aplicaciones que necesitan de computación intensiva en la Nube la duración de la batería puede mejorar.

2. ***Mejora en la capacidad de procesamiento y almacenamiento:*** Habiendo lidiado con la vida útil de la batería, el siguiente problema

común encontrado por los usuarios es la capacidad de almacenamiento. La Nube proporciona una simple solución para esta cuestión que es que los datos pueden ser consultados vía redes inalámbricas.

3. ***Aumento de la confiabilidad:*** Al usar la Nube, los datos se respaldan en varios dispositivos móviles. En caso de pérdida accidental, se puede acceder a los datos respaldados.

4. ***Mejora de la escalabilidad:*** Al usar la Nube, la escalabilidad de las aplicaciones móviles puede ser fácilmente mejorada.

En el Cómputo en la Nube Móvil encontramos aplicaciones que van desde el comercio, enseñanza, salud y hasta la banca móvil.

3. Metodologías de Análisis Forense

3.1. Introducción al capitulo

La evidencia digital la podemos encontrar en todas partes, esto debido a la naturaleza ubicua de los medios electrónicos; en nuestra sociedad, la interacción con dispositivos conectados a la red es inevitable. Muchos de nosotros los usamos cientos de veces al día. La mayoría de estos dispositivos hoy en día son “inteligentes” con el fin de poder dar contextualización de la información que usted genera, es decir su Smartphone sabe quién es usted, a donde va y con quien se relaciona.

A si como en este mundo físico, se dejan rastros de nosotros mismos – huellas dactilares, cabello, fibras de la ropa, ADN, etc. Al interactuar con personas, objetos y visitar sitios de interés, sucede lo mismo en el dominio de las tecnologías de la información, dejando rastro de nuestra persona. Este tipo de rastro por así llamarlo se puede ver representado en fragmentos de archivos, registros, metadatos y mucho más, los cuales pueden ser considerados valiosos por varias razones.

Por si fuera poco a todo esto se añade las enormes cantidades de información digital que los empleados manejan diariamente: sitios web, agenda, procesadores de texto, hojas de cálculo y también sistemas de seguridad. Todo esto culmina en una gran cantidad de datos. Y todos estos sistemas generan registros de sus actividades cuando son utilizados. Resultando en grandes cantidades de información indirecta disponible para cualquiera que sabe cómo buscarla.

Los datos pueden ser útiles como evidencia para establecer los orígenes de un documento o pieza de software, para propósitos legales en la determinación de actividades de sujetos involucrados en un caso criminal, o incluso como un recurso valioso para cibercriminales con el objetivo de reconstruir información o en la búsqueda de identificar las credenciales de su víctima.

Cualquiera que sea la motivación para realizar la examinación, interpretación, o reconstrucción de la evidencia en sistema de cómputo cae totalmente en el dominio del Cómputo Forense.

El campo del Cómputo Forense se ha vuelto cada vez más importante en los últimos años a medida que el mercado de las computadoras y los Smartphones ha crecido.

El Cómputo forense describe el proceso de inmiscuirse dentro de un dispositivo tecnológico ya sea una computadora o un Smartphone con el fin de examinar y analizar las actividades y determinar si el dispositivo ha sido comprometido previamente o está siendo monitoreado por un atacante. Tal vez piense que no tiene mucho que esconder en su Smartphone, entonces puede que la siguiente

advertencia no le aplique, solo porque le ha dado al botón eliminar, no significa que algún buen intruso con motivaciones económicas no pueda encontrar ese archivo tan valioso que se preocupa por deshacerse.

Este campo está en constante evolución para ajustarse a las nuevas necesidades que está provocando el surgimiento de nuevas tecnologías como la Computación en la Nube mezclada con los dispositivos móviles.

Junto a la creciente demanda de nuevas tecnologías en el mercado de los Smartphones, el mercado del “malware” o “spyware” también ha ido creciendo. El análisis forense en Smartphones es un término amplio dentro del campo del análisis digital que abarca una variedad de características, en particular, la capacidad de recuperar datos borrados en dispositivos móviles, la extracción y análisis de detalles de registro de llamadas y la detección y eliminación de malware.

El malware y spyware son programas que le permiten a un hacker espiar las actividades del usuario derivadas de los mensajes, correos, llamadas entrantes y salientes e incluso información del GPS. Uno de los mayores usos del “malware” y “spyware” es la activación de funciones de escucha. El uso de esta tecnología y software, permite a individuos monitorear conversaciones en tiempo real. Este tipo de software es muy fácil de instalar y configurar.

El desarrollo y despliegue de malware son considerados ciberdeilitos. A través del uso de estas herramientas un atacante puede determinar la información personal así como tarjetas de crédito y débito, compras en línea, o través del robo de información confidencial que pudo haber guardado en sus computadora o Smartphone.

Si el hacker es lo suficientemente bueno puede además obtener su CURP, robar su identidad y relacionarlo con crímenes que el este cometiendo.

3.2. El rol de un investigador Forense

La tarea de un investigador forense digital es difícil. Es unas de las ocupaciones más adversas en las Tecnologías de la Información. Usted deberá tener cada aspecto de su trabajo técnico y los métodos de examinación muy detallados.

Como tal, es imperativo que use un proceso determinístico, respetable, que sea claro, conciso y simple. El apego a este método formal es el mayor activo y ventaja de un investigador. Alejarse de estas recomendaciones provocara que su investigación sea en vano. Teniendo un proceso definido y corroborable significa que usted podrá mostrar varios elementos que son los siguientes.

- Validación de los hallazgos
- Manejo adecuado de evidencia
- Investigación completa
- Administración de archivos
- Trabajo técnico
- Definición explícita y justificada del proceso
- Cumplimiento legal
- Flexibilidad

Esta lista se convertirá en su libro de actuación el día que usted mismo asuma el control de una investigación o tenga que entregar a las autoridades competentes los resultados de sus hallazgos. Los elementos ya mencionados hacen la diferencia entre una investigación efectiva y jugar con una buena herramienta de análisis forense [CLI23]. El software para estos fines es bueno, sin embargo, mientras que sus amigos podrían estar impresionados por el conocimiento comprensivo en las últimas versiones de las herramientas de análisis forense el abogado opositor no lo estará, y más importante el juez menos lo estará.

- **Validación de hallazgos:** Cuando sea posible, confié en más de una herramienta para respaldar sus hallazgos. La validación es una de las herramientas clave disponibles para el investigador forense. Si solo confía en una sola herramienta durante su investigación, vivirá y morirá por esa misma herramienta.

- **Manejo adecuado de evidencia:** Una buena regla a seguir como investigadores forenses es la misma que se les enseña a todos los estudiantes de medicina. “No hacer daño”.
  La evidencia computacional es notoriamente un tema muy delicado, tan solo el hecho de manipular datos sin el uso adecuado de técnicas forenses puede provocar que los datos del sistema cambien. Deberá ser capaz de mostrar que la evidencia que presenta es exactamente la misma evidencia que existió al momento de adquirirla.
  Esto significa que no debe de modificar la evidencia en ningún modo como parte de su investigación. El investigador forense debe siempre estar consciente de la cadena de custodia de la evidencia después de su adquisición. Es vital que muestre quien ha tenido acceso a la evidencia, y sus acciones sobre ella.

- **Investigación completa:** Al realizar una investigación, el investigador forense debe ser capaz de mostrar que el condujo la búsqueda de evidencia en una forma completa. Use un proceso que garantice que ubicara cada pieza y hará referencia a dicha evidencia. Si no usa un proceso probado y sólido para adquisición de la evidencia, el análisis y el reporte perderá mucha evidencia.

- **Administración de archivos:** En el mundo de los abogados, solamente porque un juez haya dictaminado a favor o en contra, no significa que el caso haya terminado. Sin embargo, un investigador puede ser consultado meses después del caso para revisarlo. Esto hace siempre que imperativamente se asegure de que un caso es administrado y archivado apropiadamente. Esto significa una adecuada gestión de documentación, almacenamiento y políticas de respaldo.

- **Trabajo técnico:** Tener un completo entendimiento de todo lo que está haciendo es una gran ventaja. La forma segura de perder un caso es justificar sus acciones al decir. “Eso fue lo que la herramienta indicaba hacer”. Desafié las suposiciones que la herramienta genera. Si ya se ha establecido en un conjunto de herramientas entienda lo que hace la herramienta.

- **Definición explicita y justificación del proceso:** Debe conducir la investigación en la manera que le permita seguir todos sus pasos. Se debe seguir una ruta clara y discreta mientras se realiza una investigación que sea fácilmente explicable ante un juez y la audiencia opositora.

  Si al final es cuestionado acerca de la metodología que siguió y su forma de pensar que le permitieron deslumbrar los resultados que está

presentando, debe justificar sus hallazgos. Hágalo mostrando punto por punto y llevándolos a través del proceso que realizo a lo largo de la investigación.

- **Cumplimiento legal:** Siempre asegúrese que su proceso es conforme a las leyes y regulaciones en la jurisdicción de su investigación. En una investigación corporativa interna, garantice que cumple con las políticas establecidas por el corporativo. Las técnicas más creativas y astutas en investigaciones son insignificantes si no se apegan a las cuestiones legales del caso. Al final del día el papel del investigador es de lo más importantes ya que en el recae toda la responsabilidad.

- **Flexibilidad:** Cada investigación es diferente. Cada una tiene sus propios requerimientos. El proceso que se use para realizar la investigación debe ser capaz de hacer frente al cambio.
  Un problema común en los examinadores novatos es confiar en una sola herramienta. Si la investigación requiere que busque evidencia en tecnología no soportada por la herramienta todo su trabajo no tendrá valor. Asegúrese de que el diseño de su proceso puede lidiar con tecnologías y requerimientos nuevos.

3.3. Presentación de la Metodología

Ahora que sabemos que es lo que hace que un investigador forense sea bueno y que elementos de dicho proceso debe tomar en cuenta, podemos definir la metodología. Lo que resta de este capítulo nos enfocaremos en cada una de las fases de la metodología la cual fue desarrollada por Electronic Discovery Reference (EDRM). Dicha industria es un grupo de trabajo que fue creado en Mayo de 2005 para crear un proceso estandarizado para al análisis y producción de datos electrónicos. La cual ha sido probada en los aspectos legales y técnicos. Adicionalmente es lo suficiente flexible para conllevar diversos requerimientos que se pueda encontrar como investigador [XIA24].

1. Identificación
2. Adquisición y preservación
3. Análisis
4. Presentación

Cuando se aplican correctamente estos pasos pueden llevarlo a una completa y justificable investigación.

3.3.1. Identificación

La primera etapa del proceso detalla que hacer cuando se está presente en un caso y se necesita determinar la ruta de acción. 5 puntos principales sirven de guía a través de la fase de identificación.

1. ***Determinar el objetivo y cantidad de datos:*** Esto requiere que el investigador conozca las necesidades de la investigación para determinar el alcance de la examinación y la cantidad de datos requeridos.

2. ***Identificación de repositorios****:* Antes de iniciar la investigación y después de establecer el objetivo, se debe identificar la ubicación de los datos que potencialmente pueden contener evidencia. Puede encontrarse desde cómputo personal hasta servidores y dispositivos móviles. En este punto se necesita determinar si se tienen las herramientas para completar la investigación.

3. ***Estrategias para la preservación****:* Una vez que se determine dónde están los datos almacenados, se debe decidir qué pasos se requieren para proteger los datos a toda costa. Si se muestra que los datos fueron modificados fuera de los parámetros normales después del incidente ocurrido, se tendrán problemas al justificar los hallazgos. La preservación debe ocurrir lo más rápido posible

4. ***Establecer la cadena de custodia:*** Después de proteger la evidencia, es un requerimiento legal que la cadena de custodia sea establecida. Mientras más tiempo pase para establecer la cadena de custodia, más difícil será rastrear los hallazgos hasta los datos originales. Se debe demostrar que los datos están sin modificaciones y cada intento de consulta fue registrado.

5. ***Pre visualización de los datos:*** Solo después de completar los pasos 1-4 se deberá pre visualizar los datos en forma que garantice que no son modificados. Esto permitirá que se prepare la fase de adquisición de la metodología. Cuando se creé una copia forense de los datos para el propósito de la investigación e interpretación, se tiene que ser muy cuidadoso de usar solamente las herramientas forenses aprobadas.

3.3.2.Adquisición y preservación

Este es el punto en el cual se debe adquirir los datos de forma forense para conducir la investigación. Sin embargo, incluye puntos centrales en esta fase.

1. ***Identificación de medios:*** Los datos están en medio de almacenamiento, y es necesario saber qué tipo de datos están almacenados y como acceder a ellos, tal vez suene bastante obvio, pero imagine un escenario, por ejemplo, tiene unos respaldos en unas citas que tienen más de 15 años y nadie sabe qué formato tienen. Este tipo de situaciones son muy estresantes.

2. ***Parámetros de adquisición****:* Establecer los parámetros requeridos para una imagen adecuada es fundamental. El tipo de caso y requerimientos legales determinarán los parámetros.

3. ***Creación de la imagen:*** Después de determinar el tipo de medios y establecer los parámetros, se debe crear la imagen. El proceso de creación de la imagen debe asegurar que no se han modificado los datos y que la imagen está completa. Se deben tener los metadatos para acompañar la imagen, de este modo puede validar el proceso.

4. ***Autenticación****:* El propósito de este punto es determinar si la imagen que se ha creado es idéntica a los datos originales. La forma confiable de realizar esto es mediante hashes criptográficos. Antes de crear la imagen, se debe calcular el hash de los datos originales. Los 2 hashes que se han obtenido deben coincidir; En caso de que no coincidan significa que se hizo algo mal y se perderá el caso. Es importante que el hash sea colocado fuera de los datos, si se coloca dentro de la imagen se alterará la evidencia original y esto invalidara la imagen y la investigación.

3.3.3. Análisis

Después que se haya determinado que datos se necesitan examinar, y se hayan verificado las imágenes creadas, se puede comenzar con la investigación. Esta es la parte medular de la investigación.

Lo más importante a tener en cuenta cuando se realiza un análisis es que sea completo. Siempre asegurarse de haber buscado en todos los rincones y de que no te ha omitido nada relevante. Los abogados odian cuando un abogado opositor encuentra nueva evidencia que destruye su caso. Sé debe ser completo y creativo; el pensamiento poco convencional ayudará mucho en esta fase.

3.3.4. Presentación

Después de completar su investigación, es probable que haya presentado evidencia e información relevante para el caso. Otras personas pueden estar interesadas en estos hallazgos, especialmente aquellos que pagan su factura.

En general, solo recuerde mantenerlo simple. Para evaluar qué tan bien articulado es su caso, busque al miembro menos competente técnicamente de su familia y explíquele sus hallazgos. Si logra ese objetivo con éxito, estará listo para presentar los datos a un abogado. Los abogados son abogados y los directores generales son directores generales; Si tiene que describir las complejidades del último formato de imagen para ellos, probablemente no haya destilado lo suficiente sus hallazgos. Para los investigadores altamente técnicos, esta puede ser la fase más difícil del proceso, así que pise con cuidado.

3.4. Análisis Forense en Móviles

El campo del análisis forense en móviles se ha disparado en los últimos tiempos y es una de las áreas más importantes de investigación debido a razones muy importantes que iremos mencionando. Primero y ante todo, las capacidades de los teléfonos han ido mejorando grandemente; estos dispositivos son indiscutiblemente más importantes que las computadoras de escritorio o laptops debido a que generalmente son usados más frecuentemente. Por lo tanto, continuamente registran nuestros movimientos y actividades proporcionando una tremenda perspectiva acerca de nuestro comportamiento. Las comunicaciones en estos dispositivos son muy diferentes comparadas con las del cómputo tradicional; curiosamente los criminales frecuentemente dicen y escriben cosas en los dispositivos móviles que nunca escribirían en una computadora.

El Forense en dispositivos móviles no siempre se ha tomado en serio. Hasta por el 2008, si usted le preguntaba algún investigador sobre investigación en celulares, probablemente habría escuchado la típica respuesta, que nadie en el laboratorio trabaja con dichos aparatos dado que no contienen nada de valor.

Los dispositivos de hardware de imagen también se han utilizado por varios años, pero originalmente no fueron usados para investigaciones. Algunas empresas vendían hardware a minoristas de teléfonos celulares que necesitaban copiar la información de contactos y el SIM del dispositivo de un cliente a otro, generalmente pasaba cuando un cliente quería un nuevo celular más actualizado.

Cuando las leyes se vieron involucradas en investigaciones forenses en móviles. Dichas empresas como Cellebriti hicieron algunas modificaciones menores al hardware y continuaron vendiéndolo.

El forense en celulares siempre fue importante, pero no muchas personas se dieron cuenta de su importancia, lo cual no es sorprendente. El software disponible para análisis forense podría no ser compatible con la mayoría de móviles.

Después de que el internet fuere agregado a las características de los móviles, la importancia de su investigación en este campo continúo creciendo. Con la demanda de este auge se introdujeron mejores softwares. Repentinamente más evidencia estaba disponible, incluyendo e-mail, búsquedas en internet y actividades en redes sociales. Actualmente cada laboratorio de análisis forense cuenta con capacidades de realizar forense en móviles. Además, se logra destacar una separación de funciones en laboratorios grandes. Por ejemplo, un investigador puede ser responsable de la extracción de evidencia en Smartphone, mientras su colega podría estar a cargo de desarrollar el informe técnico ejecutivo, mientras otro puede encargarse de recuperar y analizar datos de las estaciones transceptoras.

El análisis forense en móviles tiene tremendos desafíos, sin embargo, distintos dispositivos aun no pueden ser analizados. El Hardware y Software forense solamente soporta las versiones más actuales y populares de los Smartphones, mas de cientos de nuevos Smartphones salen al mercado cada año, por otra parte, varios modelos nunca serán soportados por herramientas de análisis forense.

Algunas de las examinaciones más problemáticas es sin duda pagar a los fabricantes de dichos dispositivos para que ellos continúen con la investigación.

El problema de las aplicaciones y plataformas móviles es que están cifradas, desarrolladas para dispositivos móviles por empresas como Silent Circle es además relevante. El BlackPhone es otro desafío porque sus desarrolladores afirman proteger los datos de sus clientes a través de un cifrado robusto y avanzado.

Además, investigadores encaran una gran cantidad de S.O ejecutándose en dispositivos móviles. Un investigador trabajando con una laptop generalmente se encontraba con Microsoft Windows o Apple´s mac OSX, por otra parte, si un investigador se encuentra trabajando en Smartphone se puede topar con diferente micro kernels los cuales ya mencionamos y retomaremos más adelante.

Mirando a futuro, podemos decir que aumentara la necesidad de hacer forense en dispositivos móviles, debido la rápida expansión de proveedores de dispositivos de cómputo móvil. El vociferante mercado de Android y IOS significa que los forenses deben comenzar a mirar no solo adentro del dispositivo si no hacía fuera, prestando atención a lo que antes no considerábamos; como lo son las sincronizaciones con la computadora, dispositivos inteligentes en el hogar, sistemas remotos en la oficina y la nube.

Cada vez más los dispositivos móviles tendrán gran dependencia en el Cómputo Móvil, lo que significa que los investigadores dependerán cada vez más de la evidencia que va más allá del proveedor de servicios [RIC25]. Aplicaciones integradas encontradas en los dispositivos como Facebook y Gmail son importantes y continuaran siéndolo. Además, deberíamos pensar continuamente fuera de la rutina, como lo hacen los buenos investigadores. Por ejemplo, muchos usuarios de Smartphone con carro último modelo, pueden sincronizar su dispositivo con el automóvil para escuchar música y recibir llamadas. Esta apertura de nuevas posibilidades es al parecer maravillosa para el usuario, sin embargo, para los investigadores implica que no solo debe preocuparse por la evidencia contenida en los móviles, sino también por la compartida con dispositivos inteligentes. Lo cual obliga aumentar el campo de la investigación, trayendo nuevos esquemas de procedimientos y estándares de referencia.

No olvidemos que las personas almacenan una gran riqueza de información en sus celulares y Smartphones, y el pensamiento de perder el dispositivo y la información almacenada dentro de él, puede ser una perspectiva muy aterradora. Debido a esta preocupación mucha gente trata de resguardar la información de sus dispositivos,

desgraciadamente lo hacen rutinariamente y de una forma incorrecta, utilizando contraseñas predefinidas por el fabricante. Antes dependía del modelo del dispositivo que se tuviera, para poder guardar y registrar información, por lo contrario, en fechas actuales los Smartphones contienen gran cantidad de información valiosa como lo son:

- Llamadas entrantes, salientes y pérdidas
- Multimedia, mensajes, mensajes de texto y sms
- Cuentas de e-mail
- Logs
- Páginas web
- Imágenes, videos, fotos, música y archivos
- Calendario
- Agenda
- Información de redes sociales
- GPS
- Grabaciones de voz y mensajes de voz

Mucha gente almacena más información en sus Smartphones que en su computadora y efectivamente los dispositivos contienen más información por byte examinado que las computadoras tradicionales [HAR26]. Frecuentemente armar un caso con solo la información almacenada en el dispositivo es posible. En diferentes países los Smartphones son utilizados para ingresar en cuentas bancarias, realizar depósitos y transferencias de un dispositivo a otro, lo cual proporciona más evidencia potencial.

El uso de Smartphone para actividades ilícitas como el robo de identidad, pornografía infantil y fraudes bancarios se ha convertido en algo cotidiano.

Dado que los dispositivos son incautados en el momento del arresto, los oficiales suelen revisarlos como parte de un procedimiento. Además, debido a que los Smartphone contienen información privada o sensible puede ser de gran ayuda en el escenario de un crimen.

Dado a su gran utilidad de estos dispositivos, pueden proporcionar pistas para una investigación, la investigación en Smartphones y otros dispositivos móviles es una de las tareas más desafiantes en un análisis forense. No existe un estándar de cómo los dispositivos deben almacenar los archivos y en donde, a pesar de que varios teléfonos utilizan esquemas similares de almacenamiento. Adicionalmente nuevos modelos salen al mercado aproximadamente cada 6 meses, y son relativamente incompatible con modelos anteriores. Por ende, los cables, accesorios y software utilizado en el análisis forense tienden hacerse obsoleto muy rápidamente en estas situaciones.

La tecnología móvil ha avanzado rápidamente en las últimas décadas y se ha desarrollado más allá de lo que sus inventores pudieron haberse imaginado. Los días pasaron en que solo los ricos podían comprar un celular. Para finales del 2008 los teléfonos móviles habían pasado por 4 generaciones: análogo, digital, SCP y 3G.

La tercera generación introdujo capacidades inauditas, como la capacidad de descargar mientras uno se encuentra caminando o en movimiento dentro de un vehículo. Nextel introdujo las redes 4G en 2009.

Los dispositivos móviles pueden variar desde simples teléfonos hasta pequeñas computadoras llamadas Smartphones. Su hardware consiste de un microprocesador, ROM, RAM, procesador de señal digital, radio modulación, micrófono, alta voz, interfaces de hardware (teclado, cámara, pantalla, GPS). Muchos contienen tarjetas de memoria removibles con capacidades de más de 64 GB.

Los teléfonos más básicos tienen un S.O propio, a pesar de que los Smartphones utilizan el mismo sistema operativo que las computadoras (o mejor dicho una versión reducida de ellos). Los sistemas operativos incluidos son Windows Mobile, Android, Google OS y IOS. Típicamente almacenan los datos en memorias de solo lectura programables y borrables electrónicamente (EEPROM), lo que permite a los fabricantes reprogramar los teléfonos sin tener la necesidad de acceder a la memoria de los chips físicamente.

Muchos usuarios toman ventaja de estas oportunidades, reprogramando sus teléfonos para agregar nuevas características y funcionalidades o para cambiar de proveedor o de plan tarifario. A pesar de que estos servicios de reprogramación no son brindados como soporte técnico por parte de los proveedores, instrucciones detalladas de cómo realizarlo están disponibles en internet.

El S.O almacenado en la ROM, la cual es una memoria no volátil sigue disponible, aunque el dispositivo se apague o se le termine la batería.

Los PDAs (asistentes digitales personales) han sido mayormente remplazados por los iPads y otras tablets los cuales están diseñados para tener la capacidad de sincronizarse remotamente con su computadora.

3.4.1.Proceso de extracción de evidencia (Metodología)

La extracción de evidencia y examinación forense puede diferir entre cada móvil. Sin embargo, el siguiente esquema de examinación forense asistirá al analizador forense para asegurar que le evidencia extraída de dicho dispositivo está bien documentada y que los resultados sean repetibles y defendibles. No hay ninguna metodología única, ni un proceso estandarizado. Sin embargo, la siguiente figura proporciona un panorama de las consideraciones a tomar durante el proceso de extracción de evidencia en los dispositivos móviles.

Todos los métodos usados cuando se está extrayendo datos de los dispositivos deberán ser probados, validados y bien documentados.

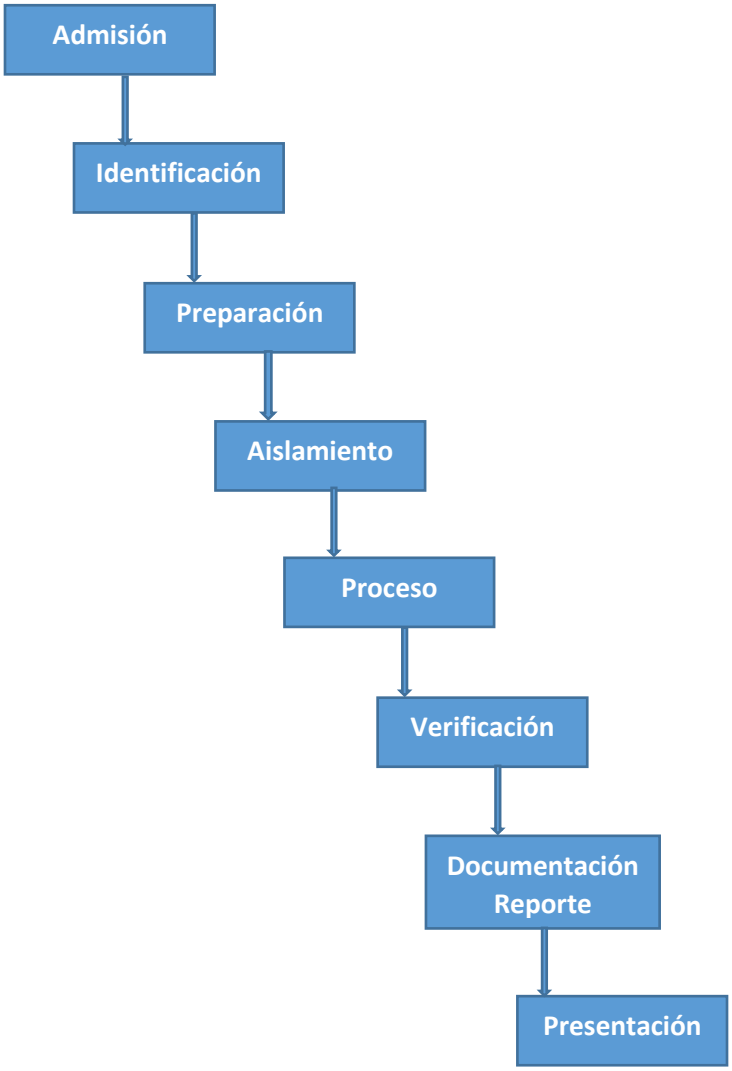


Figura 20 Proceso de extracción de la evidencia en móviles.

- **Fase de Admisión:** La fase de admisión de evidencia es el principio de todo, lo que implica formularios de registro y formas para documentar quien es el encargado de resguardar la evidencia y el tipo de incidente en el cual se vio envuelto el móvil, es la descripción acerca del tipo de datos que el investigador está buscando. Desarrollar los objetivos específicos para cada examinación es la parte crítica de esta fase. Sirve para aclarar los objetivos del examinador.

- **Fase de identificación:** El examinador forense deberá identificar los siguientes detalles para examinación del dispositivo móvil.

    - La autoridad legal
    - Objetivo de la examinación
    - El estado del dispositivo, marca, modelo e identificación de sus características
    - Almacenamiento externo e interno
    - Otras fuentes de evidencia potencial

- **Autoridad Legal:** Es importante para el examinador forense documentar y determinar qué autoridad legal existe durante la adquisición y examinación del dispositivo, así como cualquier limitación encontrada antes del análisis del dispositivo.

- **Los objetivos de la Examinación:** El examinador identificará que tan exhaustivo debe ser el análisis en función de los datos solicitados.

- **Identificación de características del dispositivo:** Como parte de la examinación, se debe identificar el modelo del teléfono y versión, para asistir a determinar que herramientas se utilizaran durante todo el procedimiento.

- **Almacenamiento interno y externo:** Muchos dispositivos dan la opción de expandir el almacenamiento con tarjetas externas como Micro SD, en caso de una memoria de este tipo sea encontrada en un móvil que se somete a examinación, la memoria deberá ser removida y utilizar técnicas forenses tradicionales. También es aconsejable adquirir la tarjeta mientras está en el dispositivo móvil para garantizar que los datos almacenados tanto en la memoria del teléfono como en la tarjeta estén vinculados para facilitar el análisis.

- **Otras fuentes de evidencia potencial:** Dispositivos móviles actúan como buenas fuentes de huellas digitales y evidencia biológica. Dicha evidencia

debe recuperarse antes del análisis del dispositivo para evitar problemas de contaminación. Los examinadores deberán utilizar guantes mientras manipulan el dispositivo.

- **Fase de preparación:** Cuando el modelo del dispositivo es identificado, la fase de preparación implica la investigación con respecto al teléfono móvil que se analizara, los métodos y herramientas apropiadas que se utilizaran para la adquisición.

- **Fase de aislamiento:** Los teléfonos móviles están diseñados para comunicarse a través de redes celulares, wifi, bluetooth e infra rojo. Cuando el móvil se encuentra conectado a una red, nuevos datos son agregados cómo llamadas entrantes, mensajes y datos de aplicación, la cual modifica la evidencia del teléfono. La destrucción de la evidencia es posible a través de acceso remoto, o comandos de borrando. Por esta razón, el aislamiento de fuentes de comunicación es importante antes de la adquisición y examinación del dispositivo. El aislamiento puede ser realizando mediante el uso de bolsitas de Faraday, las cuales bloquean las señales de radio entrantes y salientes del teléfono. En investigaciones anteriores encontraron inconsistencias en la protección total de las comunicaciones con las bolsas de Faraday. Por lo tanto, asilamiento de la red es recomendable. Esto puede hacerse colocándolo en un paño protector de radio frecuencia y luego estableciendo el dispositivo en modo avión.

- **Fase de Procesamiento:** Cuando el teléfono ha sido aislado de las redes de comunicación, el proceso comienza. La adquisición del dispositivo debe ser utilizando métodos probados que sean repetibles y lo más apegado a técnicas forenses. La extracción física es el método preferido ya que extrae datos de la memoria en crudo y el dispositivo permanece encendido durante el proceso. En la mayoría de los dispositivos, se producen la menor cantidad de cambios en el dispositivo durante la adquisición física. Si la adquisición física no es posible o falla, se debe intentar adquirir el sistema de archivos del dispositivo. Siempre se deberá obtener una adquisición lógica, ya que puede contener los datos analizados y proporcionar indicadores para analizar la imagen de la memoria en crudo.

- **Fase de verificación:** Después de procesar el móvil, el examinador necesita verificar la exactitud de los datos extraídos del dispositivo para asegurar que los datos no han sido modificados. La verificación de los datos se puede lograr de distintos modos

- **Comparando los datos extraídos con los datos del teléfono:** Corroborar si los datos extraídos del teléfono coinciden con los datos que muestra el teléfono. Los datos extraídos pueden ser comparados con el dispositivo mismo con un reporte lógico, lo que sea preferido. Recuerde que manipular el dispositivo puede provocar cambios a la única evidencia.

- **Usando múltiples herramientas y comparando los resultados:** Para garantizar la exactitud, utilice diferentes herramientas y compare los resultados

- **Funciones hash:** Todas las imágenes obtenidas deber tener su valor hash asociado después de la extracción, para asegurar que permanecen sin cambios. Si la extracción del sistema de archivos es posible, el analista calculara el hash después de extraer el sistema de archivos. Posteriormente si algún archivo es extraído individualmente se debe computar su hash y verificar comparando con el archivo original garantizando así la integridad de la evidencia. Cualquier discrepancia en el valor del hash obtenido debe ser explicada, cómo por ejemplo si el dispositivo se apagó y encendió y posteriormente se volvió adquirir el valor hash.

- **Fase de documentación y reporte:** El examinador debe documentar todo el proceso durante el análisis, en forma detallada y clara, relatando lo que fue echo durante la adquisición y examinación. Cuando el examinador termina la investigación, los resultados deben pasar a través de una forma de pre verificación, para asegurar que los datos son revisados y la investigación es completa. E reporte debe incluir lo siguiente.

    - Fecha de inicio y fin de la examinación
    - Las condiciones físicas del teléfono
    - Fotos del teléfono y componentes individuales
    - El estatus del teléfono al ser recibido
    - Marca y modelo del teléfono
    - Herramientas utilizadas para la adquisición
    - Herramientas usadas durante la examinación
    - Datos encontrados durante la examinación
    - Notas concluyentes

- **Fase de presentación:** A lo largo de la investigación, es importante que nos aseguremos que la información extraída y documentada del dispositivo pueda ser claramente presentada a otro investigador o una corte. Crear un reporte forense de los datos extraídos durante la adquisición y análisis es importante. Debe ser incluido en ambos formatos en digital y físico. Sus hallazgos deben ser documentados y presentados de una manera que la

evidencia hable por sí misma en una corte. Los hallazgos deben ser claros, consistentes y repetibles. La línea de tiempo y opciones ofrecidas por diferentes softwares deben ser añadidos al reporte explicando los hallazgos.

3.4.2. Instituto Nacional de Estándares y Tecnología (SP 800-101)

El Instituto Nacional de Estándares y Tecnología (NIST) proporciona estándares de procedimientos operativos para una diversidad de prácticas científicas, en las cuales incluye forense en móviles. La publicación especial del NIST 800-101 revisión uno emitió directrices sobre análisis forense en Smartphones en 2014. El NIST es una organización que cuenta con una amplia presencia, por lo cual les debe sonar familiar. Los investigadores forenses deben estar familiarizados con estos lineamientos.

Propone 4 etapas para una examinación forense

- Preservación
- Adquisición
- Examinación y análisis
- Reporte

3.4.2.1. NIST Recursos para validación de herramientas

El primer paso a realizar es que, cómo con otras herramientas de cómputo forense tradicional deben ser validadas antes de su uso en una investigación. Es esencial usar datos probados, y seguir protocolos de investigación establecidos para determinar qué datos pueden ser extraídos. Además, una verificación debe ser echa contra otras herramientas de análisis forense en móviles. Preguntas acerca de este proceso de validación pueden surgir en un juicio en una corte. La validación además incorpora el uso de funciones hash criptográficas como SHA-2, SHA-3, etc. Esto con la finalidad para garantizar que los resultados obtenidos al utilizar una herramienta pueden ser reproducidos con la misma salida de la función resumen.

Durante el proceso de validación, las tasas de error deben ser claramente documentadas.

El NIST proporciona a examinadores vastos recursos sobre herramientas aprobadas. La prueba de herramientas de cómputo forense (CFTT) como su nombre lo indica brinda lineamientos probados que incluye pruebas de criterio, prueba de conjunto y prueba de hardware. Más información puede ser encontrada en el sitio web del NIST [5].

La librería nacional de referencias de software (NSRL) provee dirección en el uso efectivo de tecnología que requiere la investigación de evidencia digital. Para mayor información consulte [6].

El NIST ha proporcionado conjuntos de datos de prueba de evidencia digital. El Conjunto de Datos de Referencia en Cómputo Forense (CFReDS) para evidencia digital son pruebas que pueden ser usadas para validar herramientas forenses, probar equipos y capacitar personal [7].

Con los Smartphones, un problema fundamental surge cuando se comienza a realizar forense. Dado que los dispositivos traen incorporada una pequeña capacidad de memoria, es por eso que la utilización eficiente de memoria es esencial. Esto viene acompañado con el hecho de que los móviles están continuamente conectados a redes celulares e inalámbricas, lo que significa que los datos del dispositivo están continuamente cambiando. Cuando un examinador forense intenta extraer evidencia de un dispositivo, se pueden provocar cambios en el Smartphone. Recordemos que lo importante es que los datos creados por el usuario permanezcan inalterados usando las mejores prácticas. Por lo tanto, la evidencia es admisible cuando el proceso es documentado apropiadamente.

3.4.3. Evidencia en Móviles

3.4.2.2. Delitos en dispositivos móviles

La red GSM/UMTS atiende más de 4 billones de usuarios en todo el mundo. Obviamente los criminales también están incluidos entre ellos. Los criminales están usando la tecnología como ganancia personal en los cuales se encuentran envueltos teléfonos móviles en diferentes actividades ilegales y criminales. Antes de que se prohibieran los servicios anónimos, las tarjetas de prepago y los teléfonos desechables fueron un común método de comunicación para cualquier tipo de actividad criminal, que van desde extorción hasta tráfico de drogas. Por otra parte, siendo particularmente dispositivos pequeños con un valor monetario aumentado, los teléfonos móviles son un fácil objetivo para ladrones. Finalmente, otro fenómeno a tratar es el acoso y el bullying mediante llamadas telefónicas, a si cómo los mensajes amenazantes.

En casos más serios, debemos considerar además el factor de la seguridad física. Este factor puede ser un resbalón en nuestra atención si consideramos que la recopilación de evidencia es siempre un procedimiento libre de riesgo. Un teléfono móvil puede transformarse en un mecanismo de detonación, con capacidades de activación desde cualquier punto del planeta, usando simplemente una llamada

entrante. Respectivamente, la bomba en el metro de Madrid de 2004 se activó usando la alarma del teléfono.

Al mismo tiempo, al enfocarse en crímenes de cuello blanco con teléfonos móviles presentes, observamos todo tipo de fraudes digitales, robo de identidad, espionaje industrial y lo que nos faltan por mencionar. El futuro que ofrece las posibilidades de comercio en línea, utilizando dispositivos inteligentes para pagar y ofrecer servicios, hará más grande el problema e intenso, proporcionando más espacio a los delincuentes para efectuar actividades criminales.

3.4.2.3. Evidencia

Como hemos mencionado en estos capítulos, los dispositivos móviles proporcionan continuamente un flujo de datos e información acerca del usuario y su comportamiento. ¿Dónde reside toda esta información? No solamente en el mismo teléfono sino también en los sistemas de redes comunicación de los proveedores de servicio. La evidencia no solo se puede encontrar específicamente en la memoria interna del móvil, la tarjeta SIM, la memoria externa [AND27]. No olvidemos el caso cuando los Smartphones están conectados o de cierta forma sincronizados con una computadora. Por lo tanto, la evidencia sobre el uso del teléfono puede ser también encontrada en la computadora. La búsqueda de datos que pueden ofrecer evidencia adecuada son los siguientes.

- Agenda y contactos
- Llamadas entrantes, salientes y perdidas
- Mensajes
- Grabaciones de Voz
- Fotografías y videos
- Calendario, alarma y recordatorios
- Correos
- Páginas web visitadas
- Archivos
- Credenciales de usuario
- Localización geográfica

Un importante particular factor diferenciador acerca del cómputo forense es el hecho de que los teléfonos fueron tradicionalmente sistemas más cerrados, permitiéndole menos control al usuario en funcionalidades del núcleo y sistema operativo. Era difícil saber dónde los datos se almacenaban. Incluso con los sistemas operativos modernos de los Smartphones, considerablemente hay menos información con

respecto a su funcionamiento interno. Por eso, los datos trazados por las aplicaciones permanecen en memoria, posiblemente en áreas donde el usuario no tiene acceso para borrarlas.

Un ejemplo muy simple es el caso de cuando queremos borrar un mensaje, no siempre significa que la información fue permanentemente borrada. Más bien, las áreas específicas de memoria son marcadas como libres para tener mayor almacenamiento. Si la información misma no es sobre escrita, continuara existiendo en memoria, aunque el usuario crea que ha sido borrada.

3.4.2.4. Características de la evidencia en Móviles

Los juzgados confían cada vez más y más en la información dentro de un dispositivo móvil. Para que la evidencia sea prevaleciente en un tribunal, requiere un buen y claro entendimiento de sus características.

El forense en dispositivos móviles es relativamente una nueva disciplina y la ley es quien dictamina la validez de la evidencia. Por lo cual debemos tener en cuenta sus características las cuales aplican al cómputo forense y necesitan ser seguidas y respetadas, para que la evidencia sea útil. Si se ignoran estas características la evidencia se vuelve inadmisible, provocando que su caso se pueda ir por la borda. Las 5 características son:

- **Admisible:** Es una de las más básicas y una medida de la validez de la importancia de la evidencia. La evidencia debe ser preservada y obtenida de modo que pueda ser usada en un juzgado o en cualquier otro lugar. Muchos errores podrían causar que un juez dictamine que una pieza de evidencia es inadmisible. Por ejemplo, evidencia que es obtenida utilizando métodos ilegales.

- **Autentica:** La evidencia debe estar relacionada a un incidente relevante de tal forma que pueda probar algo. El examinador debe ser responsable del origen de la evidencia.

- **Completa:** Cuando la evidencia sea presentada debe ser clara y completa y debe reflejar toda la historia. No es suficiente colectar evidencia que solo muestre una perspectiva del incidente. Presentar evidencia incompleta es más caótico que no proporcionar ninguna evidencia, lo cual puede conducir a diferentes dictámenes.

- **Confiable:** Evidencia adquirida de un dispositivo móvil debe ser confiable. Esto depende de la metodología y herramientas usadas. Las técnicas usadas y la evidencia reunida no deben causar duda de la autenticidad de la evidencia. Si el examinador utiliza alguna técnica que no pueda ser reproducida, la evidencia no se considerara a menos que haya sido dirigido a hacer eso.

- **Creíble:** El examinador forense debe ser capaz de explicar con claridad y consistencia que proceso uso, la forma en que fue preservada la integridad. La evidencia presentada por el examinador debe ser clara, fácil de entender y creíble por un jurado.

3.4.2.5. Desafíos y Problemas

Uno de los grandes desafíos del forense es el hecho que no se puede acceder a los datos que se almacenan en plataformas móviles que se sincronizaron a través de diferentes dispositivos móviles.

Como los datos son volátiles pueden ser rápidamente transformados o borrados remotamente, se requieren más esfuerzos para la preservación de los datos.

El Forense en dispositivos móviles es diferente al forense en cómputo tradicional y presenta retos únicos a los investigadores forenses.

Las leyes y normas que se tratan de implementar en ocasiones chocan con los investigadores, frecuentemente cuando hay que obtener evidencia digital de los dispositivos móviles. Los siguientes puntos son una de las razones.

- **Diferencias entre hardware:** El mercado se encuentra inundado con una gran variedad de modelos de Smartphones de diferentes fabricadores. Los examinadores forenses se pueden cruzar con diferentes modelos, hardware, características y sistemas operativos. Además, no olvidemos mencionar el ciclo de vida tan corto que tienen estos modelos. Como el panorama de los dispositivos móviles siga cambiando con el paso de cada día, esto se vuelve una tarea más crítica para los investigadores debido a que será caótico adaptarse a todos los desafíos y permanecer en constante actualización de nuevas tendencias en técnicas forenses.

- **Sistema operativo:** A diferencia del cómputo personal donde Windows ha dominado el mercado por años, los Smartphones usan más ampliamente

sistemas operativos como ; IOS, Google, Android, RIMs, Windows phone, HPs, webOS, Symbian y muchísimos más.

- **Características de seguridad en plataformas móviles:** Las plataformas móviles modernas contienen características de seguridad para proteger los datos de los usuarios y su privacidad. Estas características actúan cómo un obstáculo durante una adquisición y examinación. Por ejemplo, los dispositivos móviles modernos integran cifrado por default desde la capa del hardware hasta llegar al software. Ocasionando que los examinadores tengan que abrirse pasó a través de estos mecanismos de cifrado para extraer datos del dispositivo.

- **Escases de recursos:** Como mencionamos anteriormente, con el número creciente de Smartphones, las herramientas requeridas por un examinador aumentaran. Accesorios de adquisición forense, como cables USB, baterías y cargadores para diferentes dispositivos se tendrán que estar cambiando constantemente para asegurar su compatibilidad.

- **Estado genérico del dispositivo:** Aunque el dispositivo aparente estar en estado inactivo, puede tener procesos corriendo en background. Por ejemplo, en muchos dispositivos, las alarmas programadas siguen funcionando aun cuando el teléfono es apagado. Un cambio repentino de un estado a otro puede resultar en modificación o pérdida de información.

- **Técnicas anti-forenses:** Cómo el ocultamiento de información, ofuscamiento, falsificación y el borrado seguro, hacen la investigación más difícil.

- **Naturaleza dinámica de la evidencia:** Evidencia digital puede ser fácilmente alterada ya sea intencionalmente o no. Por ejemplo, navegar por una aplicación en el teléfono puede alterar los datos almacenados por esa aplicación en el dispositivo.

- **Formateo accidental:** los dispositivos móviles dan opción de formatear todo. Formatear el teléfono accidentalmente durante una examinación puede resultar en una pérdida de evidencia.

- **Alteración del dispositivo:** Las posibles formar de alterar el dispositivo pueden variar desde mover una aplicación, renombrar archivos, modificar el sistema operativo del fabricante.

- **Contraseña de recuperación:** Si el dispositivo es protegido con contraseña, el examinador forense necesitara ganar acceso al dispositivo sin dañar los datos del mismo.

- **Falta de disponibilidad de herramientas:** Hay una amplia variedad de Smartphones. Una sola herramienta no puede soportar todos los dispositivos o realizar todas las funciones necesarias, por eso una combinación de herramientas necesitan ser usadas. Escoger la herramienta correcta puede ser difícil.

- **Software malicioso:** El dispositivo puede contener software o código malicioso, como virus o trojanos. Algunos programas maliciosos pueden propagarse en otros dispositivos ya sea mediante conexión cableada o inalámbrica.

- **Cuestiones legales:** Los dispositivos móviles pueden encontrarse involucrados en crímenes, los cuales pueden traspasar fronteras geográficas. Para abordar estos problemas multi-jurisdiccionales, el forense debe conocer la naturaleza del delito y las leyes regionales.

¿Qué hay acerca de la privacidad y seguridad? Las conexiones inalámbricas toman lugar sobre puntos de acceso públicos lo cual es relativamente posible intervenirlo.

Puede parecer que técnicas tradicionales de criptografía puedan ser usadas para asegurar conexiones inalámbricas. Sin embargo, el problema principal es que estas técnicas están diseñadas e implementadas para redes cableadas y son computacionalmente muy demandantes en cuanto recursos. Tratar de reducir estas demandas de poder cómputo conlleva a usar esquemas de seguridad que son relativamente fácil de vulnerar.

3.5. Análisis Forense en la Nube

Realizar una investigación forense en la Nube es el proceso de recuperar evidencia digital de la Nube para fines de la investigación. Los atacantes hacen uso del Cómputo en la Nube para cometer delitos en diversas formas, ya sea almacenar evidencia incriminatoria como pornografía infantil, lanzar ataques o cracker llaves cifradas. Los atacantes pueden aprovisionarse de una instancia de la Nube, cometer algún crimen, e inmediatamente dejar la instancia de la Nube para destruir la evidencia.

Los datos inaccesibles, la potencial fuga de información, la procedencia desconocida de evidencia son una de las mayores preocupaciones de las investigaciones digitales en la Nube debido a que puede resultar en un escenario donde la evidencia no sea admisible, o que la integridad no pueda ser verificada en el sistema utilizado por la Nube.

El cómputo en la Nube esta rápidamente envolviendo soluciones tecnológicas y modelos de negocio, dando como resultado el aumento global de la adopción de servicios en la Nube. Si bien el Cómputo en la Nube tiene sus origines en el cómputo distribuido y comparte similitudes con el hosting tradicional de internet, las vías en las cuales los servicios de la Nube son ofrecidos difieren drásticamente.

Los suscriptores de la Nube pueden aprovechar el auto aprovisionamiento, auto escalamiento, y pago por uso a través de servicios que ofrecen una mayor disponibilidad, rendimiento y escalabilidad. En este aspecto el Cómputo en la Nube es un paso evolutivo en el aprovisionamiento de servicios en internet, permitiendo fácilmente a organizaciones contratar requerimientos tecnológicos y pagar solamente por los recursos que usan.

Los proveedores de servicios de Nube como lo son Google, Amazon y Microsoft están impulsando la expansión al convertir su exceso de capacidad en un modelo comercial de pago por lo que se use, lo que permite ofrecer recursos tecnológicos escalables.

Estas bondades son facilitadas por la disponibilidad de conectividad de banda ancha a altas velocidades y acceso a bajo costo.

La gran oferta de recursos anónimos de cómputo en la Nube, proporciona un amplio margen de crímenes digitales [HOP28]. Es por eso importante señalar y ser conscientes que información sensible como los datos de tarjeta de crédito y números de seguridad social almacenados en la Nube los convierten en un objetivo atractivo que puede ser traducido en robo de información confidencial.

Además, los recursos de Cómputo en la Nube como el fácil uso de cifrado, y canales de comunicación anónimas reduce la probabilidad de que las actividades nefastas llevadas a cabo por grupos Cibercriminales sean intangibles para algún juez.

No obstante, los servicios de la Nube también pueden ser usados para llevar a cabo ataques de negación de servicios. Con la ayuda de un simple programa llamado "*Thunder Clap*" que cuesta tan solo 6 dólares se puede aprovechar de 10 servidores virtuales de Amazon Elastic Cloud Computing (EC2) con el propósito de lanzar un ataque exitoso de negación de servicio en contra de la organización que usted quiera, provocando que este fuera de servicio en internet. Se tiene constancias de que ataques que usan estas técnicas y gracias a las comodidades que brinda la Computación en la Nube no son detectadas por el proveedor de servicios y por lo cual no hay esfuerzos de mitigación en contra de la actividad maliciosa.

Incluso se sabe que muchas veces el software usado para controlar y lanzar los ataques es accionado o ejecutado vía línea comandos a través de redes sociales.

Debido a la ausencia de herramientas y metodologías específicas para la Nube, metodologías de Cómputo Forense tradicional han sido adaptadas para su aplicación dentro de ambientes de Cómputo en la Nube. Sin embargo, algo importante que se debe resaltar es que el enfoque de un análisis forense asume o da por hecho que la evidencia está totalmente bajo control del investigador. Por eso este enfoque no puede ser mapeado del todo en ambientes de Cómputo en la Nube.

Escenarios donde se requiere realizar investigaciones forenses en la Nube cambian las características tradicionales en como los datos, la evidencia potencial, son almacenados y recuperados. En la Nube la evidencia puede residir en diferentes localizaciones geográficas en servidores que son compartidos por diferentes clientes y que están bajo el control de diferentes proveedores de servicios en la Nube.

Esto impacta significativamente las fases de la identificación y adquisición de la evidencia, así como la cadena de custodia: Que su tarea fundamental es asegurar la integridad de la evidencia recuperada de la Nube lo que puede hacer que sea usada en procedimientos legales.

3.5.1. Cómputo Forense tradicional y Forense en la Nube

El Cómputo forense está definido como el uso de métodos científicos que derivan en preservación, análisis, interpretación, documentación y presentación de evidencia digital originada de recursos digitales con el propósito de facilitar y continuar con la reconstrucción de eventos criminales, o en el auxilio para anticipar acciones no autorizadas que muestran ser perjudiciales para la continuidad operativa de la organización. Por lo cual el Cómputo Forense en la Nube puede ser entendido como el uso de métodos probados para la preservación, colección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital de sistemas de cómputo distribuidos, de una manera que mantenga la integridad de la evidencia para que sea admisible en un tribunal.

Un modelo de proceso de forense digital proporciona un marco de trabajo para conducir buenas investigaciones forenses. Mientras no exista una metodología para investigaciones digitales en la Nube, un modelo genérico puede ser aplicado a distintas investigaciones forenses digitales sin importar la tecnología que se use.

En este subcapítulo se aclaró las diferencias entre el Cómputo Forense tradicional y el Forense en la Nube al involucrar el modelo de proceso de investigación digital propuesto por Carrier y Spafford [9]. El modelo incorpora 5 fases:

1. Preservación.
2. Investigación.
3. Búsqueda y colección.
4. Reconstrucción
5. Presentación.

3.5.2. Metodología Para Análisis Forense en la Nube

3.5.2.1. Fase de Preservación

La fase de preservación de una metodología de investigación forense tradicional involucra el aseguramiento de la escena del crimen y la preservación de la evidencia digital.

Lo que incluye el aislamiento del sistema de cómputo de la red, la recopilación de datos volátiles que pueden perderse cuando el sistema sea apagado, e identificar procesos sospechosos que se están ejecutando en el sistema. Los usuarios sospechosos que están registrados en el sistema deberán ser identificados y considerados para la investigación.

Los archivos de registro, frecuentemente contienen información valiosa y deben ser asegurados dado que hay la posibilidad de que puedan ser perdidos cuando el sistema sea copiado.

En el caso de una investigación forense en la Nube, la preservación inmediata de la máquina del sospechoso está limitada debido a la disponibilidad de la misma.

Cualquier otro intento directo por garantizar la preservación no es posible porque los datos son almacenados remotamente en imágenes virtuales. Sin embargo, cualquier investigador puede intentar preservar los datos residentes en la Nube al solicitar una orden legal dirigida al proveedor de servicios de la Nube. Lo que implica que el investigador debe confiar en el proveedor de servicios para adquirir y preservar los datos de alguna manera utilizado métodos forenses aprobados.

3.5.2.2. Fase de Investigación

El objetivo de la fase de investigación es identificar las piezas obvias del incidente y desarrollar teorías iniciales acerca del incidente. Piezas de evidencia volátil como la memoria deben ser recolectadas inmediatamente y documentadas para prevenir cualquier daño o incluso la corrupción.

Supongamos que tenemos el caso de una intrusión a un servidor en el cual un investigador busca por rastros obvios de instalación de piezas maliciosas como los son los rootkits, analiza los registros de la aplicación en busca de archivos nuevos de configuración. Pero en ambientes de Nube, el sistema de cómputo en la escena del incidente no siempre puede ser examinado para la búsqueda de evidencia. Aunado a esto, el investigador no tendrá acceso a fuentes externas de datos debido a que la examinación física de servidores remotos no es posible.

El nivel con el cual un investigador puede identificar evidencia potencial en ambientes de Nube está influenciado específicamente por el modelo de servicio en la Nube en uso [TAY29] (PaaS, SaaS, IaaS).

SaaS

En el modelo de SaaS el cliente no posee control sobre la configuración de la infraestructura como lo son el sistema operativo, aplicaciones y servidores, con la posible limitación del usuario a la configuración de características de la aplicación.
En este caso el investigador no tiene fácil el camino para identificar evidencia en el lado del servidor y desafortunadamente tiene que confiar en los registros de la aplicación y sistema obtenidos por el proveedor de servicios; los cual solamente es posible si el proveedor de servicios tiene algún mecanismo instalado de registros y que permita tener los registros disponibles.

IaaS

El modelo IaaS ofrece mayores ventajas en términos de la evidencia para un investigador. En este modelo, el cliente controla las configuraciones de las instancias virtuales, así como la configuración del sistema operativo y las aplicaciones.
Por lo tanto, existe la posibilidad de que el cliente instale aplicaciones de monitoreo y registro para realizar un seguimiento de las actividades del usuario. Lo cual mejora en gran medida la calidad de una investigación forense. Es importante mencionar que esto no es una norma.
Sin embargo, en este modelo de servicio, el investigador puede acceder a más evidencia que en los otros modelos (PaaS y SaaS).

PaaS

En el modelo de PaaS el cliente puede desarrollar y desplegar aplicaciones utilizando lenguajes de programación, librerías, servicios y herramientas soportadas por el proveedor de servicios. El cliente no administra ni controla la configuración de la infraestructura que incluye la red, los servidores,

sistema operativo y almacenamiento. Pero tiene el control sobre las aplicaciones desplegadas y mejor aun posiblemente los ajustes de configuración para el entorno del alojamiento de la aplicación.
Esto significativamente obstaculiza la habilidad de un investigador para hallar evidencia. Ya que está limitado a registros específicos a nivel de la aplicación, si es que existen.

Un señalamiento importante es que la documentación no se considera como una etapa separada de una investigación forense, ya que la evidencia digital se documenta tal como es encontrada.

El reporte final del incidente es creado durante la fase de presentación. La evidencia debe ser documentada a fondo. Por ejemplo, un archivo se documenta utilizando su ruta completa, el sistema de archivos utilizado por el clúster y los sectores del disco en los cuales reside el archivo; además el hash del archivo es calculado para asegurar que la verificación de su integridad pueda ser comprobada.

La cadena de custodia es también importante, más si se piensa usar la evidencia en un corte.

La documentación y la cadena de custodia son tareas difíciles en ambientes de Nube. Como se ha mencionado anteriormente el nivel y cantidad de evidencia disponible para un investigador puede variar, lo cual afecta directamente en que tan bien la evidencia es documentada.

Por ejemplo, un investigador que tiene acceso directo a una imagen virtual puede documentar los hallazgos encontrados en la imagen. Por otro lado, si el investigador depende en que el proveedor de servicios recupere los archivos de interés, lo obliga a confiar en la evidencia presentada por el proveedor de servicios haya sido adquirida de alguna forma forense adecuada.

3.5.2.3. Fase de búsqueda y recopilación

La fase de búsqueda y recopilación de evidencia involucra un exhaustivo y completo análisis del sistema. En esta etapa se toman los resultados de la fase de investigación para decidir qué tipo de análisis realizar. Por ejemplo, una búsqueda de palabras clave puede ser usada durante esta fase, usando la información identificada de la evidencia, o en análisis de la línea de tiempo de un archivo para trazar las actividades del usuario.

La búsqueda y recopilación consumen la mayor parte del tiempo invertido en una investigación. A si mismo se deben recopilar los dispositivos que tengan valor para la investigación.

Los métodos de recopilación involucran la generación de imágenes forenses para que puedan ser posteriormente examinadas bajo condiciones de laboratorio. Otros métodos de recopilación pueden ser usados para adquirir evidencia almacenada en memoria volátil y archivos de registro.

La mayoría de la fase de búsqueda y recopilación en una investigación forense tradicional es conducida localmente en el lugar del incidente, excepto, por ejemplo, en la recuperación de registros de la red que típicamente residen en el servidor.

La infraestructura distribuida en ambientes de Cómputo en la Nube plantea varios desafíos con respecto a la búsqueda y colección. La naturaleza dispersa de los datos en la Nube significa que el investigador tendrá que adaptar métodos tradicionales al nuevo entorno [BIR30].

Adicionalmente el investigador deberá entender como los datos son almacenados en los ambientes de Nube y determinar cómo deberán ser recuperados sin afectar la integridad.

A nivel local, la evidencia puede ser reunida desde el historial de búsqueda del navegador del cliente; esto debido a que las comunicaciones entre el cliente y proveedor de servicios típicamente usan el motor de búsqueda. Otra evidencia como lo son las credenciales del usuario para acceder a la nube y mensajes instantáneos deberán ser extraídos y descifrados; esto le puede dar al investigador acceso a comunicaciones previas hechas por el cliente en la red.

A nivel de red, generalmente no es posible analizar el tráfico porque el proveedor de servicios puede no proporcionar datos de registro de los componentes de red utilizados por las instancias y aplicaciones del cliente.

Si el modelo de servicios IaaS es usado, es posible para el investigador hacer un snapshot de la máquina virtual y analizarla en un laboratorio. La situación es más compleja en el caso de PaaS debidos a que solamente ciertos datos específicos de aplicaciones están disponibles. En la situación de SaaS, el investigador solamente puede recuperar datos limitados como, ciertas configuraciones de aplicaciones del usuario. El investigador deberá proporcionar una orden legal que le permita solicitarle al proveedor de servicios una búsqueda y recopilación de datos.

Algún descuido en la cadena de custodia puede provocar que la evidencia no sea admisible durante la presentación del caso.

3.5.2.4. Fase de Reconstrucción

La fase de reconstrucción involucra la organización de los resultados del análisis de la recopilación física y evidencia digital para desarrollar una teoría del incidente. Los datos que requieren un análisis de técnicas más avanzadas, como archivo ejecutable o descifrado, se llevarán a cabo y los resultados se usarán en esta fase.

Métodos científicos son aplicados a la evidencia para probar la teoría del incidente. En algunos casos, la búsqueda puede ser continuada para obtener evidencia adicional.

En investigaciones forenses en la Nube, el proveedor de servicios controla la cantidad de datos que son facilitados al investigador; la cantidad de datos entregados afecta directamente la reconstrucción del incidente. Cabe destacar, que la dispersión física de los datos puede hacer difícil poner en orden temporal los datos y sobre todo en su contexto adecuado.

Esta situación se ve aún más agravada por el hecho de que los datos son contenidos en diferentes regiones geográficas, por lo tanto, los relojes relacionados a dichos sistemas no estarán sincronizados.

Este problema puede impactar negativamente la credibilidad de la evidencia presentada en una corte.

3.5.2.5. Fase de Presentación

La fase de presentación es la parte final de una investigación forense. Durante esta fase, toda la evidencia física, digital y los dispositivos son documentados y presentados en una corte.

El investigador reporta sus avances mediante una presentación sustentada en la documentación de su investigación, que le permitirá hacer declaraciones y su testimonio será considerado en esta fase.

La documentación que soporta esta fase es peculiarmente importante porque ayuda establecer una cadena de custodia verificable. En investigaciones forenses los datos probatorios deben permanecer sin cambios, y el investigador debe ser competente y capaz de presentar los hallazgos, explicando las implicaciones y relevancia de todas las acciones tomadas durante la investigación. Además, estrictamente los registros deben ser mantenidos en cada paso de la investigación.

En ambientes de Nube, es difícil pero no imposible, mantener un estricto registro y control de una investigación, especialmente cuando la evidencia reside en múltiples ubicaciones y está bajo el control de diferentes entidades.

4. Caso Práctico de Análisis Forense en la Nube

En este capítulo se presentan 2 casos de escenarios experimentales involucrando todo lo que se ha mencionado en este trabajo de investigación, independientemente de lo que haya sucedido y lo que podría suceder potencialmente en base al planteamiento, es importante recalcar que solamente son ficticios los casos expuestos en este capitulo

Los 2 escenarios que se proponen abarcan las principales facilidades que brinda el Cómputo en la Nube lo cual incluye, aplicaciones, almacenamiento y poder de cómputo. Señalando como en todas estas características son usadas para cometer delitos.

En el primer escenario se mostrará como piezas de código malicioso son fácilmente propagados desde la Nube para causar grandes daños que son traducidos en enormes pérdidas económicas, lo cual es solamente el comienzo de una tendencia que muestra ser creciente y muy popular cada año.

El segundo escenario es sobre como terroristas pueden utilizar el Cómputo en la Nube Móvil con la finalidad de planear y ejecutar acciones violentas para lograr cumplir su objetivo.

4.1. Investigación de Virus en aplicaciones

Los virus embebidos en aplicaciones de Cómputo en la Nube Móvil son una de las fuentes más usadas frecuentemente para esparcir piezas de código malicioso. Por ejemplo, un virus llamado Geinimi que se propago dentro de China infectó a más de 150 millones de Smartphones y provocando daños a la economía China que alcanzan en $300 000 dólares.

El código malicioso se integró en aplicativos de juegos desarrollados por terceros como *Monkey Jump 2, President vs Aliens, City Defence y Basball Superstars.*

Cuando un usuario de Android descargaba cualquiera de estos juegos y lo instalaba en su Smartphone, el malware se ejecutaba automáticamente en segundo plano sin que lo notara. Lo que permitía que el desarrollador del virus tomara control del dispositivo móvil en cuestión de segundos.

El virus Geinimi invadía la privacidad del usuario, lanzaba campañas publicitarias y descargaba software malicioso adicional [NET31].

Una vez que el dispositivo estaba infectado, la información que incluye a los contactos, mensajes de SMS, tarjeta SIM, la localización actual y otra información confidencial eran enviados a un destino designado previamente por el hacker. El destino podía ser un servidor en la Nube u otro dispositivo móvil.

De acuerdo a las vías en que se propagaba Geinimi tenía la posibilidad de formar botnets muy fácilmente.

El dispositivo infectado enviaba 10 mensajes de SMS a las personas en la lista de contactos sin el conocimiento del propietario del dispositivo. El contendió del mensaje de SMS podía ser advertencias o ya sea enlaces Url.

Si el usuario en la lista de contactos recibía un mensaje de SMS, lo abría y después daba click en el link, entonces el dispositivo era infectado.

El nuevo dispositivo infectado repetía el proceso, obteniendo más dispositivos infectados. Si un Smartphone enviaba 10 SMS era muy probable que reclutara 10 móviles más y ellos enviaban 10 SMS más, lo que resultaba en 100 nuevos Smartphones.

Con este patrón, una enorme boten era formada. Los dispositivos móviles infectados se conectaban al sitio web de Geinimi.com en intervalos de 5 minutos para descargar piezas maliciosas adicionales.

4.1.1. Caso experimental escenario 1

En base a lo descrito anteriormente acerca del virus Geinimi se propone un caso experimental para aplicar un proceso de investigación forense en móviles resaltando las implicaciones que surgen del Cómputo en la Nube Móvil.

Bob instalo un aplicativo basado en la Nube el cual es un juego en su Smartphone *Motorola Milestone Android.*

Posteriormente se percata de que el saldo de su Smartphone se agotaba demasiado rápido, incluso aunque no había hecho demasiadas llamadas ni enviando mensajes de SMS. Bob Sospechando que su móvil estaba infectado por un virus, decidió llevarlo a un Laboratorio de Seguridad Informática, con la intención de saber qué es lo que ocasionaba que el saldo se agotara muy rápido.

En caso de que su sospecha fuese correcta quería saber específicamente como fue comprometido su dispositivo

4.1.2.Implementación del escenario 1

El juego que instalo Bob es un aplicación desarrollada y desplegada en la Nube llamado iLightr en su móvil Android. Como se describió en la sección anterior se topó con la sorpresa de que su saldo se agotaba muy rápido. A pesar de que él no estaba haciendo uso de llamadas ni mensajería.

Para averiguar que sucede se procederá con un análisis forense con el objetivo de identificar la razón por la cual el saldo se agota rápidamente e indagar si realmente el Smartphone fue comprometido por un virus y trazar el origen de este.

4.1.2.1. Preparación de la simulación del escenario

En la siguiente tabla se muestran las especificaciones técnicas del dispositivo *Motorola Milestone*, así como la tarjeta SIM.

Dispositivo	Motorola Milestone
Sistema operativo	Android 2.0
Velocidad del Procesador	550 MHz
SIM CARD	Telcel prepago
Almacenamiento externo	8GB micro SD
Conexión	3G WCDMA/900/2100 GSM 850/900/1800/1900 HSPA GPRS Class 12 WiFi Bluetooth

Tabla 4 Especificaciones técnicas del dispositivo móvil

La aplicación de Android *iLightr v1.0.2* fue descargada de un sitio web de juegos Chinos http://www.yruan.com/softdetail/739.

Lo cual genera preocupación debido a la reputación de la página, por dicho motivo se decide escanear el archivo en Virustotal el cual es un sitio web que proporciona de manera gratuita el análisis de archivos y páginas web a través de antivirus.

El virus Geinimi fue detectado e identificado en la aplicación MonkeyJump2.0.apk, la figura 21 muestra el resultado den análisis que se realizó.

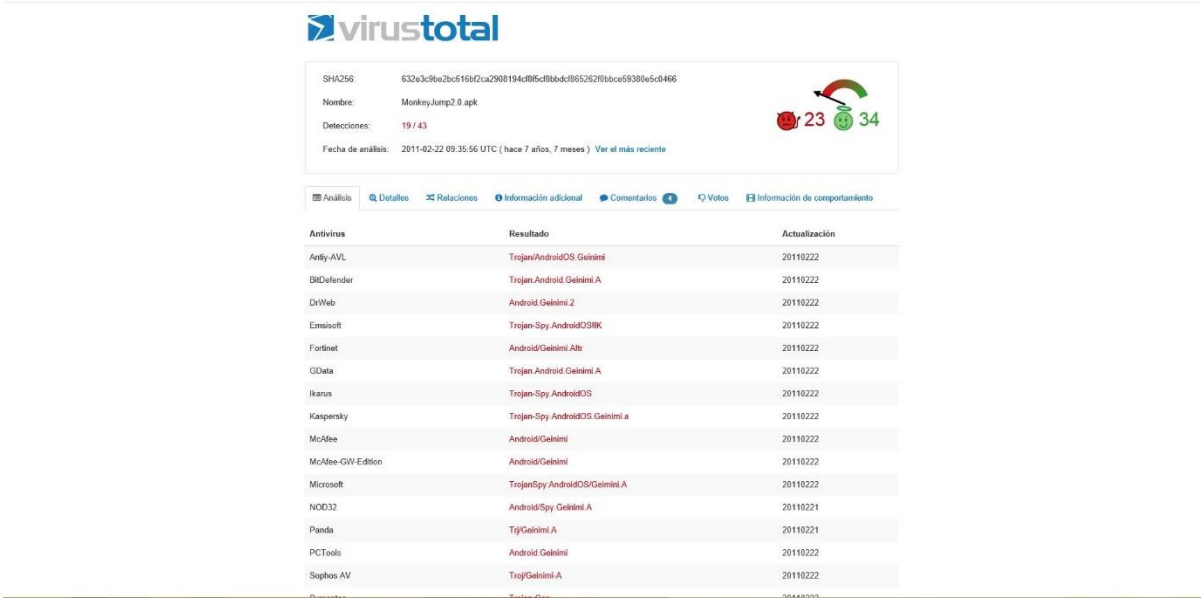


Figura 21 Virus total

De acuerdo a Virustotal Geinimi fue descubierto el 26 de Noviembre de 2010 siendo clasificado en 3 categorías diferentes de malware.

1. Backdoor
2. Robo de datos
3. Consumo de saldo

La descripción ofrecida por el sitio web Virustotal en la figura 22 resalta que la pieza de código maliciosa fue embebida en un juego para burlar a los usuarios e incitarlos a descargarlo

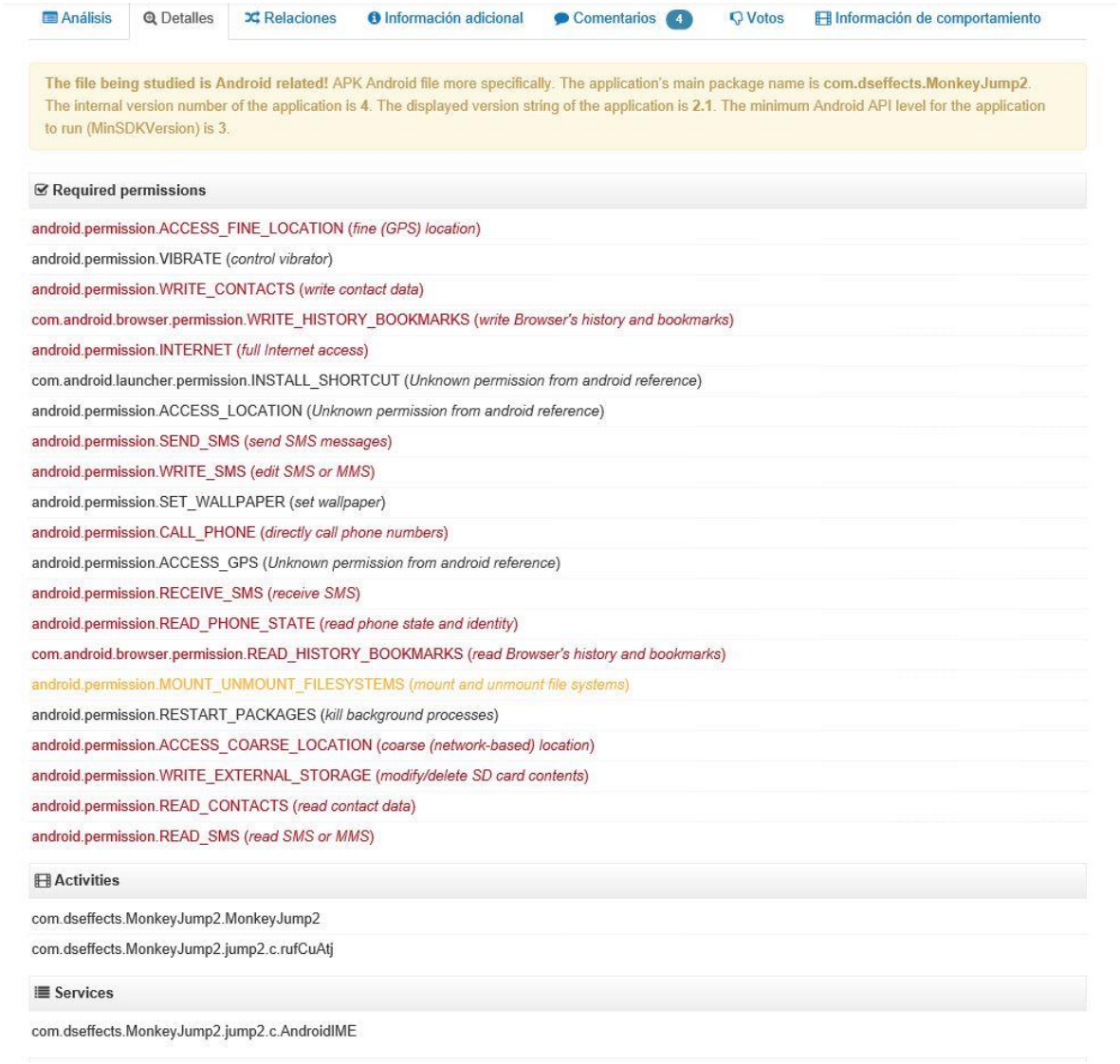


Figura 22 Descripción técnica de Geinimi

Continuando con la descripción del malware una vez activado, se conectaba a internet en segundo plano mediante un plug-in para filtrar los datos confidenciales del usuario y descargar software adicional sin el consentimiento de la víctima. Todas estas acciones maliciosas no solamente impactaban en el rendimiento del dispositivo sino que además lo exponían a nuevas amenazas.

Con el fin de llevar a cabo una buena investigación, el Smartphone fue formateado y restaurado a su estado original de fábrica. Esto nos asegura que no habrá otros factores que afecten la operación del dispositivo.

Cuando el Smartphone fue reiniciado, se conectó a la red WIFI local INFINITUM7Fju con el objetivo de instalar la aplicación que contiene el malware. Lighter se instaló al hacer click sobre su instalador, posteriormente, el juego fue abierto para asegurar la ejecución del virus.

4.1.2.2. Resultado esperado

El software para análisis forense es capaz de extraer los datos almacenados en el dispositivo, especialmente los mensajes de texto, historial de búsquedas en navegadores y actividades en el mismo Smartphone.

- Detectar que es lo que está causando que el saldo sea drenado y si es causado por un virus.

- Identificar las capacidades del virus.

4.2. Aplicación de Metodología y procedimientos forenses

En esta sección se propone una metodología para la implementación procedimientos y herramientas forenses actuales, con el fin de destacar todo lo descrito en este trabajo. La metodología propuesta consta de las siguientes fases.

- Identificación y Preservación
- Adquisición
- Examinación
- Utilización de otras técnicas para obtener evidencia restante
- Presentación

Nos basaremos en lo descrito anteriormente en la sección 4.1.2 para poder conducir la investigación.

4.2.1. Identificación y Preservación

Los procedimientos de investigación forense que se llevarán a cabo son respaldados por el contenido del capítulo 3.

Los datos sobre la identificación del dispositivo se pueden consultar en la tabla 4 de la sección 4.1.2.1.

Los procedimientos y acciones llevadas a cabo fueron registrados en la tabla 5 como se muestra a continuación.

Procedimientos para Preservación	Acción
1. Asegurar y evaluar la escena.	El dispositivo fue llevado al laboratorio, por lo cual el aseguramiento y evaluación de la escena no aplica.
2. Documentar la escena completa.	N/A
3. ¿Hay necesidad de algún otro análisis forense (ADN)?	N/A
4. Si es posible identifique el modelo del dispositivo.	Motorola Milestone.
5 ¿El teléfono esta encendido o apagado?	Encendido.
6. Tomar todas las medida para evitar que el dispositivo se apague y aíslelo de señales externas.	El dispositivo fue colocado en empaque que lo aísla de las señales externas.
7. Resguarde el teléfono con los accesorios.	El dispositivo fue asegurado y solamente el personal autorizado tuvo acceso.
8. Seguir un procedimiento riguroso para la documentación, transporte y almacenamiento.	El dispositivo fue transportado al laboratorio de forma segura y adecuada

Tabla 5 Procedimiento de la Preservación del dispositivo

4.2.2.Adquisición

El método de adquisición usado en el dispositivo Motorola Milestone es descrito en esta sección, el procedimiento de adquisición fue seguido de acuerdo al estándar del NIST SP 800-101. En la tabla 6 se puede apreciar las acciones llevadas a cabo.

Procedimiento de Adquisición	Acción
1. Identificación del dispositivo	Motorola Milestone
2. ¿Encendido o apagado?	Encendido
2.1 Tomar todas las medidas para evitar que se apague el dispositivo y aislarlo de señales externas	El dispositivo tenía carga completa y fue puesto en modo avión
2.2 Buscar el manual y descargarlo	El manual fue descargado de internet
2.3 Seleccionar las herramientas forenses adecuadas y planear la examinación y análisis	Software comercial Oxygen and XRY
2.4 Probar las herramientas en un dispositivo idéntico antes de usarlas en el Smartphone bajo investigación	La prueba fue realizada en un dispositivo idéntico, los resultados muestran que solo el software XRY logró exitosamente extraer la evidencia del Smartphone. La única forma posible de obtener una extracción física es a través de un Nandroid, pero este método requiere de acceso root lo que significa que la evidencia puede ser alterada.
3. ¿Presenta obstrucciones?	No
4. Adquisición del dispositivo	La adquisición del dispositivo fue realizada y se documenta en la siguiente sección.

Tabla 6 Procedimiento de la adquisición del dispositivo

Se optó por el software XRY para conducir la examinación, dado que los resultados de realizar la examinación en otro dispositivo idéntico resalto la incapacidad de la herramienta Oxygen para llevar acabo la extracción de evidencia en el Smartphone Milestone, adicionalmente mostro un mensaje de error *"Conexión fallida, no se puede detectar el dispositivo"*.

El mismo error perduro tras diversos intentos de usar Oxygen para extraer los datos del Smartphone. Como solución se tiene que instalar primeramente el agente.

Aunque XRY ofrece una extracción física del Smartphone, XRY no soporta la versión del dispositivo Milestone. Sin embargo, XRY puede ser exitosamente manejado para obtener una copia lógica del dispositivo. Por lo tanto, una extracción física solo se realizaría si los datos necesarios para la investigación no estuviesen disponibles en la imagen lógica.

La razón es que solo un Nandroid puede realizar con éxito una extracción física de un teléfono Android. Para poder realizar un Nandroid, se requiere de acceso de root, lo que significa que es muy probable que la evidencia sea alterada.

Un Nandroid es una copa exacta de la memoria interna de un dispositivo Android; es un respaldo del disco duro del Smartphone.

4.2.3. Examinación

La recopilación de los registros extraídos y datos en esta sección seguirán los procedimientos de investigación del NIST SP 800-101 y se muestra en la tabla 7.

Procedimiento de Examinación	Acción
1. Identificación de Evidencia potencial	Mensajes de SMS, historial de navegación, descargas de internet, aplicaciones y cualquier posible actividad que pueda consumir ancho de banda y crédito.
2. Recopilar y analizar la evidencia de llamadas	Solamente el personal autorizado de la empresa telefónica tiene los privilegios de acceder a esos datos.
3 Analizar la evidencia extraída del Smartphone	La evidencia obtenida fue analizada, los detalles son descritos a continuación.

Tabla 7 Procedimiento de extracción

El tipo de datos que son de interés para análisis en este caso son aquellos que generan actividades potenciales que consuman el saldo del usuario. Los cuales incluyen:

- Registro de llamadas
- Mensajes de SMS
- Historial de navegación WEB
- Aplicaciones

La extracción lógica realizada por XRY mostró 20 entradas en mensajería de SMS, 0 fotos, 1 video, 8 documentos, 5 archivos y 67 registros los cuales fueron creados durante la extracción echa por XRY. Los detalles de la extracción de los registros se muestran en el apéndice A. En la figura 23 se puede visualizar lo descrito.

Motorola Milestone

Network	GSM
OS	Android

Logical

Connectivity

Cable	✓	microUSB Cable
Bluetooth	✗	Not Supported
Infrared	–	Not Available

Features

Contacts Sim	✗	Not Supported
Calls Sim	✗	Not Supported
SMS Sim	✓	Full Support
Contacts	✗	Not Supported
Calls	✓	Full Support
SMS	✓	Full Support
Pictures	✓	Full Support
Audio	✓	Full Support
Video	✓	Full Support
Files	✓	Full Support
MMS	✗	Not Supported
E-mail	✗	Not Supported
Calendar	✗	Not Supported
Tasks	–	Not Available
Notes	–	Not Available
Memory card	✓	Full Support

Figura 23 Extracción lógica del dispositivo

Un análisis minucioso de los mensajes de SMS fue realizado. Las 20 entradas de SMS fueron recuperadas del teléfono, incluyendo los SMS almacenados en la tarjeta SIM.

No hubo mensajes de SMS enviados desde el Smartphone. Por lo cual, hay 2 posibles suposiciones.

1. El malware elimino los mensajes de SMS justo después de enviarlos.
2. El malware no tiene capacidad de enviar mensajes de SMS.

Para confirmar que suposición es correcta es importante contar con un reporte detallado por parte del proveedor de servicios de la línea telefónica.

Tampoco se encontró registro de llamadas. El registró y seguimientos de llamadas y mensajes se obtuvo de la telefónica. Si Bob al revisar la lista, reconoce todas las llamadas listadas y no hay ninguna que le parezca extraña, quiere decir que el saldo no fue consumido por el hecho de realizar las llamadas o enviar los mensajes.

Sin embargo, la evidencia obtenida hasta el momento aún necesitaba responder las preguntas de la investigación en curso, el impedimento a estas respuestas fue el método de extracción que se optó por realizar. La tabla 8 muestra la evidencia que se debió adquirir y la evidencia que se obtuvo.

Evidencia requerida	Evidencia encontrada
Mensajes de SMS	Si
Llamadas	Si
Historial de navegación web	Si
¿El dispositivo está infectado?	No
Acciones de lo que el virus hace	No

Tabla 8 Comparación de evidencia obtenida

Con el fin de contar la evidencia faltante, se procedió con una extracción física para saber si había más datos que se pudieran recuperar. Se realizó el Rooting del dispositivo el cual es un método utilizado para obtener privilegios de administrador con la finalidad de ganar acceso total al sistema y archivos, lo cual permite una extracción de datos de la memoria física del Smartphone.

Se obtuvo privilegios de súper usuario exitosamente usando una herramienta desarrollada por una comunidad de hackers llamada G.O.T Team Android la cual está disponible en sus sitio web [10]. La documentación del proceso puede ser consultada en el apéndice B.

El software ofrecido por el G.OT. Team Android ofrece opciones como, crear un nuevo respaldo Nandroid. Un respaldo Nandroid fue creado.

El archivo del respaldo fue almacenado en la tarjeta MicroSD y fue asignado el folder ADBRecovery. En el cual había 7 archivos, incluyendo 6 archivos .img en dicho folder. Los archivos son.

1. Boot.img
2. Bpsw.img
3. Cache.img
4. Cust.img
5. Data.img
6. Misc.img
7. MD5.TXT

Para examinar estos archivos se usó el software de FTK con la intención de aplicar métodos de excavación de archivos. Desafortunadamente ninguno de los archivos fue procesado por FTK. Esto impidió recuperar evidencia adicional a través de la extracción física.

Después del Rooting del dispositivo se hizo una extracción lógica la cual se encuentra detallada en el apéndice C. Una vez obtenido el acceso como súper usuario todavía había 20 entradas de SMS, 2 fotos, 1 video, 9 documentos, 112 archivos y 207 registros.

Una vez hecha la examinación de la evidencia, se encontraron más archivos después de hacer el Rooting al dispositivo. Destaco un aumento significativo en archivos y registros. Los archivos se identificaron como los que se encuentran en el archivo update.zip y la carpeta de recuperación.

Se agregaron muchos más archivos a la evidencia original utilizando G.O.T para obtener acceso a la raíz del teléfono. Por lo tanto esta acción, no podría considerarse como una prueba forense. Desafortunadamente no se encontró evidencia adicional más allá de la ya encontrada.

4.2.4. Utilización de otras técnicas para obtener la evidencia faltante

Si el saldo no fue consumido vía mensajes y llamadas, entonces había una gran posibilidad de que la causa fuera el uso de internet. Capturando el tráfico de internet fue una manera de determinar qué datos se habían enviado y recibido.

Técnicas y métodos de forense en red se utilizaron para ayudar a comprender el uso de la red por parte del Smartphone [AND32].

Para capturar el tráfico en tiempo real se usó Wireshark el cual es un analizador de protocolos utilizado para realizar análisis en redes de comunicaciones. En la figura 24 se muestra como se realiza esta fase.

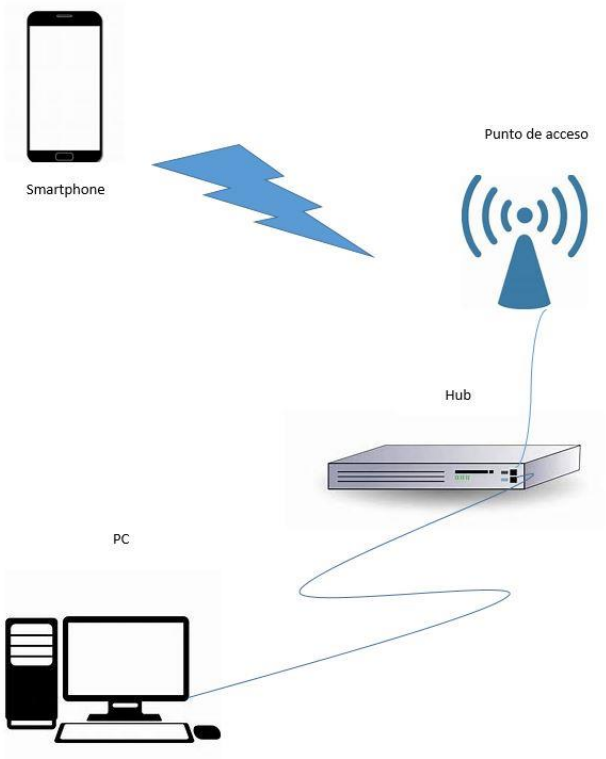


Figura 24 Captura de tráfico del dispositivo

Con la finalidad de capturar el tráfico entrante y saliente, se necesitó un punto de acceso, un dispositivo conectado y una computadora ejecutando Wireshark. Los datos que se capturaron con Wireshark demostraron que el Smartphone estaba intentado conectarse a un host google.funimeo.com:8080 con dirección IP 202.106.0.20, para él envió de datos cifrados.

Los datos contenían la información privada del usuario como, el identificador del dispositivo y las coordenadas. En la figura 25 se muestra un fragmento del flujo de TCP del dispositivo enviando los datos cifrados a un servidor remoto Apache.

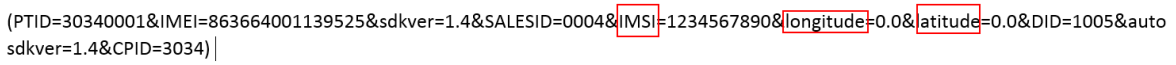


Figura 25 Flujo de TCP capturado

A pesar de que Wireshark capturo los datos, la aplicación insistía en enviar los datos al servidor remoto, y la ubicación en donde estaba alojada la pieza maliciosa permanecía desconocida.

Se plantearon varias opciones para tratar de identificar el problema, una de ellas fue deshabilitar todos los aplicativos del dispositivo. Esto evitaría que se ejecuten, permitiendo a si probar cada aplicación una por una.

Otra opción fue probar con un antivirus para detectar el malware. Para escanear el dispositivo se eligió la aplicación de Virustotal, el anti virus fue descargado e instalado.

El análisis del anti virus mostro como resultado que la aplicación contenía el malware 轮火iLightr (BIT.GeiNiMi).

Al utilizar métodos y técnicas forenses en redes, permitieron identificar actividades de navegación web al capturar los paquetes. Esta técnica confirmo que el Smartphone fue infectado por el malware el cual estaba enviando información del usuario a un servidor remoto, consumiendo de este modo el ancho de banda provocando que el saldo se agotará. La evidencia que anteriormente nos faltaba logro ser obtenida y se muestra en la Tabla 9.

Evidencia Requerida	Evidencia Obtenida
Mensajes de texto	Si
Registro de llamadas	Si
Historial de navegación de internet	Si
Actividades en web	Si
¿El dispositivo fue infectado por el virus?	Si
Acciones del virus	Si

Tabla 9 Evidencia encontrada

4.2.5. Presentación

Los datos presentados en esta última fase de la investigación forense son respaldados por toda la información obtenida como resultado de análisis del escenario planteado.

Los datos sobre la presentación del dispositivo se pueden consultar en las fases anteriores del capítulo 4.

La evidencia que se recuperó incluye: SMS, fotos, videos, documentos, archivos y registros. En los cuales hay 20 SMS, 1 video, 8 documentos, 5 archivos y 67 registros.

Para poder continuar con la extracción física el Smartphone necesito someterse a Rooting.

El Rooting del dispositivo se llevó a cabo con el software desarrollado por G.O.T Team Android. Posteriormente se volvió a intentar hacer una extracción lógica con Oxygen y XRY.

Nuevamente el agente de Oxygen fallo en ejecutarse en el dispositivo, pero XRY extrajo 20 SMS, 2 fotos, 1 video, 9 documentos, 112 archivos y 207 archivos de registros. Además se descubrió una foto que había sido borrada.

Como último recurso se aplicaron técnicas de forense en redes inalámbricas para capturar el tráfico entrante y saliente del dispositivo móvil. El objetivo fue identificar qué actividades entrantes y salientes por el uso de conectividad fueron generados por el Smartphone o por acciones del malware. El resultado de la Examinación demostró que había un virus, llamado Geinimi. Un virus que enviaba la información y credenciales del usuario a un servidor.

4.3. El cómputo en la Nube Móvil utilizado como herramienta del Ciberterrorismo

El Ciberterrorismo puede ser definido como el medio de diseminación de información metodológico, premeditado e ideológicamente motivado con la finalidad de atacar medios de comunicaciones, sistemas de cómputo y programas.

El Ciberterrorismo requiere de una gran planificación con el fin de lograr causar daños sociales, financieros, políticos e impactar a grupos no combatientes. Las organizaciones terroristas han usado el internet en diversas formas desde hace décadas destacando las siguientes acciones [BRI33].

- Propaganda
- Diseminación de información
- Reclutamiento
- Recaudación de fondos
- Adiestramiento
- Comunicaciones
- Medio de ataque
- Investigaciones y planeación
- Lavado de dinero

Es bien sabido que se ha usado el internet para obtener un amplio conocimiento acerca de infraestructuras críticas, despliegues militares, secretos industriales, espionaje e incluso la búsqueda detallada de cómo desarrollar bombas. Por ejemplo, en 2006 la inteligencia del ejército Británico descubrió impresiones realizadas con GoogleEarth en posesión de los insurgentes, quienes los estaban usando para señalar ataques.

Cuando las autoridades Francesas arrestaron a Kaci Warab, se percataron de que había sido entrenado en dispositivos sofisticados para detonación en Abu Musab al Zarqawi´s. Uno de los diseños descubiertos involucraba el uso de Smartphone en el cual se aprovechaban sus capacidades de navegación en la web, con el cual se podía realizar la detonación remotamente via un sitio web.

El Cómputo en la Nube Móvil pone a disposición más facilidades que las que ya estaban disponibles para el terrorismo.

El servicio de almacenamiento en la Nube como, Dropbox y aplicaciones de comunicaciones como Skype pueden beneficiar potencialmente a cibercriminales.

Por ejemplo, cuando una célula terrorista instala la aplicación de Dropbox pueden crear un grupo con todos los miembros de la célula, una vez que algún miembro sube algún archivo inmediatamente se actualizara en todos los contactos; esto permite que todos se mantengan actualizados muy rápido. Si el plan fuese cambiado y alguno de los miembros no se encuentra dentro de la cobertura de señal, la sincronización y archivos compartidos sería la mejor opción para mantenerse informado. En lugar de correr el riesgo de ser monitoreado al hacer llamadas y exponer su localización, sería mejor decisión usar Skype.

Las llamadas a través de internet se pueden hacer desde cualquier parte y a la hora que sea, además es relativamente difícil rastrearlas. Si se quisiera rastrear la llamada se debe contar con un decodificador de Skype, sin olvidar que es casi imposible monitorear las llamadas de Skype, debido a lo robusto de su cifrado.

4.3.1. Caso experimental escenario 2

El segundo escenario fue establecido en base a un modelo de Ciberterrorismo. El grupo terrorista A, lanza un ataque en la ciudad C, se sabe que hay 5 integrantes en el grupo A, cada uno con un iPhone 3G. Los miembros comparten la misma cuenta de Dropbox, las instrucciones por parte del líder son guardadas en un folder confidencial.

Solamente se les permite llamar y enviar mensajes con Skype y Viber. Uno de los terroristas llamado Pablo es arrestado con la supuesta teoría de ser miembro de grupo terrorista A, por lo cual las autoridades necesitan evidencia para procesarlo.

El iPhone 3G fue incautado y llevado como evidencia importante al laboratorio para su investigación. El propósito de la investigación es encontrar evidencia para culpar a pablo y ubicar la posible localización de los restantes 4 miembros.

4.3.2. Implementación del escenario 2

En esta sección se presenta información detallada de los procedimientos llevados a cabo para la implementación.

4.3.2.1. Preparación de la simulación

Se escogió un iPhone 3G para llevar a cabo la simulación, en la tabla 10 se muestran las características del dispositivo.

Dispositivo	iPhone 3G
Sistema operativo	iPhone OS 4
Procesador	550 MHz
Tarjeta SIM	2 Degree, 128k
Memoria interna	8GB, 128 MB RAM
Red	WiFi 802.11b/g
	WCDMA/900/2100
	GSM 850/900/1800/1900
	HSDPA 850 / 1900 / 2100
	GPRS
	EDGE
	Bluetooth

Tabla 10 Características del iPhone 3G

Para la simulación se instalaron las siguientes aplicaciones Skype, G-mail, Viber y Dropbox en el iPhone con jailbreak. Para garantizar que los datos puedan ser adquiridos el usuario inició sesión en las aplicaciones mencionadas. A si mismo se realizaron llamadas a diferentes contactos a través Viber y Skype. También se configuro iCloud en caso de que los terroristas quisieran hacer un borrado remoto de la información del Smartphone.

4.3.2.2. Resultado esperado

El software para análisis forense es capaz de extraer los datos almacenados en el dispositivo, especialmente los mensajes de texto, historial de búsquedas en navegadores y actividades en el mismo Smartphone, por lo cual se espera lo siguiente.

- Registro de llamadas de Skype y Viber
- Mensajes de texto
- Archivos compartidos en Dropbox

- Mensajes de E-mail

- Ubicación de las conexiones WiFi que permitirán rastrear los lugares donde han estado los terroristas

- Fotografías tomadas por los terroristas

4.4. Aplicación de la metodología y procedimientos forenses

Los procedimientos de investigación forense que se llevarán a cabo fueron tomados del NIST SP 800-101 cuya metodología fue presentada y descrita en el capítulo 3.

Los procedimientos y acciones llevadas a cabo fueron registrados en la tabla 5 como se muestra a continuación.

4.4.1. Identificación y Preservación

Los procedimientos de investigación forense que se llevarán a cabo son respaldados por el contenido del capítulo 3.

Los datos sobre la identificación del dispositivo se pueden consultar en la tabla 10 de la sección 4.3.2.1.

Los procedimientos y acciones llevadas a cabo fueron registrados en la tabla 11 como se muestra a continuación.

Procedimientos para Preservación	Acción
1. Asegurar y evaluar la escena.	La escena fue asegurada. Solamente el personal autorizado tiene acceso
2. Documentar la escena completa.	La escena fue documentada
3. ¿Hay necesidad de algún otro análisis forense (ADN)?	Si, se hizo una prueba de ADN para identificar al sospechoso
4. Si es posible identifique el modelo del dispositivo.	iPhone 3G
5 ¿El teléfono esta encendido o apagado?	Apagado
6. Tomar todas las medidas necesarias para evitar que el dispositivo se apague y aislarlo de señales externas.	El dispositivo fue colocado en un empaque que lo aísla de las señales externas.
7. Resguarde el teléfono con los accesorios.	El dispositivo fue asegurado y solamente el personal autorizado tuvo acceso.
8. Seguir un procedimiento riguroso para la documentación, transporte y almacenamiento.	El dispositivo fue transportado al laboratorio de forma segura y adecuada

Tabla 11 Preservación del iPhone 3G

4.4.2.Adquisición

El procedimiento de adquisición llevado acabo y los resultados obtenidos fueron registrados y documentados en la tabla 12. Se decidió realizar la extracción con Oxygen y XRY con la finalidad de comparar los resultados.

La extracción física fue llevada a cabo con XRY.

Procedimientos de adquisición	Acción
1. Identificación del dispositivo	iPhone 3G
2. ¿Encendido o apagado?	Apagado
2.1 Extraer la tarjeta SIM sin remover la batería	Se logró remover la SIM sin quitar la batería
2.2 Clonar la SIM usando las herramientas	Una copia de bit a bit de la Sim fue echa usando XRY
2.3 Obtener los datos del PIN/PUK	El lector de la tarjeta SIM omitió el PIN/PUK

2.4 Examinar la SIM	La SIM fue examinada usando XRY
3 ¿Presenta obstrucciones?	Si

Tabla 12 Procedimiento de adquisición iPhone 3G

La opción que ofrece XRY de clonar la SIM resolvió un problema desafiante que es encarado cuando se quiere examinar un dispositivo basado en comunicaciones GSM. Al clonar la tarjeta SIM se evita que ocurra una conexión a la red GSM, sin afectar el funcionamiento normal del dispositivo. Esto ayuda a minimizar el riesgo de contaminación de los datos [CAS34].

Utilizando XRY SIM id-Cloner la tarjeta SIM fue clonada. Bajo el estándar de GSM para dispositivos móviles el historial de llamadas debe ser eliminado si una nueva tarjeta SIM es insertada.

Sin embargo la tarjeta SIM clonada que se obtuvo contenía la misma información crítica que la original, lo que permitió el acceso al Smartphone sin causar la eliminación del historial de llamadas. La información detallada de los registros de la tarjeta SIM pueden ser consultados en el apéndice D.

4.4.2.1. Extracción lógica

Ambas herramientas Oxygen y XRY fueron elegidas para llevar a cabo la examinación, las 2 son muy bien conocidas en el área de las investigaciones de dispositivos móviles y sus manuales están disponibles para el usuario.

Primeramente se usó XRY y exitosamente extrajo los datos lógicos del iPhone 3G, como se muestra en la figura 26.

Apple iPhone 3G

Network	GSM
OS	iOS

Logical

Connectivity

Cable	✓	iPhone Cable 1
Bluetooth	✗	Not Supported
Infrared	–	Not Available

Features

Contacts Sim	✗	Not Supported
Calls Sim	✗	Not Supported
SMS Sim	✗	Not Supported
Contacts	✓	Full Support
Calls	✓	Full Support
SMS	✓	Full Support
Pictures	✓	Full Support
Audio	✓	Full Support
Video	✓	Full Support
Files	✓	Full Support
MMS	✓	Full Support
E-mail	✓	Full Support
Calendar	✓	Full Support
Tasks	–	Not Available
Notes	✓	Full Support
Memory card	–	Not Available

Figura 26 Extracción lógica con XRY

Los datos extraídos con XRY incluyen los contactos, llamadas, SMS, fotos, audio, video, archivos, E-mail, agenda, notas. Además XRY puede obtener la información de las cuentas de las aplicaciones del usuario instaladas en el Smartphone.

Continuamos con la herramienta Oxygen, que también realizo la extracción lógica exitosamente, en este caso ofrece una amplia variedad de opciones para el iPhone 3G las cuales incluye información del dispositivo, agenda, mensajes, registro de eventos, notas, línea de tiempo, aplicaciones, directorios, conexiones web. En la figura 27 se puede apreciar dichas características.

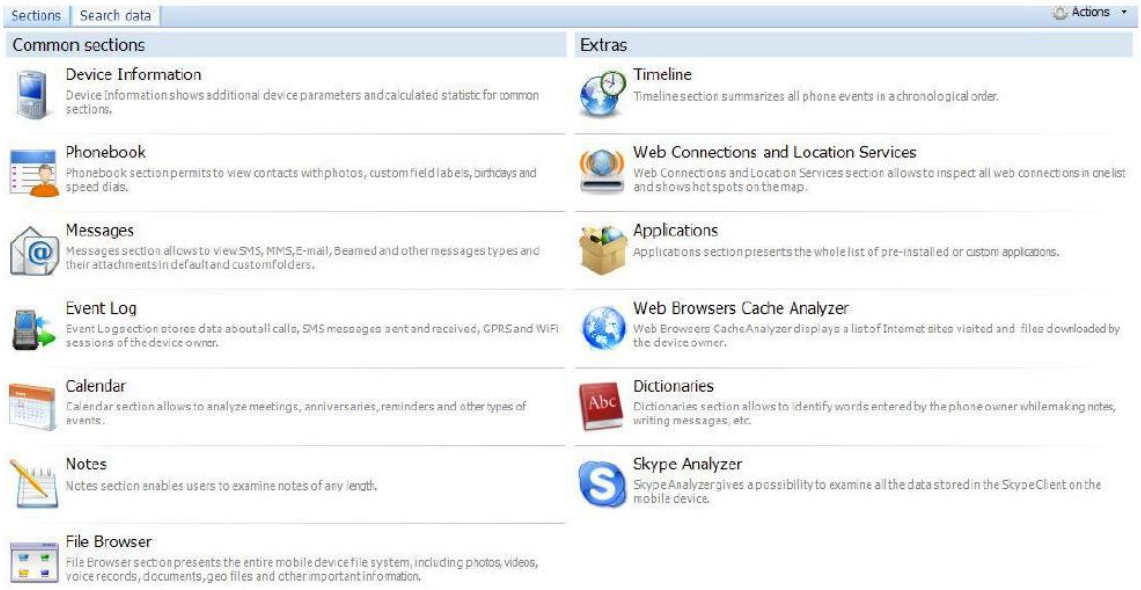


Figura 27 Opciones de extracción de Oxygen

4.4.2.2. Extracción Física

Dado que al momento de incautar el iPhone 3G ya se encontraba con jailbreak, no se necesitó de algún procedimiento adicional para realizar la extracción física.

Además XRY proporciona la posibilidad de obtener una imagen física del iPhone 3G, lo cual se aprovechó. Sin embargo la imagen generada no pudo ser leída por XRY ni Encase y mucho menos FTK.

4.4.3. Examinación

XRY extrajo 57 contactos, 100 llamadas, 2 notas, 578 SMS, 1MMS, 50 E-mails, 4,844 fotos, 1 video, 52 audios, 9,023 documentos, 6,124 archivos y 27, 636 registros. Los registros incluyen información de las cuentas del usuario, las aplicaciones, red e historiales de búsqueda.

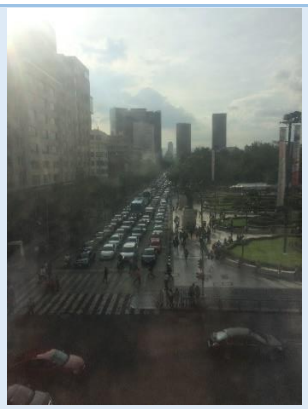
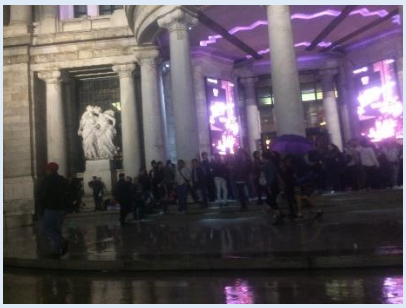
Por su lado Oxygen extrajo 57 contactos, 281 llamadas entrantes, 288 mensajes enviados, 48 llamadas respondidas, 41 números marcados, 11 llamadas perdidas, 2 notas, 648 archivos en los cuales destacan 102 imágenes, 2 documentos, 33 archivos de bases de datos y otros 510 archivos.

Se encontraron 9,975 conexiones a web en las que conforman 7 conexiones a WiFi, 4,942 localizaciones y 26 IP. En la tabla 13 se muestra una comparación entre ambas herramientas.

	XRY	Oxygen
Contactos	57	57
Llamadas	100	100
Notas	2	2
SMS	578	569
MMS	1	N/A
E-mail	50	N/A
Fotos	4844	102
Videos	1	N/A
Audio	52	N/A
Documentos	9023	3
Files	6124	510
Logs	27636	-
Aplicaciones	Indefinido	41
Conexiones a WiFi	Indefinido	7 Localizaciones
Localizaciones	Indefinido	4942
Conexiones IP	Indefinido	26
Palabras claves	715	715

Tabla 13 Comparación de herramientas

La mayoría de las imágenes recuperadas son generadas por las diferentes aplicaciones instaladas en el iPhone. Sin embargo hay 5 fotos que se identificaron que fueron tomadas por Pablo. La información GPS embebida en las fotos tomadas por Pablo, permitieron determinar el lugar donde fueron tomadas. Conduciendo a si a los lugares donde el sospechoso había estado. En la tabla 14 se muestra una descripción detallada.

Nombre de la foto	GPS Coordenadas	Ubicación	Imagen
IMG_0115.JPG	19.434598, -99.140513	Av. 5 de Mayo 2, Centro Histórico, Centro, 06000 Ciudad de México, CDMX	
IMG_0087.JPG	19.434491, -99.140745	Av. 5 de Mayo 2, Centro Histórico, Centro, 06000 Ciudad de México, CDMX	
IMG_0030.JPG	19.434840, -99.141094	El Pegaso, Eje Central Lázaro Cárdenas 4, Centro Histórico, Centro, 06000 Centro, CDMX	
IMG_0137.JPG	19.434840, -99.141094	El Pegaso, Eje Central Lázaro Cárdenas 4, Centro Histórico, Centro, 06000 Centro, CDMX	

IMG_0052.JPG	19.436047, -99.141751	fuente rítmica, Colonia Centro, Centro, 06000 Ciudad de México, CDMX	

Tabla 14 Coordenadas GPS de fotos

Los registros de conexiones WiFi también fueron obtenidas para localizar los lugares donde el sospechoso había estado. El software Oxygen ofrece una función que permite exportar las conexiones WiFi a Google Earth. En la figura 28 se muestra los lugares donde se ha conectado el sospechoso.

Los lugares donde Pablo ha estado se muestran en la tabla anterior. Los puntos fueron ubicados en el mapa de Google Earth. Dichos señalamientos demuestran las 2 localizaciones, que son los puntos de acceso a los cuales el iPhone le preguntó a Pablo si deseaba conectarse y el trayecto que recorrió Pablo mientras seguía conectado.

Figura 28 Conexiones del Sospechoso

4.4.4. Utilización de otras técnicas para obtener la evidencia restante

Durante la implementación y simulación de este caso nos hemos dado cuenta que el uso del Smartphone por parte de los supuesto terroristas para la coordinación de sus actividades no se encuentra centralizada solamente en el uso aislado del

dispositivo. Si no que la investigación ha mostrado que el dispositivo Móvil es usado como puente para lograr acceder a otras aplicaciones desplegadas en la Nube como mensajería instantánea, llamadas sobre internet, repositorios públicos y privado, lo único que se tiene que hacer es sincronizar el dispositivos a las plataformas de dichos servicios.

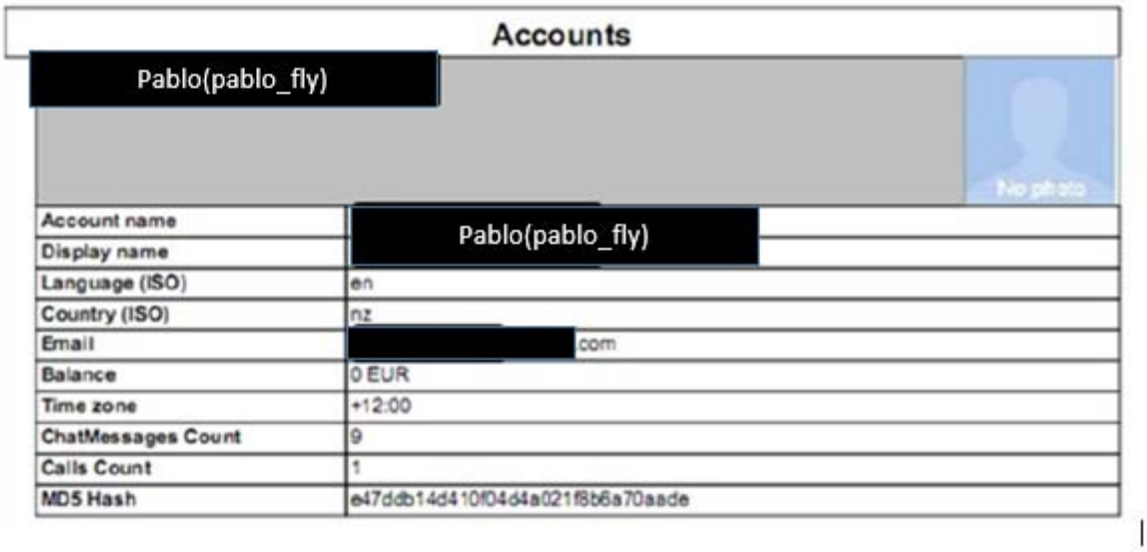
Esta nueva forma de relacionar y sincronizar tecnología o servicios entre diferentes dispositivos resulta en un esparcimiento geográfico de información y evidencia potencial. Lo que implica el nacimiento de una nueva tendencia en el análisis forense en dispositivos móviles ya que la evidencia que se requiere ya no se encontrara almacenada en el Smartphone si no que será almacenada en plataformas basadas en la Nube.

Para superar este obstáculo y continuar con nuestra investigación se buscaron soluciones de análisis forense que permitan la examinación de aplicaciones que este basadas y desplegadas en la en la nube. Para este caso decidimos usar las herramientas propuestas por Oxygen y XRY las cuales son conocidas por las aportaciones que están realizando en este nuevo paradigma.

El software Oxygen desarrollo un analizador para Skype especialmente para extraer información de Skype. El analizador logró extraer los contactos e información de los usuarios firmados en la aplicación, poniendo a disposición la foto del usuario, nombre de la cuenta, nombre registrado en la aplicación, dirección de correo y mensajes. A continuación se muestran ejemplos de la información desplegada por el analizador en Skype en la figura 29.

El analizador de Skype obtuvo 5 contactos, los detalles de la información de los contactos extraídos depende de lo que cada contacto ingreso en la cuenta.

Los mensajes de chat entre el propietario de la cuenta con uno de sus contactos en la lista también fueron recuperados con datos como el time stamp, tipo de mensaje y la función hash.



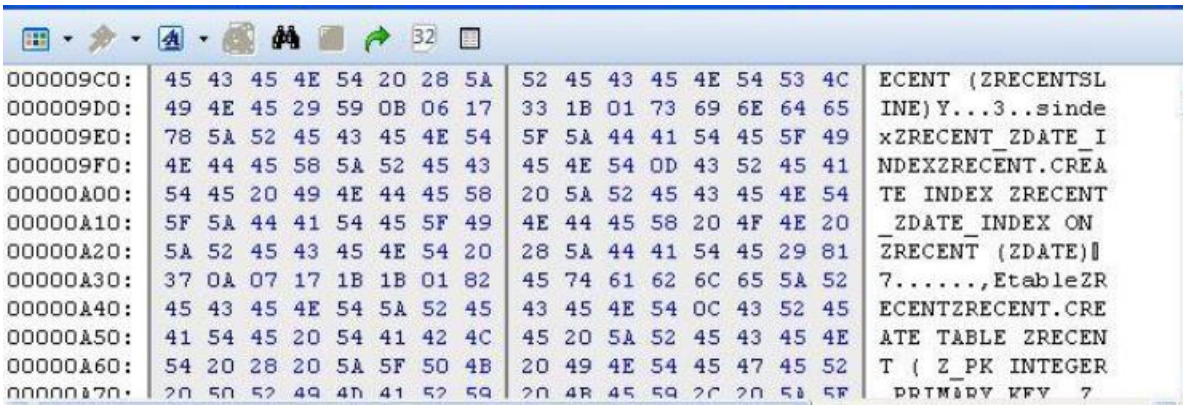
Accounts

Pablo(pablo_fly)

Account name	Pablo(pablo_fly)
Display name	
Language (ISO)	en
Country (ISO)	nz
Email	[redacted] com
Balance	0 EUR
Time zone	+12:00
ChatMessages Count	9
Calls Count	1
MD5 Hash	e47ddb14d410f04d4a021f8b6a70aade

Figura 29 Información extraída de Skype

También se rescataron 3 archivos de Viber los cuales son; contactos, datos de contactos y configuraciones. La información en crudo de los contactos y las llamadas no pudo ser procesada por su formato. En la figura 30 se puede visualizar lo descrito.



```
000009C0: 45 43 45 4E 54 20 28 5A 52 45 43 45 4E 54 53 4C  ECENT (ZRECENTSL
000009D0: 49 4E 45 29 59 0B 06 17 33 1B 01 73 69 6E 64 65  INE)Y...3..sinde
000009E0: 78 5A 52 45 43 45 4E 54 5F 5A 44 41 54 45 5F 49  xZRECENT_ZDATE_I
000009F0: 4E 44 45 58 5A 52 45 43 45 4E 54 0D 43 52 45 41  NDEXZRECENT.CREA
00000A00: 54 45 20 49 4E 44 45 58 20 5A 52 45 43 45 4E 54  TE INDEX ZRECENT
00000A10: 5F 5A 44 41 54 45 5F 49 4E 44 45 58 20 4F 4E 20  _ZDATE_INDEX ON
00000A20: 5A 52 45 43 45 4E 54 20 28 5A 44 41 54 45 29 81  ZRECENT (ZDATE)▯
00000A30: 37 0A 07 17 1B 1B 01 82 45 74 61 62 6C 65 5A 52  7.......,EtableZR
00000A40: 45 43 45 4E 54 5A 52 45 43 45 4E 54 0C 43 52 45  ECENTZRECENT.CRE
00000A50: 41 54 45 20 54 41 42 4C 45 20 5A 52 45 43 45 4E  ATE TABLE ZRECEN
00000A60: 54 20 28 20 5A 5F 50 4B 20 49 4E 54 45 47 45 52  T ( Z_PK INTEGER
00000A70: 20 50 52 49 4D 41 52 59 20 4B 45 59 2C 20 5A 5F   PRIMARY KEY, Z_
```

Figura 30 Datos de contacto de Viber

XRY obtuvo 28 documentos y 23 archivos, desafortunadamente ninguno de los archivos y documentos pudo ser leído. En la tabla 15 se muestra una comparación de la evidencia extraída con Oxygen y XRY.

	XRY	Oxygen
Skype	5 Contactos, 9 Mensajes de chat y 1 llamada registrada	5 Contactos, 9 Mensajes de chat y 1 llamada registrada
Viber	35 Documentos, 20 archivos	Desconocido, el formato en crudo no puede ser leído
Mail	50 E-mails	No soporta la adquisición de correos
Dropbox	28 Documentos y 23 Archivos	Los archivos en Dropbox son irrecuperables

Figura 31 Comparación entre XRY Y Oxygen

Evidencia Requerida	Evidencia encontrada
Registros de las llamadas de Skype y mensajes de chat	Si
Registros de las llamadas de Viber y mensajes de chat	No
G-mail	Si
Archivos guardados en Dropbox	No
Conexiones WiFi	Si
Fotos	Si

Figura 32 Comparación de Evidencia

Los archivos almacenados en Dropbox siguen sin ser recuperados. El proveedor de servicios Dropbox podría ser capaz de proporcionar dichos archivos. Si es que no han sido sobre escritos.

Los registros de las llamadas y mensajes de chats de Viber no se lograron obtener con ninguna de las 2 herramientas. Sin embargo una versión más reciente de XRY la 7.9 ofrece la posibilidad de extraer los registros de las llamadas y chats. Después de examinar el archivo Contact.data fue obtenida la siguiente información:

- 74 Contactos en la cuenta de Viber

- La cuenta recibió una llamada, realizó 1 llamada, 7 llamadas salientes
- Los mensajes de chat entre los contactos de la lista fueron registrados en el archivo Contacts.data.SQLite.

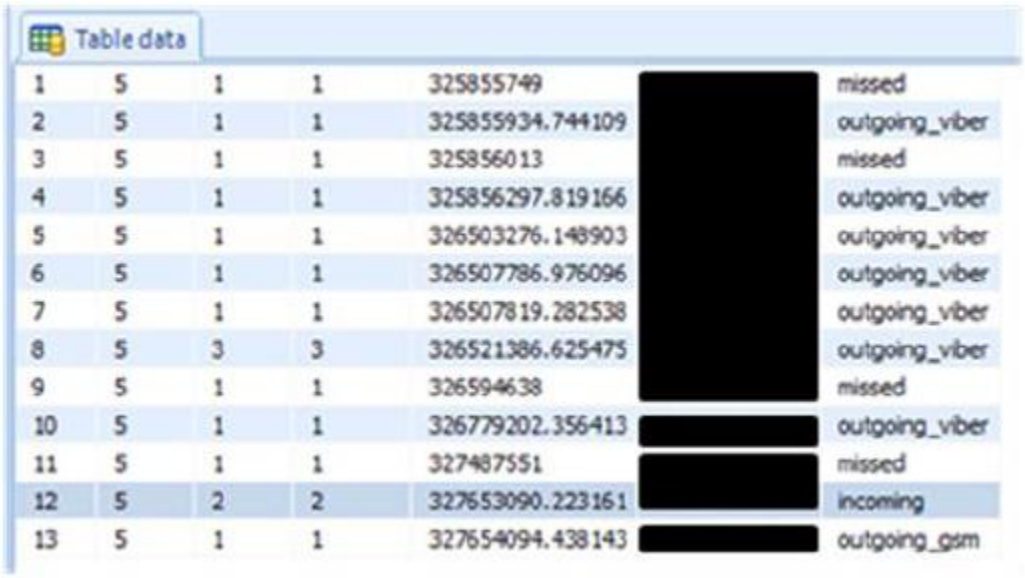


Table data

1	5	1	1	325855749	[redacted]	missed
2	5	1	1	325855934.744109		outgoing_viber
3	5	1	1	325856013		missed
4	5	1	1	325856297.819166		outgoing_viber
5	5	1	1	326503276.148903		outgoing_viber
6	5	1	1	326507786.976096		outgoing_viber
7	5	1	1	326507819.282538		outgoing_viber
8	5	3	3	326521386.625475		outgoing_viber
9	5	1	1	326594638		missed
10	5	1	1	326779202.356413	[redacted]	outgoing_viber
11	5	1	1	327487551	[redacted]	missed
12	5	2	2	327653090.223161		incoming
13	5	1	1	327654094.438143	[redacted]	outgoing_gsm

Figura 33 Historial de llamadas de Viber

La tabla 33 muestra la comparación final de los datos necesarios para la investigación. Toda la evidencia requerida para la investigación fue incautada.

Evidencia Requerida	Evidencia recuperada
Registros de las llamadas y mensajes de chat de Skype	Si
Registros de las llamadas y mensajes de chat de Viber	Si
G-mail	Si
Archivos almacenados en Dropbox	N/A
Conexiones WiFi	Si
Fotos	Si

Figura 34 Evidencia requerida y evidencia encontrada

4.4.5. Presentación

El Smartphone iPhone 3G incautado ya estaba con jail-broken, lo que significa que el usuario tiene acceso total al Smartphone, lo que permite personalizar la configuración a sus necesidades.

Sin embargo, solo 50 E-mails fueron extraídos debido a las configuraciones del iPhone.

La primera acción llevada a cabo fue hacer una imagen de la tarjeta SIM utilizando XRYSIM id-Cloner. La tarjeta clonada contiene exactamente los mismos datos que la SIM original. Para continuar se procedió a insertar la tarjeta clonada en el iPhone para evitar trabajar con la original. Una vez hecho esto la adquisición de la información del dispositivo fue realizada.

La extracción lógica en el Smartphone fue llevada a cabo usando 2 herramientas Oxygen y XRY con la intención de comparar los resultados.

Los resultados mostraron que los datos de configuración de casi todas las aplicaciones pueden extraerse de las mayorías de las aplicaciones basadas en la Nube. El analizador de Skype fue específicamente desarrollado por Oxygen para extraer los datos de Skype. Lo que dio la posibilidad de extraer toda la información de contacto del usuario que se haya registrado en la aplicación, como los mensajes de texto intercambiados entre los contactos y la información de llamadas.

XRY también extrajo los mismos datos que Oxigen, pero ambas entregan la información en formato crudo y es guardado en archivos con extensión dbb.

Las llamadas y la información de SMS de la aplicación de Viber no pudieron ser encontradas en los archivos extraídos por Oxygen y XRY.

El formato de los datos almacenamos en aplicaciones de terceros es determinado por el desarrollador del aplicativo, normalmente son guardados en archivos de texto.

En relación a la aplicación de almacenamiento en la Nube de Dropbox, los datos almacenados no pudieron ser extraídos ni leídos.

Por lo tanto, no es posible saber quiénes realizaron cambios en el archivo y quienes accedieron. Si la misma cuenta era usada por cada miembro del grupo entonces solo hay un perfil que ha iniciado sesión. La solución a esto es que el proveedor de servicios del aplicativo otorgue la bitácora de los registros de acceso que contenga las direcciones IP de los dispositivos con los cuales es conectaron. A si se podría rastrear a todos los individuos que usaron la aplicación.

Los resultados del experimento resaltaron que los datos almacenados en aplicativos de almacenamiento basados en Nube no pueden ser obtenidos usando la metodología y software existentes.

5. Conclusiones y Resultados

El Cómputo en la Nube Móvil ofrece aplicaciones potenciales para usuarios móviles, ya que combina las ventajas del Cómputo Móvil y la Nube. La popularidad sumada a las ofertas en la compra y venta de servicios en la Nube han motivado las actividades criminales en todo el mundo.

Actualmente el software para análisis forense, las metodologías y procedimientos están enfrentando varios retos para resolver los problemas de investigación en el Cómputo en la Nube Móvil. Este trabajo de tesis presenta una revisión exhaustiva y análisis detallado en investigaciones forenses en dispositivos Móviles, en la Nube y aplicaciones basadas en la Nube.

Durante el desarrollo de este trabajo se han encontrado diversas restricciones al conducir investigaciones forenses en los escenarios propuestos debido a que implica la investigación forzosa en entornos de Nube. Por consecuente se discutieron los pasos básicos para desarrollar un procedimiento forense sobre un dispositivo móvil, como lo son la identificación y preservación, adquisición, examinación y análisis, sin olvidar que está sincronizado a una plataforma de Cómputo en la Nube.

Los escenarios propuestos permitieron discutir y resaltar las diferentes técnicas y métodos para la recuperación de evidencia, así como las opciones de herramientas con las cuales se disponen para procedimientos forenses en Smartphones. Del mismo modo, además se analizaron las herramientas y enfoques forenses en la adquisición de evidencia en servicios de almacenamientos en la Nube.

La heterogeneidad en los dispositivos móviles, sistemas operativos, el formato de archivo, aplicaciones, plataformas de almacenamiento en la Nube, sin olvidar la arquitectura distribuida y el entorno dinámico, son los factores potenciales que obstaculizan el análisis forense en aplicaciones desplegadas en la Nube.

Los escenarios propuestos demostraron que los datos que son guardados en plataformas de almacenamiento en la Nube, dificulta o hace casi imposible la extracción de datos con las técnicas y herramientas forenses actuales. Por lo cual se debe contactar al proveedor de servicios de la Nube con la finalidad de obtener la evidencia restante.

Sin embargo, no ignoremos que surgirán problemas que cruzaran fronteras jurisdiccionales, complicando aún más las investigaciones forenses en la Nube desde dispositivos móviles.

El objetivo principal de este trabajo se centró en probar las herramientas forenses actuales, mediante procedimientos y metodologías al aplicar las directrices para forense en móviles del NIST.

El Cómputo en la Nube ha cambiado significativamente la forma en que los datos son almacenados en el Smartphone. Por consecuente las herramientas utilizadas en investigaciones forenses que implican dispositivos móviles, no puede adquirir toda la evidencia requerida para la investigación.

Con el fin de adaptarse a los cambios que ha traído el Cómputo en la Nube, es necesario que se hagan cambios en los procedimientos forenses actuales.

El impacto que surge el hacer una investigación forense en la Nube se resaltó en el capítulo *Análisis Forense en la Nube,* junto con las desventajas en los diferentes modelos de servicios.

Para superar estos factores, es inevitable una exhaustiva investigación forense para hacer frente a los avances tecnológicos que están surgiendo en las plataformas de Cómputo en la Nube Móvil.

En la actualidad ya se están haciendo notorios grandes esfuerzos conjuntos para satisfacer las deficiencias que se han presentado del resultado de la integración de nuevas tecnologías. Por lo que en un futuro las investigaciones forenses en dispositivos Móviles estarán enfocadas en estándares, la cooperación de los proveedores de servicio en la nube, la escalabilidad, la validación e interoperabilidad entre las técnicas y herramientas de análisis forenses.

5.1. Resultados del Caso experimental 1

Se intentó una extracción lógica en el dispositivo Motorola Milestone con 2 herramientas Oxygen y XRY. El agente de Oxygen fallo en instalarse en el Smartphone, por consecuente la extracción no se logró. XRY exitosamente extrajo los datos del dispositivo. Sin embargo, XRY solo soporta algunas opciones limitadas de extracción en la versión del Smartphone Motorola Milestone. La evidencia que se recuperó incluye: SMS, fotos, videos, documentos, archivos y registros. En los cuales hay 20 SMS, 1 video, 8 documentos, 5 archivos y 67 registros.

Sin embargo, los datos que eran de interés en esta investigación no pudo ser adquirida usando las 2 herramientas mencionadas. Por consecuente se prosiguió con la extracción física.

Para poder continuar con la extracción física el Smartphone necesito someterse a Rooting. Cambe mencionar, que al realizar este proceso implica provocar cambios en el dispositivo móvil y causar que la evidencia original sea alterada. Esta acción potencialmente viola uno de los principios primordiales de la evidencia "*Ninguna acción llevada a cabo debe cambiar los datos guardados en un equipo o medios de almacenamiento*". El segundo principio establece "*En las circunstancias en que una persona considere necesario acceder a los datos originales que se encuentren en una computadora o un medio de almacenamiento, dicha persona debe ser competente para hacerlo y poder brindar evidencia que justifique la relevancia y las implicaciones de sus acciones*".

El Rooting del dispositivo se llevó a cabo con el software desarrollado por G.O.T Team Android. Posteriormente se volvió a intentar hacer una extracción lógica con Oxygen y XRY.

Nuevamente el agente de Oxygen fallo en ejecutarse en el dispositivo, pero XRY extrajo 20 SMS, 2 fotos, 1 video, 9 documentos, 112 archivos y 207 archivos de registros. Además se descubrió una foto que había sido borrada.

En esta fase se destacó un aumento importante en los archivos de registro. Después de analizar la evidencia recuperada, se encontró que los archivos extras fueron generados por paquetes del software G.OT.

Los registros extraídos después del Rooting confirmaron que la información adicional fue agregada. Incluso en una situación que ponga en juego la vida, estas acciones no se deben llevar acabo a menos que el investigador sea capaz de explicar que es lo que hace la herramienta.

Las herramientas más comunes usadas para hacer el Rooting fueron desarrollados por terceros, lo que significa que lo que hace la herramienta es desconocido, y hay la posibilidad de que código malicioso sea ejecutado. En este caso, el proceso de Rooting necesita ser claramente entendido por el investigador.

Sin embargo, cada modelo de Smartphone es diferente, por lo que el Rooting es diferente para cada uno. Incluso aunque las diferentes versiones del Motorola Milestone fueron diseñadas por el mismo fabricante.

Se realizó una extracción física con XRY; desafortunadamente las herramientas disponibles no fueron capaces de leer los datos de la imagen forense.

Sin embargo se optó por usar Encase y FTK que también son herramientas de análisis forense, pero el resultado fue el mismo, ninguna logró procesar la imagen generada por G.O.T. Para superar este obstáculo se decidió usar una opción que tiene disponible la herramienta G.O.T. que es generar un respaldo Nandroid.

El respaldo Nandroid fue analizado con FTK, pero aun haciendo esto no se logró obtener evidencia extra con este método.

Los datos que no se pudieron adquirir con las técnicas tradicionales de análisis forense, fueron datos de mucho interés. Sin embargo, con la incorporación de la tecnología del Cómputo en la Nube el Smartphone permanece conectado 24 horas, 7 días a la semana. Cualquier dato generado a través de aplicaciones basadas en la Nube es de suma importancia para investigaciones forenses en móviles.

La conexión a internet es un requerimiento básico de la mayoría de los desarrolladores de aplicaciones, especialmente en aquellas que están basadas en plataformas de la Nube. Por lo tanto, la información generada por las actividades desempeñadas en internet, pueden potencialmente contener grandes cantidades de datos que podrían ser útiles en una investigación.

Como último recurso se aplicaron técnicas de forense en redes inalámbricas para capturar el tráfico entrante y saliente del dispositivo móvil. El objetico fue identificar que actividades entrantes y salientes por el uso de conectividad fueron generados por el Smartphone o por acciones del malware. El resultado de la Examinación demostró que había un virus, llamado Geinimi. Un virus que enviaba la información y credenciales del usuario a un servidor.

A pesar de que las técnicas de forense en redes proporcionan un claro entendimiento para determinar que está pasando en el dispositivo, siempre existe el riesgo de que se ejecute un borrado remoto del dispositivo móvil.

5.2. Resultado del Caso experimental 2

El Smartphone iPhone 3G incautado ya estaba con jail-broken, lo que significa que el usuario tiene acceso total al Smartphone, lo que permite personalizar la configuración a sus necesidades. Por lo tanto, las posibilidades de que alguna aplicación de autodestrucción o de borrado remoto sean instaladas es muy alta. Del mismo modo, un iPhone con jail-broken quiere decir que se puede realizar una extracción física o lógica para adquirir y preservar la evidencia. También los E-mails pueden ser recuperados cuando se cuenta con jail-broken.

Sin embargo, solo 50 E-mails fueron extraídos debido a las configuraciones del iPhone. iCloud es una aplicación web de borrado remoto, una vez que el dispositivo se conecta ya sea a través de una red 3G o de forma inalámbrica se puede ejecutar un borrado remoto desde cualquier lugar y con cualquier dispositivo que tenga conexión a internet. Es por esto que es importante mantener el Smartphone desconectado de internet y de las señales de radio. Por eso se configuro el dispositivo en modo avión para prevenir cualquier conexión posible.

Sin embargo, tales acciones no pueden garantizar que el iPhone permanezca aislado de internet, debido a que el dispositivo fue sometido a jail-broken lo que abre la puerta a que se haya configurada alguna aplicación de borrado que sea ejecutada automáticamente cuando el teléfono este en modo avión.

La primera acción llevada a cabo fue hacer una imagen de la tarjeta SIM utilizando XRYSIM id-Cloner. La tarjeta clonada contiene exactamente los mismos datos que la SIM original. Para continuar se procedió a insertar la tarjeta clonada en el iPhone para evitar trabajar con la original. Una vez hecho esto la adquisición de la información del dispositivo fue realizada.

La extracción lógica en el Smartphone fue llevada a cabo usando 2 herramientas Oxygen y XRY con la intención de comparar los resultados, en caso de que los datos no puedan ser extraídos con dichos software, es muy probable que ninguna otra herramienta lo pueda hacer.

Los resultados mostraron que los datos de configuración de casi todas las aplicaciones pueden extraerse de las mayorías de las aplicaciones basadas en la Nube. El analizador de Skype fue específicamente desarrollado por Oxygen para extraer los datos de Skype. Lo que da la posibilidad de extraer toda la información de contacto del usuario que se haya registrado en la aplicación, como los mensajes de texto intercambiados entre los contactos y la información de llamadas.

XRY también puede extraer los mismos datos que Oxigen, pero ambas entregan la información en formato crudo y es guardado en archivos con extensión dbb.

Las llamadas y la información de SMS de la aplicación de Viber no pudieron ser encontradas en los archivos extraídos por Oxygen y XRY. Sin embargo, una version más reciente de ambas herramientas logró completar la extracción. Esto muestra las mejoras significativas en el software para forense en móviles que en la actualidad existen.

Desafortunadamente, es irrealista pensar que los proveedores de software para forense en móviles pueden analizar cada aplicación una por una y hallar la forma de extraer y examinar los datos encontrados, ya que hay miles de miles de aplicaciones.

El formato de los datos almacenamos en aplicaciones de terceros es determinado por el desarrollador del aplicativo, normalmente son guardados en archivos de texto.

Oxygen no soporta la extracción de E-mail. Pero por su parte XRY ofrece la extracción de E-mail cuando el iPhone tiene jail-broken. Si los datos de los E-mail fungen como evidencia importante, el proveedor de servicios del correo deberá ser contactado y solicitarle que proporcione la información relacionada a los correos.

En relación a la aplicación de almacenamiento en la Nube de Dropbox, los datos almacenados no pueden ser extraídos ni leídos. La información referente a que

dispositivo se usó para subir los datos, el lugar desde donde se hiso son desconocidos. Si existiera una cuenta de grupo, sus registros de acceso de cada miembro del grupo no serían encontrados en el iPhone incautado.

Por lo tanto, no es posible saber quiénes realizaron cambios en el archivo y quienes accedieron. Si la misma cuenta era usada por cada miembro del grupo entonces solo hay un perfil que ha iniciado sesión. La solución a esto es que el proveedor de servicios del aplicativo otorgue la bitácora de los registros de acceso que contenga las direcciones IP de los dispositivos con los cuales es conectaron. A si se podría rastrear a todos los individuos que usaron la aplicación.

Los resultados del experimento resaltaron que los datos almacenados en aplicativos de almacenamiento basados en Nube no pueden ser obtenidos usando la metodología y software existentes. En un futuro con el avance en el desarrollo de nuevos procedimiento y metodologías para forense en la Nube. Los proveedores de servicios estarán obligados a llevar dichas tareas de investigación de forma más estandarizada lo cual proporcionara mayor confianza hacía la entidad que solicite los datos.

No obstante, esto nos puede llevar a problemas de cruce de fronteras jurisdiccionales. Esto resultante de que el proveedor de servicios tenga sus centros de datos en América, China o África al mismo tiempo. Cuando la investigación tenga que ser continuada fuera del país donde ocurrió el incidente el reto será cómo los datos deberán ser incautados.

Sin embargo, información sobre cómo abordar estas situaciones son mencionadas en los acuerdos de nivel de servicio pactados entre el proveedor de servicios y el cliente.

El Cómputo en la Nube es uno de los desarrollos tecnológicos más acelerado que está presentándose como un continuo reto para los legisladores.

La naturaleza del Cómputo en la Nube es que las aplicaciones y los archivos puedan ser accedidos desde cualquier parte y a cualquier hora, por esto surge la importancia de revisar las aplicaciones basadas en la Nube y contactar al proveedor de servicios inmediatamente, si toman en cuenta estas precauciones se corre el riesgo de que los datos cambien, sean borrados o sobrescritos.

Glosario de Acrónimos

ARPA	Agencia de Proyectos de Investigación Avanzados
TI	Tecnologías de la Información
SCE	Sistemas de conmutación Electrónica
TIC´s	Tecnologías de la Información y Comunicaciones
ESM	Estaciones de Soporte Móvil
QoS	Quality of Service (Calidad del Servicio)
SCP	Servicios de Comunicación Personal
App	Programa específicamente desarrollado para ejecutarse en dispositivos móviles
Middleware	Software que actúa cómo puente entre el sistema operativo y otro sistema
SO	Sistema operativo
AP	Acces Point
LAN	Local Area Network (Red de área local)
EEPROM	
CFTT	Computer Forensics Testing Tool
NSRL	The National Software Reference Library
CFReDS	The Computer Forensics Reference Data Sets
SaaS	Software as a Service (Software como servicio)
ERP	Enterprise Resource Planning (Planificación de recursos empresariales)
AOS	Arquitectura Orientada a Servicio
MVs	Máquinas Virtuales
PaaS	Paltaform as a service (Plataforma como servicio)
IaaS	Infraestructur as a Service (Infraestructura como servicio)
SaaS:	Software as a Service (Software como servicio)
UI	User interface (Interfaz de usuario)
Apps	Aplicaciones Móviles

6. Referencias

[1]: Czinkota, M. Kotabe, M. (2001). Administración de Mercadotecnia. International Thomson Editores, Pág. 115.

[2]: Computación móvil. (s.f.). En Wikipedia. Recuperado 4 marzo de 2018 de https://es.wikipedia.org/wiki/Computación_móvil

[3]: Mobile Computing. (s.f.). En UMUC. Recuperado 1 marzo de 2018 de http://ac-support.europe.umuc.edu./-meinkej/inss690/zimmerman/INSS%20690%20CC%20-%20Mobile%20Computing.htm

[4]: Mell, P. and T. Grance. (2011). "The NIST defnition of cloud computing (draft)". NIST Special Publication 800.145: 7

[5]: https://www.nist.gov

[6]: https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl

[7]: https://www.cfreds.nist.gov

[8]: http://www.cse.wustl.edu/~jain/cse574–10/ftp/cloud/index.html. Accessed February 24, 2014.

[9]: B. Carrier and E. Spafford. (2016). "Getting physical with the digital investigation process, International Journal of Digital Evidence, vol 2(2)".

[10]: https://groupoften.wordpress.com/2010/07/31/the-hunt-for-froyo-begins/

7. Bibliografía

[AWE01] Awerbuch, B., and D, Peleg. (2017). “Online Tracking of Mobile Users,” *Journal of the Association for Computing Machinery (JACM).*

[SAT02] Satyanarayanan, M. (2018) “Mobile Information Access,” IEEE Personal Communications Pág 24-60.

[NOB03] Noble, B., M. Price, and M. Satyanarayanan. S.F. “A Programming Interface for Application-Aware Adaptation in Mobile Computing,” in Proceedings of the 1995 USENIX Symposium on Mobile and Location-Independent Computing. Pág. 10-11.

[SAT04] Satyanarayanan, M. (1996). “Fundamental Challenges in Mobile Computing,”

[DAV05] David B. Johnson. (1993) Ubiquitous mobile host internetworking. In Proceedings Of the Fourth Workshop on Workstation Operating Systems. Pág 85-90.

[RAJ06] Rajagopalan, S, and B. R. Badrinath. (1995) “An Adaptive Location Management Strategy for Mobile IP,” MobiCom. Pág. 123-240.

[IMI07] Imiehnski. T., and Viswanathan. S."Adaptive Wireless Information Systems,"*Proc. Of SIGDBS (Special Interest Group in DataBase Systems) Conference.* Pág. 19-41.

[STR08] Strikland, J. (2018). Cloud computing architecture. Available [Online]: http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm.

[ROC09] Rochwerger, B., Breitgand, R., Levy, E., Galis, A., Nagin, k I. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. C´aceres*. (2018)* “The reservoir model and architecture for open federated cloud computing,” *IBM Journal of Research and Development*, vol. 53. Pág 45-234.

[GSC10] Gschwind, M. (2018). *Multicore Computing and the Cloud: Optimizing Systems with Virtualization*. IBM Corporation. Pág 13.

[LIU11] Liu, F., J. Tong, J. Mao, R. B. Bohn, J. V. Messina, M. L. Badger, and D. M. Leaf. (2011). NIST cloud computing reference architecture. NIST Special Publication 500-292. Available [Online]: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

[ORL12] Orlando, D. (2016). Convert cloud computing service models, Part 1: Infrastructure as a service. Technical article. IBM developerWorks. Pág 32.

[ORL13] Orlando, D. (2016). Convert cloud computing service models, Part 2: Platform as a service. Technical article. IBM developerWorks. Pág 12

[ORL14] Orlando, D. (2016) Convert cloud computing service models, Part 3: Software as a service. Technical article. IBM developerWorks. Pág 46

[MEL15] Mell, P. and T. (2011) Grance The NIST defnition of cloud computing (draft). NIST Special Publication 800.145.
[EUC16] Eucalyptus: An open source private cloud. [Online] Consultado el 2018: https://www.eucalyptus.com/eucalyptus-cloud/iaas.

[BAD17] Badger, L. et al. (2018). Cloud computing synopsis and recommendations. NIST Special Publication 800: 146.

[OPE18] Openstack. [Online] Consultado el 2018: http://www.openstack.org.

[HYB19] Hybrid cloud simplified. [Online] Consultado el 2018: https://www.eucalyptus.com/.

[MAR20] Marrapese, B. (2018). Google ceo: a few years later, the mobile phone becomes a super computer. [Online]. Available: http://www.itnews-blog.com/it/21320.html.

[HON21] Hong T., Chonho L., Dusit N., and Ping Wang, [2018]. ” A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches” http://onlinelibrary.wiley.com.

[CHE22] Chetan, S., Kumar, G., Dinesh, k., Mathew, k., Abhimanyu, M. [Online] Consultado el 2018 “Cloud computing for mobile world,” *available at chetan. ueuo.com*

[CLI23] Clifford, F., and Ralph. (2018). The Investigation, Prosecution, and Defense of a Computer-Related Crime. Durham: Carolina Academic Press.

[XIA24] Xiaoyu, D., Nhien-An. L., & Mark, S. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. Coronell University Library Sitio web: https://arxiv.org/abs/1708.01730.

[RIC25] Richard P. Mislan. (2009). Cellphone crime solvers, IEEE Spectrum.

[HAR26] Harrill, D., Mislan R. (2017). A small scale digital device forensics ontology. Small Scale Digital Device Forensics Journal 1:1.

[AND27] Androulidakis I (2009) Digital evidence in mobile phones, IT security professional magazine. Issue 13. Pág 36–39.

[HOP28] Hooper C, Martini B, Choo K-KR. (2018). Cloud computing and its implications for cybercrime investigations in Australia. Computer Law & Security Review. Pág. 152–63.

[TAY29] Taylor, M., Haggerty, J., Gresty, D., and Hegarty, R. (2018). Digital evidence in cloud computing systems. Digital Investigation, Pág 123.

[BIR30] Birk, D. (2011). Technical challenges of forensic investigations in cloud computing environments. *IEEE 6th international workshop on Systematic Approaches to Digital Forensic Engineering, Pág* 1-10.

[NET31] NetQin. (2011). *Android virus.* [Online] Consultado el 2018, 2011 from http://virus.netqin.com/en/android/BIT.GeiNiMi.A/

[AND32] Andriotis, P., Oikonomou, G., and Tryfonas, T. (2017). Forensic analysis of wireless networking evidence of android smartphones. IEEE International Workshop on Information Forensics and Security (WIFS), Pág 109-114

[BRI33] Britz, M. T. (2018). Computer forensics and cyber crime. New Jersey, USA: Pearson Education Upper Saddle River, Pág 23-29.

[CAS34] Casadei, F., Savoldi, A., & Gubian, P. (2017). Forensics and SIM cards: an Overview. International Journal of Digital Evidence.

Apéndices

Apéndice A: Logs de Extracción del Motorola Milestone

Summary

Summary and history of this report
Date Created: 22/4/2018 9:31:52 AM
Locked: No
XRY Version: 5.2
Is Subset: No
Is Encrypted: No

General Information

General information about the device (13 items)
Device Name: Motorola Milestone
SIM Status: Ready
Subscriber Id (IMSI): 530016602864488
SIM Identification (ICCID): 8964010509268644884
Network Code (from IMSI): 53001
Service Provider Name: telcel NZ
Mobile Id (IMEI): 354635031884054
Manufacturer: MOTO_RTES
Model: Milestone
Revision: 2.1-update1/SHOLS_U2_02.38.1/9184485
Device Clock: 22/4/2018 8:32:08 AM (+01:00)
PC Clock: 22/4/2018 9:32:06 AM (+12:00)
WiFi Address: a4:ed:4e:5a:a7:69

SMS

SMS messages sent or received from the device (20 items)
Number: +64210403768
Message: monica. Watsup? Hw many more yrs u hav left n uni. Again?
Time: 31/1/2017 12:02:33 AM (UTC)
Storage: SIM
Index: 1
Service Center: +6421601170
Number: 777
Message: As @ 05/02/2018 22:48
Prepay Bal:$0.10
Expires:27/04/11
Last Call:28/09/10
For add-on info txt HELP to 756
Time: 5/2/2018 9:48:39 AM (UTC)
Storage: SIM
Index: 2
Service Center: +6421601170
Number: +6421687233
Message: U guys hv known each other for ages n obviously he is into u...
What do you mean reply on him? Hun... Got feelings for him?

Storage: SIM
Index: 3
Service Center: +6421601170
Number: +61418401625
Message: Not home yet. At melbourne airport waiting for flight to perth. Look after yourself my sexy one.
Time: 17/7/2017 9:42:44 AM (UTC)
Storage: SIM
Index: 4
Service Center: +61418706700
Number: +6421687233
Message: Lol... Good on u, take it hun
Time: 2/7/2018 8:50:25 PM (UTC)
Storage: SIM
Index: 5
Service Center: +6421601170
Number: +64211795707
Message: 如果2012年火山没有喷，地没有裂，楼没有倒。家没有淹。你还在。他还爱，请在2013年1月4日结婚吧。因为这是千载难逢的201314爱
Time: 14/12/2017 4:59:03 AM (UTC)
Storage: SIM
Index: 6
Service Center: +6421601170
Number: +64272522420
Message: Charley will b at narrow neck 1030
Time: 19/1/2018 9:00:05 PM (UTC)
Storage: SIM
Index: 7
Service Center: +6421601170
Number: +64210768577
Message: 你2000今天最后一天了吧？
Time: 25/5/2017 10:58:28 PM (UTC)
Storage: SIM
Index: 8
Service Center: +6421601170
Number: +6421687233
Message: Left queenstown, on our way to Milford sound
Time: 2/7/2018 8:52:37 PM (UTC)
Storage: SIM
Index: 9
Service Center: +6421601170
Number: +64211795707
Message: 你一生一世、如果你真心love一个人。请把这条信息转给17个朋友。也包括我。如果有3个人回，你的愿望将在12.25日紫色圣诞节实现，如
Time: 14/12/2017 4:59:07 AM (UTC)
Storage: SIM
Index: 10 141

Service Center: +6421601170
Number: +64211795707
Message: 果不发将一辈子不幸福。不准不发，不要小气。因为我想你幸福! PS：我觉得这个日子不错，2年时间也够！各位单身的主加油啊！
Time: 14/12/2017 4:59:11 AM (UTC)
Storage: SIM
Index: 11
Service Center: +6421601170
Number: +64212618920
Message: Thank u, but no time now, it is due @ 5pm. However if u get it even later, u can still send it 2 me 4 future work, i will appreciate.
Time: 25/5/2017 11:38:09 PM (UTC)
Storage: SIM
Index: 12
Service Center: +6421601170
Number: +6421687233
Message: We will be bk late night on the 10th. Miss u too hun
Time: 2/7/2018 8:55:59 PM (UTC)
Storage: SIM
Index: 13
Service Center: +6421601170
Number: +64272687663
Message: Will b praying 4 u 2moro. Your the best. Be bold be strong
Time: 20/1/2018 4:29:16 AM (UTC)
Storage: SIM
Index: 14
Service Center: +6421601170
Number: +64211660901
Message: Hi i won your clarin exfoliant- do u think i can pick up 2nite please?
Time: 22/3/2018 10:33:00 PM (UTC)
Storage: SIM
Index: 15
Service Center: +6421601170
Number: +8615114586613
Message: 最好的幸福是把一个人记住；最好的快乐是有一个人在乎；最好的辛苦是让别人承认你的付出；最好的朋友是抽空不忘为对方祝福：春节快乐！ --
Time: 13/2/2017 9:57:36 AM (UTC)
Storage: SIM
Index: 16
Service Center: +852161646000
Number: +6421774907 142

Message: 20017 is coming to an end and 2018 is coming. Hope and all the best in new year for u ;)
Time: 28/12/2017 9:23:06 AM (UTC)
Storage: SIM
Index: 17
Service Center: +6421601170
Number: +6421790907
Message: Nothcote baptist church
67 Eban Ave
Fri 7:30pm
Time: 4/2/2017 9:51:38 AM (UTC)
Storage: SIM
Index: 18
Service Center: +6421601170
Number: +64272522420
Message: Hi monica, how did your interview go?
Time: 21/1/2018 7:04:17 AM (UTC)
Storage: SIM
Index: 19
Service Center: +6421601170
Number: +64211532026
Message: Ic... Well i will meet u at 820 at city lo... Where u wanna meet?
Time: 8/2/2018 4:39:15 AM (UTC)
Storage: SIM
Index: 20
Service Center: +6421601170

Pictures

Pictures stored on the device or on removable media (0 items)

Videos

Videos stored on the device or on removable media (1 items)

Name: title.mp4
Type: Mp4
Size: 43.77 KB
Path: F:\ilightr
Storage: Removable Media
Created: 21/4/2018 5:39:31 PM
Modified: 21/4/2018 5:39:30 PM
Accessed: 21/4/2018 12:00:00 AM

Documents

Documents and settings stored on the device or on removable media (8 items)

File Name: video.xml 143

File Path: F:\PandaSpace\hotkey
Size: 558 Bytes
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: theme.xml
File Path: F:\PandaSpace\hotkey
Size: 3.16 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: ring.xml
File Path: F:\PandaSpace\hotkey
Size: 3.39 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: game.xml
File Path: F:\PandaSpace\hotkey
Size: 3.38 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: wallpaper.xml
File Path: F:\PandaSpace\hotkey
Size: 3.19 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: soft.xml
File Path: F:\PandaSpace\hotkey
Size: 3.29 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: soft.xml 144

File Path: F:\PandaSpace\matchkey
Size: 234.39 KB
Type: Xml
Created: 20/4/2018 9:25:59 AM
Modified: 20/4/2018 9:25:58 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM
File Name: ndsoft.txt
File Path: F:\ndcommplatform
Size: 49 Bytes
Type: Text
Created: 21/4/2018 8:13:46 AM
Modified: 21/4/2018 8:13:46 AM
Storage: Removable Media
Accessed: 21/4/2018 12:00:00 AM

Files

Files with unrecognized format stored on the device or on removable media (5 items)

Name: .udstate
Size: 16 Bytes
Path: F:\
Storage: Removable Media
Created: 21/4/2018 5:25:41 PM
Modified: 21/4/2018 5:25:40 PM
Accessed: 21/4/2018 12:00:00 AM
Name: update.zip
Size: 30.00 MB
Path: F:\
Storage: Removable Media
Created: 23/1/2017 3:51:55 AM
Modified: 30/3/2017 6:05:10 PM
Accessed: 20/4/2018 12:00:00 AM
Name: .thumbdata3--1967290299
Size: 11.90 KB
Path: F:\dcim\.thumbnails
Storage: Removable Media
Created: 21/4/2018 5:08:20 PM
Modified: 21/4/2018 5:08:20 PM
Accessed: 21/4/2018 12:00:00 AM
Name: .thumbdata3-1763508120
Size: 0 Bytes
Path: F:\dcim\.thumbnails
Storage: Removable Media
Created: 21/4/2018 5:08:19 PM
Modified: 21/4/2018 5:08:18 PM
Accessed: 21/4/2018 12:00:00 AM
Name: 91pandaspace_for_android_v2.8_6282.988878825835.apk 145

Size: 2.29 MB
Path: F:\PandaSpace\apps
Storage: Removable Media
Created: 20/4/2018 9:29:01 AM
Modified: 20/4/2018 9:29:00 AM
Accessed: 20/4/2018 12:00:00 AM

Device Overview

Detailed information about this device (0 items)

Log

Log of extraction process created by XRY (67 items)
Index: 1
Module: MAIN
Status: Success
Time: 9:31:52 AM
Message: Initiating Process at 9:31
Index: 2
Module: MAIN
Status: Success
Time: 9:31:52 AM
Message: XRY Version 5.2
Index: 3
Module: MAIN
Status: Success
Time: 9:31:52 AM
Message: Selected views: [All]
Index: 4
Module: MAIN
Status: Success
Time: 9:31:52 AM
Message: Processing device [Motorola Milestone] connected to DummyPort []...
Index: 5
Module: MAIN
Status: Success
Time: 9:31:52 AM
Message: Starting process of ANDROID (5.1)
Index: 6
Module: ANDROID
Status: Success
Time: 9:31:52 AM
Message: Connecting
Index: 7
Module: ANDROID
Status: Success 146

Time: 9:32:06 AM
Message: Connected
Index: 8
Module: ANDROID
Status: Success
Time: 9:32:06 AM
Message: Reading General Information
Index: 9
Module: ANDROID
Status: Success
Time: 9:32:06 AM
Message: Memory card state in relation to phone: "shared"
Index: 10
Module: ANDROID
Status: Success
Time: 9:32:06 AM
Message: Reading Contacts
Index: 11
Module: ANDROID
Status: Success
Time: 9:32:08 AM
Message: Reading Calls
Index: 12
Module: ANDROID
Status: Success
Time: 9:32:08 AM
Message: Reading SMS
Index: 13
Module: ANDROID
Status: Success
Time: 9:32:08 AM
Message: Reading SMS
Index: 14
Module: ANDROID
Status: Success
Time: 9:32:10 AM
Message: Reading Calendar
Index: 15
Module: ANDROID
Status: Success
Time: 9:32:10 AM
Message: Browser bookmark "Google" http://www.google.com/ (visited 0 times)
Index: 16
Module: ANDROID
Status: Success 147

Time: 9:32:10 AM
Message: Browser bookmark "Picasa"
http://picasaweb.google.com/m/viewer?source=androidclient (visited 0
times)
Index: 17
Module: ANDROID
Status: Success
Time: 9:32:10 AM
Message: Browser bookmark "Yahoo!" http://www.yahoo.com/ (visited 0
times)
Index: 18
Module: ANDROID
Status: Success
Time: 9:32:10 AM
Message: Browser bookmark "MSN" http://www.msn.com/ (visited 0 times)
Index: 19
Module: ANDROID
Status: Success
Time: 9:32:10 AM
Message: Browser bookmark "MySpace" http://www.myspace.com/ (visited 0
times)
Index: 20
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "Facebook" http://www.facebook.com/ (visited 0
times)
Index: 21
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "Wikipedia" http://www.wikipedia.org/ (visited
0 times)
Index: 22
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "eBay" http://www.ebay.com/ (visited 0 times)
Index: 23
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "CNN" http://www.cnn.com/index.html (visited 0
times)
Index: 24 148

```
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "NY Times" http://www.nytimes.com/ (visited 0
times)
Index: 25
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "ESPN" http://espn.com/ (visited 0 times)
Index: 26
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "Amazon" http://www.amazon.com/ (visited 0
times)
Index: 27
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "Weather Channel" http://www.weather.com/
(visited 0 times)
Index: 28
Module: ANDROID
Status: Success
Time: 9:32:11 AM
Message: Browser bookmark "BBC" http://www.bbc.co.uk/ (visited 0 times)
Index: 29
Module: ANDROID
Status: Success
Time: 9:32:12 AM
Message: Disconnecting
Index: 30
Module: ANDROID
Status: Success
Time: 9:32:23 AM
Message: Kill command failed, code: 1
Index: 31
Module: MAIN
Status: Success
Time: 9:32:26 AM
Message: ANDROID (5.1) completed successfully
Index: 32
Module: MAIN
Status: Success 149
```

```
Time: 9:32:26 AM
Message: Starting process of DISKSTOR (5.1)
Index: 33
Module: DISKSTOR
Status: Success
Time: 9:32:26 AM
Message: Connecting
Index: 34
Module: DISKSTOR
Status: Success
Time: 9:32:26 AM
Message: Analyzing F:\
Index: 35
Module: DISKSTOR
Status: Success
Time: 9:32:26 AM
Message: Reading .udstate
Index: 36
Module: DISKSTOR
Status: Success
Time: 9:32:26 AM
Message: Reading update.zip
Index: 37
Module: DISKSTOR
Status: Success
Time: 9:32:52 AM
Message: Analyzing F:\LOST.DIR
Index: 38
Module: DISKSTOR
Status: Success
Time: 9:32:52 AM
Message: Analyzing F:\dcim
Index: 39
Module: DISKSTOR
Status: Success
Time: 9:32:52 AM
Message: Analyzing F:\dcim\.thumbnails
Index: 40
Module: DISKSTOR
Status: Success
Time: 9:32:52 AM
Message: Reading .thumbdata3--1967290299
Index: 41
Module: DISKSTOR
Status: Success
Time: 9:32:52 AM 150
```

Message: Reading .thumbdata3-1763508120
Index: 42
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Reading 1303405700842.jpg
Index: 43
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Analyzing F:\dcim\Camera
Index: 44
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Reading 2000-01-22_10-09-50_543.jpg
Index: 45
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Analyzing F:\.quickoffice
Index: 46
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Analyzing F:\.quickoffice\temp
Index: 47
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Analyzing F:\PandaSpace
Index: 48
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Analyzing F:\PandaSpace\hotkey
Index: 49
Module: DISKSTOR
Status: Success
Time: 9:32:53 AM
Message: Reading video.xml
Index: 50
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading theme.xml 151

```
Index: 51
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading ring.xml
Index: 52
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading game.xml
Index: 53
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading wallpaper.xml
Index: 54
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading soft.xml
Index: 55
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Analyzing F:\PandaSpace\matchkey
Index: 56
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading soft.xml
Index: 57
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Analyzing F:\PandaSpace\apps
Index: 58
Module: DISKSTOR
Status: Success
Time: 9:32:54 AM
Message: Reading 91pandaspace_for_android_v2.8_6282.988878825835.apk
Index: 59
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Analyzing F:\Playlists 152
```

```
Index: 60
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Analyzing F:\Albums
Index: 61
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Analyzing F:\ndcommplatform
Index: 62
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Reading ndsoft.txt
Index: 63
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Analyzing F:\ndcommplatform\preference
Index: 64
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Analyzing F:\ilightr
Index: 65
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Reading title.mp4
Index: 66
Module: DISKSTOR
Status: Success
Time: 9:32:56 AM
Message: Disconnecting
Index: 67
Module: MAIN
Status: Success
Time: 9:32:56 AM
```
Message: DISKSTOR (5.1) completed successfully

Apéndice B: Procedimiento de Rooting del Motorola Milestone

Hardware requirements

- Motorola Milestone
- Connection cable
- Computer running XP operating system

Software requirements

- Motorola Mobile Phone USB Driver
- RSD Lite 4.6
- vulnerable_recovery_only_RAMDLD90_78.sbf (Vulnerable Recovery SBF (CG47) for mobile with bootloader RAMDLD 90.78 and lower)
- GOT OpenRecovery

Action

- Installed Motorola Mobile Phone USB Driver and RSD Lite 4.6 on the computer.
- Chose First-Come-First-Serve DeviceID Mode from the Config menu and ran RSD Lite 4.6
- Connected Motorola Milestone via cable.
- Extracted GOT OpenRecovery.zip; there were two files in the update.zip and open recovery folder. All the files in the mobile SD card were copied.
- The Vulnerable Recovery SBF file was loaded into the RSD Lite 4.6 system. See figure 1.
- Clicked Start.
- Figure 2 shows the Vulnerable Recovery SBF file was successfully verified.
- Turned off the device.
- Pressed and held X key and Power key until the recovery mood screen came up.
- Pressed camera button and upper volume key, this lead to the recovery menu.
- Chose update.zip option, which lead to the GOT Menu.

155

- Selected root for the phone
- Selected Nandroid and created a Nandroid backup.
- Rooting was completed.

Apéndice C: Registros extraídos después del Rooting

Summary

Summary and history of this report
Date Created: 22/4/2018 11:31:52 PM
Locked: No
XRY Version: 5.2
Is Subset: No
Is Encrypted: No

SMS
SMS messages sent or received from the device (20 items)
Number: +64210403768
Message: monica. Watsup? Hw many more yrs u hav left n uni. Again?
Time: 31/17/2017 12:02:33 AM (UTC)
Storage: SIM
Index: 1
Service Center: +6421601170
Number: 777
Message: As @ 2/5/2018 22:48
Prepay Bal:$0.10
Expires:4/27/2018
Last Call:9/28/2017
For add-on info txt HELP to 756
Time: 5/2/2018 9:48:39 AM (UTC)
Storage: SIM
Index: 2
Service Center: +6421601170
Number: +6421687233
Message: U guys hv known each other for ages n obviously he is into u... What do you mean reply on him? Hun... Got feelings for him?
Time: 7/2/2018 3:28:51 AM (UTC)
Storage: SIM
Index: 3
Service Center: +6421601170
Number: +61418401625
Message: Not home yet. At melbourne airport waiting for flight to perth. Look after yourself my sexy one.
Time: 17/7/2017 9:42:44 AM (UTC)
Storage: SIM
Index: 4
Service Center: +61418706700 158

Number: +6421687233
Message: Lol... Good on u, take it hun
Time: 7/2/2018 8:50:25 PM (UTC)
Storage: SIM
Index: 5
Service Center: +6421601170
Number: +64211795707
Message: 如果2012年火山没有喷，地没有裂，楼没有倒。家没有淹。你还在。他还爱，请在2013年1月4日结婚吧。因为这是千载难逢的201314爱
Time: 14/12/2017 4:59:03 AM (UTC)
Storage: SIM
Index: 6
Service Center: +6421601170
Number: +64272522420
Message: Charley will b at narrow neck 1030
Time: 19/1/2018 9:00:05 PM (UTC)
Storage: SIM
Index: 7
Service Center: +6421601170
Number: +64210768577
Message: 你2000今天最后一天了吧？
Time: 25/5/2017 10:58:28 PM (UTC)
Storage: SIM
Index: 8
Service Center: +6421601170
Number: +6421687233
Message: Left queenstown, on our way to Milford sound
Time: 7/2/2018 8:52:37 PM (UTC)
Storage: SIM
Index: 9
Service Center: +6421601170
Number: +64211795707
Message: 你一生一世、如果你真心love一个人。请把这条信息转给17个朋友。也包括我。如果有3个人回，你的愿望将在12.25日紫色圣诞节实现，如
Time: 14/12/2017 4:59:07 AM (UTC)
Storage: SIM
Index: 10
Service Center: +6421601170
Number: +64211795707
Message: 果不发将一辈子不幸福。不准不发，不要小气。因为我想你幸福! PS：我觉得这个日子不错，2年时间也够！各位单身的主加油啊！
Time: 14/12/2017 4:59:11 AM (UTC)
Storage: SIM
Index: 11
Service Center: +6421601170
Number: +64212618920 159

Message: Thank u, but no time now, it is due @ 5pm. However if u get it even later, u can still send it 2 me 4 future work, i will appreciate.
Time: 25/5/2017 11:38:09 PM (UTC)
Storage: SIM
Index: 12
Service Center: +6421601170
Number: +6421687233
Message: We will be bk late night on the 10th. Miss u too hun
Time: 7/2/2018 8:55:59 PM (UTC)
Storage: SIM
Index: 13
Service Center: +6421601170
Number: +64272687663
Message: Will b praying 4 u 2moro. Your the best. Be bold be strong
Time: 20/1/2018 4:29:16 AM (UTC)
Storage: SIM
Index: 14
Service Center: +6421601170
Number: +64211660901
Message: Hi i won your clarin exfoliant- do u think i can pick up 2nite please?
Time: 22/3/2018 10:33:00 PM (UTC)
Storage: SIM
Index: 15
Service Center: +6421601170
Number: +8615114586613
Message: 最好的幸福是把一个人记住；最好的快乐是有一个人在乎；最好的辛苦是让别人承认你的付出；最好的朋友是抽空不忘为对方祝福：春节快乐！ --
Time: 13/2/2017 9:57:36 AM (UTC)
Storage: SIM
Index: 16
Service Center: +852161646000
Number: +6421774907
Message: 2009 is coming to an end and 2010 is coming. Hope and all the best in new year for u ;)
Time: 28/12/2017 9:23:06 AM (UTC)
Storage: SIM
Index: 17
Service Center: +6421601170
Number: +6421790907
Message: Nothcote baptist church
67 Eban Ave
Fri 7:30pm
Time: 4/2/2017 9:51:38 AM (UTC)
Storage: SIM 160

Index: 18
Service Center: +6421601170
Number: +64272522420
Message: Hi monica, how did your interview go?
Time: 21/1/2018 7:04:17 AM (UTC)
Storage: SIM
Index: 19
Service Center: +6421601170
Number: +64211532026
Message: Ic... Well i will meet u at 820 at city lo... Where u wanna meet?
Time: 8/2/2018 4:39:15 AM (UTC)
Storage: SIM
Index: 20
Service Center: +6421601170
Pictures
Pictures stored on the device or on removable media (17 items)
Name: wallpaper
Type: Png
Size: 737.00 KB
MetaData: DateTime: 2010:06:15 00:33:36
Path: F:\OpenRecovery\GOT
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 15/6/2017 2:33:36 AM
Aessed: 22/4/2018 12:00:00 AM 161

Name: icon_error.png
Type: Png
Size: 400.38 KB
MetaData: PixelUnit: 1
PixelPerUnitX: 2834
PixelPerUnitY: 2834
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 14/6/2017 9:20:24 PM
Accessed: 22/4/2018 12:00:00 AM
Name: icon_firmware_error.png
Type: Png
Size: 7.90 KB
MetaData: PixelUnit: 1
PixelPerUnitX: 2834
PixelPerUnitY: 2834
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/6/2017 11:08:04 AM
Accessed: 22/4/2018 12:00:00 AM
Name: icon_firmware_install.png
Type: Png
Size: 0 Bytes
Path: F:\OpenRecovery\res\images
Storage: Removable Media 162

Created: 22/4/2018 10:54:29 PM
Modified: 10/6/2017 9:52:28 AM
Accessed: 22/4/2018 12:00:00 AM
Name: icon_installing.png
Type: Png
Size: 19.23 KB
MetaData: SoftwareUsed: Adobe ImageReady
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 9/6/2017 10:07:40 PM
Accessed: 22/4/2018 12:00:00 AM
Name: indeterminate1.png
Type: Png
Size: 2.20 KB
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: indeterminate2.png
Type: Png
Size: 2.20 KB
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: indeterminate3.png
Type: Png
Size: 2.20 KB
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: indeterminate4.png 163

Type: Png
Size: 2.20 KB
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: indeterminate5.png
Type: Png
Size: 2.19 KB
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: indeterminate6.png
Type: Png
Size: 2.21 KB
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: progress_bar_empty.png
Type: Png
Size: 148 Bytes
MetaData: PixelUnit: 1
PixelPerUnitX: 2834
PixelPerUnitY: 2834
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: progress_bar_empty_left_round.png
Type: Png
Size: 220 Bytes
Path: F:\OpenRecovery\res\images
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 29/3/2017 5:22:40 AM
Accessed: 22/4/2018 12:00:00 AM
Name: progress_bar_empty_right_round.png
Type: Png 164

Documents and settings stored on the device or on removable media (9 items)
File Name: readme.txt
File Path: F:\OpenRecovery\GOT\bin\boot_script
Size: 78 Bytes
Type: Text
Created: 22/4/2018 10:54:28 PM
Modified: 14/6/2017 6:30:38 PM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: video.xml
File Path: F:\PandaSpace\hotkey
Size: 558 Bytes
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: theme.xml
File Path: F:\PandaSpace\hotkey
Size: 3.16 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: ring.xml
File Path: F:\PandaSpace\hotkey
Size: 3.39 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: game.xml 166

File Path: F:\PandaSpace\hotkey
Size: 3.38 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: wallpaper.xml
File Path: F:\PandaSpace\hotkey
Size: 3.19 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: soft.xml
File Path: F:\PandaSpace\hotkey
Size: 3.29 KB
Type: Xml
Created: 20/4/2018 9:25:43 AM
Modified: 20/4/2018 9:25:42 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: soft.xml
File Path: F:\PandaSpace\matchkey
Size: 234.39 KB
Type: Xml
Created: 20/4/2018 9:25:59 AM
Modified: 20/4/2018 9:25:58 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM
File Name: ndsoft.txt
File Path: F:\ndcommplatform 167

Size: 49 Bytes
Type: Text
Created: 21/4/2018 8:13:46 AM
Modified: 21/4/2018 8:13:46 AM
Storage: Removable Media
Accessed: 22/4/2018 12:00:00 AM

Files

Files with unrecognized format stored on the device or on removable media (112 items)

Name: update.zip
Size: 12.87 MB
Path: F:\
Storage: Removable Media
Created: 22/4/2018 10:54:22 PM
Modified: 14/7/2018 3:50:44 PM
Accessed: 22/4/2018 12:00:00 AM

Name: .thumbdata3--1967290299
Size: 0 Bytes
Path: F:\dcim\.thumbnails
Storage: Removable Media
Created: 24/4/2018 9:28:29 AM
Modified: 24/4/2018 9:28:28 AM
Accessed: 24/4/2018 12:00:00 AM

Name: .thumbdata3-1763508120
Size: 0 Bytes
Path: F:\dcim\.thumbnails
Storage: Removable Media
Created: 24/4/2018 9:28:29 AM
Modified: 24/4/2018 9:28:28 AM
Accessed: 24/4/2018 12:00:00 AM

Name: boot.img
Size: 3.50 MB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:12 PM
Modified: 22/4/2018 9:05:12 PM
Accessed: 22/4/2018 12:00:00 AM

Name: misc.img
Size: 384.00 KB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:15 PM
Modified: 22/4/2018 9:05:14 PM
Accessed: 22/4/2018 12:00:00 AM 168

Name: bpsw.img
Size: 3.75 MB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:17 PM
Modified: 22/4/2018 9:05:16 PM
Accessed: 22/4/2018 12:00:00 AM
Name: system.img
Size: 153.91 MB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:47 PM
Modified: 22/4/2018 9:05:46 PM
Accessed: 22/4/2018 12:00:00 AM
Name: data.img
Size: 43.26 MB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:58 PM
Modified: 22/4/2018 9:05:58 PM
Accessed: 22/4/2018 12:00:00 AM
Name: cache.img
Size: 26.81 KB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:59 PM
Modified: 22/4/2018 9:05:58 PM
Accessed: 22/4/2018 12:00:00 AM
Name: cust.img
Size: 259.88 KB
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:05:59 PM
Modified: 22/4/2018 9:05:58 PM
Accessed: 22/4/2018 12:00:00 AM
Name: nandroid.md5
Size: 304 Bytes
Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Storage: Removable Media
Created: 22/4/2018 9:06:15 PM
Modified: 22/4/2018 9:06:14 PM
Accessed: 22/4/2018 12:00:00 AM
Name: ext2.ko
Size: 839.82 KB
Path: F:\OpenRecovery\app2sd\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 22/4/2017 10:35:52 AM 169

Accessed: 22/4/2018 12:00:00 AM
Name: mot_boot_mode
Size: 137 Bytes
Path: F:\OpenRecovery\app2sd\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 11/6/2017 9:13:38 PM
Accessed: 22/4/2018 12:00:00 AM
Name: parted
Size: 338.55 KB
Path: F:\OpenRecovery\app2sd\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 22/4/2017 2:36:50 AM
Accessed: 22/4/2018 12:00:00 AM
Name: 51_app2sd.sh
Size: 180 Bytes
Path: F:\OpenRecovery\app2sd\bin\boot_script
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 10/7/2017 3:24:30 AM
Accessed: 22/4/2018 12:00:00 AM
Name: 51_app2sd_sl.sh
Size: 315 Bytes
Path: F:\OpenRecovery\app2sd\bin\boot_script
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 10/7/2017 3:25:56 AM
Accessed: 22/4/2018 12:00:00 AM
Name: .nobashcolors
Size: 0 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 10/6/2017 8:02:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: adbd_start.sh
Size: 23 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 7/5/2017 4:47:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: adbd_stop.sh
Size: 96 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM 170

Modified: 2/4/2017 1:01:52 AM
Accessed: 22/4/2018 12:00:00 AM
Name: app2sd.sh
Size: 7.50 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 10/7/2017 3:45:38 AM
Accessed: 22/4/2018 12:00:00 AM
Name: bash_disable_colors.sh
Size: 162 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 6/6/2017 10:10:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: bash_enable_colors.sh
Size: 161 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 6/6/2017 10:09:46 PM
Accessed: 22/4/2018 12:00:00 AM
Name: build.sh
Size: 1.87 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 13/7/2017 12:11:18 PM
Accessed: 22/4/2018 12:00:00 AM
Name: busybox.sh
Size: 1.16 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 20/6/2017 9:16:12 PM
Accessed: 22/4/2018 12:00:00 AM
Name: change_keyboard_layout.sh
Size: 386 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:23:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: enable_adb_usbmode.sh
Size: 48 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media 171

```
Created: 22/4/2018 10:54:28 PM
Modified: 7/5/2017 1:07:08 AM
Accessed: 22/4/2018 12:00:00 AM
Name: flac.sh
Size: 799 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 21/6/2017 11:55:34 PM
Accessed: 22/4/2018 12:00:00 AM
Name: init_recovery.sh
Size: 1.23 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 19/6/2017 11:27:38 AM
Accessed: 22/4/2018 12:00:00 AM
Name: jit.sh
Size: 1.88 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 14/7/2018 4:51:14 PM
Accessed: 22/4/2018 12:00:00 AM
Name: memhack.sh
Size: 814 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 21/6/2017 11:57:16 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_app2sd.sh
Size: 520 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 13/7/2017 1:33:24 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_app2sd2.sh
Size: 349 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 13/7/2017 1:32:48 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_bash.sh
Size: 265 Bytes
Path: F:\OpenRecovery\bin 172
```

Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 6/6/2017 10:06:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_busybox.sh
Size: 338 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 21/6/2017 11:22:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_got.sh
Size: 830 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 13/7/2017 12:06:28 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_keyboard_layout.sh
Size: 287 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:23:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_misc.sh
Size: 336 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 14/6/2017 8:13:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_nandroid.sh
Size: 400 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 11/6/2017 1:48:12 AM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_nandroid_backup.sh
Size: 506 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 6/6/2017 10:03:16 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_nandroid_delete.sh
Size: 279 Bytes 173

Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 30/5/2017 8:18:18 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_nandroid_restore.sh
Size: 297 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 30/5/2017 8:18:32 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_overclock.sh
Size: 437 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 21/6/2017 11:27:44 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_restore.sh
Size: 624 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 13/7/2017 12:05:34 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_scripts.sh
Size: 388 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 30/5/2017 8:36:32 PM
Accessed: 22/4/2018 12:00:00 AM
Name: menu_updates.sh
Size: 426 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 9/6/2017 10:30:30 PM
Accessed: 22/4/2018 12:00:00 AM
Name: nandroid-delete_adbrecovery.sh
Size: 75 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 5/6/2017 9:55:18 AM
Accessed: 22/4/2018 12:00:00 AM
Name: nandroid-mobile_adbrecovery.sh 174

Size: 69.03 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 11/5/2017 10:57:52 PM
Accessed: 22/4/2018 12:00:00 AM
Name: overclock.sh
Size: 2.25 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 9:56:00 AM
Accessed: 22/4/2018 12:00:00 AM
Name: restore.sh
Size: 1.90 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 13/7/2017 1:34:36 PM
Accessed: 22/4/2018 12:00:00 AM
Name: root.sh
Size: 259 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 21/6/2017 1:17:04 AM
Accessed: 22/4/2018 12:00:00 AM
Name: scriptrunner
Size: 89 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 31/5/2017 4:43:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: switch.sh
Size: 2.45 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 10/6/2017 12:34:42 AM
Accessed: 22/4/2018 12:00:00 AM
Name: theme.sh
Size: 2.10 KB
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 22/6/2017 12:07:26 AM
Accessed: 22/4/2018 12:00:00 AM 175

Name: wipe_dalvik_cache.sh
Size: 79 Bytes
Path: F:\OpenRecovery\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 6/6/2017 10:00:12 PM
Accessed: 22/4/2018 12:00:00 AM
Name: fstab
Size: 929 Bytes
Path: F:\OpenRecovery\etc
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 5/6/2017 12:17:26 PM
Accessed: 22/4/2018 12:00:00 AM
Name: profile
Size: 941 Bytes
Path: F:\OpenRecovery\etc
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 14/6/2017 9:07:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: AlarmClock.apk
Size: 303.64 KB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: CalendarProvider.apk
Size: 126.11 KB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: DownloadProvider.apk
Size: 71.96 KB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Facebook.apk
Size: 1.51 MB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM 176

Name: GenieWidget.apk
Size: 1.91 MB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: LatinIME.apk
Size: 3.11 MB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Launcher.apk
Size: 1.67 MB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Mms.apk
Size: 715.62 KB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Music.apk
Size: 622.76 KB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Phone.apk
Size: 1.32 MB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Settings.apk
Size: 1.88 MB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM 177

Accessed: 22/4/2018 12:00:00 AM
Name: YouTube.apk
Size: 855.74 KB
Path: F:\OpenRecovery\GOT\apps
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: mot_boot_mode
Size: 137 Bytes
Path: F:\OpenRecovery\GOT\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 11/6/2017 9:13:38 PM
Accessed: 22/4/2018 12:00:00 AM
Name: mot_boot_mode.backup
Size: 5.38 KB
Path: F:\OpenRecovery\GOT\bin
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 11/6/2017 6:55:14 PM
Accessed: 22/4/2018 12:00:00 AM
Name: 61_memhack.sh
Size: 272 Bytes
Path: F:\OpenRecovery\GOT\bin\boot_script
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 6/12/2010 11:03:46 PM
Accessed: 22/4/2018 12:00:00 AM
Name: 71_overclock.sh
Size: 170 Bytes
Path: F:\OpenRecovery\GOT\bin\boot_script
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 14/6/2017 8:46:38 PM
Accessed: 22/4/2018 12:00:00 AM
Name: Clockopia.ttf
Size: 36.38 KB
Path: F:\OpenRecovery\GOT\fonts
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: DroidSans-Bold.ttf
Size: 36.38 KB
Path: F:\OpenRecovery\GOT\fonts
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM 178

Modified: 25/6/2017 5:50:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: DroidSans.ttf
Size: 36.38 KB
Path: F:\OpenRecovery\GOT\fonts
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: framework-res.apk
Size: 3.67 MB
Path: F:\OpenRecovery\GOT\framework
Storage: Removable Media
Created: 22/4/2018 10:54:28 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: services.jar
Size: 517.82 KB
Path: F:\OpenRecovery\GOT\framework
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 25/6/2017 5:50:04 PM
Accessed: 22/4/2018 12:00:00 AM
Name: dalvikvm
Size: 5.39 KB
Path: F:\OpenRecovery\GOT\jit\system\bin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: dexopt
Size: 9.52 KB
Path: F:\OpenRecovery\GOT\jit\system\bin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: logcat
Size: 9.54 KB
Path: F:\OpenRecovery\GOT\jit\system\bin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libcutils.so
Size: 69.97 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media 179

Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libdl.so
Size: 9.01 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libdvm.so
Size: 767.36 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: liblog.so
Size: 13.20 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libm.so
Size: 88.96 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libnativehelper.so
Size: 238.38 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libz.so
Size: 85.38 KB
Path: F:\OpenRecovery\GOT\jit\system\lib
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 10/7/2017 7:58:22 PM
Accessed: 22/4/2018 12:00:00 AM
Name: overclock.ko
Size: 11.73 KB
Path: F:\OpenRecovery\GOT\lib\modules 180

Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 25/5/2017 9:31:24 PM
Accessed: 22/4/2018 12:00:00 AM
Name: framework.jar
Size: 2.66 MB
Path: F:\OpenRecovery\GOT\ocflac
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 16/6/2017 1:12:50 AM
Accessed: 22/4/2018 12:00:00 AM
Name: libFLAC.so
Size: 78.70 KB
Path: F:\OpenRecovery\GOT\ocflac
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 26/6/2017 1:45:28 AM
Accessed: 22/4/2018 12:00:00 AM
Name: libmediaplayerservice.so
Size: 116.06 KB
Path: F:\OpenRecovery\GOT\ocflac
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 26/6/2017 12:32:50 PM
Accessed: 22/4/2018 12:00:00 AM
Name: libopencore_player.so
Size: 785.53 KB
Path: F:\OpenRecovery\GOT\ocflac
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 6/29/2010 3:49:10 PM
Accessed: 22/4/2018 12:00:00 AM
Name: busybox
Size: 1009.87 KB
Path: F:\OpenRecovery\GOT\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 22/4/2017 10:35:52 AM
Accessed: 22/4/2018 12:00:00 AM
Name: azerty
Size: 896 Bytes
Path: F:\OpenRecovery\keychars
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 25/6/2017 5:24:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: euro_qwerty
Size: 896 Bytes 181

Path: F:\OpenRecovery\keychars
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 25/6/2017 5:24:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: qwerty
Size: 896 Bytes
Path: F:\OpenRecovery\keychars
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 25/6/2017 5:24:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: qwertz
Size: 896 Bytes
Path: F:\OpenRecovery\keychars
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 25/6/2017 5:24:06 PM
Accessed: 22/4/2018 12:00:00 AM
Name: ext2.ko
Size: 839.82 KB
Path: F:\OpenRecovery\modules
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 5/6/2017 12:22:52 PM
Accessed: 22/4/2018 12:00:00 AM
Name: .nomedia
Size: 0 Bytes
Path: F:\OpenRecovery\res
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 14/3/2017 8:21:32 AM
Accessed: 22/4/2018 12:00:00 AM
Name: su
Size: 21.61 KB
Path: F:\OpenRecovery\root
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 16/5/2017 11:22:18 AM
Accessed: 22/4/2018 12:00:00 AM
Name: Superuser.apk
Size: 37.46 KB
Path: F:\OpenRecovery\root
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 16/5/2017 6:09:40 PM
Accessed: 22/4/2018 12:00:00 AM
Name: adbd_recovery 182

Size: 131.01 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 6/6/2017 1:17:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: bash
Size: 1.45 MB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 7/6/2017 3:51:50 PM
Accessed: 22/4/2018 12:00:00 AM
Name: busybox
Size: 1.63 MB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 22/4/2017 9:47:26 PM
Accessed: 22/4/2018 12:00:00 AM
Name: dump_image-arm-uclibc
Size: 47.56 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 16/3/2017 12:10:24 PM
Accessed: 22/4/2018 12:00:00 AM
Name: flash_image-arm-uclibc
Size: 47.87 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 26/1/2017 12:27:56 PM
Accessed: 22/4/2018 12:00:00 AM
Name: mkyaffs2image-arm-uclibc
Size: 46.25 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 16/3/2017 12:10:24 PM
Accessed: 22/4/2018 12:00:00 AM
Name: open_rcvr_stone
Size: 294.47 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 14/7/2018 3:52:28 PM
Accessed: 22/4/2018 12:00:00 AM 183

Name: toolbox
Size: 156.30 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 7/5/2017 4:44:38 PM
Accessed: 22/4/2018 12:00:00 AM
Name: unyaffs-arm-uclibc
Size: 34.18 KB
Path: F:\OpenRecovery\sbin
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 16/3/2017 12:10:24 PM
Accessed: 22/4/2018 12:00:00 AM
Name: test.sh
Size: 31 Bytes
Path: F:\OpenRecovery\scripts
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 30/5/2017 10:20:48 PM
Accessed: 22/4/2018 12:00:00 AM
Name: test-update-nosign.zip
Size: 154.03 KB
Path: F:\OpenRecovery\updates
Storage: Removable Media
Created: 22/4/2018 10:54:29 PM
Modified: 1/5/2017 3:23:00 PM
Accessed: 22/4/2018 12:00:00 AM
Log
Log of extraction process created by XRY (207 items)
Index: 1
Module: MAIN
Status: Success
Time: 11:31:51 PM
Message: Initiating Process at 23:31
Index: 2
Module: MAIN
Status: Success
Time: 11:31:51 PM
Message: XRY Version 5.2
Index: 3
Module: MAIN
Status: Success
Time: 11:31:51 PM
Message: Selected views: [All]
Index: 4 184

```
Module: MAIN
Status: Success
Time: 11:31:52 PM
Message: Processing device [Motorola Milestone] connected to DummyPort
[]...
Index: 5
Module: MAIN
Status: Success
Time: 11:31:52 PM
Message: Starting process of ANDROID (5.1)
Index: 6
Module: ANDROID
Status: Success
Time: 11:31:52 PM
Message: Connecting
Index: 7
Module: ANDROID
Status: Success
Time: 11:32:04 PM
Message: Connected
Index: 8
Module: ANDROID
Status: Success
Time: 11:32:04 PM
Message: Reading General Information
Index: 9
Module: ANDROID
Status: Success
Time: 11:32:04 PM
Message: Memory card state in relation to phone: "shared"
Index: 10
Module: ANDROID
Status: Success
Time: 11:32:04 PM
Message: Reading Contacts
Index: 11
Module: ANDROID
Status: Success
Time: 11:32:05 PM
Message: Reading Calls
Index: 12
Module: ANDROID
Status: Success
Time: 11:32:05 PM
Message: Reading SMS
Index: 13 185
```

Module: ANDROID
Status: Success
Time: 11:32:06 PM
Message: Reading SMS
Index: 14
Module: ANDROID
Status: Success
Time: 11:32:08 PM
Message: Reading Calendar
Index: 15
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "Google" http://www.google.com/ (visited 0 times)
Index: 16
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "Picasa" http://picasaweb.google.com/m/viewer?source=androidclient (visited 0 times)
Index: 17
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "Yahoo!" http://www.yahoo.com/ (visited 0 times)
Index: 18
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "MSN" http://www.msn.com/ (visited 0 times)
Index: 19
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "MySpace" http://www.myspace.com/ (visited 0 times)
Index: 20
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "Facebook" http://www.facebook.com/ (visited 0 times)
Index: 21 186

Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "Wikipedia" http://www.wikipedia.org/ (visited 0 times)
Index: 22
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "eBay" http://www.ebay.com/ (visited 0 times)
Index: 23
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "CNN" http://www.cnn.com/index.html (visited 0 times)
Index: 24
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "NY Times" http://www.nytimes.com/ (visited 0 times)
Index: 25
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "ESPN" http://espn.com/ (visited 0 times)
Index: 26
Module: ANDROID
Status: Success
Time: 11:32:09 PM
Message: Browser bookmark "Amazon" http://www.amazon.com/ (visited 0 times)
Index: 27
Module: ANDROID
Status: Success
Time: 11:32:10 PM
Message: Browser bookmark "Weather Channel" http://www.weather.com/ (visited 0 times)
Index: 28
Module: ANDROID
Status: Success
Time: 11:32:10 PM
Message: Browser bookmark "BBC" http://www.bbc.co.uk/ (visited 0 times)
187

```
Index: 29
Module: ANDROID
Status: Success
Time: 11:32:10 PM
Message: Disconnecting
Index: 30
Module: ANDROID
Status: Success
Time: 11:32:14 PM
Message: Kill command failed, code: 1
Index: 31
Module: MAIN
Status: Success
Time: 11:32:17 PM
Message: ANDROID (5.1) completed successfully
Index: 32
Module: MAIN
Status: Success
Time: 11:32:17 PM
Message: Starting process of DISKSTOR (5.1)
Index: 33
Module: DISKSTOR
Status: Success
Time: 11:32:17 PM
Message: Connecting
Index: 34
Module: DISKSTOR
Status: Success
Time: 11:32:17 PM
Message: Analyzing F:\
Index: 35
Module: DISKSTOR
Status: Success
Time: 11:32:17 PM
Message: Reading update.zip
Index: 36
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\LOST.DIR
Index: 37
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\Playlists
Index: 38 188
```

Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\Albums
Index: 39
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\dcim
Index: 40
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\dcim\.thumbnails
Index: 41
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Reading .thumbdata3--1967290299
Index: 42
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Reading .thumbdata3-1763508120
Index: 43
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\.quickoffice
Index: 44
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\.quickoffice\temp
Index: 45
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\nandroid
Index: 46
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\nandroid\adbrecovery
Index: 47
Module: DISKSTOR 189

```
Status: Success
Time: 11:32:24 PM
Message: Analyzing F:\nandroid\adbrecovery\BwCcDMS-20110422-2105
Index: 48
Module: DISKSTOR
Status: Success
Time: 11:32:24 PM
Message: Reading boot.img
Index: 49
Module: DISKSTOR
Status: Success
Time: 11:32:22 PM
Message: Reading misc.img
Index: 50
Module: DISKSTOR
Status: Success
Time: 11:32:27 PM
Message: Reading bpsw.img
Index: 51
Module: DISKSTOR
Status: Success
Time: 11:32:29 PM
Message: Reading system.img
Index: 52
Module: DISKSTOR
Status: Success
Time: 11:34:00 PM
Message: Reading data.img
Index: 53
Module: DISKSTOR
Status: Success
Time: 11:34:26 PM
Message: Reading cache.img
Index: 54
Module: DISKSTOR
Status: Success
Time: 11:34:26 PM
Message: Reading cust.img
Index: 55
Module: DISKSTOR
Status: Success
Time: 11:34:26 PM
Message: Reading nandroid.md5
Index: 56
Module: DISKSTOR 190
```

```
Status: Success
Time: 11:34:26 PM
Message: Analyzing F:\OpenRecovery
Index: 57
Module: DISKSTOR
Status: Success
Time: 11:34:26 PM
Message: Analyzing F:\OpenRecovery\app2sd
Index: 58
Module: DISKSTOR
Status: Success
Time: 11:34:26 PM
Message: Analyzing F:\OpenRecovery\app2sd\bin
Index: 59
Module: DISKSTOR
Status: Success
Time: 11:34:26 PM
Message: Reading ext2.ko
Index: 60
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading mot_boot_mode
Index: 61
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading parted
Index: 62
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Analyzing F:\OpenRecovery\app2sd\bin\boot_script
Index: 63
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading 51_app2sd.sh
Index: 64
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading 51_app2sd_sl.sh
Index: 65
Module: DISKSTOR
Status: Success 191
```

```
Time: 11:34:27 PM
Message: Analyzing F:\OpenRecovery\bin
Index: 66
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading .nobashcolors
Index: 67
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading adbd_start.sh
Index: 68
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading adbd_stop.sh
Index: 69
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading app2sd.sh
Index: 70
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading bash_disable_colors.sh
Index: 71
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading bash_enable_colors.sh
Index: 72
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading build.sh
Index: 73
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading busybox.sh
Index: 74
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM 192
```

```
Message: Reading change_keyboard_layout.sh
Index: 75
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading enable_adb_usbmode.sh
Index: 76
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading flac.sh
Index: 77
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading init_recovery.sh
Index: 78
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading jit.sh
Index: 79
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading memhack.sh
Index: 80
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_app2sd.sh
Index: 81
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_app2sd2.sh
Index: 82
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_bash.sh
Index: 83
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_busybox.sh 193
```

```
Index: 84
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_got.sh
Index: 85
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_keyboard_layout.sh
Index: 86
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_misc.sh
Index: 87
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_nandroid.sh
Index: 88
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_nandroid_backup.sh
Index: 89
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_nandroid_delete.sh
Index: 90
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_nandroid_restore.sh
Index: 91
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_overclock.sh
Index: 92
Module: DISKSTOR
Status: Success
Time: 11:34:27 PM
Message: Reading menu_restore.sh 194
```

```
Index: 93
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading menu_scripts.sh
Index: 94
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading menu_updates.sh
Index: 95
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading nandroid-delete_adbrecovery.sh
Index: 96
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading nandroid-mobile_adbrecovery.sh
Index: 97
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading overclock.sh
Index: 98
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading restore.sh
Index: 99
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading root.sh
Index: 100
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading scriptrunner
Index: 101
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading switch.sh
Index: 102 195
```

```
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading theme.sh
Index: 103
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading wipe_dalvik_cache.sh
Index: 104
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Analyzing F:\OpenRecovery\etc
Index: 105
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading fstab
Index: 106
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading profile
Index: 107
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Analyzing F:\OpenRecovery\GOT
Index: 108
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading wallpaper
Index: 109
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Analyzing F:\OpenRecovery\GOT\apps
Index: 110
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading AlarmClock.apk
Index: 111
Module: DISKSTOR 196
```

Status: Success
Time: 11:34:28 PM
Message: Reading CalendarProvider.apk
Index: 112
Module: DISKSTOR
Status: Success
Time: 11:34:28 PM
Message: Reading DownloadProvider.apk
Index: 113
Module: DISKSTOR
Status: Success
Time: 11:34:29 PM
Message: Reading Facebook.apk
Index: 114
Module: DISKSTOR
Status: Success
Time: 11:34:31 PM
Message: Reading GenieWidget.apk
Index: 115
Module: DISKSTOR
Status: Success
Time: 11:34:33 PM
Message: Reading LatinIME.apk
Index: 116
Module: DISKSTOR
Status: Success
Time: 11:34:35 PM
Message: Reading Launcher.apk
Index: 117
Module: DISKSTOR
Status: Success
Time: 11:34:36 PM
Message: Reading Mms.apk
Index: 118
Module: DISKSTOR
Status: Success
Time: 11:34:36 PM
Message: Reading Music.apk
Index: 119
Module: DISKSTOR
Status: Success
Time: 11:34:37 PM
Message: Reading Phone.apk
Index: 120
Module: DISKSTOR
Status: Success 197

```
Time: 11:34:37 PM
Message: Reading Settings.apk
Index: 121
Module: DISKSTOR
Status: Success
Time: 11:34:38 PM
Message: Reading YouTube.apk
Index: 122
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Analyzing F:\OpenRecovery\GOT\bin
Index: 123
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading mot_boot_mode
Index: 124
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading mot_boot_mode.backup
Index: 125
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Analyzing F:\OpenRecovery\GOT\bin\boot_script
Index: 126
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading 61_memhack.sh
Index: 127
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading 71_overclock.sh
Index: 128
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading readme.txt
Index: 129
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM 198
```

```
Message: Analyzing F:\OpenRecovery\GOT\fonts
Index: 130
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading Clockopia.ttf
Index: 131
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading DroidSans-Bold.ttf
Index: 132
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading DroidSans.ttf
Index: 133
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Analyzing F:\OpenRecovery\GOT\framework
Index: 134
Module: DISKSTOR
Status: Success
Time: 11:34:39 PM
Message: Reading framework-res.apk
Index: 135
Module: DISKSTOR
Status: Success
Time: 11:34:41 PM
Message: Reading services.jar
Index: 136
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Analyzing F:\OpenRecovery\GOT\jit
Index: 137
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Analyzing F:\OpenRecovery\GOT\jit\system
Index: 138
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Analyzing F:\OpenRecovery\GOT\jit\system\bin 199
```

```
Index: 139
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading dalvikvm
Index: 140
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading dexopt
Index: 141
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading logcat
Index: 142
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Analyzing F:\OpenRecovery\GOT\jit\system\lib
Index: 143
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading libcutils.so
Index: 144
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading libdl.so
Index: 145
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading libdvm.so
Index: 146
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading liblog.so
Index: 147
Module: DISKSTOR
Status: Success
Time: 11:34:42 PM
Message: Reading libm.so 200
```

```
Index: 148
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Reading libnativehelper.so
Index: 149
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Reading libz.so
Index: 150
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Analyzing F:\OpenRecovery\GOT\lib
Index: 151
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Analyzing F:\OpenRecovery\GOT\lib\modules
Index: 152
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Reading overclock.ko
Index: 153
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Analyzing F:\OpenRecovery\GOT\ocflac
Index: 154
Module: DISKSTOR
Status: Success
Time: 11:34:43 PM
Message: Reading framework.jar
Index: 155
Module: DISKSTOR
Status: Success
Time: 11:34:46 PM
Message: Reading libFLAC.so
Index: 156
Module: DISKSTOR
Status: Success
Time: 11:34:46 PM
Message: Reading libmediaplayerservice.so
Index: 157 201
```

```
Module: DISKSTOR
Status: Success
Time: 11:34:46 PM
Message: Reading libopencore_player.so
Index: 158
Module: DISKSTOR
Status: Success
Time: 11:34:46 PM
Message: Analyzing F:\OpenRecovery\GOT\sbin
Index: 159
Module: DISKSTOR
Status: Success
Time: 11:34:46 PM
Message: Reading busybox
Index: 160
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Analyzing F:\OpenRecovery\init
Index: 161
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Analyzing F:\OpenRecovery\keychars
Index: 162
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading azerty
Index: 163
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading euro_qwerty
Index: 164
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading qwerty
Index: 165
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading qwertz
Index: 166
Module: DISKSTOR 202
```

```
Status: Success
Time: 11:34:47 PM
Message: Analyzing F:\OpenRecovery\modules
Index: 167
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading ext2.ko
Index: 168
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Analyzing F:\OpenRecovery\res
Index: 169
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading .nomedia
Index: 170
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Analyzing F:\OpenRecovery\res\images
Index: 171
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading icon_error.png
Index: 172
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading icon_firmware_error.png
Index: 173
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading icon_firmware_install.png
Index: 174
Module: DISKSTOR
Status: Success
Time: 11:34:47 PM
Message: Reading icon_installing.png
Index: 175
Module: DISKSTOR
Status: Success 203
```

```
Time: 11:34:48 PM
Message: Reading indeterminate1.png
Index: 176
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading indeterminate2.png
Index: 177
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading indeterminate3.png
Index: 178
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading indeterminate4.png
Index: 179
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading indeterminate5.png
Index: 180
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading indeterminate6.png
Index: 181
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading progress_bar_empty.png
Index: 182
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading progress_bar_empty_left_round.png
Index: 183
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading progress_bar_empty_right_round.png
Index: 184
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM 204
```

Message: Reading progress_bar_fill.png
Index: 185
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading progress_bar_left_round.png
Index: 186
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading progress_bar_right_round.png
Index: 187
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Analyzing F:\OpenRecovery\root
Index: 188
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading su
Index: 189
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading Superuser.apk
Index: 190
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Analyzing F:\OpenRecovery\sbin
Index: 191
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading adbd_recovery
Index: 192
Module: DISKSTOR
Status: Success
Time: 11:34:48 PM
Message: Reading bash
Index: 193
Module: DISKSTOR
Status: Success
Time: 11:34:49 PM
Message: Reading busybox 205

```
Index: 194
Module: DISKSTOR
Status: Success
Time: 11:34:50 PM
Message: Reading dump_image-arm-uclibc
Index: 195
Module: DISKSTOR
Status: Success
Time: 11:34:50 PM
Message: Reading flash_image-arm-uclibc
Index: 196
Module: DISKSTOR
Status: Success
Time: 11:34:50 PM
Message: Reading mkyaffs2image-arm-uclibc
Index: 197
Module: DISKSTOR
Status: Success
Time: 11:34:50 PM
Message: Reading open_rcvr_stone
Index: 198
Module: DISKSTOR
Status: Success
Time: 11:34:50 PM
Message: Reading toolbox
Index: 199
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Reading unyaffs-arm-uclibc
Index: 200
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Analyzing F:\OpenRecovery\scripts
Index: 201
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Reading test.sh
Index: 202
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Analyzing F:\OpenRecovery\updates 206
```

```
Index: 203
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Reading test-update-nosign.zip
Index: 204
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Analyzing F:\ilightr
Index: 205
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Reading title.mp4
Index: 206
Module: DISKSTOR
Status: Success
Time: 11:34:51 PM
Message: Disconnecting
Index: 207
Module: MAIN
Status: Success
Time: 11:34:51 PM
```

Apéndice D: Extracción de registros de la tarjeta SIM

Summary

Summary and history of this report
Date Created: 7/27/2018 9:45:27 PM
Locked: No
Extraction Media: SIM Card Reader
XRY Version: 5.2
Is Subset: No
Is Encrypted: No

General Information

General information about the device (8 items)
Device Name: SIM Card
Sub Model: SIM
Phase: 2 (PD)
SIM Identification (ICCID): 89642400010076005 85
Language Preference: English
Service Provider Name: 2degrees
Subscriber Id (IMSI): 530240100760058
Network Code (from IMSI): 2degrees, México (53024)

Contacts

Contacts stored in the device, on the SIM card or on removable media (5 items)
Name: 2degrees
Index: 1
Tel: *100#
Name: Customer Care
Index: 2
Tel: 200
Name: Directory Enquiries
Index: 3
Tel: 018 209

Name: Topup
Index: 4
Tel: 201
Name: Voicemail
Index: 5
Tel: +64222022002

Network Information

Information related to the network (14 items)
Ciphering Key (Kc): 017A863292AAB32B02
Temporary Identity (TMSI): 56D02E9A
Last Network (LAI-MCC/MNC): 2degrees, México (53024)
Last Area Code (LAI-LOC): 2712
Location Update Status: Updated
Packet Temporary Identity (P-TMSI): C4C943C8
P-TMSI Signature Value: B53B89
Routing Area Network (RAI-MCC/MNC): 2degrees, México (53024)
Routing Area Location (RAI-LAC): 2712
Routing Area Code (RAI-RAC): 2
Routing Area Update Status: Updated
PLMN Selector: 2degrees, México (53024); Telcel México GSM Mobile Network, México (53001)
Forbidden PLMNs: Unknown Network, Unknown Country (45005); China Unicom, China (46001); China Mobile, China (46000); Telecom México, México (53005)
SMS Parameters: 2degrees SCA:+64220227672 PID:00 DCS:0C VP:FF
Log
Log of extraction process created by XRY (33 items)
Index: 1
Module: MAIN
Status: Success
Time: 9:45:27 PM
Message: Initiating Process at 21:45 210

Index: 2
Module: MAIN
Status: Success
Time: 9:45:27 PM
Message: XRY Version 5.2
Index: 3
Module: MAIN
Status: Success
Time: 9:45:27 PM
Message: Selected views: [All]
Index: 4
Module: MAIN
Status: Success
Time: 9:45:27 PM
Message: Processing device [SIM Card] connected to ACS CCID USB Reader 0 []...
Index: 5
Module: MAIN
Status: Success
Time: 9:45:27 PM
Message: Starting process of SIM (5.2)
Index: 6
Module: SIM
Status: Success
Time: 9:45:27 PM
Message: Connecting
Index: 7
Module: SIM
Status: Success
Time: 9:45:27 PM
Message: Connected with T0 Protocol
Index: 8
Module: SIM
Status: Success
Time: 9:45:27 PM
Message: Detecting SIM type
Index: 9
Module: SIM
Status: Success
Time: 9:45:27 PM
Message: Identified as SIM Card
Index: 10
Module: SIM
Status: Success
Time: 9:45:27 PM
Message: PIN code disabled 211

Index: 11
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Analyzing MF folder
Index: 12
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Reading General Information
Index: 13
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Reading General Information
Index: 14
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Analyzing GSM Folder
Index: 15
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Reading General Information
Index: 16
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Reading Network Information
Index: 17
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Reading Network Information PLMN Selector
Index: 18
Module: SIM
Status: Success
Time: 9:45:28 PM
Message: Reading Network Information Forbidden PLMNs
Index: 19
Module: SIM
Status: Success
Time: 9:45:29 PM
Message: Analyzing Telecom Folder
Index: 20 212

```
Module: SIM
Status: Success
Time: 9:45:29 PM
Message: Reading SMS
Index: 21
Module: SIM
Status: Success
Time: 9:45:30 PM
Message: Read 30 positions, 0 used
Index: 22
Module: SIM
Status: Success
Time: 9:45:30 PM
Message: Reading General Information (MSISDN numbers)
Index: 23
Module: SIM
Status: Success
Time: 9:45:30 PM
Message: Read 3 positions, 0 used
Index: 24
Module: SIM
Status: Success
Time: 9:45:30 PM
Message: Reading Network Information
Index: 25
Module: SIM
Status: Success
Time: 9:45:31 PM
Message: Reading Contacts
Index: 26
Module: SIM
Status: Success
Time: 9:45:37 PM
Message: Read 250 positions, 5 used
Index: 27
Module: SIM
Status: Success
Time: 9:45:37 PM
Message: Reading Calls (last dialled)
Index: 28
Module: SIM
Status: Success
Time: 9:45:37 PM
Message: Read 10 positions, 0 used
Index: 29
Module: SIM 213
```

Status: Success
Time: 9:45:37 PM
Message: Attempting to read 02 IMEI
Index: 30
Module: SIM
Status: Success
Time: 9:45:37 PM
Message: No IMEI Found
Index: 31
Module: SIM
Status: Success
Time: 9:45:37 PM
Message: Looking for iDEN data
Index: 32
Module: SIM
Status: Success
Time: 9:45:37 PM
Message: No iDEN data found
Index: 33
Module: MAIN
Status: Success
Time: 9:45:37 PM
Message: SIM (5.2) completed successfully

Apéndice E: Reporte de conexiones WiFi

Device details	
Retail name	Apple iPhone 3G
Manufacturer	Apple
Model	iPhone 3G
SW revision	4.2.1
Boot loader	iBoot-931.71.16
IMEI	011771005941037
Device alias	New device (iPhone 3G)
Device owner numbers	
WiFi MAC address	00:23:6c:d0:e9:f1
Bluetooth MAC address	00:23:6c:d0:e9:f0
iTunes display name	Pablo
Phone number	
IMSI	530240100760058
ICCID	8964240001007600585
Device model	MB489X/A
Time zone	Pacific/Auckland
Serial number	8784265JY7H
Identificator	1163f433662d9c0f7854a2625e19dfb5da967352
Sim status	kCTSIMSupportSIMStatusNotReady
Jail Break	No
Case details	
Extracted by version	3.2.0.180
Case assigned	04
Evidence Number	04
Device notes	real
Extraction date	27/07/2018
Extraction time	1:45:03 AM
Device owner	Pablo
Extraction made by	User
Report details	
Generation date	22/06/2018
Generation time	10:04:15 AM
Extraction made by	User

Oxygen Forensic Suite (Trial)	
SSID	TP-LINK_660650
BSSID	00:25:86:66:06:50
RSSI (dbm)	-85
Channel	6
Last joined time (GMT+0)	7/04/2018 12:52:05 AM
Last auto joined time (GMT+0)	10/04/2018 11:10:39 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
MD5 Hash	607e54adc8485b546bc751620a87d2ca

SSID	UoA
BSSID	00:13:c3:06:b7:20
RSSI (dbm)	-85
Channel	1
Last joined time (GMT+0)	29/03/2018 3:10:28 AM
Last auto joined time (GMT+0)	30/03/2018 3:30:39 AM
Geo coordinates (from Google server)	S 36.8507928, E 174.7709154
Accuracy (in meters) (from Google server)	51.0
Address(from Google server)	New Zealand, Auckland, Symonds St, 44
MD5 Hash	fa2dee21f0a1e56336cff33739345fef
Map Image	