



Análisis Forense de dispositivos móviles iOS y Android.

Nombre Estudiante: Marco Antonio Alvarez Murillo

MEMORIA FINAL

Nombre Consultor: Cristina Pérez Solà.

Fecha de Entrega: 04/01/2016



Aquesta obra està subjecta a una llicència de [Reconeixement-NoComercial-CompartirIgual 3.0 Espanya de Creative Commons](https://creativecommons.org/licenses/by-nc-sa/3.0/es/)

Dedicatoria.

A mi hija Dayanna lo más grande de mi vida, a Soraya por su paciencia, a mi madre María Elena por sus consejos, a mi padre René Wilfrido por su enseñanza, “el estudio es mi mejor herencia”, a mis hermanos Patricia, Mauricio y Javier porque siempre están a mi lado,

A Francisco, José, Kelvin, Michael, Xavier por su amistad y su apoyo incondicional.

RESUMEN.

El objetivo principal del Trabajo de Fin de Grado es dar un enfoque en la aplicación de métodos y procesos para el Análisis Forense Digital en dispositivos móviles que utilizan los sistemas operativos que se ejecutan bajo las plataformas *iOS* y *Android* .

El protocolo que se utiliza para esta investigación se basa en los estándares y normas: ISO / IEC 27037, RFC 3227, UNE 71505 y UNE 71506. La metodología está estructurada en cinco fases: asegurar, identificar, preservar, analizar e informar sobre las evidencias de tal manera que puedan ser aceptadas y formar parte de un proceso legal.

A la vez, este documento proporciona técnicas científicas antes los desafíos que analistas forenses pueden enfrentarse como: obtener privilegios de administrador, acceso completo a los dispositivos de almacenamiento, configuración del sistema, desactivar métodos de seguridad que implementa el dispositivo.

Por último, en las distintas fases de este proyecto final de carrera existen *Pruebas de Concepto* para demostrar su viabilidad, para lo cual, se utilizan herramientas de open source como de tipo comercial.

(ABSTRACT).

The main objective of this research is to apply methods and processes for the Digital Forensic Analysis in mobile devices utilizing operative systems running under IOs and Android platforms. The main objective of this research is to apply methods and processes for the Digital Forensic Analysis in mobile devices utilizing operative systems running under IOs and Android platforms.

The protocol utilized for this investigation is based on the following standards: ISO/IEC 27037, RFC 3227, UNE 71505 and UNE 71506. The methodology used is structured in five phases as follows: Assure, Identify, Preserve, Analyze and Report evidences that could form part of a legal process.

This document also provides techniques in regards to challenges that Forensic Analysts could face like obtaining administrator privileges in order to have complete access to storage devices, system configuration, disabling the security on the device.

In addition this study explains the used of hash functions that can be used to verify the data integrity with the purpose of protecting the evidence and ensuring the correct storage or transmission of the data.

Lastly throughout the various phases of this final degree project there are *Proofs of Concept* which is a realization of a certain method or idea to demonstrate its feasibility, utilizing software forensic tools of open source code as well as commercial software licenses.

Índice de contenido

Capítulo 1: Plan de Trabajo.....	8
1.1 Propósito y justificación.....	8
1.2 Objetivos.....	8
1.2.1 Objetivos generales.....	8
1.2.2 Objetivos específicos.....	9
1.3 Metodología.....	9
1.4 Resultados esperados.....	10
1.5 Estructura del trabajo.....	11
1.5.1 Planificación Temporal.....	12
Capítulo 2: Metodología para el Análisis Forense.....	14
1. Ciencias Forenses.....	14
1.1 Definición.....	14
1.2 Principio de intercambio de Lorcad.	14
1.3 Definición de Informática Forense.....	14
1.4 Evidencia digital.....	15
2. Fases del Análisis Forense.....	15
2.1 Asegurar la escena.....	15
2.2 Identificar la evidencia.....	16
2.3 Adquisición de las evidencias.....	17
2.3.1 Agentes que determinan la adquisición de una investigación en sistemas móviles.....	17
2.3.1 Desbloqueo de dispositivos que utilizan passcode, PIN, PUK.....	20
2.4 Análisis e investigación de la evidencia.....	21
2.4.1 Herramientas de Análisis.....	22
2.4.2 Línea temporal.....	22
2.4.3 Análisis virtualizado.....	22
2.5 Informe Pericial.....	22
Capítulo 3: Hacking de dispositivos móviles iOS.....	23
3.1 Arquitectura iOS.....	23
3.2 Modelo de Seguridad de iOS.....	24
3.3 Atacando el passcode en iOS.....	24
3.3.1 Análisis del passcode en la grasa de la superficie.....	25
3.3.2 Ataque por Fuerza Bruta.....	25
3.4 Jailbreak.....	26
3.4.1 Tipos de Jailbreak.....	26
3.4.2 Herramientas para Jailbreak.....	26
3.5 Atacar la ID de Apple.....	30
3.5.1 Vulnerabilidad por mensajes en la pantalla.....	30
3.5.2 Vulnerabilidad por aplicaciones abiertas.....	31
Capítulo 4: Hacking de dispositivos móviles Android.....	33
4.1 Arquitectura de los Sistemas Android.....	33
4.2 Sistema de Archivos Android.....	34
4.3 Análisis de Vulnerabilidad para Root en Android.....	35
4.3.1 Drozer	35
4.3.2 Exploit de la vulnerabilidad CVE-2014-3153.....	37
4.3.3 Towelroot.....	37
4.2.4 KingRoot.....	37
4.2.5 SuperOneClic.....	38

4.2.6 Smart Phone Flash-Tool.....	38
4.2.7 Modificación del archivo default.prop.....	39
4.4 Ataque al passcode de Android.....	40
4.4.1 Desbloqueo del passcode por eliminación de archivos.....	40
Capítulo 5: Análisis Forense en dispositivos iOS.....	41
5.1 Adquisición de la evidencia.....	41
5.1.1 Copia bit a bit con la herramienta dd.....	41
5.1.2 Copia de Seguridad con iTunes.....	42
5.2 Iphone Analyzer	43
5.3 DS	45
Capítulo 6: Análisis Forense en dispositivos Android.....	47
6.1 Adquisición de la evidencia.....	48
6.1.1 Copia bit a bit.....	47
6.2 AFLogical OSE.....	47
6.3 Autopsy.....	49
6.4 Andriller.....	52
6.5 Análisis Forense de Base de Datos SQLite.....	53
6.5.1 Sqliteman.....	53
6.5.2 DB Browser SQLite.....	54
6.6 Análisis de Metadatos.....	55
6.6.1 FOCA.....	55
Capítulo 7: Informe Pericial.....	56
Conclusiones.....	57
Trabajo futuro.....	58
Bibliografía.....	59
Anexos.....	61
1: Instalación de Drozer.....	61
2: Compilación de los exploit zergRush y Psneuter.....	62
3: Informe Pericial.....	64
Informe Pericial dispositivos iOS.....	66
Informe Pericial dispositivos Android.....	73

Capítulo 1: Plan de Trabajo

1.1 Propósito y justificación.

El Internet es un gran sistema creado por los seres humanos, implica la conexión de millones de dispositivos que conforman redes descentralizadas para formar una gran red global. Los gobiernos en conjunto con millones de usuarios y empresas utilizan esta tecnología para el desarrollo de funciones que se desarrollan a diario.

La seguridad en Internet se convierte en una misión crítica que causa estragos en la vida cotidiana. Cada día existen miles de ataques que se materializan principalmente por estados, naciones, gobiernos, *hacktivistas* y *ciberdelincuentes*. Sin embargo, es común escuchar en los noticieros a cerca de nuevos sucesos delictivos (*violaciones, robos, pornografía infantil, asesinatos, etc.*), la investigación digital pasa a formar parte en la aportación de pruebas testificales para esclarecer dichas infracciones.

El Análisis Forense es un proceso íntegro que estudia el historial de un sistema. Está a disposición de los analistas utilizar buenas prácticas, métodos y herramientas que permita el análisis de evidencias para obtener informes detallados, los mismos que serán puestos a disposición judicial en la lucha contra el uso de la tecnología con fines delictivos.

En la actualidad existen millones de dispositivos móviles vendidos, los Sistemas Operativos más utilizados son *Android* e *iOS*. En particular, el presente estudio pretende dar un enfoque de una metodología a seguir para realizar un Análisis Forense sobre estos dispositivos.

1.2 Objetivos.

El objetivo principal de este trabajo es estudiar las principales herramientas y métodos para el Análisis Forense en dos dispositivos: el primer dispositivo con el Sistema Operativo Android y el segundo con el Sistema Operativo iOS.

1.2.1 Objetivos generales.

- a) Comprender la definición del ámbito en que se desarrolla la Informática Forense.
- b) Utilizar las diferentes fases del Análisis Forense.
- c) Estudiar las metodologías a seguir en el proceso de una investigación Forense aplicando métodos y herramientas acorde a lo establecido en las normas y leyes.
- d) Dar un enfoque a cerca de la estructura de los sistemas Android e iOS.

- e) Estudiar las herramientas de Análisis Forense Digital en más comunes en dispositivos móviles.
- f) Investigar el historial detallado de los elementos de evidencia digital que se encuentren en dispositivos móviles que utilizan los sistemas Android e iOS.
- g) Realizar el peritaje e informe pericial.

1.2.2 Objetivos específicos.

- a) Conocer ciertos métodos de utilidad para el hacking del *passcode* en iOS y Android.
- b) Investigar herramientas disponibles para Root en Android y Jailbreak en iOS.
- c) Métodos de custodia y capturar de los datos de un sistema iOS y Android.
- d) Investigar a cerca de diferentes herramientas que ofrece Santoku Linux de open source, sistema especializado para el análisis Forense en dispositivos móviles, y herramientas de Software Libre.
- e) Realizar investigaciones de Análisis Forense con herramientas comerciales .
- f) Obtener información de los dispositivos investigados.
- g) Análizar evidencias.
- h) Realizar el peritaje e informe periciales de dos dispositivos móviles, uno con el Sistema Operativo iOS y el otro con Android.
- i) Memoria final.

1.3 Metodología.

La metodología a seguir se basará en estándares, normas y regulación de acuerdo a leyes y recomendaciones existentes, se dará un enfoque de cómo realizar una investigación Forense en dispositivos móviles que servirá de guía para una investigación real. El trabajo se basa en el marco legal del estado español y la comunidad europea en conjunto con las normas:

- **ISO/IEC 27037: Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.** [1]

Documento que publicó la Organización Internacional para la Estandarización (ISO), proporciona directrices para actividades periciales en el escenario de la identificación, recolección, adquisición y preservación de la evidencia digital como medio probatorio. Utiliza procedimientos disciplinarios para facilitar en intercambio de la evidencia entre jurisdicciones y orienta a las personas en todo el proceso de manipulación de dicha evidencia.

➤ **RFC 3227: Guidelines for Evidence Collection and Archiving.** [2]

Proporciona a los administradores de sistemas directrices para la recopilación y archivo de las pruebas en un incidente de seguridad. Cuando la recopilación de pruebas se realiza de forma correcta, se evita graves errores y facilita la detección del atacante, lo que permite, aumentar en gran proporción la posibilidad de admitir el caso a un proceso judicial.

➤ **UNE 71505: Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.** [3]

Los logs de actividades proporcionan información sobre los sucesos en un sistema de información. La parte frágil de los logs es la demostración que los hechos no se han alterado en la cadena de custodia.

Define y describe conceptos de seguridad que se relacionan con la evidencia, identifica las relaciones entre el Sistema de Gestión de Evidencias Electrónicas (SGEE) y el Sistema de Gestión de Seguridad (SGSI), especifica controles de seguridad a la gestión de evidencias.

➤ **UNE 71506: Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.** [4]

Esta norma define los procesos para el análisis forense dentro del ciclo de gestión de evidencias electrónicas. Completa los procesos que conforma la Norma UNE 71505 a cerca del Sistema de Gestión de Evidencias Electrónicas.

Las buenas prácticas y el seguimiento de una metodología, facilita, garantiza y aporta seguridad en la investigación. Por ende, se evita cometer errores graves en un proceso judicial, además aporta a los *Jueces - Magistrados* la interpretación correcta de los resultados sin entrar en detalles tecnológicos y de difícil comprensión.

A más, se necesitan herramientas disponibles para el análisis. Este trabajo se utilizará: el sistema operativo Santoku Linux en conjunto con herramientas de *Open Source*; Andriller, DS7 de uso comercial, la mayoría destinadas al Análisis Forense en dispositivos móviles y generación de informes de alto nivel.

1.4 Resultados esperados

A la finalización de este trabajo se espera obtener una metodología para el análisis forense en dispositivos móviles. Los resultados esperados después de esta investigación son:

- A)** Informe pericial de dispositivo móvil con iOS.
- B)** Informe pericial de dispositivo móvil de Android.
- C)** Memoria final.

1.5 Estructura del trabajo

El presente trabajo se estructura en ocho capítulos:

I. Capítulo: Elaboración del plan de proyecto.

La Gestión de Proyectos implica la planificación de los procesos a seguir para finalizar con éxito los objetivos y el alcance dentro de un límite de tiempo establecido. Se presenta un diagrama de Gantt que sirve de guía para el control de y avance del trabajo en conjunto con la verificación de hitos.

II. Capítulo: Metodología para el Análisis Forense

Seguir una metodología es primordial para finalizar con éxito el Análisis Forense Digital de cualquier dispositivo. Se pretende dar un enfoque a cerca de la definición y fases de análisis de la informática forense en general.

III. Capítulo: Hacking de dispositivos móviles iOS.

El estudio de la arquitectura y estructura del sistema de archivos de un sistema *iOS* es fundamental antes de iniciar el análisis forense, a continuación se establecen herramientas con diferentes métodos de acceso de administrador del sistema.

IV. Capítulo: Hacking de dispositivos móviles Android.

De la misma forma que en el capítulo anterior se estudian los mismos principios para el sistemas *Android*.

V. Capítulo: Análisis Forense en dispositivos iOS.

Se establecen métodos adquisición y herramientas de análisis de tipo comercial y open source para sistemas *iOS*.

Capítulo: Análisis Forense en dispositivos Android.

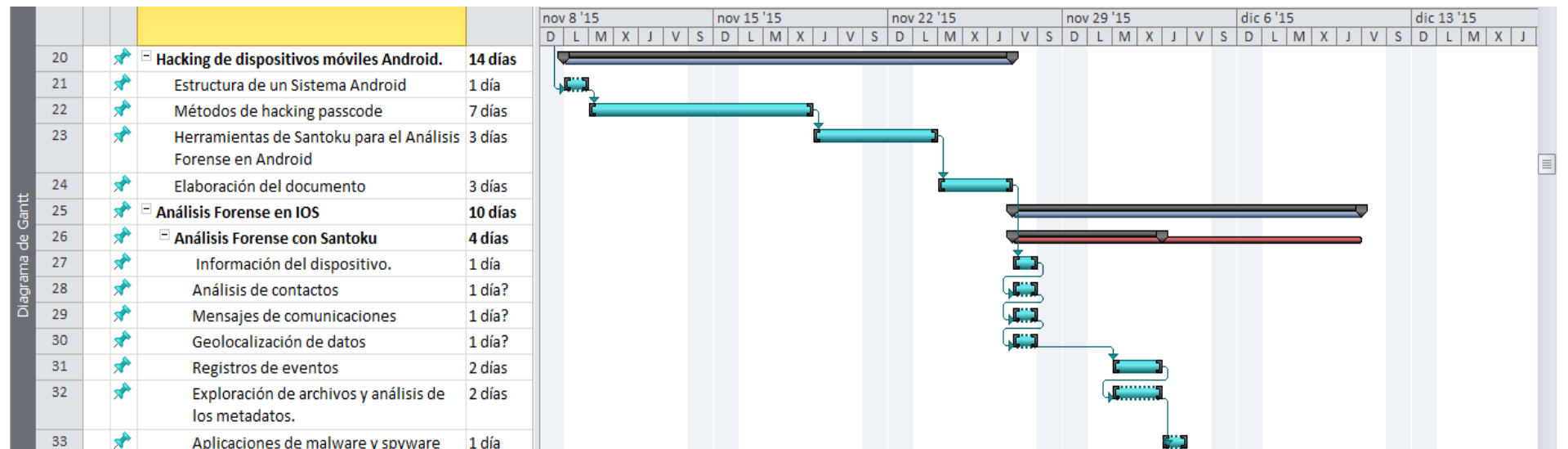
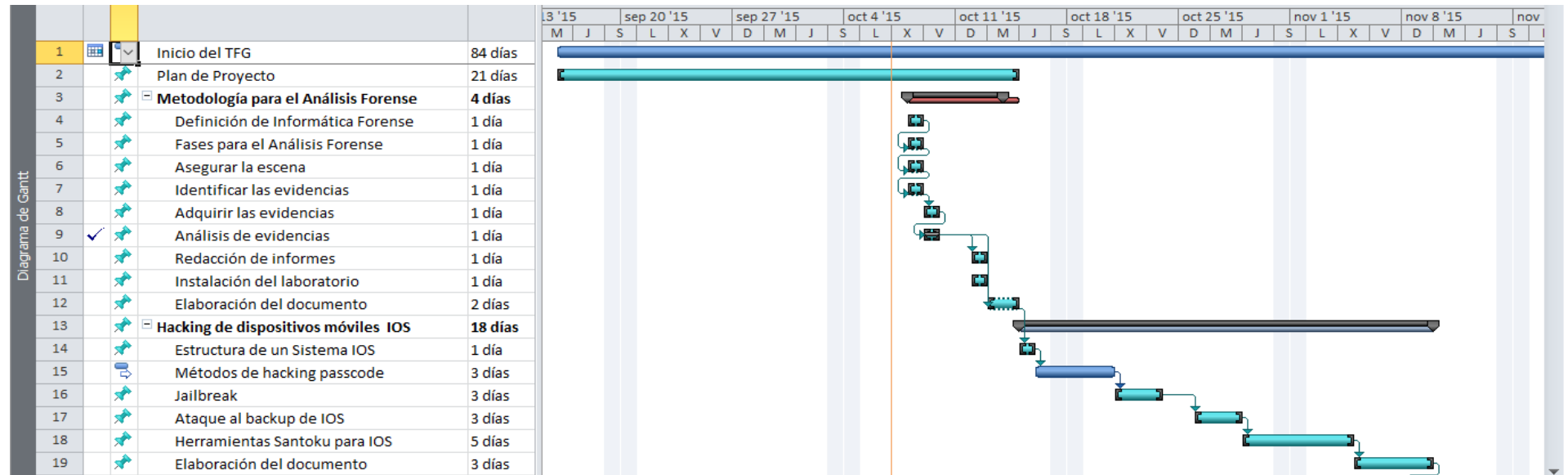
Se explica diferentes métodos para la fase de adquisición y análisis de sistemas *Android*, a la vez, herramientas de licencia comerciales y open source para el análisis forense.

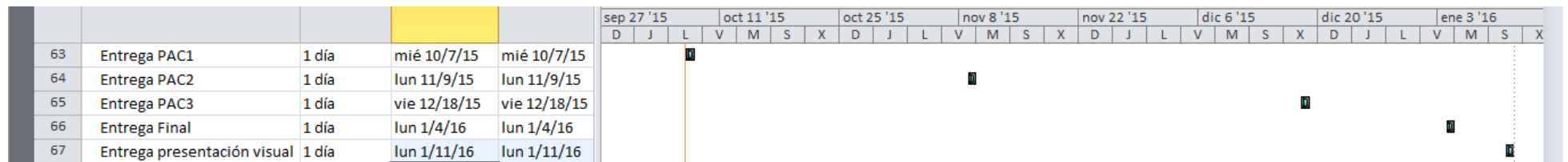
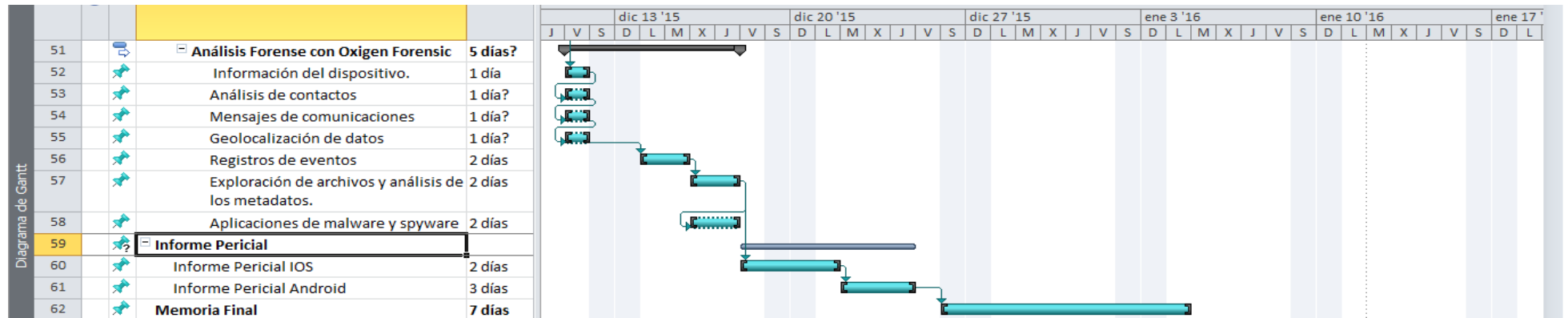
VI. Capítulo: Informe Pericial

Los informes periciales pueden ser de dos tipos: Informe Ejecutivo que permite llegar a personas con pocos conocimientos técnicos, y el Informe Técnico con todos los detalles de la investigación. En este trabajo se pretende realizar un informe que combina la parte ejecutiva y técnica como demostración pero con los principales incisos debido a la gran cantidad de información que almacena un dispositivo

- 1.** Informa pericial dispositivo iOS.
- 2.** Informe pericial dispositivo Android.
- 3.** Memoria Final.

1.5.1 Planificación Temporal.





Capítulo 2: Metodología para el Análisis Forense.

1. Ciencias Forenses.

1.1 Definición.

Las ciencias forenses se encargan de la aplicación de prácticas científicas dentro de un proceso legal. Investigadores especializados en distintas ramas localizan evidencias que proporciona pruebas concluyentes al ser sometidas a estudios en laboratorios debido a que no pueden ser observadas a simple vista.

1.2 Principio de intercambio de Lorcad.

Fue desarrollado por el Dr. Edmond Locard, Locard formuló que: “cada contacto deja un rastro”, cualquier objeto o criminal que entra en la escena del crimen transfiere material que incorpora al otro objeto y viceversa. Dicho de otra manera, alguna acción de algún individuo *-violenta-* que constituye un delito no puede ocurrir sin dejar rastros.

Las ciencias forenses poseen herramientas, técnicas y métodos científicos que se utilizan para reconstruir los hechos que se investigan con el propósito de relacionar al criminal con la víctima en una escena.

1.3 Definición de Informática Forense.

Es una disciplina que combina elementos de derecho y ciencias de la computación para recopilar y analizar datos de: sistemas informáticos, redes, comunicaciones y dispositivos de almacenamiento. Dicha rama aplica métodos científicos, herramientas e infraestructura tecnológica para la investigación de sistemas digitales con la finalidad de: **asegurar, identificar, preservar, analizar y presentar** la evidencia de manera que sea admisible como prueba en un tribunal de justicia. Este proceso normalmente se ejecuta de forma secuencial.

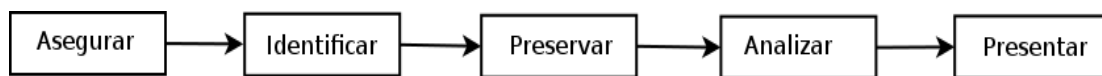


Figura 2.1: Fases de la Investigación Forense Digital.

Sin embargo, el resultado de un análisis digital en todos los casos no entra a formar parte de un proceso judicial. En numerosas ocasiones se desea investigar un sistema porque existe cierta sospecha o total seguridad *-alta probabilidad-* de haber sido víctima de un ataque o una intrusión no autorizada.

Por consiguiente, se puede definir a la Informática Forense como una ciencia que proporciona un metodología para la investigación detallada de los sucesos que ocurren en tiempo real o durante el historial de un sistema, esto conlleva, al análisis

de información detallada para esclarecer el daño causado a la víctima, así como la identidad del atacante y sus intenciones.

1.4 Evidencia digital.

En investigaciones científicas es un objeto digital que contiene información confiable como soporte para una hipótesis.

En el ámbito legal, la evidencia digital o electrónica es cualquier clase de información probatoria, dicha información está almacenada o se transmite de manera digital con la finalidad de utilizar una de las partes en un proceso judicial. Esto explica que el proceso a seguir se debe realizar con la suficiente atención en la recolección, procesamiento y almacenamiento de los objetos digitales. A menos que estén muy seguros que la evidencia no se utilizará en el juzgado, se procede a ejercer la debida precaución y cuidado de las pruebas. En muchas ocasiones una investigación que comienza como una recopilación y análisis puede convertirse en un análisis criminal.

2. Fases del Análisis Forense.

2.1 Asegurar la escena.

Esta fase se basa en la restricción del acceso para que ninguna persona u objeto pueda alterar la escena a investigar. Las personas que actúan en la investigación deben garantizar actuaciones seguras, dicho de otra manera, está prohibido utilizar procesos que no estén completamente seguros. Se puede citar una serie de normas dentro del protocolo a seguir:

- Identificar la escena y establecer un perímetro de seguridad.
- Restringir el acceso de personas y equipos informatizados en el perímetro trazado.
- Impedir el uso de dispositivos con tecnología inalámbrica.
- Preservar las huellas mediante la utilización de guantes látex.
- Valorar el análisis en red o la posibilidad de desconectar los dispositivos. La desconexión puede acarrear la pérdida de información a cerca de un delito que se pueda cometer en línea.
- Para los dispositivos de imprenta, si en el instante del análisis se encuentran con tareas de impresión, se proporciona el tiempo necesario hasta la finalización de los trabajos.
- Documentar por medio de fotografías o vídeos la fecha y hora del sistema antes de apagarlo, siempre que se encuentre esta información en la pantalla.
- Monitorizar los procesos en línea (por ejemplo, descarga de aplicaciones, archivos que se comparten, aplicaciones P2P etc.) y documentar por medio de fotografías o vídeos.
- Apagar los dispositivos encendidos se recomienda retirar la alimentación por la parte posterior del equipo.

2.2 Identificar la evidencia.

El proceso de identificación puede variar según el caso. El investigador debe confiscar una cantidad pequeña de material o al contrario, enfrentarse a la incautación de una gran cantidad de material. Sin embargo, se recomienda verificar la calidad y la validez de los materiales confiscados para validar como una prueba judicial.

- Como punto de partida, se concibe la evaluación de las evidencias volátiles y valorar la necesidad de grabarlas o no en un fichero. El investigador debe conocer que esta acción implica manipular el sistema, así pues, si se toma una decisión de esta índole debe documentarse especificando la razón o la necesidad, el analista debe conocer el riesgo que conlleva cualquier manipulación en el sistema, con la condición de que, puede convertirse en una prueba no válida en un proceso judicial.
- Realizar una lista, etiquetar el material incautado, documentar todo lo que se lleva al laboratorio y lo que no.
- Solicitar datos relevantes de las personas implicadas, como su documentación, contraseñas del sistema y usuarios o acciones que se producen durante el incidente.
- Realizar un esquema de la escena del suceso, con fotografías, vídeo, topologías de red etc.

En cuanto a los dispositivos móviles, si no se tratan adecuadamente la evidencia puede contaminarse y terminar como inválida.

- Las fuentes que incluyen en las pruebas son: los dispositivos, cables, adaptadores, medios extraíbles, UICC [5] (*Universal Integrated Circuit Card*), ordenadores personales. Los ordenadores personales pueden ser de mucha utilidad inclusive más que un dispositivo móvil, debido a que los usuarios realizan procesos de sincronización para descargar material en dispositivos de almacenamiento de mayor capacidad, o a su vez, para realizar una copia de seguridad del sistema en caso de avería. Un *backup* almacenado en un equipo puede ser de mucha utilidad si el proceso de desbloqueo de un terminal se vuelve imposible.
- Con los dispositivos incautados, no se debe permitir al propietario ni a cualquier persona no autorizada manipular el teléfono móvil, muchos dispositivos tienen códigos para borrar el contenido a las condiciones originales de fábrica. Además, se puede realizar un borrado de forma remota por lo que es imprescindible utilizar medidas de precaución como el aislamiento de la red para que no exista la posibilidad de destrucción de la evidencia por terceras personas ajenas a la investigación.
- Los analistas pueden enfrentarse a situaciones comprometidas como: material digital dentro de líquido, uso de explosivos, contaminación con sangre, etc., en estos casos se recomienda consultar a especialistas para obtener instrucciones específicas o de asistencia.

- Los dispositivos pueden encontrarse dañados o parcialmente destruidos por diferentes motivos pero que no impiden necesariamente la extracción de datos. El equipo roto se procede a transportarle al laboratorio para intentar reparar sus componentes o extraer la información en la medida posible.
- En la entrevista al propietario, es de cometido considerar la solicitud a cerca de tipos de seguridad digital que utilizan los dispositivos.
- Una vez incautados los dispositivos móviles, es necesario aislar ante cualquier tipo de comunicación. Se recomienda la utilización de Bolsas o Jaulas Faraday (*bolsas o cajas metálicas que tiene por objetivo aislar las señales inalámbricas desde las torres de móviles, redes inalámbricas, y otras fuentes de señal para proteger las pruebas durante la adquisición*).



Fuente: <https://www.paraben.com>

Figura 2.2: Fases de la Investigación Forense Digital.

2.3 Adquisición de las evidencias.

Los teléfonos tienen una gran capacidad de almacenamiento, en su interior puede existir material ilegal almacenado. Las evidencias digitales pueden modificarse o incluso eliminarse por lo que requiere un valioso cuidado para preservar la evidencia.

Cuando un usuario decide borrar un archivo, el Sistema Operativo no elimina por completo, la mayoría de ellos liberan los sectores que ocupa dicho archivo y lo marca como disponible, es decir, si no se sobrescriben los sectores la información seguirá almacenada. Por lo tanto, con la utilización herramientas forenses se puede recuperar dicha información.

Se presenta una serie de pautas para la adquisición de evidencias, borrado seguro de datos y copia bit a bit.

2.3.1 Agentes que determinan la adquisición de una investigación en sistemas móviles.

- **Características del dispositivo.**

La marca y el fabricante se puede identificar por las características visibles de un dispositivo, existen bases de datos que permiten consultar dichas características, además, se puede obtener información del detrás de la batería.

El IMEI es un número de 15 dígitos que indica el fabricante, modelo, país de aprobación. Los primeros 8 dígitos definen el Código de Tipo de Asignación (TAC), que contiene información a cerca del modelo y origen, los siguientes bits especifican el fabricante con un dígito de control al final. El ESN es un identificador de 23 bits grabado en chip, los primeros 8-14 bits identifican a los fabricantes y el resto el número de serie asignado.

- **El modo Depuración USB.**

(USB Debugging) está pensado principalmente para desarrolladores, permite abrir el acceso directo al sistema para el **SDK** de Android (*Software Development Kit*), indispensable para la conexión por cable entre los dispositivos móviles y el ordenador

Una dificultad en el proceso de investigación forense es la habilitación de USB. Si el sistema es Root, además se encuentra habilitada la depuración USB, se procede a conectar entre el ordenador y el dispositivo móvil por medio de ADB (Android Debug Bridge) para realiza la copia bit a bit.

- **¿El sistema es Root en Android o Jailbreak en iOS?.**

Una gran cantidad de usuarios tienen activado el Sistema Root en Android o Jailbreak en iOS, si es el caso, se puede establecer una conexión entre el ordenador y el dispositivo por medio de *USB* o por el protocolo *SSH*, a partir de dicha conexión, se realiza la adquisición física bit a bit del dispositivo. Si no es el caso, se procede a investigar con la finalidad de identificar bugs que permitan escalar privilegios en los dispositivos.

El siguiente desafío que un investigador se encuentra en el análisis es la extracción de datos para su posterior análisis. La extracción se puede clasificar en cinco niveles, de acuerdo al nivel que se elija se consume mayor o menor recursos. El nivel más técnico consume más recursos.

- **Extracción manual.**

Consiste en la visualización y grabación de la información de la pantalla del dispositivo, para lo cual se manipula: botones, teclado o pantalla táctil. Este método no permite acceder a los datos que han eliminado normalmente cruciales en la investigación. La información se recoge mediante fotografías de la pantalla LCD del móvil.

- **Extracción lógica.**

Se realiza mediante la conexión del dispositivo (*Cable USB, RS232, WIFI, IRDA Bluetooth.*); con la estación de trabajo. Es de obligación por parte del analista tener en cuenta los problemas asociados a este tipo de investigación, utilizar protocolos y métodos de conectividad pueden modificar los datos. La extracción se realiza mediante el uso de comandos, y la respuesta se envía a la estación de trabajo.

- **Extracción física.**

Consiste en adquirir una imagen del material incautado para el análisis, dicho método obtiene copias necesarias de la imagen original. Una vez se realiza la copia, se lleva a cabo la investigación forense sin necesidad de utilizar el dispositivo físico.

Realizar la copia de bits de los soportes originales es un proceso que se puede realizar por medio de software o hardware, se debe tener en cuenta :

Los dispositivos o unidades de almacenamiento en donde se va a realizar la copia deben estar borradas de manera segura. Existe una herramienta en Linux muy utilizada para borrado de seguro y copia bit a bit. El comando para realizar el borrado seguro es:

```
dd if=/dev/zero of=dispositivo a copiar bs=1M.
```

Las copias deben ser idénticas a la original. No debe alterarse bajo ningún motivo los datos de origen y destino.

La copia tiene que estar completa, se incluye el espacio libre sobre todo para la recuperación de la información valiosa que ha sido borrada.

```
dd if = dispositivo de origen of=dispositivo destino bs=1M
```

Aplicar la función hash sobre la información recopilada para mantener la integridad. Se puede utilizar *MD5* o *SHA-1*.

El análisis debe realizarse a partir de una segunda copia para evitar el daño del dispositivo original, con esto se logra, duplicar cuando las circunstancias lo requiera nueva copia de la primera.

Una vez extraída la imagen se debe entrega el original al juzgado, el afectado puede solicitar un contra-peritaje.

En el proceso de copia de la imagen no es necesaria la presencia del Secretario Judicial, no está obligado a conocer aspectos técnicos.

- **Hex Dumping y JTAG.**

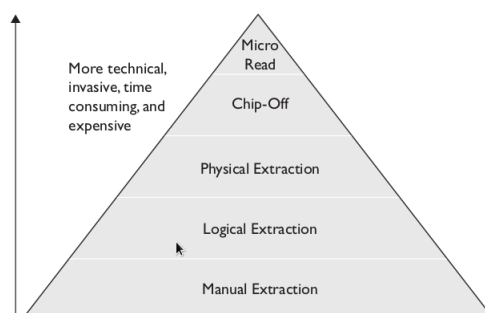
Permite el acceso directo a la información almacenada en un chip flash memory. El reto en esta investigación es utilizar la herramienta apropiada para analizar o decodificar los datos que se ha capturado, además, proporcionar una visión lógica del sistema de archivos y presentación de informes sobre estos datos. Este método requiere conectividad por cable o *WIFI* entre el dispositivo y la estación de trabajo.

- **Chip-Off**

Se extrae el *chip* de memoria del dispositivo, a continuación se crea una imagen binaria del contenido. Se necesitará software que comprende la composición física y lógica del dispositivo.

- **Micro Read**

- Captura los cambios en el gate [6] de un *chip*, utilizando un microscopio electrónico.



(Fuente: Ayers, R., Brothers, S., Jansen, W. Guidelines on Mobile Device Forensic, NIST Special Publication 800-101, Revision 1, (dx.doi.org/10.6028/NIST.SP.800-101r1), p. 17.) .

Figura 2.3 Adquisición de evidencias en dispositivos móviles.

2.3.1 Desbloqueo de dispositivos que utilizan passcode, PIN, PUK.

Durante el proceso de extracción de datos en ocasiones se encuentra la necesidad de: “desbloquear los métodos de seguridad que implantan los fabricantes y los Sistemas Operativos”. Los dispositivos investigados en algunas circunstancias no poseen ningún sistema de seguridad para acceso a los datos, principalmente por descuido o desconocimiento de los usuarios. No obstante, existen dispositivos que protegen los datos generalmente con el cifrado o necesitan de métodos de autenticación usando una contraseña, u otro medio de acceso.

En la actualidad, diferentes herramientas proporcionan funciones automatizadas que permiten omitir los mecanismos de seguridad como parte de sus productos, así como recuperar contraseñas del dispositivo bloqueado. Se pueden citar herramientas de uso comercial como: Oxigen Forensic Suite [7], DS7 [8], Encase [9]. Otro método es el uso de herramientas automatizadas de Open Source o directamente con el uso de *scripts* de acuerdo a las vulnerabilidades del sistema a investigar, la desventaja consiste en el análisis minucioso unido al método más apropiado de acuerdo al Sistema Operativo a investigar.

Los productos comerciales tienen un coste de licencia elevado, pero para empresas o miembros del estado que se dedican a realizar una gran cantidad de investigaciones forenses en dispositivos móviles es una buena alternativa si se realiza un análisis coste-beneficio.

En este trabajo, se presenta una serie de métodos para el desbloqueo de teléfonos que están protegidos con passcode, las técnicas que se utilizan dependen del: Sistema Operativo instalado, distintas versiones de los mismos, diferentes características entre una marca a otra.

- **Preguntar al propietario.**

Durante una entrevista al propietario del dispositivo, se pueden formular preguntas para obtener información a cerca del passcode, PIN, u otro sistema de autenticación.

- **Revisión de los materiales incautados.**

El propietario en ocasiones suele escribir passwords o PINs en un papel que se se mantiene: cerca del teléfono, en un ordenador para sincronizar el dispositivo o, en materiales de uso común - *ejemplo: la cartera del propietario* -. Si es así, se intentará recuperar de manera visual y usar la clave para desbloquear el teléfono.

- **Vulnerabilidades específicas.**

El método más común es utilizar vulnerabilidades de los sistemas, Smudge Attacks es un ejemplo que consiste en el análisis de la superficie de la pantalla táctil del dispositivo para determinar los dígitos o caracteres que el propietario utilizó [10]. Existen a disposición de los analistas bases de datos a cerca de las vulnerabilidades de los sistemas. [11]

- **Preguntar al proveedor de servicios**

La mayoría de proveedores ofrecen la capacidad de recuperar el PUK en línea, ingresando el número del teléfono y la información del abonado en páginas web públicas. Otro método similar es contactar con el fabricante del dispositivo, o mediante la emisión de una orden por vía judicial hacia los proveedores de servicios o fabricantes.

Sin embargo, los usuarios eligen contraseñas débiles para proteger sus dispositivos (1111, 0000, 1234), pero no se recomienda intentar desbloquear utilizando estos códigos por el riesgo que se puede ocasionar como puede ser el: borrado seguro del móvil, limpieza permanente de la memoria, etc. Los dispositivos por lo general tienen un número de intentos antes de bloquear el teléfono, el investigador puede aceptar este riesgo en los casos en que sea la única opción para la extracción de datos.

- **Métodos hardware y software.**

En los siguientes capítulos de Hacking del passcode en iOS y Android se describen algunos métodos software o hardware que se utilizan para obtener o desbloquear el passcode.

2.4 Análisis e investigación de la evidencia.

Fundamenta el estudio total del dispositivo, el analista debe conocer el funcionamiento de los sistemas operativos, análisis del historial, ficheros con sus metadatos y aplicaciones instaladas en los equipos a investigar.

- En los dispositivos móviles se encuentra información de importancia en el análisis de contactos, geolocalización, mensajes de comunicación como (*MMS, correo electrónico, Whatsapp, Tango, Skype, etc*), registro de eventos, calendario, historial del navegador, aplicaciones de redes sociales, los archivos logs de actividades.
- El investigador se enfrenta a diferentes inconvenientes en el análisis como ficheros cifrados, ficheros infectados con troyanos virus o malware, demasiada información, datos ocultos con estenografía, datos borrados.

- En ocasiones, se debe trabajar directamente sobre el dispositivos, para el efecto se utilizan herramientas hardware o software que permitan la recuperación del dispositivo sin alterar la evidencia. Esta forma de análisis se realiza cuando no se dispone de suficiente tiempo para el análisis en el laboratorio.

2.4.1 Herramientas de Análisis.

En la actualidad existen herramientas de *Open Source* como de uso comercial, permiten: adquirir, analizar y generar reportes de la investigación. Entre las herramientas más conocidas se puede citar: open source (Sistema Operativos Kali Linux, Santoku Linux que contiene herramientas para el análisis forense y auditoría digital) de uso comercial (Oxigen Forensic Kit, Andriller, DS7, Encase). En Computer Forensics Tool Catalog existe una lista detallada de herramientas disponibles para Análisis Forense en dispositivos móviles. [12].

2.4.2 Línea temporal.

Es la creación o estudio de un evento en un intervalo de tiempo específico con los detalles a cerca de los sucesos ocurridos. Ejemplos de líneas temporales: se solicita al Analista Forense verificar si se realizó una llamada, se ha conectado a una web, se hizo una copia de archivos una memoria externa etc., todo esto en un tiempo específico.

2.4.3 Análisis virtualizado.

Los analistas pueden contar tan solo con la imagen del dispositivo, existen archivos que tienen aplicaciones propias para la apertura, esto genera una gran dificultad al tener que instalar aplicaciones en un ordenador. Por este motivo se recomienda ejecutar la imagen en una máquina virtual para proceder al análisis. Si el sistema está infectado por software malicioso la *virtualización* ofrece la oportunidad de analizar su comportamiento. Este forma de análisis se le conoce como análisis en vivo.

2.5 Informe Pericial.

Se documenta y se presentan las evidencias relacionadas con el caso, justificación de los procesos investigados, la conclusión. El lenguaje utilizado debe ser formal pero no necesariamente técnico, el lector no tiene porqué conocer la parte técnica. Sin embargo el Analista Forense tiene que poseer habilidad para comunicar el resultado de la investigación de forma clara y concisa.

Capítulo 3: Hacking de dispositivos móviles iOS.

3.1 Arquitectura iOS.

La arquitectura de iOS se basa en capas, las capas de nivel superior interactúan como intermediarias entre el hardware y las aplicaciones que se desarrollan. Las aplicaciones no se comunican directamente con el hardware, se comunican a través de interfaces de sistemas, este mecanismo proporciona el desarrollo de aplicaciones que trabajan constantemente en dispositivos con diferentes capacidades de hardware.

Las capas de nivel superior se basan en las capas inferiores, proporcionan servicios y tecnologías más avanzadas para el desarrollo de aplicaciones, las capas inferiores poseen el control de los servicios básicos.

Cocoa Touch.

Es la capa principal, contiene un conjunto de *Frameworks* para el desarrollo de aplicaciones. Se recomienda usar *Frameworks* de alto nivel siempre que sea posible, porque proporcionan abstracciones orientadas a objetos para construcciones de menor nivel, esto facilita o disminuye la cantidad de código a escribir y permite encapsular características complejas como sockets o threads. Se pueden utilizar capas de nivel inferiores si no existen las características necesarias en los niveles superiores.

Media

Provee los servicios de gráficos, audio, vídeo, animación, y capacidades gráficas a la capa superior. Esta capa contiene una serie de marcos que se pueden utilizar en el desarrollo de aplicaciones.

Core Services

Contiene los servicios fundamentales del sistema que usan todas las aplicaciones.

Core OS

Se encuentra directamente sobre el hardware del dispositivo, proporciona servicios de bajo nivel que incluye: manejo del sistema de archivos, gestión de memoria, seguridad, servicios del sistema operativo, acceso a accesorios externos, drivers del dispositivo, threads.

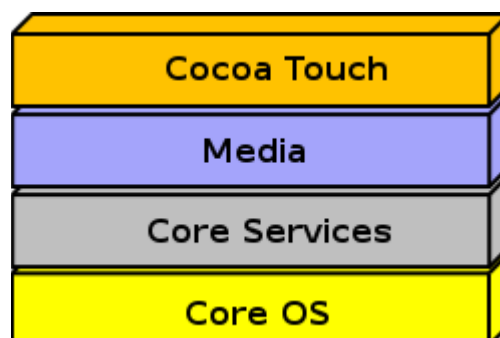


Figura 3.1: Arquitectura de iOS

3.2 Modelo de Seguridad de iOS.

Secure Boot Chain, es el proceso de inicialización del *firmware* y carga de los archivos necesarios para el arranque del sistema además, se considera la capa principal de defensa para la seguridad de esta plataforma.

Cuando un dispositivo *iOS* se enciende, el procesador ejecuta el *boot ROM* en modo de lectura. *Boot Rom* contiene la clave pública para *Apple's Root CA* que utiliza para verificar la integridad en la siguiente etapa del proceso el gestor de arranque de bajo nivel (*Low-level bootloader (LLB)*).

LLB realiza rutinas de instalación, incluye la localización de la imagen *iBoot* en la *memory flash*, así *LLB* mantiene la seguridad en *Secure Boot Chain*, para verificar la firma de la imagen de *iBoot*, si la firma no retorna el valor esperado, el dispositivo entra en modo *recovery*. *iBoot* es la segunda etapa del gestor de arranque de *iOS* para todos los dispositivos, es responsable de cargar y verificar el *Kernel* para configurar el entorno en modo de usuario.

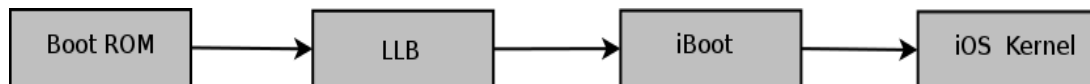


Figura 3.2: Proceso de inicialización del firmware *Secure Boot Chain*.

Code Singning es una de las características más importantes en seguridad que ofrece *iOS*. Previene la ejecución de programas no autorizados, cada vez que se ejecuta una aplicación se realiza un proceso de verificación de su firma, esto permite ejecutar aplicaciones con firmas de confianza válidas.

Por defecto, todos los datos del sistema de archivos *iOS* están cifrados con *AES*, sistema de archivos con clave que se genera cuando se carga el sistema y se almacena en el bloque 1 de *NAND flash storage*. El sistema utiliza esta clave cuando se inicia el dispositivo para descifrar la tabla y el sistema de partición. El sistema de archivos se encuentra cifrado en reposo, cuando el dispositivo está encendido el hardware basado en *crypto accelerator* desbloquea el sistema de archivos.

Adicionalmente al *crypto accelerator*, *Keychain* y cada uno de los archivos pueden ser cifrados usando *Data Protection API* que utiliza una clave derivada del *passcode*. Cuando el dispositivo está bloqueado esta información se cifra utilizando *API* y se descifra una vez que se ingresa el *passcode*, por tanto, la información del dispositivo está segura y disponible de acuerdo a este sistema.

3.3 Atacando el passcode en iOS.

En la actualidad miles de usuarios no utilizan *passcode* para bloquear sus dispositivos debido a un simple descuido o conocimientos mínimos de seguridad digital, sin embargo, usuarios con conocimientos avanzados utilizan sistemas de cifrado en conjunto con el *passcode* para proteger la información.

Un investigador forense necesitará de métodos o explotación de vulnerabilidades en el sistemas a investigar para obtener el *passcode* y desbloquear un dispositivo. A continuación se citan diferentes formas para la obtención del *passcode* en *iOS*.

3.3.1 Análisis del passcode en la grasa de la superficie.

Al utilizar el dedo para desbloquear un dispositivo por pantalla se produce un contacto en el cual se transmite la grasa corporal al dispositivo. Se puede analizar esta grasa corporal por medio una fotografía de calidad o con la técnica “Smudge Attacks on Smartphone Touch Screens” [10].

3.3.2 Ataque por Fuerza Bruta.

Gecko iPhone Toolkit.

Herramienta bajo *Windows* que realiza un ataque por fuerza bruta al passcode de un dispositivo *iOS*. Funciona con *iPhone 3GS*, *4 (GSM)*, *iPad1*, *iPod touch 3G*, *4G*.

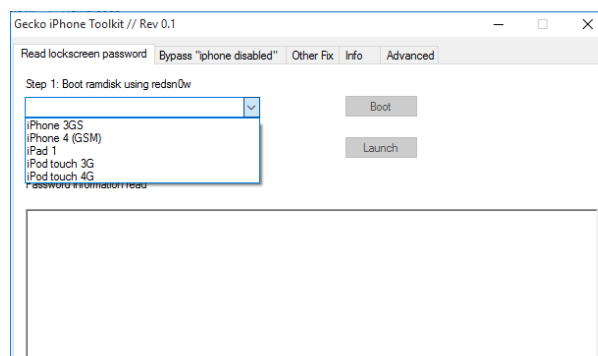


Figura 3.3: Pantalla inicio Gecko iPhone Toolkit.

IPBOX craquea el passcode de iOS 8.1.1

Una vulnerabilidad que existe en *iOS* es la utilización 4 dígitos para passcode en sus dispositivos. La herramienta de hardware *IP Box* permite realizar un ataque de fuerza bruta al passcode del *iPhone*, se puede obtener el código en un tiempo de 6 segundos hasta 17 horas. El analista debe entender que los dispositivos *iOS* por seguridad activan el borrado del dispositivo tras 10 intentos fallidos, aunque los fabricantes aseguran que funciona aunque el dispositivo tenga activada esta opción. El dispositivo implementa la vulnerabilidad *CVE-2014-4451* [13].



Figura 3.4: IP-BOX iPhone Password Unlock.

Como se describe en la sección de *Jailbreak*, *Apple* en todas las actualizaciones corrige las vulnerabilidades conocidas en su sistema *iOS*. Por tanto, depende de los investigadores en seguridad encontrar nuevas vulnerabilidades para aplicar un método y explotar diferentes formas de realizar un *Jailbreak* o desbloquear o *craquear* el *passcode* de *iOS*.

Existen herramientas de uso comercial como se habla en este trabajo como *DS7* de *Paraben* u *Oxygen Forensic Suite*. Cabe destacar que no siempre funciona en todas las

versiones debido a las constantes actualizaciones por parte de Apple. Para encontrar vulnerabilidades a cerca de iOS se puede consultar en el National Institute of Standard and Technology. [11].

3.4 Jailbreak.

En *iOS* el acceso al dispositivo o al Sistema Operativo por parte del usuario está bloqueado. La instalación de las aplicaciones se basa en la *App Store* de *Apple*. Sin embargo, comunidades *on-line* realizan estudios para proveer de acceso *Root* en los dispositivos.

Existen diferentes razones para utilizar *Jailbreak*, la principal razón por parte de los usuarios de obtener acceso *Root* desde el dispositivo se basa en incumplir los controles impuestos por la *App Store* para las aplicaciones. *Jailbreak*, permite instalar aplicaciones no firmadas desde sitios no oficiales como por ejemplo *Cydia*.

Sin embargo, realizar un *Jailbreak* tiene gran incidencia en la seguridad del dispositivo, para un analista forense permite realizar la investigación con menor dificultad, la escalada de privilegios permite el acceso directo a los datos que se almacenan en la memoria del dispositivo.

3.4.1 Tipos de Jailbreak.

- ***Untethered Jailbreak.***

Es el más deseado por los usuarios pero tiene una mayor dificultad de conseguir. Este desaparece cuando el dispositivo se reinicia el sistema. Esto se logra utilizando dos técnicas: la primera consiste en el uso de la imagen modificada en el *LLB* que permita la validación de la imagen *iBoot*, lo que permite cargar un kernel no firmado, la segunda utiliza un exploit *Corona* para iniciar el código de ejecución; un *exploit del kernel* se utiliza para parchear y colocar en un estado *Jailbroken*.

- ***Tethered Jailbreak.***

La ejecución de este *Jailbreak* no desaparece cuando el dispositivo se reinicia y requiere la utilización de un ordenador y un cable para reiniciar el dispositivo.

El Analista Forense, puede intentar por diferentes medios la extracción de datos del dispositivo sin modificar el sistema original, sin embargo, en diferentes circunstancias será necesario como mejor alternativa explotar un *Tethered Jailbreak* que permita acceder a los datos y tras el reinicio volver al estado original, esto conlleva, a documentar todo el proceso y los motivos por el cual se procede a realizar esta modificación en los sistemas *iOS*. Como recomendación se debe tener una copia de *iTunes* de las versiones anteriores y ejecutarlas en máquinas virtuales dependiendo de la versión del dispositivo *iOS* a investigar.

3.4.2 Herramientas para Jailbreak.

Las herramientas disponibles para realizar *Jailbreak* dependen de las diferentes versiones de *iOS*. Para realizar pruebas de concepto *iTunes* debe estar en la versión del sistema *iOS* que se desea realizar el *Jailbreak* porque las actualizaciones corrigen las vulnerabilidades de versiones anteriores. Se citan herramientas que efectúan el

proceso de Jailbreak en los sistemas iOS más actuales a la elaboración de este documento.

RedeSn0w.

Esta herramienta afecta a los sistemas iOS6. Al utilizar este sistema es necesario poner el dispositivo en modo *DFU (Device Firmware Update)*. El sistema automáticamente explica los pasos a seguir para el proceso de Jailbreak.

El proceso es el siguiente: ejecutar el archivo como administrador de *RedeSn0w*, a continuación se presiona e *Jailbreak - Next*. Para poner en modo DFU se pulsa el botón de encendido (*Power*) durante 3 segundos, a continuación manteniendo presionado el botón de encendido se pulsa al mismo tiempo el botón *Home* durante 10 segundos y para terminar se deja de presionar el botón de *Power* por 15 segundos.

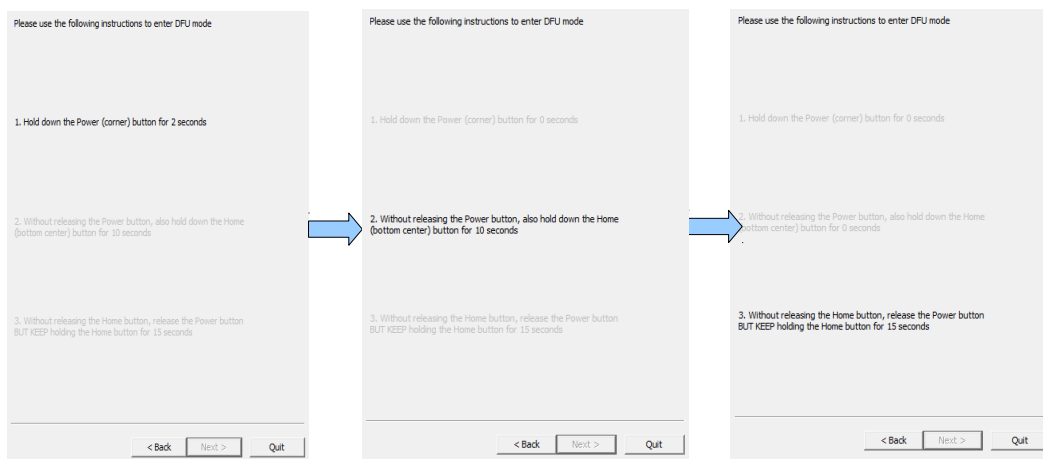
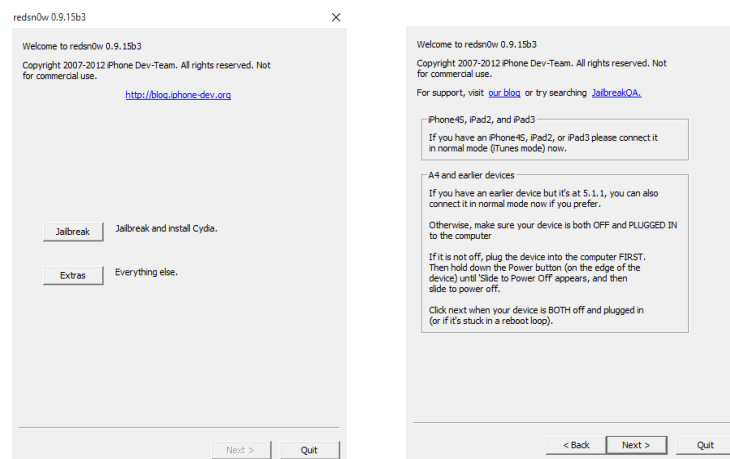


Figura 3.5: Proceso jailbreak con RedSn0w.

Evasi0n.

Afecta a las versiones 6.0 – 6.2. Es capaz de ejecutar código inicial en el dispositivo, utiliza la vulnerabilidad CVE-2013-0979 [14] y CVE-2013-0981 [15]

Evasi0n 7.

Afecta a las versiones iOS 7.0 hasta las 7.6 beta a excepción del Apple TV. Utiliza la vulnerabilidad CVE-2014-1273 [16] y CVE-2014-1272 [17].



Figura 3.6: Proceso Jailbreak con evasi0n 7.

TaiG Jailbreak para iOS 8.1.3-8.

TaiG lanzó en Junio del 2015 la herramienta de *Jailbreak* para iOS 8.1.3-8.3. [18], apoya al *untethered Jailbreak* para 8.4, que a su vez esperó a que *Apple* lance la versión de iOS 8.4 para lanzar su versión de *Jailbreak* iOS 8.4.

Para utilizar esta aplicación se necesita desactivar el *passcode* y el *find My phone*. Se ejecuta la aplicación como administrador y se sigue las instrucciones.

Conectar el dispositivo por medio del cable al ordenador, una vez TaiG reconoce el dispositivo pulsar sobre el botón iniciar (*Start*). La opción *3K Assitant 2.3.0* es opcional, a continuación después de unos minutos el software termina el proceso.

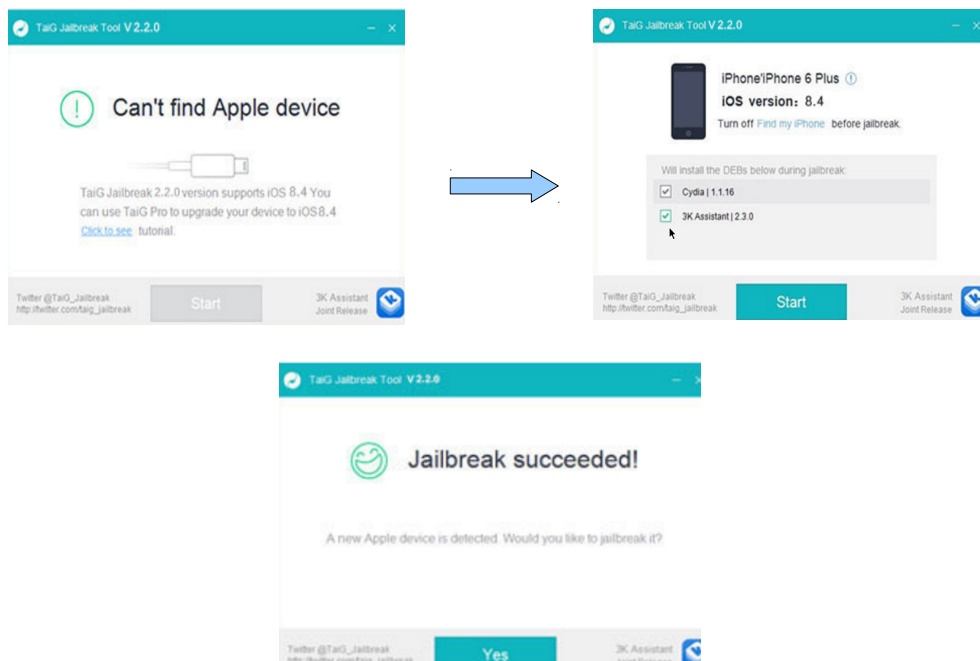


Figura 3.7: Proceso Jailbreak con TaiG.

Pangu.

En Octubre del 2015, Pangu [19] lanzó la nueva versión de su herramienta que permite hacer *Jailbreak* a los sistemas iOS 9, 9.01 y 9.02, sin embargo el 22 de

Octubre del 2015, *Apple* en su versión 9.1 soluciona las vulnerabilidades que permite elevar privilegios y ejecutar el código no oficial con privilegios de *Kernel*.

Para realizar esta prueba de concepto se necesita tener el dispositivo en modo avión, desactivar *find My phone* y conectar al ordenador.

Descargar y ejecutar como administrador la aplicación de *Pangu*.

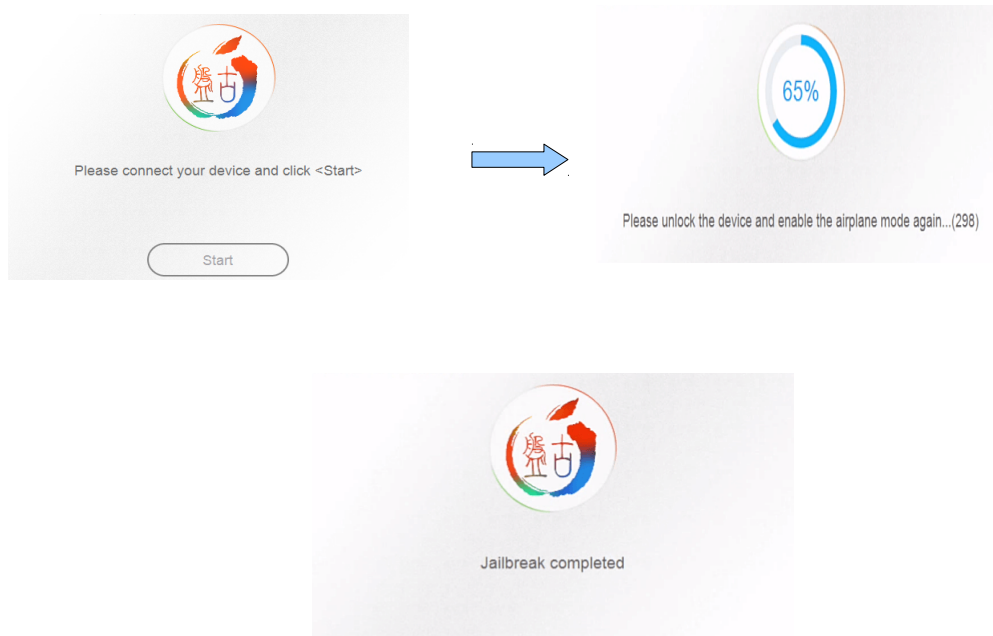


Figura 3.8: Proceso *Jailbreak* con *Pangu*.

Si el proceso de realizar el *Jailbreak* utilizando cualquier de estos o futuros métodos se realiza con éxito, se instala en el dispositivo una aplicación -*OpenSSH*- que permita la conexión segura entre el ordenador y el dispositivos para explorar el sistema de archivos.

La conexión requiere la dirección IP del dispositivo iOS que se puede obtener con la herramienta *Nmap* o directamente en el *router* consultando la dirección asignada. El nombre de usuario por defecto es: **root** y el paswrod:**alpine**

El comando utilizado es: `ssh root@ipdispositivoiOS`

```
File Edit View Search Terminal Help
root@marcopc:~# ssh root@192.168.1.14
root@192.168.1.14's password:
iPhone:~ root# ls
Application\ Support\ Library\ Media\
iPhone:~ root#
```

Figura 3.9: Conexión de dispositivos iOS por SSH

Existen herramientas como *Filezilla* para establecer la conexión por medio de entorno gráfico.

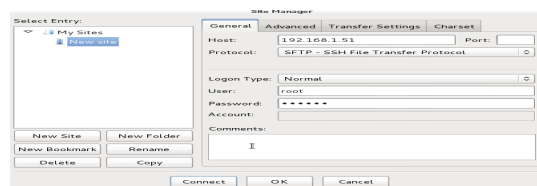


Figura 3.10: *Filezilla*, conexión por SSH a de dispositivos iOS.

Apple no ofrece información de sus dispositivos y sistemas, pues se recurre a la exploración del sistema de archivos mediante la conexión por SSH, se puede especificar una lista de localizaciones de interés en la investigación forense.

/Applications	Sistema de aplicaciones.
/var/mobile/Applications	Aplicaciones de Terceros.
/private/var/mobile/Library/Voicemail	Voicemail.
/private/var/mobile/Library/SMS	Mensajes de SMS.
/private/var/mobile/Media/DCIM	Fotos.
/private/var/mobile/Media/Videos	Videos
/private/var/mobile/Library/AddressBook.sqlitedb	Base de datos de contactos

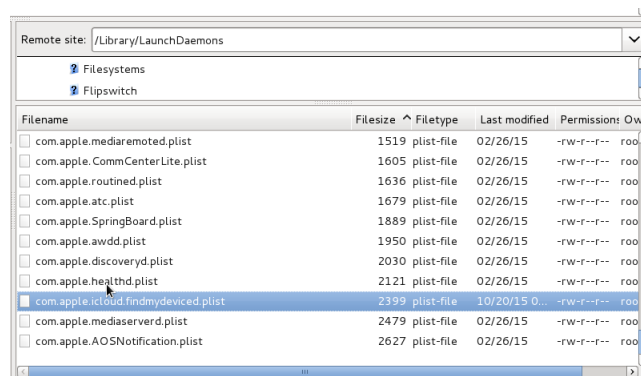


Figura 3.11: Filezilla, localización del demonio find My phone.

3.5 Atacar la ID de Apple.

El ID de Apple es el nombre de usuario para las actividades en iOS. La mayoría de usuarios no cierran las aplicaciones instaladas ni eliminan la caché en sus dispositivos

3.5.1 Vulnerabilidad por mensajes en la pantalla.

El usuario puede configurar el sistema a utilizar de alertas para los mensajes, los estilos pueden ser ninguno, tiras o alertas. Una vulnerabilidad conocida en los sistemas IOS es la alerta de los mensajes de alertas por pantalla, que permite ver los mensajes recibidos en la pantalla por cada una de las aplicaciones. Si es la configuración que tiene el usuario, existe una forma similar a la citada en anteriormente "He olvidado mi contraseña". Una opción es enviar un SMS al número

de teléfono que se enviará un mensaje que será reflejado en la pantalla. Para esto es necesario conocer el número de teléfono.

3.5.2 Vulnerabilidad por aplicaciones abiertas.

Esta prueba se realiza en dispositivos que no utilizan passcode, pero es necesario realizar el *Jailbreak* o *Backup* para la extracción física o lógica de los datos. Los usuarios tienen las aplicaciones de correo electrónico abiertas para la consulta de sus mensajes normalmente de *Outlook* o *Gmail*.

Para cualquier modificación el sistema *iOS* pedirá la clave asociada a la cuenta, se opta por la opción “*Ha olvidado su ID de Apple o la contraseña?*”, a continuación se activa la opción de enviar la contraseña por correo electrónico, la segunda opción es por medio de una pregunta de seguridad. Se elige la primera y automáticamente enviará una mensaje a la cuenta de correo para reactivar la clave.

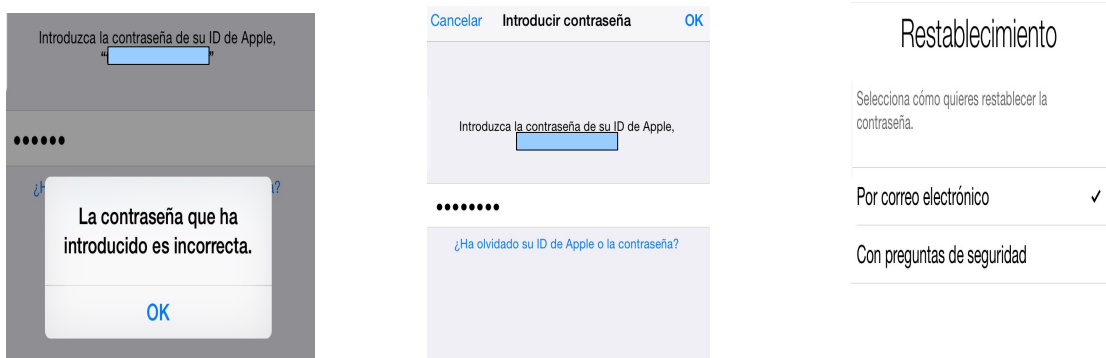


Figura 3.12: Restablecimiento de contraseña método: “Ha olvidado su ID de Apple”

Se procede a verificar el mensaje que se recibe por correo electrónico desde el dispositivo a investigar. Dicho correo electrónico especifica las instrucciones para modificar la contraseña de ID de Apple.

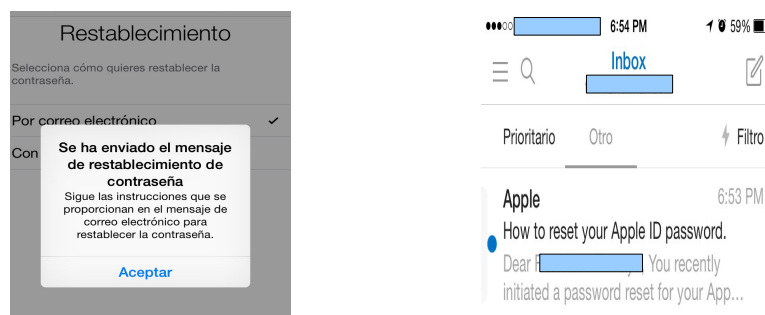


Figura 3.13: Correo electrónico restablecer la de contraseña IdApple.

Se modifica la nueva contraseña y a continuación se accede al dispositivo.

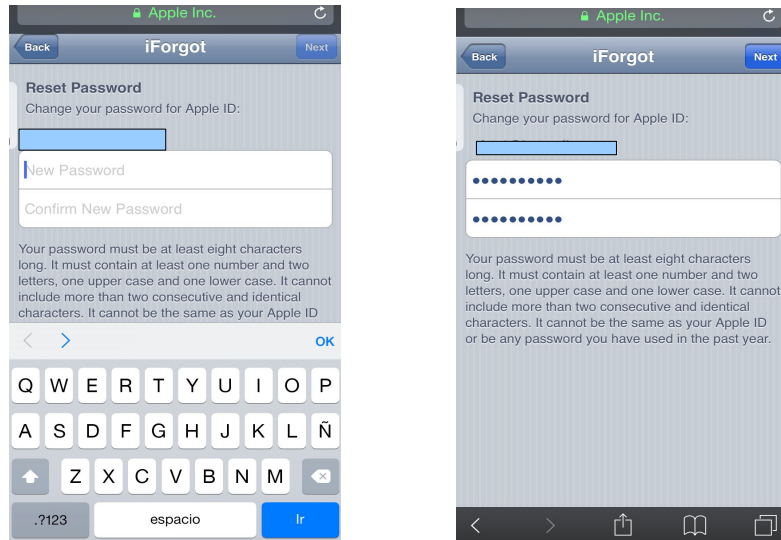


Figura 3.14: Cambio de contraseña para el Id de Apple.

Si el proceso se realiza con éxito, se hace un backup del sistema para su posterior análisis

Capítulo 4: Hacking de dispositivos móviles Android.

4.1 Arquitectura de los Sistemas Android.

En Android el flujo de datos se basa en las siguientes capas:

- **Aplications.**

Es la capa superior de Android. Las aplicaciones instaladas de fábrica o aplicaciones personales grabadas en el dispositivo se encuentran en esta.

- **Framework Applications.**

En esta capa se encuentran los servicios y bibliotecas que utilizan las aplicaciones para llamar a sus funciones.

- **Android Runtime.**

Todas las aplicaciones, el código Java-Framework se ejecuta en en una máquina virtual, el cual se convierte en código ejecutable.

- **Libraries.**

Bibliotecas nativas, demonios y servicios (escritos en C o C ++). Las Bibliotecas nativas no son más que parte del sistema operativo Android interna. Estas bibliotecas se utilizan cuando se llama a cualquier API de la capa de aplicación. Básicamente cuando se llama a cualquier API de capa de Java o de la capa superior, entonces se llama a la API de la capa nativa que está escrito en su mayoría en C / C ++, por lo que se puede decir que la API de Java se convierte en C / C ++ API.

- **Linux Kernel.**

Es la capa más compleja, incluye controladores para el hardware, redes, acceso al sistema de archivos procesos-comunicación. Cada instrucción que se ejecuta en la capa superior pasa a través del Kernel para obtener el resultado final.



Figura 4.1: Arquitectura Android. Fuente: <https://es.wikipedia.org/wiki/Android>.

4.2 Sistema de Archivos Android.

Después de dar un enfoque general a la arquitectura de Android, se entiende que es un Sistema Operativo basado Linux, su estructura de sistema de archivos no es una excepción. Android emplea varias particiones para organizar los *archivos-carpetas* en el dispositivo cada uno con su funcionalidad. Principalmente existen seis particiones, sin embargo, se debe contar con la existencia de particiones adicionales que difieren entre un modelo y otro.

/boot. Arranque.

/system. El punto de montaje es */dev/mtd/mtblock3 yaffs2*, en */dev/block/bootdevice/by-name/system* para *ext4*, formatos de archivos que se emplean en la mayoría de dispositivos. Incluye bibliotecas del sistema y aplicaciones preinstaladas.

/recovery. Recuperación

/data. UserData. */dev/mtd/mtblock5* para *yaffs2*, en */dev/block/bootdevice/by-name/userdata* para *ext4*. El sistema de archivos tiene el punto de montaje sistema de archivos, montado en */ data* - contiene las aplicaciones y los datos instalados por el usuario, incluyendo los datos de personalización

/cache. Caché. */dev/mtd/mtblock4 yaffs2*, en */dev/block/bootdevice/by-name/cache*. Se utiliza para almacenar datos temporales de caché.

/misc. Misceláneos.

Además, se presenta la tarjeta SD de particiones del sistema de archivos.

/sd card. El punto de montaje */dev/mtd/mtblock4 yaffs2*. Android *ICS* o la versión *JB* usa el directorio */data/media* para la memoria interna *sd card*, además utiliza *fuse* para el montaje del emulador interno */dev/fuse* para *ext4*.

/sd-ext.

Una de las múltiples alternativas para verificar el sistema de archivos es utilizar el Sistema Operativo Santoku Linux para establecer conexión por medio de Adb. [20]

```
marcoalvarez@PCMarco:~$ adb shell
shell@Aquaris_E5:/ $ df
Filesystem      Size  Used  Free Blksize
/dev            445.5M 128.0K 445.3M 4096
/sys/fs/cgroup  445.5M  12.0K 445.4M 4096
/mnt/asec       445.5M  0.0K 445.5M 4096
/mnt/obb        445.5M  0.0K 445.5M 4096
/dev/usb-ffs/adb: Permission denied
/system         1.5G  859.3M 628.6M 4096
/data           4.4G   3.8G 556.2M 4096
/cache          991.9M  1.5M 990.4M 4096
/persist        27.5M 112.0K  27.4M 4096
/firmware       64.0M  40.9M  23.0M 16384
/mnt/shell/emulated 4.3G   3.8G 506.2M 4096
/storage/emulated/legacy 4.3G   3.8G 506.2M 4096
1|shell@Aquaris_E5:/ $
```

Figura 4.2: Comando df. Sistema de archivos Android dispositivo Aquarius E5 4G

Nota: el sistema de arranque y partición no se muestra en la imagen 4.2. Se puede utilizar el comando *mount* para verificar los sistemas mencionados.

```
shell@Aquaris E5:/ $ mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,seclabel,nosuid,relatime,size=456148k,nr_inodes=114037,mode=755 0 0
devpts /dev/pts devpts rw,seclabel,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,seclabel,relatime 0 0
selinuxfs /sys/fs/selinux selinuxfs rw,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
none /sys/fs/cgroup tmpfs rw,seclabel,relatime,size=456148k,nr_inodes=114037,mode=755,gid=1000 0 0
tmpfs /mnt/asec tmpfs rw,seclabel,relatime,size=456148k,nr_inodes=114037,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,seclabel,relatime,size=456148k,nr_inodes=114037,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
```

Figura 4.3: Resultado del comando mount.

4.3 Análisis de Vulnerabilidad para Root en Android.

El núcleo de Android se basa en Linux, para el analista forense es importante escalar privilegios sobre todo cuando se encuentra con un dispositivo con passcode. Se puede aplicar algún método como los descritos en el trabajo para llegar a obtener dicha clave, o a su vez, buscar e intentar explotar algún tipo de vulnerabilidad en el sistema.

4.3.1 Drozer

Drozer es un *framework* destinado a la auditoría de la seguridad para Android. *Drozer* asume el papel de una aplicación de Android que permite interactuar con otras aplicaciones. Se puede realizar pruebas en un aplicación instalada para descubrir características como hacer uso del Inter-Proceso de Comunicación en Android Comunicación (*IPC*) y el mecanismo de interactuar con el sistema operativo subyacente.

Drozer se utiliza para explotar de forma remota los dispositivos Android, mediante la construcción de archivos maliciosos o páginas web que explotan las vulnerabilidades conocidas. Para ejecutar los *exploits* se utiliza un agente Drozer que es esencialmente una herramienta de administración remota. Dependiendo de los permisos concedidos a la aplicación puede ser vulnerable. Se puede instalar un agente completo o limitado en el proceso utilizando técnicas para generar *shell inversa*.

El proceso de instalación de *drozer* se puede consultar en el documento *drozer Guide User* [21], o consultar en el anexo de este documento.

En la investigación forense del dispositivo, es necesario el análisis de las aplicaciones instaladas con la finalidad de localizar archivos y base de datos que aporte información de interés. El comando *app.package.list* devuelve una lista de las aplicaciones en el dispositivo.

```
02> run app.package.list
com.qualcomm.fastdormancy (com.qualcomm.fastdormancy)
com.sqiggle.production (Tango)
com.qualcomm.timeservice (com.qualcomm.timeservice)
com.android.defcontainer (Package Access Helper)
com.android.providers.partnerbookmarks (com.android.providers.partnerbookmarks)
com.bq.lollipopupdateinfo (Lollipop Update)
com.android.contacts (Contacts)
com.android.phone (Phone)
com.qualcomm.qces (com.qualcomm.qces)
com.spotify.music (Spotify)
com.android.calculator2 (Calculator)
com.android.htmlviewer (HTML Viewer)
com.android.cellbroadcastreceiver (Cell Broadcasts)
com.google.android.gsf.login (Google Account Manager)
com.android.bluetooth (Bluetooth Share)
com.android.providers.calendar (Calendar Storage)
com.qualcomm.gsmtuneaway (com.qualcomm.gsmtuneaway)
```

Figura 4.4: Paquetes instalados en el dispositivo.

El comando `app.package.info nombredelpaquete`, devuelve información a cerca de la aplicación instalada. En la siguiente imagen se obtiene información a cerca del paquete de Facebook.

```
> run app.package.info -a com.facebook.orca
Package: com.facebook.orca
Application Label: Messenger
Process Name: com.facebook.orca
Version: 45.0.0.7.61
Data Directory: /data/data/com.facebook.orca
APK Path: /data/app/com.facebook.orca-1.apk
UID: 10097
GID: [3003, 1028, 1015, 3002, 1006]
Shared Libraries: [/system/framework/com.google.android.maps.jar]
Shared User ID: null
Uses Permissions:
- com.facebook.katana.provider.ACCESS
- android.permission.INTERNET
- android.permission.GET_ACCOUNTS
- android.permission.ACCESS_NETWORK_STATE
- android.permission.WAKE_LOCK
- android.permission.VIBRATE
- android.permission.READ_CONTACTS
- android.permission.READ_CALL_LOG
- android.permission.READ_PROFILE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.READ_PHONE_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.READ_SYNC_SETTINGS
- android.permission.RECEIVE_MMS
- android.permission.READ_SMS
- android.permission.WRITE_SMS
- android.permission.SEND_SMS
- android.permission.CHANGE_NETWORK_STATE
- android.permission.RECORD_AUDIO
- android.permission.SYSTEM_ALERT_WINDOW
- android.permission.CALL_PHONE
- android.permission.MODIFY_AUDIO_SETTINGS
- android.permission.DOWNLOAD_WITHOUT_NOTIFICATION
- android.permission.AUTHENTICATE_ACCOUNTS
- android.permission.BLUETOOTH
- android.permission.MANAGE_ACCOUNTS
```

Figura 4.5: Información sobre el paquete Facebook.

En el análisis forense se puede utilizar vulnerabilidades para llegar a la escala de privilegios. Drozer permite instalar módulos que permita investigar aspectos relacionados con Root.

Instalación de módulos para Root.

Módulo cmdClient.

El repositorio oficial módulo drozer está alojado junto al principal proyecto en Github [22] de *Módulos para drozer*. Para realizar búsqueda de módulos se puede utilizar el comando `module`. La prueba de concepto se realiza con módulos para Root en Android.

El módulo a utilizar es el módulo *“Exploit the setuid-root binary at /system/bin/cmdclient on certain devices to gain a root shell”*. [23], se procede a la instalación con la ejecución del comando:

```
module install cmdclient
```

Se ejecuta el módulo con:

```
run exploit.root.cmdclient.
```

```
dz> dz module search root
dz> dz module search root
metall0id.root.cmdclient
metall0id.root.exynosmem
metall0id.root.huaweiip2
metall0id.root.mmap
metall0id.root.scanner_check
metall0id.root.towelroot
metall0id.root.ztesyncagent

dz> module install cmdclient
Processing metall0id.root.cmdclient... Already Installed.

Successfully installed 0 modules, 1 already installed.

dz> run exploit.root.cmdclient
Not Vulnerable.
dz>
```


Figura 4.6: Búsqueda de módulos Root. Instalación y ejecución del módulo `cmdclient`

Si existe alguna vulnerabilidad se puede escalar privilegios root y ejecutar `run shell.star` para entrar en modo Root del dispositivo.

En la siguiente prueba de concepto se utiliza en módulo ZTESyncAgent “Exploit the `setuid-root` binary at `/system/bin/sync_agent` on certain ZTE devices to gain a root shell”.[24]

```
dz> module install ztesyncagent
Processing metall0id.root.ztesyncagent... Done.

Successfully installed 1 modules, 0 already installed.

dz> run exploit.root.ztesyncagent
```

Figura 4.7: Instalación y ejecución del módulo ZTESyncAgent.

4.3.2 Exploit de la vulnerabilidad **CVE-2014-3153**. [25]

Se descarga el archivo `cube_towel`. Para esta el archivo que contiene el código del exploit en lenguaje C++ es `root.c`, se ejecuta el comando:

`gcc nombredelarchivo.c -o nombredeexploit -lpthread.`

```
root@PCMarco:/home/marcoalvarez/Downloads/exploitRoot# gcc exploit.c
o exploit -lpthread
gcc: error: exploit.c: No such file or directory
root@PCMarco:/home/marcoalvarez/Downloads/exploitRoot# gcc root.c -o
xploit -lpthread
root@PCMarco:/home/marcoalvarez/Downloads/exploitRoot# ls
cube-towel.c exploit root.c
root@PCMarco:/home/marcoalvarez/Downloads/exploitRoot#
```

Figura 4.8: Comando `gcc root.c -o exploit -lpthread`

Con el comando `adb push exploit /data/local/tmp` y ejecutar con: `./exploit`

```
File Edit Tabs Help
shell@Aquaris_E5:/data/local/tmp $ ls
COPYING
Edward16741123893
saapt
busybox
exploit
gesture.key
glsl_shader_log.txt
password.key
ps_state
ps_state_grep
toolbox
zergRush.c
zgo
shell@Aquaris_E5:/data/local/tmp $ ./exploit
```

Figura 4.9: Ejecución del exploit en Android.

4.3.3 Towelroot.

Su creador asegura que este exploit lograr conseguir privilegios de Root en todos los Kernels compilados antes de 16 de Junio del 2014. [26], esta herramienta utiliza la vulnerabilidad `CVE-2014-3153`.[25]

Desde el github se puede explotar de la forma descrita anterior instalando la aplicación .apk. El comando a utilizar es: `adb install nombreakplicación.apk`.

```
system
towelroot-3-0-en-android.apk
zergRush
zergRush-master.zip
root@PCMarco:/home/marcoalvarez/Downloads# adb install towelroot-3-0-en-android.
apk
599 KB/s (113899 bytes in 0.184s)
pkg: /data/local/tmp/towelroot-3-0-en-android.apk
```

Figura 4.10: Instalación de TowelRoot.

4.2.4 KingRoot.

Aplicación que permite hacer *Root* a un terminal *Android*, siempre y cuando el sistema *Android* esté en la versión 4.2.2 y 5.1

```
towelroot-3-0-en-android.apk
zergRush
zergRush-master.zip
root@PCMarco:/home/marcoalvarez/Downloads# adb install KingoRoot.apk
985 KB/s (1120755 bytes in 1.870s)
pkg: /data/local/tmp/KingoRoot.apk
Success
root@PCMarco:/home/marcoalvarez/Downloads#
```

Figura 4.11: Instalación de KingoRoot.

4.2.5 SuperOneClic.

Es una herramienta que automatiza el proceso de instalación de los *exploits* *zergRush* [27] o *psneuter* [28] en *Android*.

Para utilizar esta herramienta, se ejecuta como administrador el archivo *.exe*.

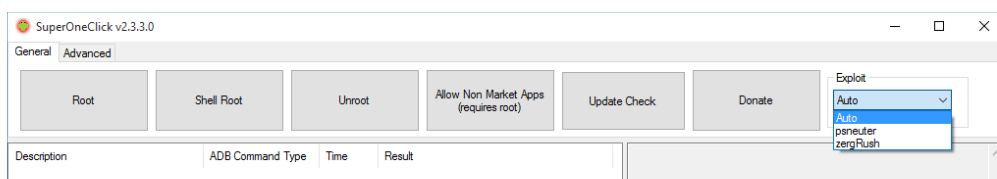


Figura 4.12: Pantalla de inicio SuperOneClick.

Se conecta el dispositivo por medio de *USB*, a continuación se presiona en el botón a *Root* o *Shell Root*, y la herramienta empezará a utilizar los *exploits* para la escala de privilegios.

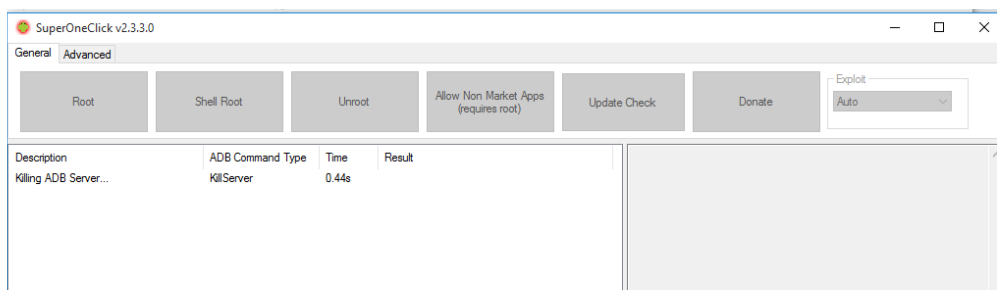


Figura 4.13 Ejecución de Root en un dispositivo Android.

4.2.6 Smart Phone Flash-Tool.

Para esta prueba de concepto se utiliza un teléfono *BQ5 4G*. Hay que tener en cuenta que es un proceso que conlleva peligro y puede perderse datos del terminal. Para este proceso se siguen las recomendaciones descritas en el vídeo de la página oficial de *BQ* [29], pero con algunas modificaciones.

- Descargar el *firmware*, *drivers* y herramientas necesarias desde la página oficial de *BQ*. [30]

- Ejecutar como administrador la herramienta *Flash-Tool*. El móvil debe estar apagado, sin conectar al ordenador.

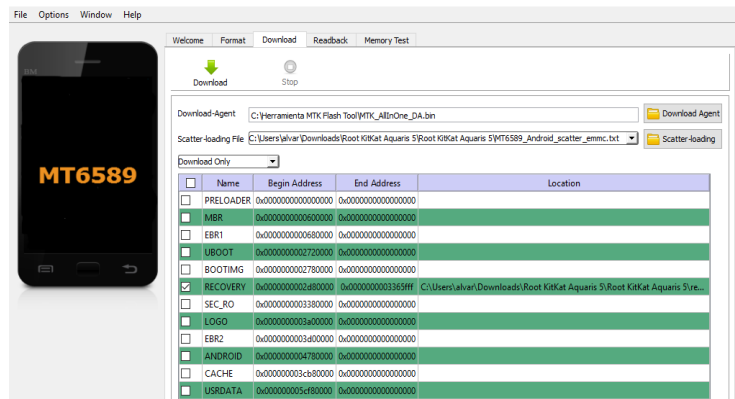


Figura 4.14: Flash Tool Download Only, Scatter-loading, Recovery.

- Se pulsa *Scatter-loading*, seleccionando el archivo *MT6589_Android_scatter_emmc.txt* que se encuentra en el firmware, modo *Download Only* y *Recovery*.
- A continuación pulsar *Download* y, conectar el dispositivo al ordenador.

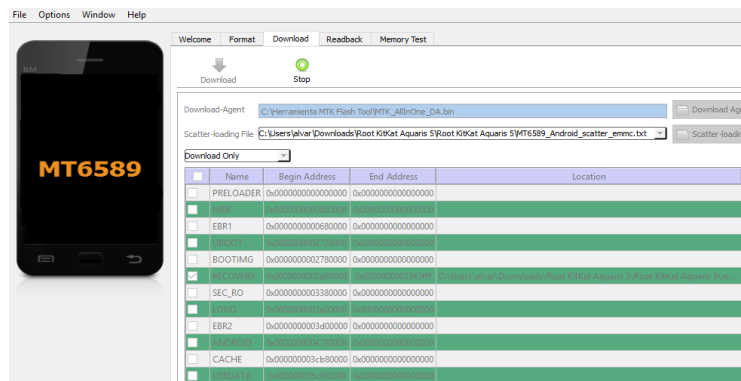


Figura 4.15: Flash Tool Download Recovery.

- Ingresar al modo *Recovery* que se instaló, pulsando el botón de encendido (*Power*) y el botón volumen (+) hasta que aparezca las letras bq, entonces se deja de presionar.
- Seleccionar *Philz Settings - Re-root System (superSu) - Yes - Apply SuperSU*.
- Encender el teléfono, descargar e instalar SuperSU. A continuación reiniciar el dispositivo.

4.2.7 Modificación del archivo *default.prop*

Para obtener privilegios root, se puede modificar el archivo *default.prop*. El primer paso es extraer el archivo al ordenador con el comando *adb pull default.prop*, a continuación modificar las instrucciones.

```

root@PCMarco:/home/marcoalvarez# adb pull default.prop
4 KB/s (238 bytes in 0.049s)
root@PCMarco:/home/marcoalvarez#

```

Figura 4.16: Extracción del archivo default.prop.

```

File Edit Search Options Help
#
# ADDITIONAL_DEFAULT_PROPERTIES
#
ro.secure=0
ro.adb.secure=1
ro.allow.mock.location=0
ro.debuggable=1
ro.tigerwolf=1
persist.sys.strict_op_enable=false
persist.sys.whitelist=/system/etc/whitelist_appops.xml
persist.sys.usb.config=None

```

Figura 4.17: Archivo de configuración default.prop.

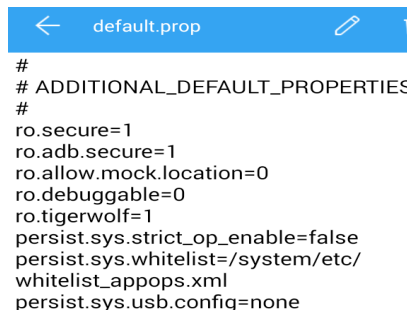
Se cambia las líneas de configuración por las siguiente

```

ro.secure=1
ro.debuggable=0

```

En el dispositivo se ejecuta el método *fastboot*, desde adb con comando *adb reboot bootloader*, a continuación se copia el archivo modificado,



```

← default.prop
#
# ADDITIONAL_DEFAULT_PROPERTIES
#
ro.secure=1
ro.adb.secure=1
ro.allow.mock.location=0
ro.debuggable=0
ro.tigerwolf=1
persist.sys.strict_op_enable=false
persist.sys.whitelist=/system/etc/whitelist_appops.xml
persist.sys.usb.config=None

```

Figura 4.18: Configuración default.prop para obtener privilegios root.

4.4 Ataque al passcode de Android.

4.4.1 Desbloqueo del passcode por eliminación de archivos.

Para eliminar el passcode cuando de introduce un PIN se eliminar el archivo */data/system/password.key*. Se necesita acceso a Root.

```

root@Aquaris_E5:/data/system # rm password.key
root@Aquaris_E5:/data/system #
root@Aquaris_E5:/data/system # root@PCMarco:/home/marcoalvarez/Downloads# clear

```

Figura 4.19: Eliminación de password.key.

Si usa el método de Bloqueo por Patrón Para eliminar el passcode cuando de introduce un PIN se eliminar el archivo */data/system/gesture.key*

```

root@Aquaris_E5:/data/system # rm gesture.key
root@Aquaris_E5:/data/system # root@PCMarco:/home/marcoalvarez/Downloads#

```

Figura 4.20: Eliminación del archivo gesture.key.

Capítulo 5: Análisis Forense en dispositivos iOS.

5.1 Adquisición de la evidencia.

Al aplicar el protocolo descrito, la fase de adquisición obtiene una copia de los dispositivos para el análisis, realizar un backup de iOS es una de las mejores alternativas; como recomendación se puede utilizar: *iTunes* para *MAC* y *Windows*, *Libimobiledevice* en *Santoku*, en adición, la copia bit a bit es otra alternativa.

Existen diferentes herramientas para la adquisición como son *dd* o *Ftk Imager*[31] (algunas herramientas forenses no reconocen el formato de esta imagen).

La siguiente alternativa es utilizar aplicaciones de uso comercial que automatizan el proceso se pueden citar: *DS7*, *Oxygen Forensic*, *BlackLight*[32], *MOBILedit*[33].

La siguiente prueba de concepto realiza una copia bit a bit del dispositivo, para lo cual se recomienda que el dispositivo esté en modo avión y el bloqueo automático deshabilitado. General-Bloqueo automático-Nunca.



Figura 5.1: Configuración en iOS para la copia bit a bit.

5.1.1 Copia bit a bit con la herramienta dd.

El protocolo ssh, es uno de los métodos que se utiliza para la conexión entre el dispositivo con el ordenador del laboratorio.

```
ssh root@IPiOS ssh root@192.168.1.2  
root@IPiOS password: alpine
```

Cuando se establece la conexión, desde *Santoku* o cualquier máquina con el Sistema Operativo *Linux* se ejecuta el comando *dd*:

```
dd if=/dev/rdisk0 bs=4096 | ssh -C root@IPdestino dd of=nombredelaimagen.
```

Se confirma la contraseña del dispositivo de destino, en este ejemplo se configuró la dirección IP de dispositivo como 192.168.1.12, la del ordenador del laboratorio con dirección IP 192.168.1.18.

```
root@marcopc:~# ssh root@192.168.1.12  
The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.  
RSA key fingerprint is df:6d:8b:4c:2c:0e:f6:0c:a2:20:6a:c1:c2:8f:fd:5a.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.12' (RSA) to the list of known hosts.  
root@192.168.1.12's password:  
iPhone:~ root# dd if=/dev/rdisk0 bs=4096 | ssh -C root@192.168.1.18 dd of=ios.dd  
root@192.168.1.18's password:
```

Figura 5.2: Copia herramienta *dd* en un dispositivo *iOS*.

Con la imagen que se obtiene y el uso de herramientas comerciales o de open source se inicia el proceso de investigación. En el próximo capítulo se estudian ciertas pautas para el análisis de imágenes con la herramienta *Autopsy*.

5.1.2 Copia de Seguridad con iTunes.

iTunes es un reproductor y tienda de contenido multimedia desarrollado por Apple, se utiliza para sincronizar iTunes con iPhones, iPads, iPods. Las plataformas compatibles con *iTunes* son *Mac* y *Windows*.

Además, *iTunes* emplea utilidades para: realizar copias de seguridad de forma local o en la nube; actualizar las nuevas versiones de los sistemas Apple. Para la copia de seguridad de un sistema *iOS* se recomienda utilizar *iTunes*.

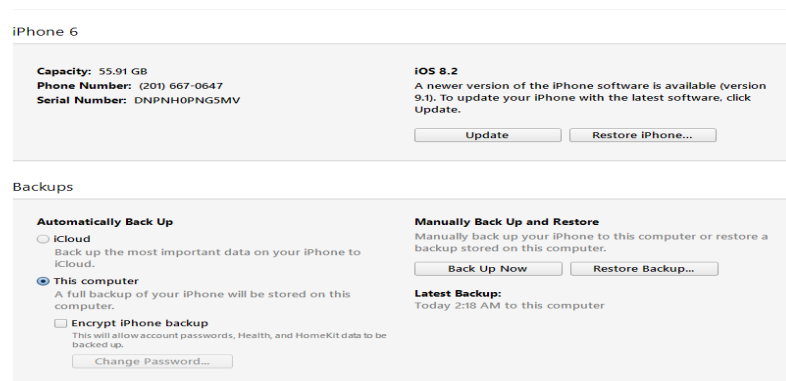


Figura 5.3: Backup local con iTunes.

Estructura de un Backup de IOS.

Los ficheros que se almacenan en la copia de seguridad se mantienen intactos, la diferencia radica en que iTunes reemplaza el nombre real del archivo por un valor hexadecimal que corresponde a un Hash SHA1 del nombre del dominio al que pertenece cada fichero. Pero, existen otros archivos con información general del sistema, que está sin cifrar y es de mucha utilidad.

Info.Plist.- Fichero que contiene características del terminal como el modelo, IMEI, aplicaciones instaladas, fecha de creación del backup, número de serie.

Manifest.Plist.- Archivo con detalles de las rutas de las aplicaciones, el número de serie, el tipo de dispositivo, UUID, e información a cerca de la seguridad.

Status.list. Información de la copia como la hora al que se realizó, si la copia es efectuó de forma completa, terminó de forma satisfactoria, el UUID.

000cae3437db21095a85771716e8874f9...	11/8/2015 4:36 AM	File	1 KB
00bbca832c2d01bc7569e9a244f669141...	11/8/2015 4:38 AM	File	1 KB
00c74f4fad7341299cf9d263152461c0...	11/8/2015 4:36 AM	File	4 KB
00c6792685bd20af71b6b155d33e9c2c...	11/8/2015 4:38 AM	File	1,412 KB
00ca777dd33466c3940470ea0468bc99c...	11/8/2015 4:36 AM	File	34 KB
00f2b105fd922b42be2259756ca03a86...	11/8/2015 4:36 AM	File	34 KB
00f4f035da4ace4174ded6d71d6162b0d...	11/8/2015 4:38 AM	File	5 KB
00f75308934c4d9c4b578fa121cdf5202...	11/8/2015 4:36 AM	File	1 KB
0a0a4dc6e9cd698cacf0c497d8b1c8602...	11/8/2015 4:36 AM	File	28 KB
0a0ac56f62dccb832dbfcd0299f24bbc...	11/8/2015 4:38 AM	File	213 KB
0a0fe145cc0eeb1f5a0df31a00fb464510...	11/8/2015 4:36 AM	File	2 KB
0a13a3fcf88224cbd3ec2934e4600a2b7...	11/8/2015 4:36 AM	File	55 KB
0a82ca307b9c44e53f85d20edc9030815...	11/8/2015 4:38 AM	File	12 KB
0a489a3013fa43fac538fb167ea4d0cedb...	11/8/2015 4:36 AM	File	38 KB
0a6848bc2a011d151d4b4e09c9f0abf75...	11/8/2015 4:36 AM	File	63 KB
0a7790fa91ce65ce5e935aa31c34e1dd9...	11/8/2015 4:38 AM	File	18 KB
0a8018b9b09b4c7e7ec7552b1048bd79...	11/8/2015 4:38 AM	File	4 KB
0a419980e37772ee7306d9f5e685381a...	11/8/2015 4:38 AM	File	1 KB
0a23265526ed7a4b13b78446a7a087380...	11/8/2015 4:38 AM	File	4 KB
0ab0a870f412c59d13886b8055bb2c961...	11/8/2015 4:36 AM	File	1 KB
0ac6841f9cae66291d80954eeb0e4fd1...	11/8/2015 4:36 AM	File	13 KB
0ad6a4a7a3f2a297f71de11f1d9bd26bf3...	11/8/2015 4:36 AM	File	2 KB
0b0af6991491da915aa9682d48791806e...	11/8/2015 4:36 AM	File	8 KB

Figura 5.4: Estructura del backup de iOS.

Ubicación de la copia de seguridad.

Sistema Operativo	PATH.
Windows 7	C:\%HOMEPATH%\Application\Data\Apple Computer\MobileSync\Backup\{UDID}.
Windows 8, 10	C:\Users\Usuario\AppData\Roaming\Apple Computer\MobileSync\Backup\{UDID}.
Mac OS	~/Library/Application Support/MobileSync/Backup/{UDID}.

5.2 Iphone Analyzer [34].

Es una herramienta de open source que trabaja principalmente con las copias de seguridad que realiza iTunes o software de terceros, la interfaz gráfica facilita la investigación en un formato legible. *Iphone Analyzer* es multiplataforma (MAC, Linux, Windows), Santoku tiene instalada la aplicación.

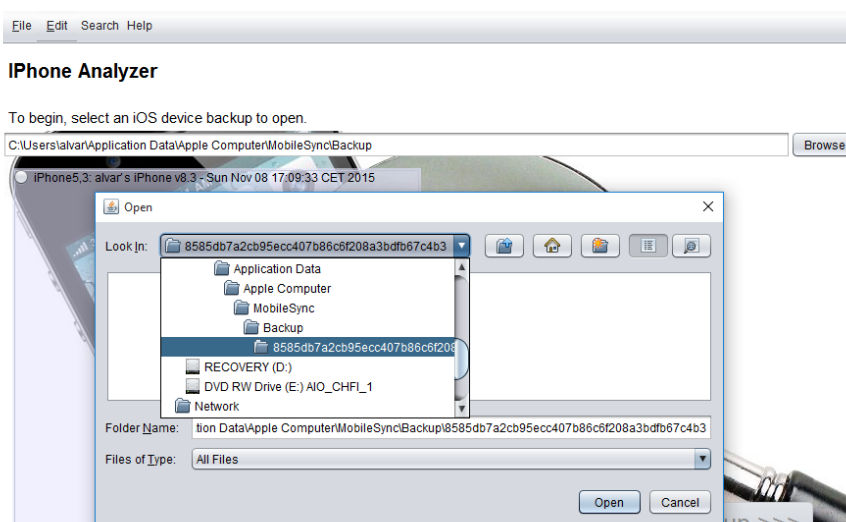


Figura 5.5: Iphone Analyzer copia de seguridad de iOS en Windows.

La pestaña *Boormarks* es la utilidad que proporciona una interfaz con relativa facilidad para analizar archivos de gran importancia en la investigación como pueden ser: la libreta de direcciones con la lista de todos los contactos, el mapa de ubicación y los *GSM* recientes, el acceso *WIFI* puntos que proporcionan una historia básica de *geo-localizacion*, los mensajes de correo, mensajes de texto, llamadas de voz *entrantes-salientes*, las imágenes almacenadas.

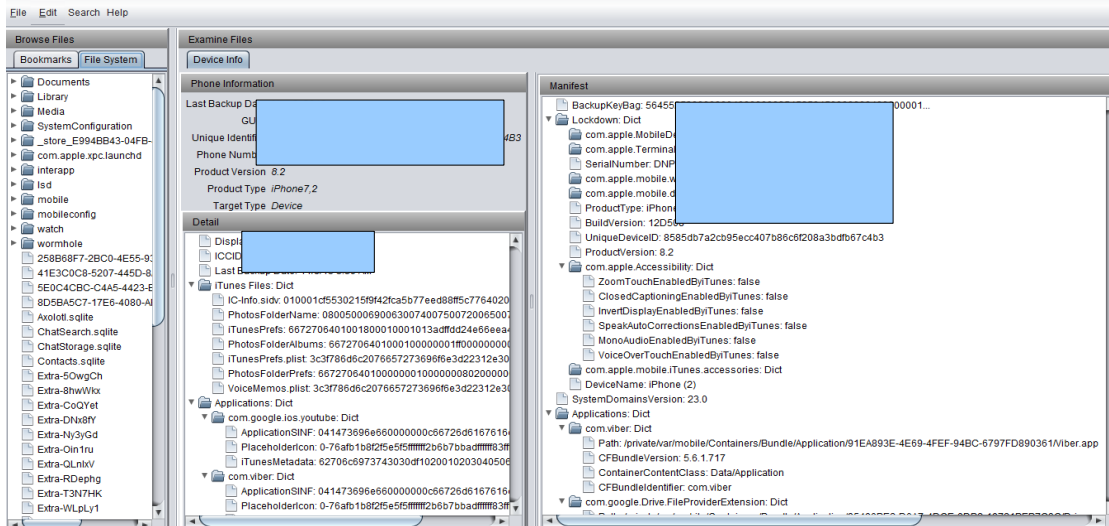


Figura 5.6: *iPhone Analyzer* estructura en árbol de la copia de seguridad de iOS.

Proporciona en su interfaz el sistema de archivos en forma de árbol, de esta manera se consigue seleccionar los directorios o abrir archivos de forma intuitiva. Los principales directorios en iOS son: documents, library, media, system configuration, sin embargo los archivos de mayor interés almacenan información en las bases de datos de SQLite que utiliza como parte integral de la aplicación.

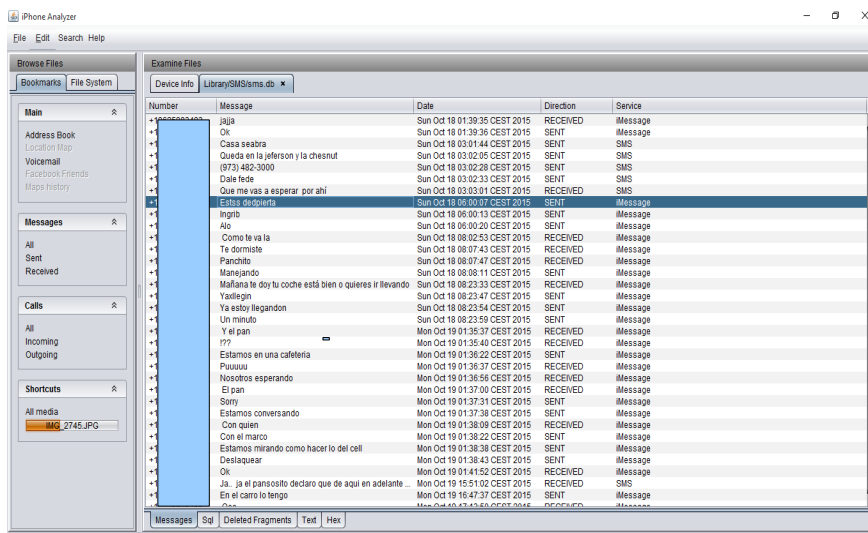


Figura 5.7: *iPhone Analyzer* análisis de mensajes.

Como desventaja se puede decir que esta aplicación carece de utilidades para generar informes, el analista realiza el trabajo manualmente lo que puede generar retrasos en la investigación.

5.4 DS

Es un software comercial desarrollado por la empresa Paraben y diseñado para exámenes forenses con prioridad en dispositivos móviles, incluye herramientas de adquisiciones lógicas, físicas, contraseñas y sistemas de archivos de una manera sencilla. Permite niveles de investigación avanzado, análisis de aplicaciones, recuperación de datos borrados, características para localizar los datos del GPS, comparación de cambios que surge en el dispositivo con el paso del tiempo, importación de copias de seguridad, e informes completos.



Figura 5.8: Pantalla inicial de DS.

Con DS se inicia con la creación, el siguiente paso es elegir la adquisición para un dispositivo físico o importar se desde el *backup*.

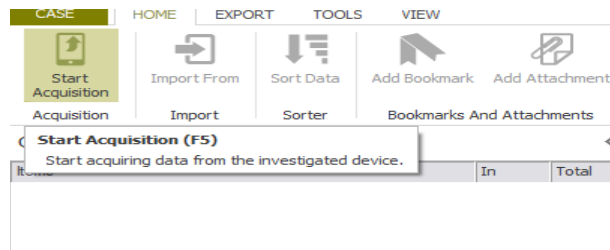


Figura 5.9: Adquisición física.

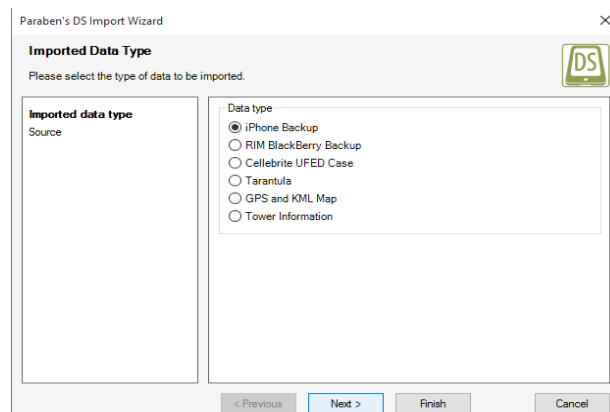


Figura 5.10: Adquisición desde el backup de IOS.

DS presenta una estructura en forma de árbol para el recorrido de archivos o carpetas, lo que facilita al analista la investigación, además permite generar automáticamente reportes de alta calidad.

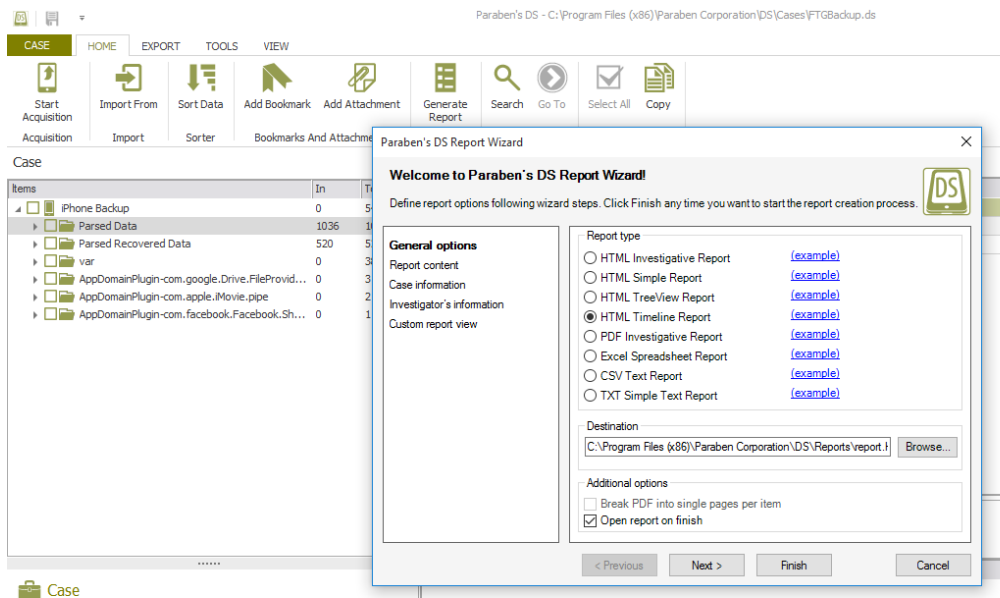


Figura 5.11: Generar informes con DS.

En el siguiente capítulo se estudia el uso de las herramientas Autopsy y FOCA, que también son de utilidad en sistemas iOS.

Capítulo 6: Análisis Forense en dispositivos Android.

6.1 Adquisición de la evidencia.

6.1.1 Copia bit a bit

En los sistemas Android, es común encontrar los puntos de montaje habituales a los bloques *MTD* [35](*Memory Technology Devices*). Los puntos de montaje para system, data, caché están asociados a distintos mtdbloks en */dev/block*. Ver figura 4.2 y 4.3.

```
root@Aquaris_E5:/sdcard # df
Filesystem      Size      Used      Free      Blksize
/dev            445.5M    132.0K    445.3M    4096
/sys/fs/cgroup  445.5M    12.0K     445.4M    4096
/mnt/asec       445.5M    0.0K     445.5M    4096
/mnt/obb        445.5M    0.0K     445.5M    4096
/system         1.5G     843.3M    644.5M    4096
/data           4.4G     4.3G     49.6M     4096
/cache          991.9M    1.5M     990.4M    4096
/persist        27.5M    112.0K    27.4M     4096
/firmware       64.0M    40.9M    23.0M    16384
/mnt/shell/emulated 4.3G     4.3G     0.0K     4096
/storage/emulated/legacy 4.3G     4.3G     0.0K     4096
/storage/emulated 445.5M    0.0K     445.5M    4096
/storage/emulated/0 4.3G     4.3G     0.0K     4096
/storage/emulated/legacy 4.3G     4.3G     0.0K     4096
root@Aquaris_E5:/sdcard #
```

Figura 6.1: Comando df en Android.

Por tanto, para realizar la copia bit a bit como primer paso es verificar que parte del sistema se va a realizar la copia, se obtiene valiosa información de system, data, caché y sd card. Con la herramienta dd se ejecuta el comando:

```
if=/dev/block/bootdevice/by-name/system of=/sdcard/system.dd bs=1M
```

De la misma manera se realiza la copia de *data*, *caché* y *sd card*, con el comando pull desde el ordenador se extrae la imagen para su posterior análisis.

```
adb pull /sdcard/system.dd
```

```
root@Aquaris E5:/ # dd if=/dev/block/bootdevice/by-name/system of=/sdcard/syst
3145728+0 records in
3145728+0 records out
1610612736 bytes transferred in 1202.456 secs (1339435 bytes/sec)
root@Aquaris E5:/ # exit
255|shell@Aquaris E5:/ $ exit
root@PCMarco:/home/marcoalvarez# adb pull /sdcar/system.dd
remote object '/sdcard/system.dd' does not exist
root@PCMarco:/home/marcoalvarez# adb pull /sdcard/system.dd
root@PCMarco:/home/marcoalvarez#
```

Figura 6.2: Copia bit a bit system, extracción de la imagen.

Se calcula el hash md5 para el archivo desde linux con el comando

```
md5sum system.dd
```

```
70a61d5780117592fe5ead1d209912b0 system.dd
```

```
root@osboxes:~/Desktop# md5sum system.dd
70a61d5780117592fe5ead1d209912b0 system.dd
root@osboxes:~/Desktop#
```

Figura 6.3: Cálculo de hash md5 archivo system.dd.

6.2 AFLogical OSE.

Permite al examinador extraer datos de gran importancia desde un dispositivo Android; los datos que se pueden extraer son: logs de llamadas, números de teléfonos de contactos, mensajes (MMS, SMS, MMSParts)

Para realizar la prueba de concepto en Android, USB debugging debe estar activado.

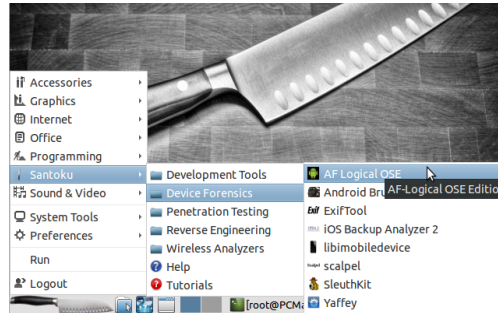


Figura 6.4: AF Logical OSE en Santoku.

El comando `adb devices`, verifica si el sistema reconoce el dispositivo, en caso contrario se procede a instalarlos drivers de acuerdo al dispositivo a investigar.

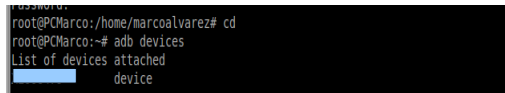


Figura 6.4: Comando adb devices.

A continuación, se extrae la información con el comando `aflogical-ose`, se aprecia que la herramienta inicia la extracción de los datos, la carpeta destino es `/root/AFLogical Ose` y los archivos tienen el formato CSV.

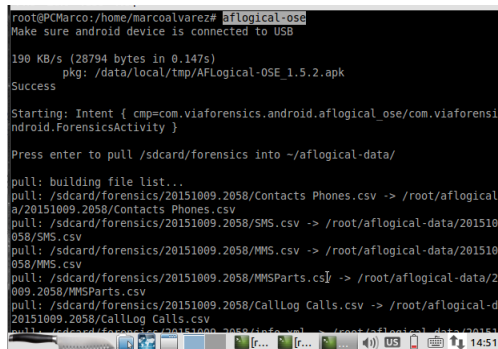


Figura 6.5: Extracción de información de un dispositivo Android con aflogical-ose.

Con esta información, el analista forense procede a investigar examinando los datos extraídos.

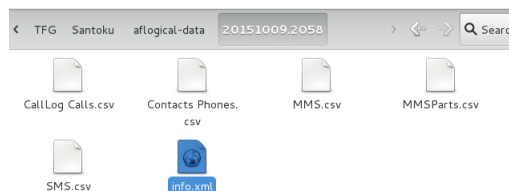


Figura 6.6: Información extraída con aflogical-ose.

La siguiente tabla siguiente especifica la información que se obtiene en cada uno de los procedentes del dispositivo.

Contacts Phones.csv	Contactos almacenados.
CallLog Calls.csv	Llamadas efectuadas-recibidas, fecha y tiempo de duración.
MMS.csv	Mensaje multimedia.
SMS.csv	Mensajes de texto.

```

info.xml
<android-forensics>
<date-time>20151009.2058</date-time>
<IMSI>214075506517277</IMSI>
<IMEI-MEID>8934072100157395354</IMEI-MEID>
<phone-type>
<MSISDN-MDN></MSISDN-MDN>
<ICCID>8934072100157395354</ICCID>
<build>
<version.release>4.4</version.release>
<version.sdk>19</version.sdk>
<version.incremental>1.8.4_20150727-1246-8G</
version.incremental>
<board>msm8916</board>
<brand>bq</brand>
<device>Aquaris_E5</device>
<display>1.8.4_20150727-1246-8G</display>
<fingerprint>bq/Aquaris_E5/Aquaris_E5:4.4.4/
KTU84P/1437972658:user/release-keys</fingerprint>
<host>ubuntu116</host>
<id>KTU84P</id>

```

Figura 6.7: Información del archivo info.xml

id	date	date_sent	protocol	read	status	type	reply_path_present	subject	body
32	1443790366918	1443790362000	63	1	-1	1	0	BUZON MOVISTAR vie, 02 - 14:52 1 mensaje nuevo de [redacted] Para escucharlo, llame gratis al 123	
43	1443789547363	1443789539000	0	1	-1	1	0	LLAMADAS PERDIDAS vie, 02 - 14:38 1 llamada de [redacted] Si desea devolver la llamada, pulse la tecla verde de su movil	
32	1443784021690	1443784020000	63	1	-1	1	0	BUZON MOVISTAR vie, 02 - 13:06 1 mensaje nuevo de [redacted] Para escucharlo, llame gratis al 123	
43	1443783956927	1443783955000	0	1	-1	1	0	Perdígale su buzón facilmente llamando gratis al 22126 LLAMADAS PERDIDAS vie, 02 - 13:05 1 llamada de [redacted] Si desea devolver la llamada, pulse la tecla verde de su movil	

Figura 6.8: Información del archivo SMS.csv.

Para finalizar se desinstala la aplicación con el comando:

```
adb uninstall com.viaforensics.android.aflogical_ose
```

6.3 Autopsy.

Es una herramienta de open source para Análisis Forense Digital, diseñado para un uso fácil e intuitivo, permite analizar de manera eficiente discos duros o sistemas de archivos de *smartphones*. Posee una arquitectura plug-in que permite encontrar módulos adicionales o desarrollar módulos personalizados en *Java* o *Python*.

Kali Linux, es un sistema operativo diseñado para auditoría de la Seguridad Informática, tiene pre-configurado *Autopsy* para su uso, esta es una buena alternativa sobre todo para el análisis forense en discos duros.

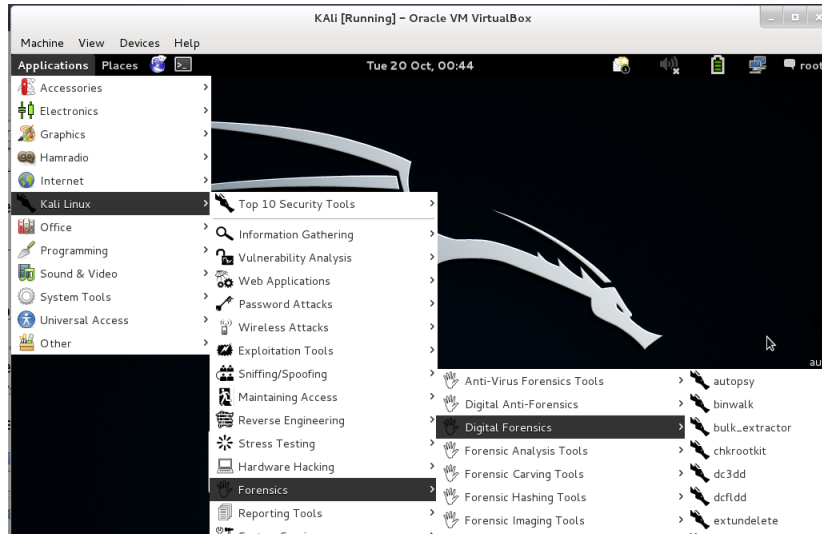


Figura 6.9: Autopsy en Kali Linux.

La interfaz de *Autopsy* en *Linux* se está diseñada para trabajar en un navegador web, la *url* para ejecutar *Autopsy* de forma local es: `http://localhost:9999/autopsy`



Figura 6.10: Interfaz de *Autopsy* en el navegador *Iceweasel*.

En esta prueba de concepto con *Autopsy* se calcula el *hash MD5* de la copia bit a bit *system.dd*, para que la prueba sea válida debe coincidir con el hash que se calculó al realizar la copia.

`70a61d5780117592fe5ead1d209912b0.`

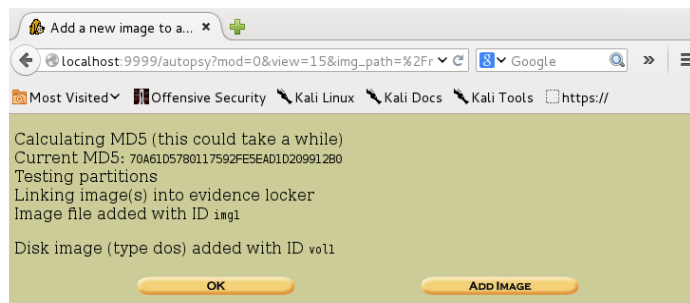


Figura 6.11: *Cálculo* del hash md5 con *Autopsy Browser*.

A más, la versión actualizada de Autopsy (version 3) se ejecuta bajo Windows, para sistemas operativos Linux y Os existe la (version 2), pero tiene como desventaja que no soporta algunos sistemas de archivos.



Figura 6.12: Nuevo caso Autopsy en Windows.

Para iniciar la investigación se crear un nuevo caso, con datos de interés como número, investigador, se agrega la imagen de la copia bit bit y de forma automática Autopsy calcula los hash de los documentos.

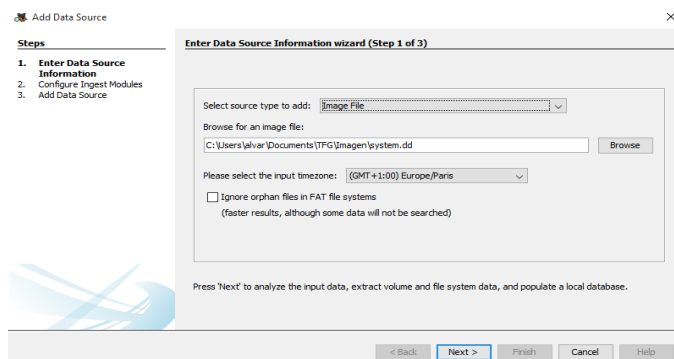


Figura 6.13: Imágen system.dd a investigar.

Autopsy presenta una estructura en forma de árbol que permite navegar por los directorios y carpetas, a su vez, permite el análisis de metadatos y la recuperación de archivos borrados indispensables en un análisis.

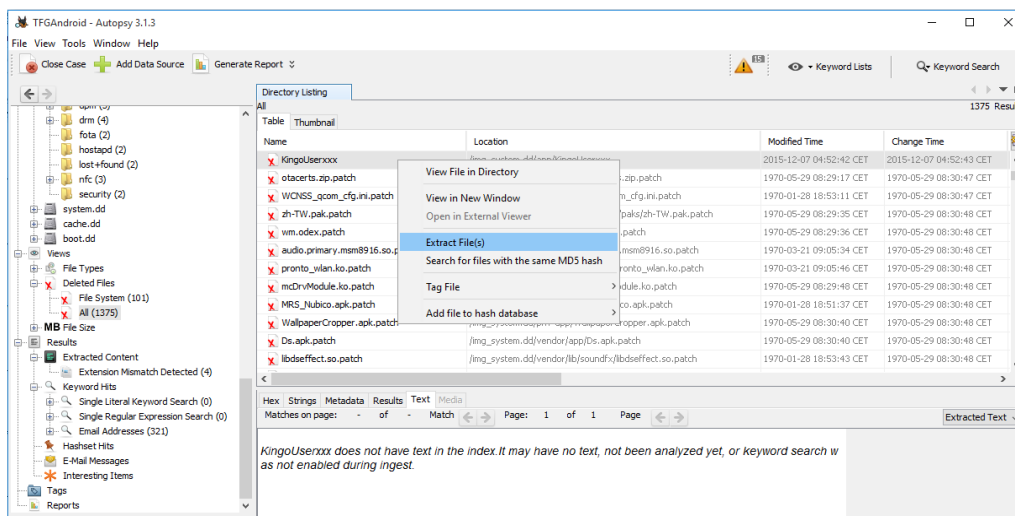


Figura 6.14: Recuperación de archivos eliminados.

6.4 Andriller.[36]

Es una aplicación de uso comercial que contiene una serie de herramientas forenses para dispositivos móviles *Android*. Realiza lectura, análisis forense, adquisición no destructiva de los dispositivos, además, posee otras características, como: Lockscreen para craqueo para el patrón (*passcode*, *el código PIN* o *contraseña*); decodificadores personalizados para datos de aplicaciones de Android y iOS, bases de datos para las comunicaciones de decodificación.

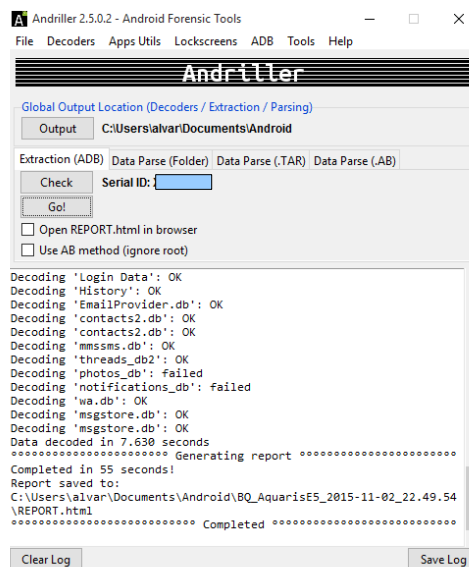


Figura 6.15: Extracción de datos de un dispositivo Android.

Andriller genera informes en formato (.xlsx\ HTML y Excel), con respecto a la información del dispositivo, análisis de contactos, mensajes de comunicación, geolocalización de datos, registros de eventos (*aplicaciones de Redes Sociales, Navegadores, Calendario.*); en conjunto con las base de datos de las aplicaciones desde las cuales se obtiene una cantidad información útil en la investigación.

Las bases de datos de las aplicaciones de mensajería (Whatsapp, Facebook, Twitter, etc.), son de gran importancia para verificar si existe algún delito por parte del usuario, Andriller permite obtener la información de manera fácil e intuitiva..

[WhatsApp Messages]
Total Items: 23,252

#	Number	Message	Time	Type
39489		Por futbol	2015-11-02 21:47:20 UTC+00:00	Sent
39488		Me preguntabn	2015-11-02 21:47:16 UTC+00:00	Sent
39487		Xd	2015-11-02 21:46:31 UTC+00:00	Inbox
39486		Perdón	2015-11-02 21:21:47 UTC+00:00	Sent
39485		Mexico 2-0	2015-11-02 21:21:38 UTC+00:00	Sent
39484		10-15 gradid	2015-11-02 21:19:31 UTC+00:00	Sent
39483		Temperatura?	2015-11-02 21:15:55 UTC+00:00	Inbox
39482		Está bien	2015-11-02 20:18:36 UTC+00:00	Sent
39481		MA's o menos	2015-11-02 20:18:32 UTC+00:00	Sent
39480		Como esta el tiempo x alli?	2015-11-02 18:57:22 UTC+00:00	Inbox
39479		O fas ara?	2015-11-02 18:57:12 UTC+00:00	Inbox
39478		A ver	2015-11-02 18:49:23 UTC+00:00	Sent
39477		Es	2015-11-02 18:48:33 UTC+00:00	Inbox
39476		Ya me contaras que tal ea	2015-11-02 18:48:32 UTC+00:00	Inbox
39475		Aveure	2015-11-02 18:17:43 UTC+00:00	Inbox
39474		Yaa	2015-11-02 18:17:34 UTC+00:00	Inbox
39473		Era de eso que hay que rellenar como 30 paginas	2015-11-02 18:15:53 UTC+00:00	Sent
39472		Ya que voy	2015-11-02 18:15:37 UTC+00:00	Sent
39471		A ver	2015-11-02 18:15:33 UTC+00:00	Sent
39470		Sii	2015-11-02 18:15:11 UTC+00:00	Inbox
39469		Cosas	2015-11-02 18:01:06 UTC+00:00	Inbox
39468		Para que entres tu tambien	2015-11-02 17:59:28 UTC+00:00	Sent
39467		Y a mirar que hacer	2015-11-02 17:59:19 UTC+00:00	Sent
39466		A ver	2015-11-02 17:59:11 UTC+00:00	Sent

Figura 6.16: Informe de Andriller a cerca de los mensajes de Whatsapp.

6.5 Análisis Forense de Base de Datos SQLite.

SQLite [37] fue creado por *Richard Hipp* como un proyecto de dominio público. Es una biblioteca que implementa bases de datos relacionales autónomas que utilizan la mayoría de las aplicaciones móviles como parte integral de las mismas, cuando se habilita todas las características de la biblioteca el tamaño en memoria de almacenamiento es inferior a 500Kb. La mayoría de aplicaciones utilizan base de datos de SQLite.

En la siguiente prueba de concepto se utiliza la base de datos de *WhatsApp*, el sistema de cifrado que se utiliza *crypto8*, por tanto el primer desafío es descifrar la base de datos, lo primero que se realiza es la extracción de el archivos, *msgstore.db.crypto8* que se encuentra en Android */sdcard/whatsapp/Databases*.

```
shell@Aquaris_E5:/sdcard/Whatsapp/Databases $ ls
msgstore-2015-12-07-1.db.crypto8
msgstore-2015-12-08-1.db.crypto8
msgstore-2015-12-09-1.db.crypto8
msgstore-2015-12-10-1.db.crypto8
msgstore-2015-12-11-1.db.crypto8
msgstore-2015-12-12-1.db.crypto8
msgstore-2015-12-13-1.db.crypto8
msgstore-2015-12-14-1.db.crypto8
msgstore.db.crypto8
shell@Aquaris_E5:/sdcard/Whatsapp/Databases $ exit
root@PCMarco:/home/marcoalvarez# adb pull /sdcard/Whatsapp/Databases/msgstore.db
846 KB/s (4229267 bytes in 4.876s)
root@PCMarco:/home/marcoalvarez#
```

Figura 6.16: Comando pull extracción del archivo *msgstore.db.crypto8*.

Aparte de la base de datos, para descifrar se necesita el archivo *key* que se encuentra en la carpeta */data/data/com.whatsapp/files*.

```
255 shell@Aquaris_E5:/data $ exit
root@PCMarco:/home/marcoalvarez# adb pull /data/data/com.whatsapp/files/key
3 KB/s (150 bytes in 0.051s)
root@PCMarco:/home/marcoalvarez#
```

Figura 6.16: Comando pull extracción del archivo *msgstore.db.crypto8*.

Se puede utilizar scripts o herramientas que permitan descifrar la base de datos. Para el ejemplo se utiliza *Andriller*.

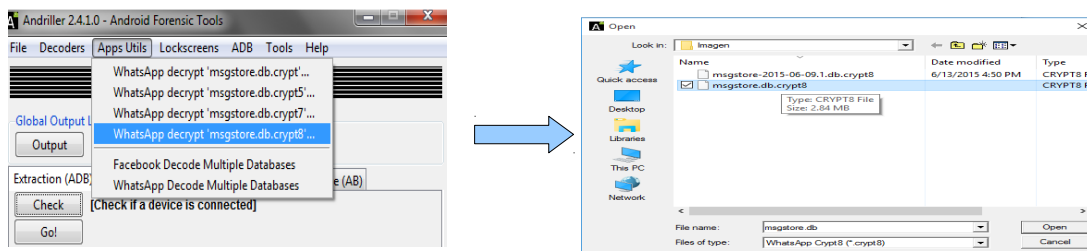


Figura 6.17: Descifrar base de datos WhatsApp con Andriller.

La aplicación solicita la clave *key* para descifrar la base de datos.

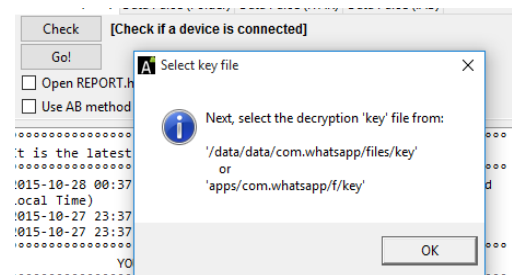


Figura 6.18: Descifrar base de datos WhatsApp con la clave KEY.

6.5.1 Sqliteman

Para administrar bases de datos SQLite existen diferentes aplicaciones, un analista forense necesita herramientas de visualización, Santoku ofrece *Sqliteman* que posee una interfaz gráfica y ejecuta instrucciones SQL.

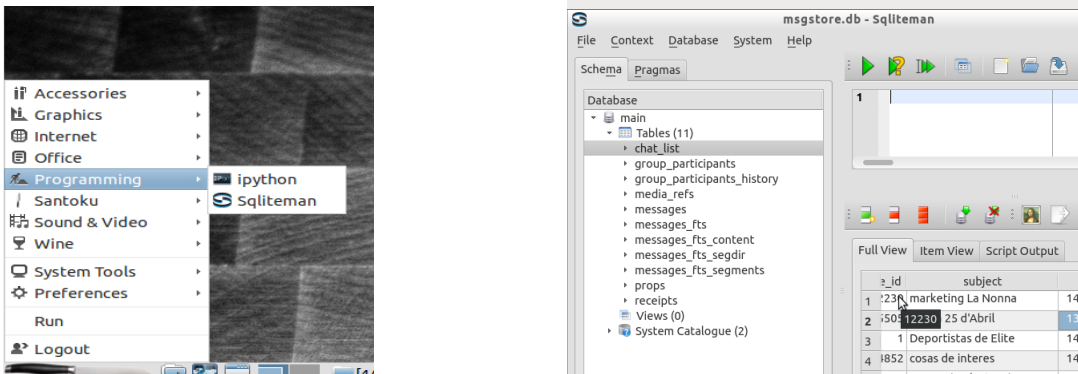


Figura 6.19: *Sqliteman* en Santoku.

6.5.2 DB Browser SQLite.

DB Browser SQLite [38], es una aplicación de *open source* para administrar análisis de base de datos SQLite con características similares descritas en *Sqliteman*.

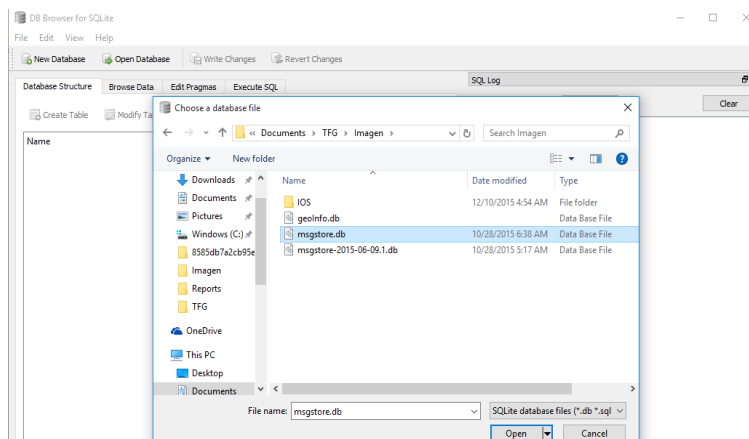


Figura 6.20: Análisis de la base de datos de WhatsApp con *DB Browser for SQLite*.

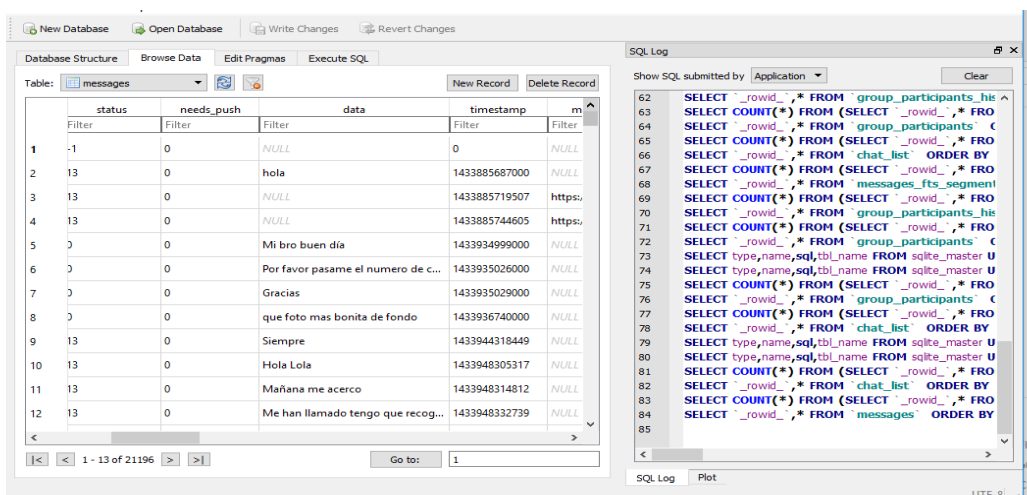


Figura 6.20: Análisis de los mensajes de WhatsApp con *DB Browser for SQLite*.

Cuando se recupera la información de la base de datos, el analista puede trabajar en la investigación.

6.6 Análisis de Metadatos.

Los metadatos es información relativa a ficheros, como el autor, fecha de creación o modificación, información oculta etc. En los dispositivos móviles es de gran utilidad para el análisis de documentos especialmente fotografías, se puede obtener marca y modelo de dispositivos, resolución, coordenadas GPS etc.

6.6.1 FOCA.

Eleven Paths define *FOCA* [39] (*Fingerprinting Organizations with Collected Archives*) como una herramienta que se utiliza principalmente para encontrar *metadatos* e información oculta en los documentos. Los documentos que esta herramienta es capaz de analizar son muy variados, los más comunes los archivos de *Microsoft Office*, *Open Office*, o ficheros *PDF*, aunque también analiza ficheros de *Adobe InDesign*, o *svg*. Existe la posibilidad de añadir ficheros locales para extraer la información *EXIF* de archivos gráficos. Con todos los datos extraídos de todos los ficheros, *FOCA* va a unir la información, tratando de reconocer qué documentos han sido creados desde el mismo equipo, qué servidores y clientes se pueden inferir de ellos.

Para analizar los archivos basta con arrastrar hacia la herramienta *FOCA* y extraer todos los *metadatos*.

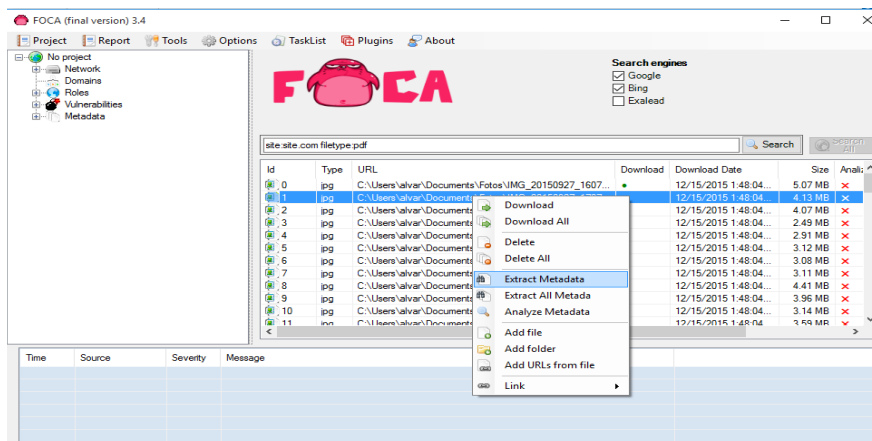


Figura 6.20: Extracción de los *metadatos* con *FOCA*.

A continuación se procede al análisis de de cada uno de los archivos.

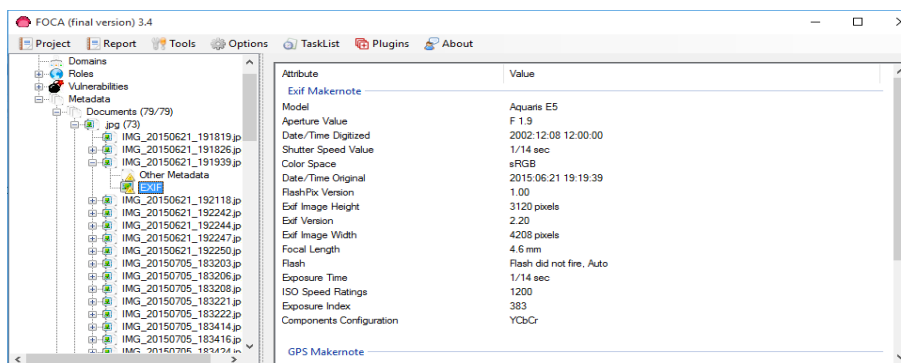


Figura 6.20: Metadatos de una imagen.

Capítulo 7: Informe Pericial.

Los Analistas Forenses Digitales son personas ajenas a un proceso judicial, poseen conocimientos científicos que les faculta para realizar un informe como medio de prueba. Los *Peritos Forenses* tienen que ser designados previamente para formar parte de una investigación digital.

Se puede establecer algunos criterios para realizar informes periciales[40]

Organizar la información

Con la información adquirida en las fases anteriores se identifica los datos más importantes, que permita llegar a determinar conclusiones.

Desarrollo del informe

Propósito.

Definir el objetivo de la investigación el personal a quién va dirigido.

Autor.

Datos del Autor(es), e información de contacto.

Incidente.

Demostrar los sucesos ocurridos de forma clara pero formal, sin utilizar un lenguaje técnico para que el personal sin conocimientos técnicos (jueces, abogados, jurado, fiscales) entienda cómo, cuándo y el impacto de los sucesos ocurridos.

Pruebas.

Especificación de las evidencias, la forma en que se adquirió, el personal que incautó las evidencias.

Detalles.

Información de la metodología y datos analizados.

Conclusión y Justificación

Documentar y justificar en base a los procesos de la investigación las conclusiones adquiridas, de tal modo que el personal que interviene en un proceso judicial pueda utilizar el informe para defender o acusar si ha cometido o no un delito en base a las leyes vigentes en la sociedad.

Conclusiones.

En el Análisis Forense Digital no se puede establecer una metodología estricta a seguir, esto conlleva a que cada Investigador utilice técnicas y habilidades que se puede adquirir en base a la experiencia. Sin embargo, esta investigación pretende dar algunas pautas que pueden servir de guía para el analista que desea realizar trabajos forenses, cada una de las fases descritas no solo se pueden utilizar para dispositivos móviles sino para cualquier dispositivo digital.

Las normas: ISO/IEC 27037, RFC: 3227, UNE 71505, UNE 71506, se pueden utilizar como una base guía de proceso de análisis. Estas normas establecen métodos y procesos a seguir pero se debe adaptar de acuerdo al sistema de legislación vigente en cada país e ir adaptando a las leyes y normas de cada uno de ellos.

Las empresas que ofrecen sus *Sistemas Operativos* actualizan constantemente para corregir vulnerabilidades que salen a la luz, por tanto, los Analistas Forenses se enfrentan a constantes desafíos porque un cierto método que funciona de manera eficaz para una versión probablemente no sea el correcto en otros dispositivos con una versión diferente.

Los productos de uso comercial contienen múltiples herramientas que automatizan el análisis, sin embargo, las licencias tienen un coste elevado lo que conlleva a realizar cambios en la planificación con herramientas diferentes que ofrecen período de prueba pero con la desventaja que no ofrecen toda la capacidad. De otro modo, si se utilizan herramientas de open source el proceso de investigación requerirá más tiempo debido a que en el laboratorio se debe instalar aplicaciones de acuerdo a sus funcionalidades.

Trabajo Futuro.

La aplicación de técnicas científicas permiten el análisis exhaustivo de un dispositivo con contenido digital, además el analista debe tener conocimientos avanzados en cuanto a la arquitectura del sistema en conjunto con técnicas de auditoría y seguridad informática.

En la actualidad existen millones de dispositivos y sistemas con arquitecturas diferentes, por tanto, un trabajo futuro es la investigación en otros dispositivos digitales que permita dar un enfoque a cerca de métodos a utilizar.

Bibliografía

- 1: Norma: SO/IEC 27037**, Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence, 2012, [En línea], http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381.
- 2: RFC: 3227**, Guidelines for Evidence Collection and Archiving, 2002, [En línea] <http://www.rfc-base.org/txt/rfc-3227.txt>.
- 3: Norma: UNE 71505**, Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales, 2013, [En línea] <http://www.aenor.es/aenor/inicio/home/home.asp>.
- 4: Norma: UNE 71506**, Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas, 2013, [En línea] <http://www.aenor.es/aenor/inicio/home/home.asp>.
- 5: Universal Integrated Circuit Card**, [En línea] <https://es.wikipedia.org/wiki/UICC>.
- 6: GET ARRAY**, [En línea] https://es.wikipedia.org/wiki/Gate_array.
- 7: Oxigen Forensic**, Oxigen Forensic Suite, [En línea] <http://www.oxygen-forensic.com/es/>
- 8: Paraben**, DS7, [En línea] <https://www.paraben.com/device-seizure.html>.
- 9: GUIDANCES SOFTWARE**, Encase Forensic, [En línea], https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r.
- 10: Aviv, A.; Katherine, G.; Mosson, E.; Blaze, Matt.; Smith, J.** Smudge Attacks on Smartphone Touch Screens, [En línea] https://www.usenix.org/legacy/events/woot10/tech/full_papers/Aviv.pdf.
- 11: National Institute of Standards and Technology**, National Vulnerability Database, [En línea] <https://web.nvd.nist.gov/view/vuln/search>.
- 12: National Institute of Standards and Technology**, Computer Forensic Tool Catalog, [En línea] <http://toolcatalog.nist.gov/index.php>.
- 13: National Institute of Standards and Technology**, Vulnerability Summary for CVE-2014-4451, 2014, [En línea] <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4451>.
- 14: National Institute of Standards and Technology**, Vulnerability Summary for CVE-2013-0979, 2014, [En línea] <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0979>.
- 15: National Institute of Standards and Technology**, Vulnerability Summary for CVE-2013-0981, 2013, [En línea] <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0981>.
- 16: National Institute of Standards and Technology**, Vulnerability Summary for CVE-2014-1273, 2014, [En línea] <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1273>.
- 17: National Institute of Standards and Technology**, Vulnerability Summary for CVE-2014-1272, 2014, [En línea] <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1272>.
- 18: TaiG V2.4.4**, [En línea] <http://www.taig.com/en/>.
- 19: Pangu, 2015**, [En línea] <http://en.pangu.io/>.
- 20: Android Debug Bridge**, [En línea] <http://developer.android.com/intl/es/tools/help/adb.html>.
- 21: MWR InfoSecurity**, drozer User Guide, 2015, [En línea] https://labs.mwrinfosecurity.com/system/assets/502/original/mwri_drozer-users-guide_2013-07-25.pdf.
- 22: Módulos para drozer**, [En línea] <https://github.com/mwrlabs/drozer-modules>
- 23: Bradberry, D.; Erasmus, T.** [En línea] <https://github.com/mwrlabs/drozer-modules/blob/master/metall0id/root/cmdclient.py>.
- 24: Bradberry, D.; Erasmus, T.** "Exploit the setuid-root binary at /system/bin/sync_agent on certain ZTE devices to gain a root shell, [En línea] <https://github.com/mwrlabs/drozer-modules/blob/master/metall0id/root/ztesyncagent.py>
- 25: National Institute of Standards and Technology**, Vulnerabilidad CVE-2014-3153, 2014, [En línea] <https://github.com/timwr/CVE-2014-3153>.
- 26: TowelRoot**, [En línea] <https://towelroot.com/>

- 27: Joshua, W.** Exploited by rewriting a FrameworkCommand object making the runCommand point to our first ROP gadge, [En línea]
<https://github.com/revolutionary/zergRush/blob/master/zergRush.c>
- 28: Psneuter the Android property service**, [En línea] <https://github.com/tmzt/g2root-kmod/tree/master/scotty2/psneuter>.
- 29: BQTV**, Reinstalación del firmware para smartphone bq Aquaris / Aquaris E, [En línea] <https://www.youtube.com/watch?v=YldQuDalmdA>.
- 30: BQ**, Mibqyyo-Descargas, [En línea] <http://www.mibqyyo.com/descargas/>
- 31: ACCESDATA**, Forensic Toolkit (FTK), [En línea], <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>.
- 32: BlackLight**, [En línea], <https://www.blackbagtech.com/software-products/blacklight-6/blacklight.html>.
- 33: Compelson**, MOBILedit, [En línea], <http://www.mobiledit.com/forensic>
- 34: iPhone Analyzer**, [En línea], <http://www.crypticbit.com/zen/products/iphoneanalyzer>.
- 35: Memory Technology Devices**, [En línea], https://en.wikipedia.org/wiki/Memory_Technology_Device.
- 36: Andriller**, [En línea], <http://andriller.com/>
- 37: SQLite**, [En línea], <https://www.sqlite.org/>
- 38: DB Browser for SQLite**,
- 39: Eleven Paths**, FOCA - Fingerprinting Organizations with Collected Archives, [En línea], <https://www.elevenpaths.com/labstools/foca/index.html>
- 40: Ayers, R; Brothers , S; Jansen, W. (2014)**. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 . Revision 1. [En línea] <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf> Pag 55-57.

Libros.

- ALONSO ,C.; RAMOS, A.** (2013). Hacking de dispositivos IOS: Iphone & Ipad. Madrid: OxWORD.
- Lázaro, F; (2013)**. Introducción a la Informática Forense. Madrid. RA-MA.
- Chell, D; Erasmus, T; (2015)**. The Mobile Application Hacker's Handbook. Jhon Wiley & Sonc INC. Indianápois. WILEY.
- Brooks, C; (2015)**. Computer Hacking Forensic Investigator Certificationk. MacGrawHill Education.
- ALONSO ,C.; RAMOS, A.** (2013). Pentesting con FOCA. Móstoles - Madrid: OxWORD.

Artículos.

- Ayers, R; Brothers , S; Jansen, W. (2014)**. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 . Revision 1.
- Aviv, Adam J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; Smith, Jonathan M.** Smudge Attacks on Smartphone Touch Screens. Revision Department of Computer and Information Science - University of Pennsylvania.

Anexos.

1: Instalación de Drozer.

Para utilizar el framework se necesita:

Java Development Kit (JDK)

Python 2.7.

Android SDK.

Adb.

Java

Esta prueba de concepto se realiza por medio del Sistema Operativo Santoku, porque existen los requisitos y herramientas se encuentran instaladas en previamente.

Para descargar el Framework Drozer hay que dirigirse a:

<https://www.mwrinfosecurity.com/products/drozer/community-edition/>



Figura 8.1: Descarga oficial de Drozer.

A continuación se procede a instalar Python con el comando: `apt-get install python-setuptools`

```
root@PCMarco:/home/marcoalvarez/Downloads# apt-get install python-setuptools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
gir1.2-appindicator3-0.1 gir1.2-json-1.0 gir1.2-timzone-1.0
gir1.2-xkl-1.0 libtimzone-1 python3-cairo python3-gi-cairo
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
python-setuptools
```

Figura 8.1.1: Instalación de Python.

Para instalar drozer se debe ubicar en la carpeta donde se realizó la descarga previamente e instalar el paquete. Se ejecuta el comando: `dpkg -i drozer_2.x.x.deb`

```
root@PCMarco:/home/marcoalvarez/Downloads# ls
drozer_2.3.4.deb
root@PCMarco:/home/marcoalvarez/Downloads# dpkg -i drozer_2.3.4.deb
(Reading database ... 254278 files and directories currently installed.)
Preparing to unpack drozer_2.3.4.deb ...
Unpacking drozer (2.3.4) over (2.3.3) ...
Setting up drozer (2.3.4) ...
root@PCMarco:/home/marcoalvarez/Downloads#
```

Figura 8.1.2: Instalación de Drozer.

o a su vez : `easy_install ./drozer-2.x.x-py2.7.egg`

```

root@PCMarco:/home/marcoalvarez/Downloads# ls
agent.apk      drozer_2.3.4.deb      drozer-2.3.4.tar.gz  LICENSE
CONTRIBUTORS drozer-2.3.4-py2.7.egg  INSTALLING           README.md
root@PCMarco:/home/marcoalvarez/Downloads# easy_install ./drozer-2.3.4-py2.7.egg
error: Not a URL, existing file, or requirement spec: './drozer-2.3.4-py2.7.egg'
root@PCMarco:/home/marcoalvarez/Downloads# easy_install ./drozer-2.3.4-py2.7.egg
Processing drozer-2.3.4-py2.7.egg
creating /usr/local/lib/python2.7/dist-packages/drozer-2.3.4-py2.7.egg
Extracting drozer-2.3.4-py2.7.egg to /usr/local/lib/python2.7/dist-packages
Adding drozer 2.3.4 to easy-install.pth file
Installing drozer-complete script to /usr/local/bin
Installing drozer script to /usr/local/bin

Installed /usr/local/lib/python2.7/dist-packages/drozer-2.3.4-py2.7.egg
Processing dependencies for drozer==2.3.4
Searching for protobuf==2.4.1
Reading https://pypi.python.org/simple/protobuf/
Best match: protobuf 2.4.1
Downloading https://pypi.python.org/packages/source/p/protobuf/protobuf-2.4.1.tar.gz#md5=72f5141d20ab1bcae6b1e00acfb1068a

```

Figura 8.1.3: Instalación de Drozer.

Para verificar la instalación, en la terminal se ejecuta: drozer

```

root@PCMarco:/home/marcoalvarez/Downloads# drozer
usage: drozer [COMMAND]

Run `drozer [COMMAND] --help` for more usage information.

Commands:
  console  start the drozer Console
  module  manage drozer modules
  server   start a drozer Server
  ssl     manage drozer SSL key material
  exploit  generate an exploit to deploy drozer
  agent   create custom drozer Agents
  payload  generate payloads to deploy drozer

```

Figura 8.1.4: Comando que verifica la instalación de Drozer.

Instalación del Agente Drozer.

El agente de Drozer está incluido en un archivo Android Package (.apk) en las distribuciones de drozer. Se puede instalar en el dispositivo usando Android Debug Bridge (adb):

\$ adb install agent.apk

```

root@PCMarco:/home/marcoalvarez/Downloads# adb devices
List of devices attached
XE006479      device

root@PCMarco:/home/marcoalvarez/Downloads# adb install agent.apk
580 KB/s (633111 bytes in 1.064s)
pkg: /data/local/tmp/agent.apk
Success

```

Figura 8.2: Instalación del Agente Drozer en el dispositivo.

Terminada la instalación de Drozer en el ordenador y el agente en el dispositivo, es necesario conectar los dos dispositivos. Para empezar se debe configurar un puerto para que el socket del ordenador se pueda conectar con el socket del dispositivo android. El puerto por defecto es el 31415.

\$ adb forward tcp:31415 tcp:31415

\$ drozer console connect .

```

marcoalvarez@PCMarco:~$ adb forward tcp:31415 tcp:31415
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
marcoalvarez@PCMarco:~$ drozer console connect
Selecting f789e211e0eal5bd ( bq Aquaris E5 4.4.4 )

..
..o..
..a..
..ro..idsnemesisand..pr
..rotectorandroidsname
..sisandprotectorandroids+
..nemesisandprotectorandroids:
..emesisandprotectorandroidsnames:
..isandp..rotectorandro..idsnem
..isisandp..rotectorandroid..snemisis
..andprotectorandroidsnemesisandprotec
..torandroidsnemesisandprotectorandroid
..snemesisandprotectorandroidsnemesisan:
..dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.4)
dz>

```

Figura 10.2.3: Conexión del socket del ordenador con socket del dispositivo.

2: Compilación de los exploit zergRush y Psneuter.

Si se desea compilar estos exploit directament, se puede realizar desde Santoku con la utilización de adb,compilando los archivos.c, y a continuación ejecutar los exploits.

ZergRush.

```
gcc zergRush.c -o zergRush -ldiskconfig -lcutils  
adb shell /data/local/tmp/ zergRush  
/data/local/tmp/ ./zergRush
```

Psneuter.

```
gcc psneuter.c -o psneuter  
adb shell /data/local/tmp/psneuter  
adb push psneuter /data/local/tmp  
sleep 5  
adb shell
```

3: INFORME PERICIAL.

DELITOS CONTRA LA SALUD DE LAS PERSONAS

ANTECEDENTES.

El Juzgado de Instrucción nº 4 de Tarragona instruyó Diligencias Previas con el nº 849/2015 y una vez concluidas las remitió a la Audiencia Provincial de Tarragona, Sección Séptima, que con fecha 01 de octubre de 2015, dictó orden de investigación por denuncias por fuertes olores que induce a una supuesta plantación y tráfico de estupefacientes en el Piso ubicado en la CALLE XXXXX de Salou: " Se declara probado que MARCO, mayor de edad y sin antecedentes penales , viven en la CALLE XXXXX , NUM XX de la localidad de Salou, portal en el que recaían sospechas que podían existir personas dedicadas a la plantación y tráfico de sustancias estupefacientes, por lo que autorizada una entrada y registro por el Juzgado de Instrucción, el día 10 de octubre de 2015. La Policía Local de Salou y Mossos d'Esquadra proceden el allanamiento del domicilio, y a la detención de Marco y Francisco, en el domicilio no se encontró ningún indicio de plantación o material para un supuesto tráfico de estupefacientes, sin embargo, se intervienen dos dispositivos móviles para la investigación de supuestos delitos. El primer teléfono BQ B5 4G y el segundo un dispositivo Iphone 6 que se introducen en Cajas Faraday y se entrega el Juzgado de Instrucción de Tarragona para su análisis.

AL JUZGADO DE INSTRUCCION N° 4 DE TARRAGONA.

ENRIQUE RODRIGUEZ FIGUEROLA, abogado, con despacho profesional en 43480 Tarragona, C/ XXXXXX, teléfono 97.XXXX, en defensa y representación de don MARCO XXXXX -FRANCISCO XXXXX, ante el Juzgado comparezco y DIGO:

- **PRIMERO.**- En fecha 01 de noviembre de 2015, cuando mi representado se encontraba en su domicilio sufrió un allanamiento, le registraron sus pertenencias sin motivo alguno, sin encontrarse ninguna plantación ni material que atente contra la salud.*
- **SEGUNDO.**- El Control, registro y cacheo efectuado no fueron legales. Las presuntas sustancias estupefacientes no existen en el domicilio ni en ningún lugar íntimo o de mi representado.*

- **TERCERA.-** Si de otra forma se interpreta el artículo 25.1 de la ley 1/92, quiere decir que el legislador ha promulgado una Norma que atenta a la libertad, justicia, igualdad, es arbitraria, deja de promover las condiciones para que la libertad y la igualdad del individuo sean reales y efectivas, ha vulnerado el derecho al libre desarrollo de la personalidad, la dignidad, los derechos inviolables que le son inherentes, incurran en discriminación por razón de sus gustos o circunstancias personales sin hacer daño a nadie, atenten a su libertad ideológica, de expresión, al derecho a la intimidad, a la educación y a la salud.
- **CUARTA.-** Artículo 24.2 de la Constitución Española, que establece la presunción de inocencia. Siendo, conforme reiterada jurisprudencia, en el ámbito sancionador administrativo, estando también establecido en el artículo 137.1 de la Ley 30/92 de Régimen Jurídico de las Administraciones Públicas y procedimiento Administrativo Común. Solicito el Análisis Forense Digital de los dispositivos incautados para descartar cualquier indicio de tráfico de estupefacientes.

SOLICITO AL JUZGADO, admita este escrito, confiera plazo para el apoderamiento apud acta, reclame el expediente y dicte sentencia en su día estimatoria de la presente demanda, anulando la resolución recaída, con expresa condena en costas.

El Juzgado de Instrucción nº 4 de Tarragona admite a trámite el escrito formulado por **ENRIQUE RODRIGUEZ FIGUEROLA**. En el plazo de 5 días se comunica a Marco Antonio Alvarez Murillo la designación de Perito informático titular y se le requiere para que en el plazo de 15 días manifieste si acepta el cargo.

Marco Antonio Alvarez Murillo acepta el nombramiento como perito informático hará en la forma que considere oportuno manifestación mediante juramento o promesa según ordena el apartado 2 del artículo 335-342.1.

INFORME PERICIAL DISPOSITIVO iOS.

Introducción.

El presente documento describe el Informe Pericial en respuesta a la investigación designado por el El Juzgado de Instrucción nº 4 de Tarragona Diligencias Previas con el nº 849/2015.

La investigación comprende el análisis de un dispositivo iOS de propiedad del Sr Francisco, dicho dispositivo fue incautado el día 10 de Octubre del 2015 por la policía de Catalunya Mossos d'Esquadra con la finalidad de investigar indicios de supuestos delitos contra la salud y tráfico de estupefacientes en su domicilio o en algún lugar clandestino.

Con el fin de esclarecer dichas sospechas se analiza el dispositivo, la información relevante se obtiene con los mensajes recibidos - enviados, que su vez, puede atribuir la influencia de otras personas, lista de contactos, el tráfico de estupefacientes, laboratorios clandestinos y su *geolocalización*, búsqueda de información para la manipulación de estupefacientes, imágenes de plantaciones.

Datos del Perito Forense Digital.

Número de Caso:	849/2015
Propiedades/Evidencia Número:	TFG - iOS
Compañía/Agencia:	UOC
Examinador:	Marco Antonio Alvarez Murillo.
Dirección1:	-----
Dirección 2:	
Ciudad:	La Pineda.
Provincia:	Tarragona.
Código postal:	43481
Country:	Spain
Teléfono:	
Fax:	
E-mail:	malvarezmu@uoc.edu
Notas:	Reporte Pericial Trabajo de Fin de Grado

Sumario del incidente.

- En la entrevista que se realiza al Sr. Francisco el 20 de Octubre del 2015, se pregunta a cerca del código de desbloqueo de su dispositivo, su respuesta es: “no existe ningún sistema de bloqueo en el dispositivo”.
- La copia de seguridad se realiza con la aplicación de iTunes.
- Se inicia la investigación exhaustiva de los documentos y aplicaciones instaladas en el dispositivo para verificar supuestos delitos.
- Las aplicaciones de mensajería instaladas en el dispositivo son: *Facebook, Messenger, Whatsapp, Skype*. Los mensajes enviados-recibidos, imágenes *geolocalización* en dichas aplicaciones así como *SMS MMS* pueden esclarecer al existencia de algún delito.
- Si existen mensajes que comprometen a otros individuos, se analiza en la lista de contactos a los involucrados a continuación, se realiza búsquedas en internet siendo la fuente principal de información las redes sociales, la finalidad es obtener información de las personas involucradas y poner en conocimiento judicial.
- Se recuperan las imágenes tomadas con el dispositivo así como las que se ha recibido en redes sociales o mensajería. Dichas imágenes pueden ser de plantaciones, laboratorios clandestinos, geolocalización o llevar información oculta para la comunicación entre individuos.
- El historial de navegación puede aportar información a cerca de cuidados de plantaciones ilegales y esclarecer si se busca formas de tratamiento de estupefacientes.

Pruebas.

Los Mossos d'Esquadra incautaron un dispositivo móvil de propiedad del Sr Francisco las siguientes características.

Program Timestamp	11/15/2015 2:27:43 AM
Manufacturer	Apple
Device model	iPhone
Build Version	12-----
Device Name	iPhone (2)
ICCID	89-----
IMEI	35-----

Last Backup Date	11/8/2015 03:39:14 AM (UTC)
Phone Number	(201)-66-----

Detalles.

Contactos

La Base de Datos de Adress Book en el dispositivo contiene datos de la lista de personas de contacto que se encuentran almacenado en el dispositivo.

ROWID	First	Last	Middle	FirstPhon...	MiddlePh...	LastPhon...	Organizati...	Department	Note	Kind	Birthday	JobTitle
1025	Manoyo									0		
1026	guillermo									0		
1027	Cafe Harri...									0		
1028	Dalia									0		
1029	Erika Rio									0		
1030	lucia elena								Birthday:J...	0		
1031	Julia Crist...									0		
1032	Freddy									0		
1033	Noldo									0		
1034	Luis Miguel									0		
1035										0		
1036	jose traba...									0		
1037	martha ill...									0		
1038	Optica									0		
1039	Triuck									0		
1040	William Otr...									0		
1041	Juan Co...									0		
1042	maria agu...									0		
1043	Marstro									0		
1044	Alejandra								Birthday:N...	0		
1045	CAMILA									0		

Calendario.

En la base de datos del calendario se observa las coordenadas GPS de un lugar fuera de España, exactamente en la ciudad de Kerny en los Estados Unidos.

ROWID	title	address	latitude	longitude	address_...	radius	routing	item_own...	alarm
6						0		0	32
7						0		172	0

Se utiliza Google Maps para obtener la localización exacta. La dirección de estas coordenadas es: -- --- -----Ave, Kearny, NJ 07032,

Dirección

GD (grados decimales)*

GMS (grados, minutos, segundos)*
 L °
 L °

* Sistema Geodésico Mundial 1984 (WGS 84)

Cuenta de correo electrónico.

La cuenta de correo que utiliza el dispositivo como la ID de Apple es -----@hotmail.com

HEN	ZSUPPO	ZVISIBLE	ZACCOU	ZPARENT	ZDATE	ZLASTOR	ZACCOU	ZAUTHEN	ZCREDE	ZIDENTIF	ZOWNINGBUND	ZUSERNAME	ZDATACL
0	0	6			434280678.880038		Holiday C...	none		1C783C7...	com.apple.data...		
1	1	25			436902839.441254					DC48E1B...		@hotmail.com	
1	1	17			436902841.21173					1E911F6...		@hotmail.com	
1	1	5			436923015.651237					C250223...	com.apple.Prefe...	@hotmail.com	
1	1	17			458488992.359718					357CDEA...	com.apple.identi...	@hotmail.com	
1	1	18			464275751.117363		iCloud			C5DF846...	com.apple.Prefe...	@hotmail.com	bplist000
1	1	1	91		464275750.899956			parent		D072B1F...	com.apple.accou...		
1	1	12	91		464275751.027312			parent		C76E4D4...	com.apple.accou...		
1	1	23	91		464275751.077126			parent		A19DA1E...	com.apple.accou...		
1	1	13			464275750.849946					57AF8547...	com.apple.accou...	@hotmail.com	
0	1	10	91		464275749.430122					BF40B36...	com.apple.accou...	@hotmail.com	
0	1	34	91		464275749.322738					31ECAC8...	com.apple.accou...	@hotmail.com	
1	1	22	91		464275750.979137			parent		18345325...	com.apple.accou...	@hotmail.com	
1	1	32	91		464275744.730548					A1DCAB3...	com.apple.accou...	@hotmail.com	
1	1	17			466613328.914564					FF9B820...	com.apple.identi...	@hotmail.com	
1	1	2	01		46R201414.50670			parent		4FA074R...	com.apple.accou...	@hotmail.com	

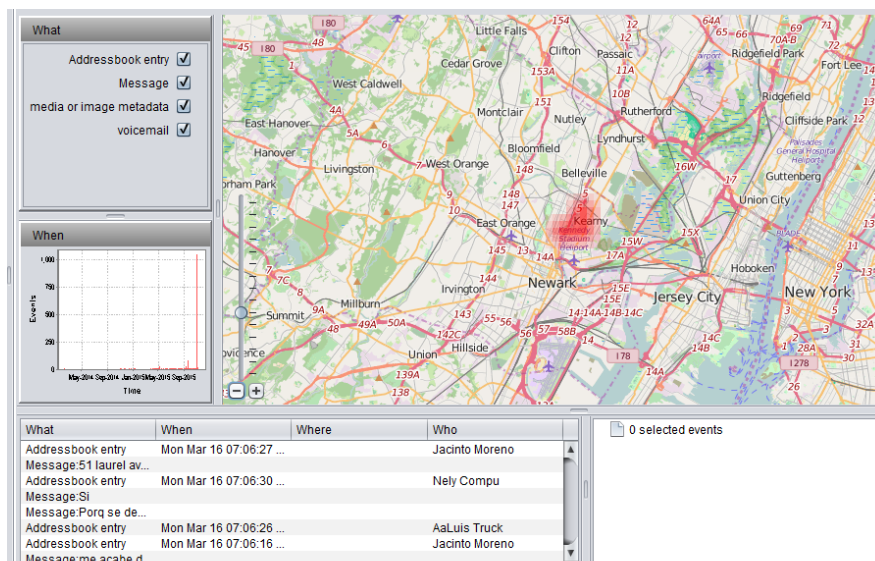
Mensajes.

SMS.

Se analizan los mensajes, en resumen los temas que se tratan es a cerca de seguros, compra de alimentos, saludos entre contactos, fútbol, información a cerca de empleo.

Number	Message	Date	Direction	Service
live.com	☺	Thu Oct 08 16:10:09 CEST 2015	SENT	iMessage
live.com	Como se llama el seguro	Thu Oct 08 19:10:25 CEST 2015	SENT	iMessage
live.com	El nombre de tu seguro	Thu Oct 08 19:10:34 CEST 2015	SENT	iMessage
live.com	Medico	Thu Oct 08 19:10:36 CEST 2015	SENT	iMessage
live.com	Fidelis	Thu Oct 08 19:15:20 CEST 2015	RECEIVED	iMessage
live.com	Llamé mañana dice	Thu Oct 08 19:15:38 CEST 2015	SENT	iMessage
live.com	Pero me llamaron que se vendio	Thu Oct 08 19:15:37 CEST 2015	RECEIVED	iMessage
live.com	No te creo	Thu Oct 08 19:15:50 CEST 2015	SENT	iMessage
live.com	Y ahora	Thu Oct 08 19:15:50 CEST 2015	SENT	iMessage
live.com	Como debes hacer	Thu Oct 08 19:16:08 CEST 2015	SENT	iMessage
live.com	Aplicar otraves	Thu Oct 08 19:23:23 CEST 2015	RECEIVED	iMessage
live.com	Pero si ya te vas a mudar a new jersey	Thu Oct 08 19:24:10 CEST 2015	SENT	iMessage
live.com	Si	Thu Oct 08 19:33:09 CEST 2015	RECEIVED	iMessage
live.com	Major pido aqui	Thu Oct 08 19:33:18 CEST 2015	RECEIVED	iMessage
live.com	Claro	Thu Oct 08 21:21:33 CEST 2015	SENT	iMessage
5	Compro comida	Thu Oct 08 21:47:05 CEST 2015	SENT	SMS

A más, los mensajes que envía en su mayoría proceden de la ciudad de Kerny



Historial de Navegación en Safari.

El historial proporciona una visión de los temas de interés que se busca en el pospositivo, en resumen son eliminatorias sudamericanas, compras *on-line*, información a cerca de dispositivos, información familiar, clima, deportes en general.

id	url	domain_e...	vi
11575	http://srx.main.ebayrtm.com/clk?RlmCk&m=512469&ch=1&g=83ee8e54149777b57ca725500139b0...	srx.main....	1
11576	https://www.google.com/search?q=amazon&ie=UTF-8&oe=UTF-8&hl=en&client=safari	google	3
11577	http://www.amazon.com/	amazon	4
11578	http://www.amazon.com/gp/aw/d/B00BJ5GD9W/ref=mp_s_a_1_1?qid=1445001198&sr=8-1&pi=SY20...	amazon	3
11579	http://www.amazon.com/gp/aw/d/B00BJ5GD9W/ref=mp_s_a_1_1?qid=1445001198&sr=8-1&pi=SY20...	amazon	1
11580	http://www.amazon.com/gp/aw/d/B00BJ5GD9W/ref=mp_s_a_1_10?k=battery+socks&prefix=battery+so	amazon	3
11581	http://www.amazon.com/gp/aw/d/B00BJ5GD9W/ref=mp_s_a_1_1?qid=1445001198&sr=8-1&pi=SY20...	amazon	1
11582	http://www.amazon.com/gp/aw/d/B00ASMLXMI/ref=mp_s_a_1_1?ie=UTF8&refRID=0BKZ8...	amazon	1
11583	http://www.amazon.com/gp/aw/d/B0009HMFPC/ref=mp_s_a_1_1?ie=UTF8&refRID=01BN582X...	amazon	1
11584	http://www.amazon.com/gp/aw/d/B0009HMFPC/ref=mp_s_a_1_1?ie=UTF8&refRID=01BN582X...	amazon	1
11585	http://www.amazon.com/gp/aw/d/B0009HMFPC/ref=mp_s_a_1_1?ie=UTF8&refRID=01BN582X...	amazon	2
11586	http://www.amazon.com/gp/aw/d/B005KQAZZ0/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11587	http://www.amazon.com/gp/aw/d/B000MQ3SE2U/ref=mp_s_a_1_1?qid=1445003257&sr=8-1&pi=SY20...	amazon	1
11588	http://www.amazon.com/gp/aw/d/B000MQ3SE2U/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	3
11589	http://www.amazon.com/gp/aw/d/B000MQ3SE2U/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	6
11590	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11591	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11592	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	7
11593	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11594	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11595	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11596	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	4
11597	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11598	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11599	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11600	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11601	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11602	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	1
11603	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	2
11604	http://www.amazon.com/gp/aw/d/B007SNUYZI/ref=mp_s_a_1_1?ie=UTF8&refRID=038GDDP7...	amazon	2

17062	11489	46637210...	nombres tortugas ninja - Google Search
17063	11490	46637211...	nombres tortugas ninja - Google Search
17064	11319	46637968...	17track - Track Global Postal
17065	11142	46638389...	craigslist north jersey jobs, apartments, personals, for sale, services, commu...
17066	11143	46638390...	north jersey cell phones - craigslist
17067	11491	46638391...	Iphone 6
17068	11492	46638393...	2 iPhone 5s cracked screen
17069	11493	46638395...	Iphone 6 64gb
17070	11249	46638401...	north jersey cell phones - craigslist
17071	11494	46638404...	IPhone 5c pink
17072	11355	46642748...	eliminatorias 2018 - Google Search
17073	11495	46642748...	FIFA.com - Copa Mundial de la FIFA Rusia 2018™ - Eliminatorias - Sudamérica
17074	11496	46642748...	Copa Mundial de la FIFA Rusia 2018™ - Eliminatorias - Sudamérica - FIFA.com
17075	11497	46642780...	
17076	11498	46642780...	FIFA.com - Clasificación Mundial FIFA/Coca Cola - Clasificación completa
17077	11499	46646189...	FIFA.com - Copa Mundial de la FIFA Rusia 2018™
17078	11498	46646171...	FIFA.com - Clasificación Mundial FIFA/Coca Cola - Clasificación completa
17079	11497	46646171...	
17080	11500	46646172...	FIFA.com - Fútbol mundial
17081	11356	46646176...	El calendario de Sudamérica para las clasificatorias Rusia 2018 Tele 13
17082	11355	46646176...	eliminatorias 2018 - Google Search
17083	11359	46646187...	linea roja - Google Search
17084	11360	46646187...	ROJADIRECTA
17085	11501	46646190...	
17086	11502	46646189...	Rojadirecta.me - zonasports
17087	11503	46646190...	ZonaSports.se [Los mejores eventos deportivos en calidad HD
17088	11504	46647546...	imei checker - Google Search
17089	11505	46647547	IPhoneIMEInfo - Free iPhone Unlock Checker

Mensajes por Whastapp.

La base de datos de WhatsApp aporta mensajes y fotografías, la imágenes se basan en deportes, rivalidad entre equipos de fútbol de Ecuador, España e Inglaterra, citas personas, deportes, viajes, estudios, salidas con amigos, reuniones laborales, mensajes familiares.

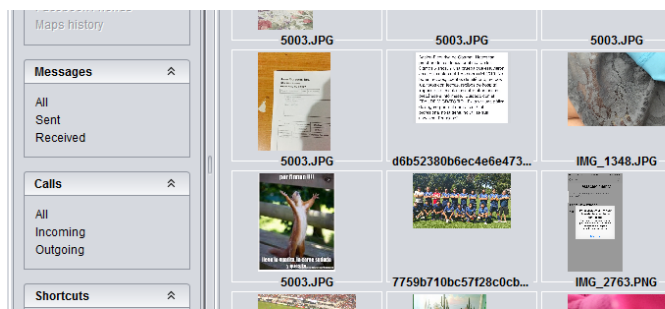
Mensajes por Facebook o Messenger y Skype.

Los mensajes que se intercambian se aprecia que son con familiares y amigos, en las fotografías de perfil de los contactos en la mayoría de casos se encuentran niños con

adultos, lo que hace pensar que son familiares. Se tratan temas de: saludos, bienestar, citas o planes. Los principales contactos son personas que viven en Ecuador, Italia, España y los EEUU.

Imágenes

Las imágenes obtenidas son principalmente personas adultas con niños aparentemente son sus hijos en base a las muestras de afecto y repetición en la mayoría de fotografías.



Resultados y Conclusiones.

Después de un análisis detallado de la evidencia digital, en conjunto con la aplicación métodos científicos para el Análisis Forense en dispositivos móviles se obtienen los siguientes resultados:

- No existe ningún tipo de comunicación oral o escrita a cerca de un posible tráfico de estupefacientes.
- El historial de navegación no constata búsquedas a cerca de cuidado y tratamiento de estupefacientes (plantaciones, fertilizantes, métodos de cultivo, purificación etc.), que determinen algún interés para obtener información y uso para fines delictivos.
- Las imágenes que se analizaron inducen a ser material de tipo personal - familiar sin contenido oculto que proporcione algún dato a cerca de un posible tráfico de estupefacientes. Además, no se encuentra archivos con contenido de laboratorios clandestinos o métodos de alteración de material ilícito.

- Los archivos borrados que se recuperaron, no contienen información que promueva interés en los temas relacionados con los incisos anteriores,
- No se encontró archivos protegidos con un sistema de cifrado o protegido con algún sistema de seguridad.
- Con la *cookie* de la aplicación Outlook se puede acceder a la cuenta de correo de hotmail que tiene sincronizada.
- Según el número de teléfono, la *geolocalización* y los mensajes que se verifica con su se puede concluir que su dirección habitual se encuentra en la ciudad Kerny.

En conclusión:

Se concluye que el Sr Francisco, tiene su domicilio habitual en la Ciudad de Kerny - New Jersey en los Estados Unidos, los principales contactos con los que se comunica se encuentran en los países de Ecuador y los Estados Unidos.

Aparentemente el acusado se encuentra en España por turismo o visita junto con el otro sospechoso el Sr. Marco. No existe evidencia de comunicación entre los detenidos sobre ningún tipo de delito.

El dispositivo incautado no contiene ningún tipo de información que permita afirmar la que existencia de algún indicio de plantaciones o tráfico de estupefacientes que atente contra la salud.

INFORME PERICIAL DISPOSITIVO ANDROID.

Introducción.

El presente documento describe el Informe Pericial en respuesta a la investigación designado por El Juzgado de Instrucción nº 4 de Tarragona Diligencias Previas con el nº 849/2015.

La investigación comprende el análisis de un dispositivo Android de propiedad del Sr Marco, dicho dispositivo fue incautado el día 10 de Octubre del 2015 por la policía de Catalunya Mossos d'Esquadra con la finalidad de investigar indicios de supuestos delitos contra la salud y tráfico de estupefacientes en su domicilio o en algún lugar clandestino.

Con el fin de esclarecer dichas sospechas se analiza el dispositivo, la información relevante se obtiene con los mensajes recibidos - enviados, que su vez, se puede atribuir la influencia de otras personas, lista de contactos, el tráfico de estupefacientes, laboratorios clandestinos y su geolocalización, búsqueda de información para la manipulación de estupefacientes, imágenes de plantaciones.

Datos del Perito Forense Digital.

Número de Caso:	849/2015
Propiedades/Evidencia Número:	TFG - Android.
Compañía/Agencia:	UOC
Examinador:	Marco Antonio Alvarez Murillo.
Dirección1:	-----
Dirección 2:	
Ciudad:	La Pineda.
Provincia:	Tarragona.
Código postal:	43481
Country:	Spain
Teléfono:	
Fax:	

E-mail:	malvarezmu@uoc.edu
Notas:	Reporte Pericial Trabajo de Fin de Grado

Sumario del incidente

- En la entrevista que se realiza al Sr. Marco el 20 de Octubre del 2015, se le pregunta a cerca del código de desbloqueo de su dispositivo: “negándose por completo a la respuesta”.
- Se procede a desbloquear el dispositivo con técnicas digitales y herramientas forenses que permiten escalar privilegios para llevar a cabo la copia intacta del dispositivo.
- Se realiza una investigación exhaustiva de los documentos y aplicaciones instaladas en el dispositivo para verificar supuestos delitos.
- Las aplicaciones de mensajería instaladas en el dispositivo son: Facebook, Twitter, Messenger, Whatsapp, Tango. En los mensajes enviados-recibidos, imágenes, geolocalización en dichas aplicaciones, así como, SMS MMS se puede esclarecer al existencia de algún delito.
- Si existen mensajes que comprometan a otras personas, se buscará en la lista de contactos a los involucrados, perfiles en las redes sociales, con la finalidad de obtener información y poner en conocimiento judicial.
- Se extraen las imágenes que se tomaron con el dispositivo así como las recibidas en redes sociales o mensajería. Dichas imágenes pueden ser de plantaciones, laboratorios clandestinos, *geolocalización* o llevar información oculta para la comunicación entre individuos.
- El historial de navegación se examina información a cerca de cuidados de plantaciones ilegales, puede esclarecer si se busca formas de tratamiento de estupefacientes.

Pruebas.

Los Mossos d'Esquadra incautaron un dispositivo móvil de propiedad del Sr. Marco con las siguientes características.

ADB serial:
Shell permissions:	shell

Manufacturer:	BQ
Model:	Aquaris E5
IMEI:	-----
Android version:	4.4.4
Build name:	1.8.4_20150727-1246-8G
Wifi MAC:	-----
Phone Number	(0034) -----

Cuentas Sincronizadas.

Accounts:	com.qualcomm.qti.calendarlocalaccount: Local com.android.localphone: PHONE com.android.sim: SIM2 com.google: -----@gmail.com com.whatsapp: WhatsApp com.facebook.auth.login: -----@hotmail.com com.twitter.android.auth.login: m----- com.sgiggle.production.account: Sincronizar amigos de Tango
-----------	--

Security (Gesture Hash):	da39a-----
Security (Lockscreen Pattern):	None
Security (Lockscreen Hash):	5CAFBE-----
Security (Lockscreen Salt):	-----
System:	Synchronised Accounts (8)
System:	Wi-Fi Passwords (13)
System:	Android Download History (27)
Web browser:	Google Chrome Passwords (2)
Web browser:	Google Chrome History (537)
Communications data:	Contacts (5,915)
Communications data:	Call logs (500)
Communications data:	SMS Messages (131)
Applications data:	Facebook Messages (9,130)
Applications data:	WhatsApp Contacts (107)
Applications data:	WhatsApp Calls (69)
Applications data:	WhatsApp Messages (23,252)

Detalles.

SMS.

Los mensajes se basan en avisos de llamadas perdidas o publicidad de empresas u operadoras móviles. En dichos mensajes se aprecia que el número asignado al dispositivo es el (0034) - 690 ----- asignado código de país España y la operadora que tiene contratado para proveer el servicio de telefonía es MOVISTAR.

MMS.

No existen mensajes con este formato.

1031		BUZON MOVISTAR vie, 02 - 14:52 1 mensaje nuevo de ----- Para escucharlo, llame gratis al 123 - Personalice su buzón fácilmente llamando gratis al 22126	2015-10-02 12:52:48 UTC+00:00	Inbox
130		LLAMADAS PERDIDAS vie, 02 - 14:38 1 llamada de ----- Si desea devolver la llamada, pulse la tecla verde de su móvil	2015-10-02 12:39:07 UTC+00:00	Inbox
129		BUZON MOVISTAR vie, 02 - 13:06 1 mensaje nuevo de ----- Para escucharlo, llame gratis al 123 - Personalice su buzón fácilmente llamando gratis al 22126	2015-10-02 11:07:01 UTC+00:00	Inbox
128		LLAMADAS PERDIDAS vie, 02 - 13:05 1 llamada de ----- Si desea devolver la llamada, pulse la tecla verde de su móvil	2015-10-02 11:05:56 UTC+00:00	Inbox

Mensajes de la aplicación *WhastApp*.

Se han recuperado 23252 mensajes que se analizan y se encuentra información acerca de deportes, viajes, estudios, salidas con amigos, reuniones laborales, mensajes familiares.

#	Number	Message	Time	Type
39489		Por futbol	2015-11-02 21:47:20 UTC+00:00	Sent
39488		Me preguntabN	2015-11-02 21:47:16 UTC+00:00	Sent
39487		Xd	2015-11-02 21:46:31 UTC+00:00	Inbox
39486		Perdón	2015-11-02 21:21:47 UTC+00:00	Sent
39485		Mexico 2-0	2015-11-02 21:21:38 UTC+00:00	Sent
39484		10-15 gradid	2015-11-02 21:19:31 UTC+00:00	Sent
39483		Temperatura?	2015-11-02 21:15:55 UTC+00:00	Inbox
39482		Está bien	2015-11-02 20:18:36 UTC+00:00	Sent
39481		MA's o menos	2015-11-02 20:18:32 UTC+00:00	Sent

Mensajes por Facebook o Messenger.

Se analizan 9130 mensajes. Los mensajes son de familiares y de amigos, en la fotografías de perfil de los contactos en la mayoría de casos se encuentran niños con adultos, lo que hace pensar que son familia. Se tratan temas de saludos, bienestar, citas o planes.

Sender	Image	Message	Recipient(s)	Time
Marco		Mexico 2-0	Francisco (ID:584-----)	2015-11-02 21:22:07 UTC+00:00
		Que no me entero Me duele la cabeza Me va a estallar	Marco (ID:164-----)	2015-11-02 21:08:32 UTC+00:00
		Marco me dices lo que estabas diciendo	Marco (ID:1648-----)	2015-11-02 21:07:19 UTC+00:00
Marco		No se	Francisco (ID:584-----)	2015-11-02 21:05:58 UTC+00:00
		Dime	Marco (ID:164-----)	2015-11-02 21:00:49 UTC+00:00
		??????	Marco A (ID:164-----)	2015-11-02 20:58:46 UTC+00:00
		Que no se oye	Marco (ID:164-----)	2015-11-02 20:57:48 UTC+00:00

Historial en Google Chrome.

La información que se desea averiguar se basa en deportes, noticias, tecnología principalmente informática, clima, mariscos, viajes, canciones y consulados.

Traductor de Google	https://translate.google.es/m/translate?hl=es	2015-11-02 14:50:07 UTC	33
Google	https://www.google.es/webhp?output=search&tbm=isch&tbo=u	2015-11-02 14:37:14 UTC	2
Google	https://www.google.es/?gws_rd=ssl	2015-11-02 14:31:05 UTC	70
Google	http://google.es/	2015-11-02 14:31:05 UTC	58
Google	http://www.google.es/	2015-11-02 14:31:05 UTC	56
	https://translate.google.es/m/translate?hl=es#en/es/fall	2015-11-02 14:28:01 UTC	1
https://m.youtube.com/watch?v=cOku4FjfGV8 is not available	https://m.youtube.com/watch?v=cOku4FjfGV8	2015-11-02 04:39:27 UTC	1
christofer hitchen sobre la iglesia catolica - YouTube	https://m.youtube.com/results?q=christofer%20.....olica&sm=3	2015-11-02 04:39:27 UTC	2
Home - YouTube	https://m.youtube.com/	2015-11-02 04:39:16 UTC	6
YouTube	http://www.youtube.com/	2015-11-02 04:38:46 UTC	3
YouTube	https://m.youtube.com/?	2015-11-02 04:38:46 UTC	3
democrito - Buscar con Google	https://www.google.com/search?q=democrito&oq=.....e&ie=UTF-8	2015-11-02 04:27:18 UTC	3
Demócrito - Wikipedia, la enciclopedia libre	https://es.m.wikipedia.org/wiki/Dem%C3%B3crito	2015-11-02 04:26:51 UTC	2

Imágenes

Las imágenes que se recuperan son principalmente de familiares con niños, su pareja aparentemente son sus hijos en base a las muestras de afecto y repetición variada

de estas personas en las diferentes fotografías.

Contactos.

Se recuperan 5915 contactos, con un 509 registros de llamadas. Al no existir indicios de delitos, no se puede establecer investigación de llamadas realizadas o recibidas en un tiempo determinado, sin embargo queda a disposición los registros de llamadas los contactos y fecha-hora.

#	Name	Number	Email	Other
1	Juan	60-----		
2	boris	63-----		
3	Salvadorvalls	68-----		
4	rafa	68-----		
5	jpar	65-----		
6	michel	63-----		

Logs de Llamadas.

#	Type	Number	Name	Time	Duration
1505	Dialled	+34649-----		2015-10-16 15:31:49 UTC+00:00	0:00:00
1504	Dialled	629-----		2015-10-02 14:35:54 UTC+00:00	0:00:45
1503	Received	629-----		2015-10-02 13:45:38 UTC+00:00	0:00:26
1502	Dialled	+3463-----		2015-10-02 13:06:01 UTC+00:00	0:02:19
1501	Dialled	62-----		2015-10-02 13:05:49 UTC+00:00	0:00:00
1500	Dialled	+3463-----		2015-10-02 12:59:02 UTC+00:00	0:00:00
1499	Dialled	62-----		2015-10-02 12:50:31 UTC+00:00	0:01:18
1498	Dialled	63-----		2015-10-02 12:43:25 UTC+00:00	0:06:45
1497	Received	63-----		2015-10-02 12:38:48 UTC+00:00	0:00:00
1496	Dialled	+3462-----		2015-10-02 11:08:27 UTC+00:00	0:01:37
1495	Received	62-----		2015-10-02 11:07:23 UTC+00:00	0:00:50
1494	Received	63-----		2015-10-02 11:06:08 UTC+00:00	0:00:55
1493	Dialled	629-----		2015-10-02 11:05:37 UTC+00:00	0:00:02
1492	Dialled	63-----		2015-10-02 11:05:04 UTC+00:00	0:00:00
1491	Dialled	+3462-----		2015-10-02 11:03:55 UTC+00:00	0:00:29
1490	Received	63-----		2015-10-01 23:07:08 UTC+00:00	

Resultados y Conclusiones.

Después de un análisis detallado de la evidencia digital, en conjunto con la aplicación de métodos científicos para el Análisis Forense en dispositivos móviles se obtienen los siguientes resultados:

- No existe ningún tipo de comunicación oral o escrita a cerca de un posible tráfico de estupefacientes.
- El historial de navegación no constata búsquedas a cerca de cuidado y tratamiento de estupefacientes (plantaciones, fertilizantes, métodos de cultivo, purificación etc.), que determinen algún interés para obtener información y uso con fines delictivos.
- Las imágenes que se analizaron insistan a pensar que son fotografías de tipo personal - familiar sin contenido oculto que proporcione algún dato a cerca de un posible tráfico de estupefacientes. Además, no se encuentra archivos con contenido de laboratorios clandestinos o métodos de alteración de material ilícito.
- Los archivos eliminados que se recuperaron, no contienen información que promueva información en temas relacionados con los incisos anteriores,
- No se encontró archivos protegidos con un sistema de cifrado o protegido con algún sistema de seguridad.
- En el dispositivo no existen ninguna aplicación de correo electrónico, en el historial no accede a ningún sitio de correo electrónico, y en al análisis de la caché no se encuentra *cookies* que relacionan algún inicio de sesión con cuentas de correo electrónico.

En conclusión:

No existe evidencia de comunicación entre los detenidos sobre ningún tipo de delito. El dispositivo incautado no contiene ningún tipo de información que permita afirmar la que existencia de algún indicio de plantaciones o tráfico de estupefacientes que atenten contra la salud.