
# DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

## CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS**

**TEMA: ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON TECNOLOGÍA IPHONE**

**AUTOR: GRANDA VELASTEGUI MÓNICA GABRIELA**

**DIRECTOR: ING. ÑACATO GERMAN**

**SANGOLQUÍ**

**2016**

## CERTIFICADO DEL DIRECTOR DEL TRABAJO DE TITULACIÓN

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

## DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

## CARRERA DE INGENIERÍA EN SISTEMAS

## CERTIFICACIÓN

Certifico que el trabajo de titulación, "ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON TECNOLOGÍA IPHONE", realizado por la Srta. MÓNICA GABRIELA GRANDA VELASTEGUI, en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la Srta. MÓNICA GABRIELA GRANDA VELASTEGUI para que lo sustente públicamente.

Sangolqui, 04 de mayo del 2016

**GERMÁN NACATO**

**DIRECTOR**

## AUTORÍA DE RESPONSABILIDAD


**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN**

**CARRERA DE INGENIERÍA EN SISTEMAS**

Yo, MÓNICA GABRIELA GRANDA VELASTEGUI, con cédula de identidad N° 171852619-5 declaro que este trabajo de titulación "ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON TECNOLOGÍA IPHONE", ha sido desarrollado o considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolqui, 04 de mayo del 2016

GRANDA VELASTEGUI MÓNICA GABRIELA

C.C. 171852619-5

# AUTORIZACIÓN

**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN**

**CARRERA DE INGENIERÍA EN SISTEMAS**

Yo, MÓNICA GABRIELA GRANDA VELASTEGUI, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON TECNOLOGÍA IPHONE", cuyo contenido, ideas y criterio son de autoría y responsabilidad.

Sangolqui, 04 de mayo del 2016

GRANDA VELASTEGUI MÓNICA GABRIELA

C.C.171852619-5

# DEDICATORIA

Quiero dedicar este trabajo con mucho amor a mis padres, que siempre han estado conmigo dándome ánimos y fortalezas en todos los ámbitos de mi vida, es por esto que este logro es de ellos.

A mi Tío Marcelo quien ha sido un pilar fundamental en toda mi vida y a quien le agradezco todo su cariño y enseñanzas que me ha regalado hasta el día de hoy. A mis hermanos quienes me han apoyado siempre en todos los caminos de mi vida y son parte de este triunfo profesional.

A mis abuelitos quienes me han guiado y han llenado de amor en el tiempo que estuvieron conmigo, llegaron a ver el proceso de mi camino profesional, a Mama Lucita quien es una abuelita hermosa que aún está presente en mi vida y me apoyado en todas las etapas de mi vida. A mi novio Oscar quien ha estado conmigo en todo este proceso de elaboración de tesis le agradezco por su amor, su apoyo constante e incondicional.

Por ultimo al Ing. German Ñacato quien ha sabido guiarme en este paso final de mi tesis y que con su paciencia y enseñanzas ha logrado que yo culmine mi proyecto.

# AGRADECIMIENTO

El presente trabajo quiero agradecer primero a mis padres ya que sin su apoyo tanto económico como emocional no podría haber conseguido todo lo que logrado, siempre estuvieron conmigo motivándome para la culminación de mi carrera.

A mi querida Universidad quien me acogió por años y en donde me forme como profesional y como persona, estoy agradecida por tantas alegrías que me ha brindado y siempre tendré los mejores recuerdos de esta mi querida Institución.

A mis profesores ya que cada uno de ellos me compartieron su conocimiento e hicieron que me enamorara de mi profesión y pudiera terminar mi carrera de la mejor manera.

# INDICE GENERAL

# INDICE DE TABLAS

# INDICE DE FIGURAS

## RESUMEN EJECUTIVO

La presente investigación, tiene como fin detallar el análisis forense de dispositivos móviles iPhone como procedimiento eficaz para determinar el grado de participación de sus usuarios en el cometimiento de un delito. El análisis surge a partir de la utilización de herramientas open source, se utilizó el método descriptivo-explicativo ya que éste permite detallar las etapas del procedimiento y la información obtenida en cada una de ellas. Como resultado se obtuvo que a través de la aplicación seleccionada, se pueda ingresar en el sistema de seguridad del dispositivo, realizar una copia exacta de la información almacenada y obtener datos consistentes. Además se aplicó un cuestionario a 100 personas en los que se determinó que un 69% de ellos había sido víctima de delito cibernético al menos en una ocasión, de las cuales en un 23% el medio usado había sido un celular. Por último se establece un estudio detallado de la arquitectura de dispositivos iPhone, sus mecanismos de almacenamiento de datos y de seguridad. Se concluye que los teléfonos iPhone se encuentran entre los equipos que más opciones de seguridad brindan a sus usuarios lo que dificulta la labor de los peritos forenses, a su vez el desarrollo de nuevas aplicaciones de software como la utilizada en este trabajo, han permitido la identificación de criminales en contravenciones penales, por lo cual se recomienda su uso.

Palabras Clave**:**

**ANÁLISIS FORENSE**

**DISPOSITIVOS MÓVILES**

**TECNOLOGÍA**

**IPHONE.**

# ABSTRACT

This research aims to detail the forensic analysis of mobile devices iPhone as an effective method for determining the degree of participation of its members in the commission of a crime. The analysis was conducted using the open source tools, the descriptive-explanatory method used since it allowed detail the stages of the procedure and the information obtained in each of them. As a result was obtained through the selected application, you can enter the security system of the device, an exact copy of the stored information and get consistent data. In addition a questionnaire to 100 people in which it was determined that 69% of them had been a victim of cyber-crime at least once, of which 23% in the medium used was a cell was applied. Finally, a detailed study of the architecture of iPhone, its data storage mechanisms and Safety. We conclude that the iPhone phones are among the teams that more security options offer their users hindering the work of the forensic experts, in turn developing new software applications as used in this work, have enabled the identification of criminals in criminal violations, so their use is recommended.

Key Words**:**

**FORENSIC**

**DEVICES MOBILE**

**TECHNOLOGY**

**IPHONE ANALYSIS.**

# ANÁLISIS FORENSE A DISPOSITIVOS MÓVILES CON TECNOLOGÍA IPHONE

"El internet, la globalización del comercio y el aumento de la economía de la información, han replanteado el papel de los sistemas de información en los negocios y la administración" (Laudon, 2004, p. 25) pero no solamente en estas áreas sino en casi todas las actividades que realiza a diario el ser humano ya que para la mayoría de decisiones juegan un papel fundamental.

Las grandes empresas de operadoras celulares han implementado en sus dispositivos aplicaciones que permiten organizar la vida de las personas hasta en los detalles más pequeños, tal es así que tareas como apuntar fechas importantes en un calendario o llevar una lista de números de contactos en una agenda escolar, saber la hora del día, grabar conversaciones o entrevistas ya no requieren de varios artefactos como libretas, grabadora o reloj, sino que se puede acceder a esto y mucho más a través de un solo dispositivo con tecnología "inteligente".

"Las compañías utilizan internet y la tecnología de redes para dirigir de manera electrónica gran parte de su trabajo, con lo que vinculan fácilmente fábricas, oficinas y fuerza de ventas en todo el mundo" (Laudon, 2004, p. 21). La proliferación de usuarios de redes sociales va en aumento a la vez que las operadoras integran el internet en los celulares permitiendo el fácil acceso a correos electrónicos, Facebook o twitter, etc. estas permiten acortar tiempo y distancia pero crean también una forma diferente de concebir el

mundo y a la vez modifican la forma de cometer delitos, tal es así que en la actualidad se habla de fraudes electrónicos, pero así mismo es posible obtener pruebas que anteriormente no hubiesen sido posibles, esto gracias al desarrollo de la tecnología.

En la actualidad el avance tecnológico en cuanto a dispositivos celulares móviles permite tener acceso a todas las ventajas que antes se tenía a través de un ordenador, pero con la ventaja de que estos son más pequeños y por tanto fáciles de llevar, las aplicaciones que se crean para estos dispositivos va en aumento, el objetivo es proporcionar a las personas mayor acceso y facilidad de comunicación, sin embargo las aplicaciones cada vez más sofisticadas sobrepasan el interés básico de brindar un enlace y convergencia de las telecomunicaciones, ahora ese dispositivo móvil presenta otra serie de servicios que permiten acceder a redes y portales en internet con una mayor facilidad.

Esta situación de mejoras en cuanto a aplicaciones y funcionalidades en los dispositivos móviles vulnera de cierta manera la información almacenada en dichos dispositivos, propician riesgos de afectaciones o fraudes electrónicos. De tal manera que se genera un espacio en el que se pueden cometer una serie de actos delictivos que atenten contra la integridad y seguridad de las personas o de grupos específicos como corporaciones.

Este mismo panorama ha propiciado el interés de ramas específicas de estudio tal es el caso del análisis forense encargado de la investigación de situaciones ilícitas producidas en los sistemas operativos o informáticos. Este análisis se enfoca en buscar o indagar autores del acto de fraude, causas, y mecanismo de acción que posibilitarán determinar la

vulnerabilidad que ha hecho posible el ataque, así como también en casos de criminalística en que los dispositivos tengan alguna relación con la escena del crimen.

El análisis forense digital sobre dispositivos móviles busca encontrar evidencias de estos dispositivos inteligentes, información relevante almacenada en los mismos. Esta indagación es posible gracias a sistemas operativos y aplicaciones que permiten copiar la información sin alterarla. Entre estos dispositivos esta la herramienta denominada Open Source que tiene varias aplicaciones para estos casos.

La presente investigación pretende estudiar sobre el análisis forense a dispositivos móviles IPhone mediante la utilización de herramientas open source. Para lo cual se enfocará en detallar el proceso y definiciones que permitan aclarar el tema de estudio.

# CAPÍTULO I.

## 1. PLANTEAMIENTO DEL PROBLEMA

### 1.1 Antecedentes

Los estudios de análisis forense en la actualidad han tomado fuerza, esto debido a que la información digital almacenada en dispositivos móviles inteligentes o informáticos es sumamente relevante en el ámbito del derecho al momento de determinar la situación de crimen o acto delictivo presentado.

La aplicación de nuevas técnicas y disciplinas que ayuden a clarificar ciertos hechos dados en la red, surgen a partir del siglo XIX. Al respecto Rodríguez especifica que "las huellas digitales, con valor identificativo, no fueron usadas hasta finales del siglo XIX. Las pruebas genéticas fueron utilizadas por primera vez en un tribunal a finales del siglo XX, en el año 1996" (Ferro, 2002, p. 228) .

A partir de este tiempo la ciencia forense dedicada al análisis de dispositivos digitales ha evolucionado con forme al avance tecnológico que se da en la actualidad con el objetivo de ser un aporte en el esclarecimiento de hechos producidos mediante la utilización indebida de información confidencial en estos dispositivos.

Rodríguez, et. al. (2012) señala:

> Muchas son las definiciones que de informática forense podemos encontrar en gran número de publicaciones, pero todas ellas –de una manera u otra– hacen hincapié en unos puntos esenciales; así, de una forma simple, podríamos definir la informática forense como un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales (p. 3).

La apreciable relevancia de aquellos datos obtenidos en dispositivos informáticos en ciertos casos ha generado el interés por el estudio y aplicación de herramientas para obtener información digital con la finalidad de presentarlas como evidencia.

Rodríguez, et. al. (2012) señala:

> A comienzo de los años 90, el FBI (Federal Bureau of Investigation) observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN. Para ello, mantuvo reuniones en su ámbito, y a finales de los años 90 se creó la IOCE (International Organization of Computer Evidence) con la intención de compartir información sobre las prácticas de informática forense en todo el mundo (p. 4).

De la misma manera en que se ha desarrollado aplicaciones para poder realizar análisis forenses digitales, se han desarrollado tecnologías cuyo objetivo es asegurar la confidencialidad de la información de los dispositivos móviles, la intención es que si el usuario pierde su celular quien lo encuentre no pueda hacer uso de la información o de las herramientas del equipo, este es el caso de los modelos iPhone de la industria celular de Apple, quienes hicieron el primer lanzamiento del modelo en enero del 2007 y tiene versiones fáciles de realizar análisis digitales hasta la tercera, sin embargo a partir de la cuarta versión, la seguridad es más infranqueable, esto debido a la proliferación de delincuentes cibernéticos que abundan en las redes y que dañan con virus el software de celulares y otros dispositivos de redes.

## 1.2 Planteamiento del Problema.

En la actualidad el uso de dispositivos móviles de tecnología mejorada va en aumento, estos a la vez que facilitan las tareas de sus usuarios, han provocado también que se creen nuevas formas de delito, existe frente a esto desconocimiento de los procesos y herramientas que se puede utilizar para comprobar a través de las bases de datos de estos equipos si se ha cometido o no un delito, una intromisión en el caso de delitos informáticos, poca difusión sobre las vulnerabilidades que los aplicativos poseen, los malware del que los usuarios pueden ser víctimas, o si el usuario de dicho dispositivo ha hecho uso inadecuado del mismo, tampoco se difunde información adecuada sobre como un dispositivo móvil puede estar involucrado en la escena de un crimen, es por ello que la presente investigación tiene como propósito dar a conocer los procedimientos de un análisis forense empleando herramientas y aplicaciones open source, la cual se aplicará

específicamente en un equipo iPhone.

Según (Pinto, 2014)

> Las tareas de análisis forense (Lázaro, 2013) en dispositivos móviles pueden volverse en muchas ocasiones una ardua labor, y bajo ciertas circunstancias como: condiciones internas de la organización, falta de conocimiento o inexistencia de estándares o buenas prácticas; y condiciones como: el desconocimiento o falta de leyes, hacen que el estudio se pueda volver incluso imposible. (p. 31).

En este sentido el análisis evidencia como proceder y cómo actúan los especialistas forenses ante el aumento de incidentes, fraudes y ataques tecnológicos. Siendo así, el análisis forense dentro de este ámbito se posiciona como una alternativa para lograr esclarecer situaciones ilícitas producidas en los sistemas operativos o informáticos, enfocando el estudio en alcanzar información sobre los actores del atraco o fraude mediante los dispositivos móviles. Sin embargo, la falta de patrones y procesos establecidos en un manual general y global para todas las instancias y establecimiento para lograr un adecuado análisis forense en el que se resguarde los datos considerados como evidencia legal obstaculizan el alcance de las funcionalidades del servicio prestado mediante los análisis forenses.

## 1.3 Objetivos

### 1.3.1 Objetivo General

Realizar el análisis forense a dispositivos móviles con tecnología iPhone para la obtención de información almacenada e interpretación, utilizando herramientas de análisis forenses open source.

### 1.3.2 Objetivos Específicos

- Examinar la arquitectura de dispositivos iPhone.
- Distinguir los diferentes mecanismos de almacenamiento de datos en dispositivos iPhone.
- Identificar los mecanismos de seguridad de los dispositivos iPhone.
- Utilizar técnicas específicas necesarias para la obtención de información en dispositivos móviles.
- Utilizar herramientas de software forense open source para dispositivos iPhone.

## 1.4 Justificación e Importancia

El panorama de acceso ilimitado a datos en internet, que presenta la nueva era por el avance tecnológico en cuanto a dispositivos móviles ha generado nuevas formas de comunicación y de actuar, los teléfonos celulares se asemejan cada vez más a un ordenador, por su capacidad y aplicaciones, lo que crea nuevos modos operandi de la delincuencia, aumentando el riesgo de ser víctima de fraude, acoso cibernético, entre otros delitos.

Para Ramo, et. al. (2004) señala:

> Con el crecimiento del número de delitos informáticos diversos países han empezado a incluir este concepto en sus legislaciones, reglamentando la admisibilidad de la información digital como evidencia en la investigación de un posible delito.
>
> En este sentido, para lograr la admisibilidad de la evidencia digital en una corte, el proceso de manipulación de la misma debe apoyarse en una técnica forense rigurosa que garantice la confidencialidad e integridad de los datos (p. 293).

Se evidencia entonces la necesidad de reforzar de algún modo la seguridad informática, para evitar todo tipo de crímenes informáticos, por ello es imprescindible especificar e implantar mecanismo que resulten prácticas de seguridad. Siendo así una de las mayores problemáticas en la actualidad es la falta de un proceso unificado que guíe a los especialistas en el ámbito forenses en su trabajo de análisis de la evidencia digital.

A diferencia de los procedimientos que se realizaban antes del aparecimiento de equipos con tecnología “inteligente” los nuevos delitos requieren de constante capacitación en los procesos de investigación, los ataques informáticos aumentan y quienes los realizan se van profesionalizando más, es por ello que los agentes policiales deben conocer también las herramientas de nuevas formas de llevar a cabo la investigación y custodia de la evidencia.

El interés de la presente investigación es realizar el análisis forense a dispositivos móviles con tecnología iPhone, mismos que son equipos de tecnología desarrollada que dan opciones avanzadas a sus usuarios para realizar sus tareas diarias y que por todos los beneficios que prestan son considerados atractivos para el cometimiento de ilícitos informáticos. De tal manera a la par que se desarrollan aplicaciones para los compradores de estos celulares, se desarrollan también aplicaciones que permiten a los especialistas obtener información necesaria en la investigación de los casos en que estos equipos son parte de la evidencia, tales como herramientas open source.

Para realizar el análisis forense de estos dispositivos es necesario primero comprender la estructura de la tecnología iPhone, para posteriormente especificar actividades aplicables a diversos entornos y dispositivos con herramientas adecuadas que permitan la recuperación de información sin alteración alguna.

Esta investigación se convierte en una guía útil para quienes realizan el estudio de estos dispositivos, para apoyarlos en su labor, para facilitar la obtención de la información de manera adecuada.

## 1.5 Alcance

En cuanto al alcance del análisis forense y el papel fundamental que cumple en la actualidad esta disciplina radica en sus objetivos y su trascendencia. Si bien es cierto que la informática forense sobre dispositivos móviles surge a raíz del voraz avance e innovación en temas tecnológicos aplicados a los dispositivos móviles inteligentes, que al mismo

tiempo han propiciado un panorama de riesgos a posibles ataques o delitos informáticos, puesto que a la par del surgimiento de tecnologías que facilitan el trabajo en temas judiciales, se evidencia también un crecimiento de nuevos mecanismos para el cometimiento delitos y fraudes.

Para Rueda, et. al. (2001) determina:

> La informática forense es una disciplina de la ciencia forense que nace de la necesidad de adquirir una nueva fuente de evidencias. Con el auge de los dispositivos móviles, los cibercriminales han dirigidos sus ataques hacia estos dispositivos (p.1).

De tal manera que en vista de esta situación que influye directamente sobre las personas que cuentan con un dispositivo con ciertas características es necesario llevar a cabo un análisis y estudio a profundidad destinado al uso de quienes se dediquen a este tipo de oficio con el fin de facilitar el respectivo investigación forense a través de herramientas específicas. Con el objetivo último de aportar con evidencia que sirva como soporte en procesos judiciales.

Por otro lado, como se menciona que el acelerado ritmo de mejoras y avances en cuanto a tecnología y aplicaciones con el afán de brindar mayores servicios en telefonía replantean el horizonte de la misma.

Para Rueda, et. al. (2014) determina:

> Los dispositivos móviles han venido en constante evolución. El desarrollo de su hardware y software ha permitido que se lleven actividades más complejas que realizar una llamada o enviar un mensaje de texto.
>
> A estos dispositivos le hemos confiado más actividades personales y laborales. Cada día se maneja más volumen de información y de mayor importancia (p.1).

Conforme a lo mencionado, el caso de los teléfonos iPhone cuyo sistema operativo y capacidad de almacenamiento y procesamiento de datos van en aumento, es importante entender la estructura del este dispositivo. Por ello el análisis forense va más allá de localizar evidencia electrónica y de recopilarla. Requiere de una comprensión, adquirir, analizar y entender todo lo que conforma el análisis y la arquitectura del dispositivo a analizarse. De tal manera que al momento de recuperar los datos todos los factores y elementos mencionados confluyen entre sí para culminar con un proceso exitoso.

## 1.6 Factibilidad de recursos

Factibilidad se refiere a la disponibilidad de los recursos necesarios para llevar a cabo los objetivos señalados.

> El estudio de factibilidad es un instrumento que sirve para orientar la toma de decisiones en la evaluación de un proyecto y corresponde a la última fase de la etapa pre-operativa o de formulación dentro del ciclo del proyecto. Se formula con base en información que tiene la menor incertidumbre posible para medir las

posibilidades de éxito o fracaso de un proyecto de inversión, apoyándose en él se tomará la decisión de proceder o no con su implementación. , (Gestiopolis.com Esperto, 2001)

En cuanto a la factibilidad de recurso para la ejecución del presente trabajo investigativo se centra principalmente en el acceso a la información para recabar datos y estudios relacionados al tema para contrastar, organizar y generar un conocimiento que contribuya en el análisis forense de dispositivos móviles con tecnología iPhone mediante herramientas como open source.

Por tanto esta investigación se enmarca dentro de los estudios de la Escuela Politécnica del Ejército, de allí que cuenta con el apoyo y aprobación de la misma institución. Además, como requerimientos básicos para efectuar la investigación se cuenta con requerimientos mínimos de hardware y del software. La factibilidad de recursos contempla tres factores que son, el operativo, el técnico y el económico.

### 1.6.1 Factibilidad operativa

Se refiere a todos aquellos recursos donde interviene algún tipo de proceso; esta factibilidad depende de los recursos humanos que participan durante la operación del proyecto. Durante esta etapa se identifican todas aquellas actividades que son necesarias para lograr el objetivo y se evalúa y determina todo lo necesario para lograr con el objetivo.

En el caso del análisis Forense se ha determinado cuáles son las fases que deberá seguir el personal especializado, estas son: Fase preparatoria, Fase de análisis y Fase de resultado del análisis y posterior informe de las cuales se hablará en el siguiente capítulo de manera más detallada.

### 1.6.2 Factibilidad Técnica.

La factibilidad técnica se refiere a los recursos necesarios, es decir las herramientas, conocimientos, habilidades, experiencia, que son necesarios para efectuar las actividades o procesos que requiere el proyecto. El proyecto debe considerar si los recursos técnicos actuales son suficientes o deben complementarse.

Kendall en su estudio sobre Análisis y Diseño de Sistemas, considera que:

> Una gran parte de la determinación de recursos tiene que ver con la valoración de la factibilidad técnica. Al analista debe encontrar si los recursos técnicos actuales pueden ser mejorados o añadidos, en forma tal que satisfagan, la petición bajo consideración. Sin embargo, algunas veces las "adiciones" a los sistemas existentes son costosas y no valen la pena. (…) Aquí es donde es benéfica la experiencia del analista de sistemas, debido a que mediante el uso de su propia experiencia. (Kendall & Kendall, 2011, pág. 52)

Para la realización del análisis forense se cuenta con personal especializado tales como: personal investigador, técnicos, custodio de la evidencia, examinador analista, cada uno con su rol y función. Para el desarrollo de este proyecto se utilizará el equipo celular adecuado, herramientas open source y personal especializado.

### 1.6.3 Factibilidad Económica

Se refiere a los recursos económicos y financieros necesarios para desarrollar o llevar a cabo las actividades o procesos y/o para obtener los recursos básicos que deben considerarse como el costo del tiempo, el costo de la realización y el costo de adquirir nuevos recursos.

> En la factibilidad económica los recursos básicos a considerar son: el tiempo propio y el del equipo (…) El costo de hacer un estudio de sistema completo, el costo del tiempo de los empleados (…) El costo estimado de hardware y el costo estimado del software (Kendall & Kendall, 2011, pág. 53)

Para la realización del proyecto este no se requiere muchos recursos económicos pues se cuenta con el dispositivo que cumple las características para el análisis y las aplicaciones de código libre.

## 1.7 Gestión del Proyecto

La gestión del proyecto se refiere al equipo de trabajo y las tareas de las que cada uno será responsable, estas se contemplan  más adelante en la fase preparatoria del análisis forense en la que se define las obligaciones de cada persona a cargo de éste.

La gestión de un proyecto de tecnología informática tiene tres etapas importantes:

1. Organización del equipo de trabajo
2. Desarrollo del plan del proyecto
3. Ejecución del proyecto

En la etapa de Organización se define quien estará a cargo de la dirección, qué áreas de especialización son vitales para ejecutar el proyecto, qué información es necesaria y a la vez los roles y responsabilidades de los miembros, los que deben poseer habilidades específicas, dentro de las cuales está la capacidad de investigación, facilidad de expresión verbal y escrita y amplios conocimientos.

Los miembros claves del equipo del proyecto deben ser identificados y contratados según varios criterios, incluyendo:

- Experiencia en las áreas identificadas del proyecto
- Conocimiento o acceso a información vital para el proyecto
- Capacidad de investigación y otras habilidades necesarias (Smetoolkit, 2012)

En la etapa de Desarrollo del proyecto, algunas de las cosas a tomar en cuenta son: Razón, alcance y limitaciones del proyecto, Elementos claves, tareas, actividades, y

responsabilidades asociadas, Recursos v problemas potenciales, criterios de evaluación de rendimiento (Smetoolkit, 2012)

La etapa de Ejecución del proyecto, se refiere a la puesta en marcha de lo planificado, en esta etapa se realiza  informes de avance programados para determinar cuánto se ha hecho.

# CAPÍTULO II.

# 2. MARCO TEÓRICO

## 2.1 HISTORIA DEL ANÁLISIS FORENSE

En los últimos años la ciencia informática y digital ha revolucionado y modificado los modos y estilos de vivir; a partir de los años 80 en que introdujo internet en el mercado, este acompaña a las personas en todas sus tareas, quienes han remplazado muchos productos y artefactos que organizaban su vida, por el ordenador y posteriormente por los dispositivos celulares, pero a estos beneficios acceden personas procedentes de entornos diversos y con intenciones diversas también, tanto así que la modalidad de delitos cambiaron también a partir de las nuevas tecnologías informáticas, es por ello que las naciones han debido cambiar o modificar sus leyes para poder registrar los delitos informáticos e incluir en sus sistemas judiciales el reconocimiento de nuevos medios de evidencia o pruebas como lo son las digitales, las cuales puedan servir en casos judiciales.

> El campo de la informática forense se inició en la década de 1980. En 1984, fue creado un programa del FBI, conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART, o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", comenzó a trabajar en este campo. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense.

> En 1997, se reconoció ampliamente que los funcionarios encargados de hacer cumplir la ley en todo el mundo tenían que ser bien versados en la forma de adquirir la evidencia de las computadoras, un hecho puesto de manifiesto en un comunicado del G8 en 1997. INTERPOL celebró un simposio sobre informática forense al año siguiente, y en 1999, el programa CART del FBI abordó 2000 casos individuales. (eHow en Español)

Con los avances en la informática y el fácil acceso a internet, esta gama de la informática se hizo muy importante y necesaria para los agentes policiales, de manera que se realizan estudios específicos en ordenadores y dispositivos móviles, denominados análisis forense, el cual a través de procesos para evaluar la evidencia.

De la misma manera que se realizan estudios para determinar causa y muerte en casos de homicidios, se realiza en informática forense análisis de las causas en delitos informáticos, las compañías son las más interesadas en este tipo de análisis ya que les permite asegurar ingresos al determinar causantes o intromisiones en sus sistemas informáticos.

Según (Mattison, 2009) establece que:

> El tema de Técnicas Estadísticas y su aplicación al Análisis Forense es vasto, pero el resumen ayudara a obtener una visión general del área. Está claro que una inversión de la industria en la exploración y aplicación de Técnicas Estadísticas a

> los restos del Análisis Forense, sin duda producirá amplios y efectivos beneficios para la industria durante los próximos años. El resultado final del proceso de Análisis Forense es el Reporte de Resultados de Análisis Forense. A pesar que la formula específica y el formato para el reporte variará de acuerdo a la organización, el caso específico bajo revisión, y el propósito del análisis, hay ciertos elementos claves que deben ser incluidos, tales como Resumen del caso/ dominio, revisión de los procedimientos, ingreso en riesgo y la revisión de remediación. (p.90)

En la actualidad este proceso está mucho más desarrollado que en sus inicios, y básicamente consiste en comprobar a través del análisis a la evidencia digital, el grado de participación en un delito de las personas implicadas.

> El primer delito informático que se cometió en el Ecuador fue en el año 1996 en un caso conocido, que fue denunciado pero que nunca obtuvo sentencia y es sobre el redondeo que se realizaba en las planillas realizadas por el antiguo EMETEL, y que no se sabía a donde se dirigían estas cantidades que muchas veces eran demasiado pequeñas para que cause discusión, pero ya en grandes cantidades era una cantidad de dinero muy apreciable, en esto se puede decir que se utilizó la técnica del salami o roundingdown. (Cuenca, 2013)

## 2.2 ANÁLISIS FORENSE

El Análisis forense hace referencia a la investigación de hechos y evidencias, haciendo uso de la ciencia y la tecnología. Por tanto el análisis forense es una disciplina de la ciencia forense y de la investigación que alude a los mecanismos usados para conservar y recuperar la información digital sin ningún tipo de alteración.

Ramos, et. al. (2004) especifica:

> La informática forense como aplicación de las ciencias de la computación a la investigación criminal, ofrece la posibilidad de, metodológicamente identificar, recuperar, preservar, reconstruir, validar, analizar, interpretar, documentar y presentar evidencia digital como parte de la investigación de un incidente informático. (p. 293).

Otra definición que permite entender con mayor claridad el análisis forense determina que el análisis forense se asocia a la ciencia de la evidencia.

Rueda, et. al. (2001) señala:

> Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura describir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación forense ofrece un análisis de la información residente en dichos equipos (p. 3).

El análisis forense digital se realiza con técnicas que ayudan a extraer información valiosa de discos, sin alterar el estado de los mismos. La aplicación de técnicas precisas permite obtener datos informáticos en los que se buscará patrones de comportamiento específicos, las técnicas también permiten descubrir información oculta en el disco.

### 2.2.1 Informática Forense

> La informática forense es una rama de las ciencias forenses, que involucra la aplicación de la metodología y la ciencia para identificar, preservar, recuperar, extraer, documentar e interpretar pruebas o evidencias procedentes de fuentes digitales con el fin de facilitar la reconstrucción de los hechos encontrados en la escena del crimen, para luego usar dichas evidencias como elemento material probatorio en un proceso judicial (p. 8).

La Informática forense es una ciencia que se crea para reducir el porcentaje de fraudes electrónicos, permite solucionar conflictos relacionados con la tecnología, su principal objetivo es asegurar el principio de seguridad en las redes, para ello investiga los sistemas de información y detecta vulnerabilidades.

### 2.2.2 Marco legal

En el Ecuador los primeros tipos penales informáticos que se incluyeron en la Legislación Ecuatoriana fueron en el año 2002 en el proyecto para la creación de la ley de comercio electrónico, firmas electrónicas y mensajes de datos, (Cuenca, 2013) algo que ya se había discutido en el año 1999 formando comisiones con organismos interesados

directamente como el CONATEL, posteriormente estos delitos fueron incluidos en el Código Penal. (Cuenca, 2013).

Varios fueron los incidentes que marcan la necesidad de incluir los nuevos delitos en la Legislación Ecuatoriana, como el acoso sexual por redes que vulnera los derechos generalmente de adolescentes que se inician en el ciber espacio.

En 2010, en Ecuador se registraron 866 denuncias de este tipo que no estaban tipificadas como ciber delitos, la Fiscalía los ingresó como apropiación ilícita. En 2011 se incrementaron a 3.200 las denuncias, lo cual alertó a las autoridades y se prepararon las estrategias para minimizarlo.

> En el año 2012 empezó a operar la Unidad de Crimen Cibernético en Ecuador y se conocieron los primeros 60 casos de este tipo de delitos. En 2013 se contabilizaron 433 denuncias y en los primeros 5 meses de 2014 hay 167 registradas. (…) El general Zapata señaló que en 2010 elaboraron un estudio sobre los delitos cibernéticos que concluyó en la creación de la policía especializada en este campo, en la tipificación de los delitos cibernéticos, lo que está contemplado en el Código Orgánico Integral Penal (COIP), y en la firma del convenio de Budapest. Este tratado internacional busca enfrentar los delitos informáticos mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y la cooperación entre las naciones. (El telégrafo, 2012).

Para cometer un delito cibernético, basta con contar con la herramienta ya que el espacio es lo de menos, desde cualquier lugar del mundo por lo que se requiere de la cooperación Internacional.

> El fraude electrónico es el delito cibernético que más se comete en Ecuador, especialmente el que se realiza a través de cajeros automáticos, que en 2013 representó el 46% de las denuncias, seguido por el 37% de los robos a través de la banca virtual por transferencias, previo a la sustracción de las claves de acceso. (El telégrafo, 2012).

Los delitos informáticos tienen alcance incluso institucional, dado los conocimientos de los operadores computacionales se puede llegar a cometer ilícitos de diversa índole, un ejemplo es el mal uso que funcionarios del Registro Civil estaban haciendo de las tecnologías en el año 2012 cambiando los datos de las cédulas, para lo que ingresaron en el sistema macro de la institución".

> Siguiendo con este tipo de ejemplos, otro caso sucedió en el año 2012 también cuando "Valiéndose de la computación, otras 2 personas vulneraron las seguridades del Biess, crearon claves de algunos clientes y gestionaron préstamos por más de $ 85.000". En el COIP se tipifica este tipo de acciones desde los artículos 229 al 234, de la sección tercera sobre los delitos contra la seguridad de los activos de los sistemas de información y comunicación. (El telégrafo, 2012).

El Ciberdelito ha proliferado en el Ecuador porque las tecnologías avanzan y cada vez hay màs usuarios y consumidores de ésta, las ventajas que ofrecen los dispositivos mòviles denominados inteligentes debido a la cantidad de aplicaciones que tienen, que los asemejan a un ordenador, facilitan el cometimiento de delitos, los cuales pueden ser desde la extorsión, acoso, clonación celular, hasta la producción y envío de pornografia infantil.

En el Código Orgánico Integral Penal, que rige actualmente desde hace un año, se tipifican los siguientes delitos que se pudieran cometer a través de la informática digital o contando con un dispositivo móvil:

> Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.
>
> Art.190. Apropiación fraudulenta por medios electrónicos.
>
> Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles
>
> Art.192.- Intercambio, comercialización o compra de información de equipos terminales móviles Art. 193. Reemplazo de identificación de terminales móviles. Art194. Comercialización ilícita de terminales móviles.
>
> Artículo 212.- Suplantación de identidad
>
> Art. 231.- Transferencia electrónica de activo patrimonial. Art. 354.Espionaje (COIP, 2014).

### 2.2.3 Modelo forense

Un modelo forense se enmarca dentro del análisis forense o la informática forense como proceso complementario a un proceso legal judicial. Este especifica los patrones de procedimientos para recopilar información o evidencia digital almacenada en un dispositivo móvil con la finalidad de no perderla ni alterarla y que se califique como información valida.

Para Rueda, et. al. (2001) determina.

> Desde sus inicios se ha desarrollado algunos modelos forenses para ayudar a desarrollar de mejor forma el proceso por el cual pasa la información, desde la extracción hasta la etapa final de la entrega del informe parcial.
>
> Algunos de los modelos que han surgido a través de los años son: Casey (2000), el modelo publicado por el U.S Dep. of Justice (2001), el modelo Lee (2001), el modelo Reith, Carr y Gunsch (2002), el Modelo integrado de Brian Carrier y Eugene Spafford (2003), el modelo mejorado propuesto por Venansius Baryamureeba y Flerence Tuchabe (2004) y el modelo extendido de Séamus Ó Ciardhuáin (2004). (Arquillo Cruz, 2007) (De León Huertas, 2009) (p. 3).

Un modelo forense de acuerdo a las características del sistema operativo en que se pretende hacer el análisis, permitirá: detectar inconformidades; obtener evidencias; localizar vulnerabilidad; hacer hallazgos en bases de datos, textos planos, logos de

aplicativos; reconstrucción de delitos informáticos; investigar fraudes. Determinar con evidencias, las caudas de une evento o delito, cometido desde un dispositivo móvil.

## 2.3 DISPOSITIVOS MÓVILES

Un dispositivo móvil se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, se los puede transportar a cualquier lugar. Brindan la posibilidad de conexión, acceso a datos, comunicación y otras actividades. Es decir se habla de dispositivos portátiles que acompañan al usuario a todo lugar, dentro de estos encontramos computadoras portátiles ya sean laptops o notebook, celulares de diferente tecnología dentro de los que se encuentran los denominados “inteligentes”, tablets, relojes inteligentes, etcétera.

Los dispositivos móviles tienen capacidad de almacenamiento y herramientas que facilitan las tareas de sus usuarios, se pueden conectar a una red sin la necesidad de cables. De la misma forma se caracteriza por tener la capacidad de conexión permanente o temporal a la red, si bien hemos pasado del texto al ordenador, con estos dispositivos trasladamos las tareas del ordenador a artefactos de menor tamaño que cumplen con tareas similares, en la actualidad predominan los celulares inteligentes debido a la cantidad de aplicaciones a las que el usuario tiene acceso y con las cuales sus tareas se facilitan.

(Tardaguila, 2009) determina:

> Se pueden definir como aquellos micro-ordenadores que son lo suficientemente ligeros como para ser transportados por una persona, y que disponen de la capacidad de batería suficiente como para poder funcionar de forma autónoma. Normalmente, son versiones limitadas en prestaciones, y por tanto en funcionalidades, de los ordenadores portátiles o de sobremesa. Por cierto, los ordenadores portátiles no se consideran como dispositivos móviles, ya que consumen más batería y suelen ser un poco más pesados de lo que se espera de algo pensado para llevar siempre encima. (p. 4)

De esta manera se determina que los dispositivos móviles son una versión micro de un ordenador, con las características tecnológicas adecuadas que permiten establecer una interacción gracias a sus aplicaciones.

Algunos de los ejemplos de estos dispositivos son los siguientes:

- Paginadores.
- Comunicadores de bolsillo.
- Internet Creen Phones.
- Sistemas de navegación de automóviles.
- Sistemas de entretenimiento.
- Sistemas de televisión e Internet (WebTV).
- Teléfonos móviles.
- Organizadores y asistentes personales digitales (Guevara, 2012)

De acuerdo a (Santiago, Trabaldo, Kamijo, & Fernández, 2015)

> Se denomina dispositivo móvil (Mobile device), también conocido como computadora de bolsillo o computadora de mano (palmtop o handheld), a todo tipo de computadora de tamaño pequeño, con capacidades de procesamiento, memoria suficiente y conexión a internet, diseñada para una función específica pero con capacidades para llevar a cabo otras tareas más amplias. (p. 25)

De los dispositivos móviles el que más destaca es el celular móvil, cuyas características se han modificado a las necesidades de los usuarios que día a día se multiplican. No todos los dispositivos móviles cuentan con las capacidades y características de un ordenador, dado que algunos ofrecen menos beneficios que otros respecto a memoria y herramientas de tareas y son diseñados para ciertas funciones más limitadas que los nuevos modelos.

### 2.3.1 Clasificación de los dispositivos móviles

En cuanto a la clasificación de los dispositivos móviles estos responden a ciertas características que a partir de ello se establecen aspectos o criterios que permiten diferencias tres categorías relacionadas a la capacidad o proporción de datos de cada modelo, estos pueden ser limitados, básicos y mejorados.

Así establecen (Santiago, Trabaldo, Kamijo, & Fernández, 2015)

a) Dispositivos móviles de datos limitados: se caracteriza por poseer pantallas pequeñas, principalmente de tipo texto, y servicios de datos generalmente limitados a SMS y acceso WAP.

b) dispositivo móvil de datos básico: en este caso, la pantalla es de mediano tamaño, el menú o navegador está basado en iconos por medio de una rueda o cursor y permite el acceso a e- mail, lista de direcciones, SMS, navegador Web básico, etc.

c) Dispositivo móvil de datos mejorado: dispone de pantalla mediana o grande, navegación de tipo Stylus o táctil (Apple), aplicaciones de MS Office (Word, Excel, Power Point), aplicaciones corporativas usuales en versión móvil (como SAP), portales intranet y sistemas operativos, como el Windows Mobile. (p. 36).

Los dispositivos Móviles de datos limitados generalmente pertenecen a modelos más sencillos y económicos, las aplicaciones son limitadas, permiten acceso a internet pero su plataforma es menos sofisticada, las pantallas son de tamaño más grande que los dispositivos móviles de datos Básicos, los modelos que resaltan de este tipo de dispositivos son los Smartphone que entran también en la categoría de teléfonos inteligentes, las principales diferencias entre los dispositivos móviles básicos y los de Datos Mejorados radica en las aplicaciones que estos últimos ofrecen como navegación de tipo stylus, aplicaciones corporativas usuales, portales intranet, la forma de navegación de datos

mejorados supera la ofrecida por los de datos básicos, además que éste tipo de dispositivos incluyen los open source , como Windows Mobile.

De esta gama de dispositivos los que son de nuestro interés son los teléfonos inteligentes, cuya tecnología destaca de los otros por la cantidad de aplicaciones, herramientas y beneficios que otorgan al usuario, además de la seguridad de confidencialidad de información.

### 2.3.2 Características

Dentro de las características que resaltan y definen a los dispositivos móviles esta principalmente el tamaño y tecnología, se determina que los dispositivos móviles responden a ciertas particularidades similares que comparten en su mayoría.

Para (Morillo, 2010)

- Son aparatos pequeños.
- La mayoría de estos aparatos se pueden transportar en el bolsillo del propietario o en un pequeño bolso.
- Tienen capacidad de procesamiento.
- Tienen conexión permanente o intermitente a una red.
- Tienen memoria (RAM, tarjetas MicroSD, flash, etc.).
- Normalmente se asocian al uso individual de una persona, tanto en posesión como en operación, la cual puede adaptarlos a su gusto.

Tienen una alta capacidad de interacción mediante la pantalla o el teclado. En la mayoría de los casos, un dispositivo móvil puede definirse con cuatro características que lo diferencian de otros dispositivos que, aunque pudieran parecer similares, carecen de algunas de las características de los verdaderos dispositivos móviles.

Estas cuatro características son:

1) movilidad

2) tamaño reducido

3) comunicación inalámbrica

4) interacción con las personas (p. 7).

En los teléfonos móviles los teclados son de un tamaño realmente reducido o táctil, permitiendo la escritura directa en la pantalla.

## 2.4 ANÀLISIS FORENSE EN DISPOSITIVOS MÒVILES

El análisis forense digital aplicado en dispositivos móviles, es aquella investigación detenida y meticulosa que se realiza con el objeto de determinar algún dato de relevancia en la información digital almacenada en un dispositivo móvil inteligente, como la identificación de rastros digitales, para que los resultados de tal investigación, puedan ser presentados como evidencia y lograr aportar en la solución de algún delito.

Dentro del análisis forense para los dispositivos móviles parte de los diferentes estudios se aconseja efectuar el respectivo examen por partes, para mantener un orden que ayude a mantener la fiabilidad de las evidencias, entre ellas dos sumamente importantes: el ME o el equipo móvil propiamente dicho, y el segundo que corresponde al SIM o el módulo de suscriptor.

Existen diferencias entre el análisis forense que se realiza a un sistema informático y el análisis forense que se lleva a cabo en dispositivos móviles. Las principales causas que hacen diferente un análisis forense en sistemas informáticos de un análisis forense realizado en dispositivos móviles, son las siguientes:

- La variedad de fabricantes y modelos de teléfonos que existen en el mercado de telefonía celular.
- La heterogeneidad que se presenta tanto en la configuración de hardware, sistema operativo, forma de acceso y tipo de aplicaciones que manejan los teléfonos móviles.
- La información volátil y dinámica que poseen los teléfonos móviles en lo que es información de localización e información personal.
- En la mayoría de los casos, los fabricantes de teléfonos móviles optan por crear y aplicar sus propios protocolos e interfaces para uso de sus sistemas operativos, ocasionando que para los analistas forenses sea más difícil realizar una investigación.

- Las herramientas que se disponen en el mercado, que se pueden utilizar para recuperar contenido son variadas, se tiene modelos y marcas de teléfonos móviles que muchas veces no son compatibles con todas las herramientas.
- Existe poca literatura sobre el análisis forense de teléfonos móviles, en especial de teléfonos inteligentes. (Maleza, 2011)

Los principales inconvenientes que se dan en el momento de realizar análisis forense a los dispositivos móviles consiste precisamente en las herramientas de análisis que se han de aplicar, ya que se debe tomar en cuenta varias características propias del celular incautado, tales como: modelo, marca, que determinan la facilidad o dificultad en el procedimiento, en el caso de los dispositivos iPhone, sus fabricantes utilizan sus propios protocolos.

Las diferencias de los análisis de sistemas operativos y de dispositivos móviles radican principalmente en sus sistemas operativos y que las herramientas que se encuentran en el mercado para realizar tales análisis son menos accesibles respecto a los celulares.

## 2.5 TECNOLOGÍA

La definición que utiliza la Organización Mundial de la propiedad Intelectual en su Guía de licencias para países en desarrollo, define a la tecnología como aquel conocimiento sistemático para la fabricación de un producto, la aplicación de un proceso, o el suministro de un servicio, si este conocimiento puede reflejarse en una

invención, un diseño industrial, modelo de utilidad o en una variedad de una nueva planta… (Echarri, 1999)

La Tecnología hace referencia a las formas en que las personas cambiamos nuestro entorno, es producto de la ciencia y la ingeniería y se la aplica en casi todas las áreas de la vida, la tecnología se va desarrollando a la par que el hombre avanza, ya sea para comunicarnos de mejor manera o para controlar enfermedades, se han desarrollado inventos que permiten mejorar la calidad de vida de las personas, la tecnología se desarrolla dese la edad de piedra y evoluciona con el paso del tiempo.

### 2.5.1 Tecnología iPhone

La tecnología iPhone hace referencia a equipos Apple, en lo que respecta telefonía móvil, el Sistema operativo de IPhone discierne de los Android porque a diferencia de éste su software es de código cerrado y sólo Apple puede realizar modificaciones.

El Sistema IOS es creado específicamente para IPhone, las aplicaciones de IOS funcionan bien con Google pero no con Android, es decir las aplicaciones de un iPhone no funcionan en un Android.

El iPhone es un teléfono móvil cuyas características de forma y composición lo posicionan como un teléfono móvil inteligente, su capacidad y aplicaciones disponibles permiten al usuario acceder a una infinidad de información mediante las redes e internet.

Ariza, et. al. (s.a) determina:

> El iPhone es un dispositivo móvil creado por Apple, caracterizado principalmente por combinar tres productos en uno: un teléfono revolucionario, un iPod2 de pantalla ancha y un innovador dispositivo de internet que permite navegar en la web, recibir correos electrónicos con HTML enriquecido y navegación web completa (p. 3).

#### 2.5.1.1 Estructura de un iPhone

La estructura del iPhone responde a un teléfono de alto rendimiento por tanto se lo considera inteligente, similar a un ordenador. Como parte estructural más importante se especifican partes de un iPod y un teléfono.

Ariza, et. al. (s.a) determina:

> El iPhone es un teléfono inteligente que integra funcionalidades de iPod y teléfono celular [26]. Es en esencia un computador ejecutando una versión del sistema operativo Leopard UNIX OS de Apple, diseñado principalmente para minimizar las escrituras sobre la memoria flash, de forma tal que se puede conservar y preservar datos por periodos largos de tiempo, incluso por mucho más tiempo que lo que un computador de escritorio podría hacerlo (p. 3).

Los teléfonos IPhone se caracterizan por la pantalla Touch, memoria amplia desde 8 a 16 Gb de NAND flash. En el caso de 8 Gigabytes. El iPhone posee en su interior un especial procesador (Xataka Movil, 2008), tal como se indica en la tabla No.1

**Tabla 1.**
Estructura de un iPhone

| Dimensiones y peso | Color | Capacidad |
|---|---|---|
| Alto: 115,5 mm<br>Ancho: 62,1 mm<br>Fondo: 12,3 mm<br>Peso: 133 g | Modelo de 8 GB: negro<br>Modelo de 16 GB: negro o blanco | Unidad flash de 8 o 16 GB |
| Telefonía y redes inalámbricas | **Pantalla** | **Sonido** |
| UMTS/HSDPA (850, 1.900 y 2.100 MHz)<br>GSM/EDGE (850, 900, 1.800 y 1.900 MHz)<br>Wi-Fi (802.11b/g)<br>Bluetooth 2.0 + EDR<br>GPS asistido | Panorámica Multi-Touch de 3,5 pulgadas (en diagonal)<br>Resolución de 480 por 320 píxeles a 163 ppp<br>Posibilidad de alternar entre distintos idiomas y alfabetos | Respuesta de frecuencias: de 20 a 20.000 Hz<br>Formatos de sonido compatibles: AAC, AAC protegido, MP3, MP3 VBR, Audible (formatos 2, 3 y 4), Apple Lossless, AIFF y WAV<br>Límite de volumen máximo configurable por el usuario |
| Vídeo | **Cámara y fotos** | **Tipos de documentos compatibles:** |
| H.264 a un máximo de 1,5 Mb/s, 640 por 480 píxeles, | 2 megapíxeles<br>Etiquetado geográfico de fotos<br>Integrada con los programas de iPhone y de terceros | .jpg, .tiff, .gif, .doc y .docx (Word de Microsoft), htm y .html (página web), .key (Keynote), .numbers (Numbers), .pages (Pages), .pdf |

### 2.5.1.2 Teléfonos inteligentes

Los teléfonos móviles inteligentes son aquellos teléfonos puestos en el mercado cuya capacidad de funcionalidad es bastante similar al de un computador, los teléfonos inteligentes se caracterizan por su procesador de datos, y la capacidad de instalación de

diversas aplicaciones que facilitan una serie de actividades al usuario. Estos dispositivos inteligentes son de alta calidad, de un alto procesamiento, un porcentaje elevado de memoria y resolución.

El termino inteligente hace referencia a la posibilidad de usarlo como una suerte de computadora de bolsillo, y cada vez más – en algunos casos- llega incluso a remplazar a las computadoras personales (s.p).

En Ecuador la cantidad de usuarios de esta tecnología ha ido en aumento según lo indica el siguiente gráfico:

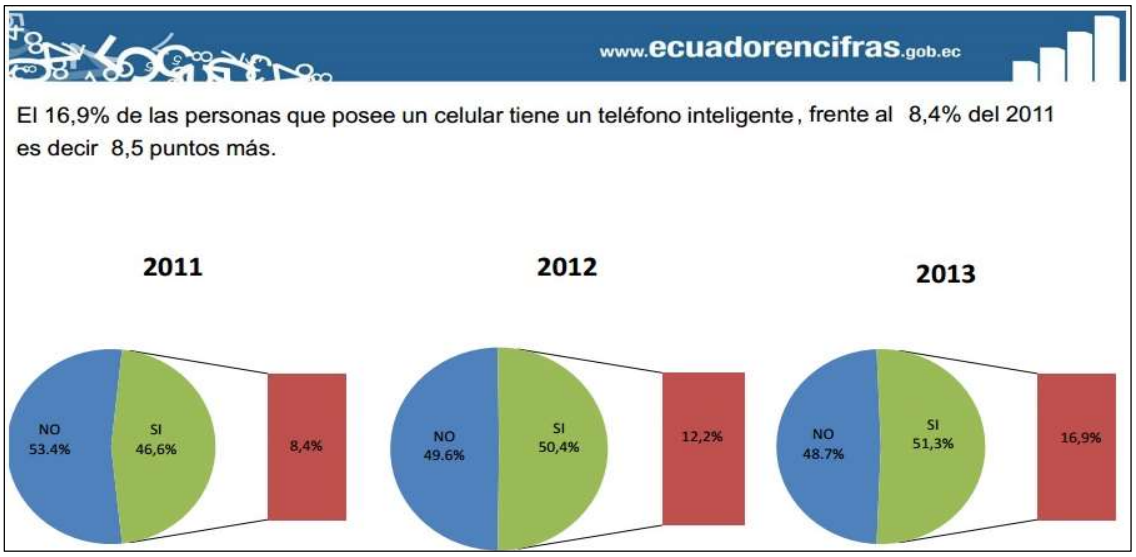



**Figura 1.** Usuarios a nivel nacional de celulares inteligentes
**Fuente:** (INEC, 2014)

Los teléfonos móviles inteligentes de última generación cuentan con una capacidad de procesamiento y almacenamiento amplio que permiten la instalación de diversidad de aplicaciones y programas para mejorar las tareas efectuadas por el teléfono, la capacidad de procesamiento de un teléfono inteligente se asemeja a un computador.

Chiles (2014) determina que:

> Un teléfono inteligente tiene más poder de procesamiento, memoria y resolución que los teléfonos celulares. Tienen sistemas operativos (OS) de las que le permite instalar aplicaciones (…) de software de terceros para su uso con el dispositivo. Con una rapidez comparada al de un computador de mesa (p. 91).

## 2.6 EVIDENCIA DIGITAL

De acuerdo a Eogan Cassey "La evidencia digital es un tipo de evidencia física, que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales" (Maleza, 2011) La evidencia digital a diferencia de las evidencias tradicionales, se encuentra en un formato binario de 1 y 0 que requiere ser descifrado con técnicas específicas.

Rueda, et. al. (2001) señala que "se define la evidencia digital como todos los datos que de manera digital que se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática" (p. 2). Por tanto la evidencia digital son aquellos datos e información posible, almacenada en un dispositivo informático o digital, que recogido de la manera adecuada puede ser considerado como evidencia de importancia frente a un hecho de delitos informáticos.

### 2.6.1 Legitimidad de la evidencia Digital

Una evidencia digital no se considera como tal hasta que el juez así lo determine, sin embargo según el artículo 471 del Código Orgánico Integral Penal de Ecuador, en el caso de tener videos como evidencia, no es necesaria la autorización judicial si las grabaciones de prueba de un ilícito se las obtiene en lugares públicos y de libre circulación donde se hayan instalado los dispositivos.

> La norma incluye, además de los videos, fotografías, datos informáticos, discos y otros medios análogos o digitales obtenidos de forma espontánea. Estas pruebas serán conocidas por el juez de la causa en audiencia privada, la que contará con dos peritos, el fiscal y las partes involucradas. Todos deberán realizar un juramento para mantener la reserva de la información. (El Universo, 2014)

Las normas que contempla el COIP, puesto en vigencia desde el 10 de agosto de 2014, acerca de los medios tecnológicos como prueba, da validez de estos como prueba en un proceso juzgatorio, cuando no se han obtenido ilícitamente y cuando cuentan con la autorización del juez, pero por otro lado no se requiere autorización judicial para las grabaciones de audio, imágenes de video o fotografía, relacionadas a hechos constitutivos de infracción, cuando son registradas de modo espontáneo al momento mismo de su ejecución, por los medios de comunicación, por cámaras de vigilancia o seguridad, por cualquier medio tecnológico, por particulares en lugares públicos y de libre circulación.

De tal manera el COIP viabiliza la utilización de medios tecnológicos, especialmente el video, estas evidencias serán estudiadas por el Sistema especializado integral de investigación de medicina legal y ciencias forenses.

> Sobre la “Retención de la correspon-dencia”, física, electrónica o de cualquier otro tipo o forma de comunicación es in-violable; pero el juzgador, podrá autorizar al fiscal, previa solicitud motivada, que re-tenga, abra o examine la correspondencia, cuando haya suficiente evidencia para pre-sumir que la misma tiene alguna informa-ción útil para la investigación; para lo cual se notificará previamente al interesado y con su concurrencia o no, se leerá la corres-pondencia o el documento, en forma reser-vada, informando del particular a la vícti-ma y al procesado o su defensor público o privado; la diligencia se realizará aunque no acudan los sujetos procesales, quienes serán reemplazados por dos testigos; pero todo los que intervengan deben guardar reserva. (…)
>
> Si la correspondencia u otros documen-tos están relacionados con la infracción que se investiga, se los agregará al expediente fiscal, después de rubricados; pero en caso contrario, se los devolverá al lugar de don-de fueron tomados o entregados al intere-sado. Si se trata de escritura en clave o en otro idioma, inmediatamente se ordenará su desciframiento por peritos en criptogra-fía o su traducción. (Blum, 2014)

### 2.6.2 Adquisición de evidencia

Las evidencias permiten, tras un exhaustivo análisis, determinar no sólo a los criminales sino detectar insuficiencias como vistas a mejorar la política de seguridad de una organización investigativa con fines de control delictivo.

Según (Colobran Huguet, Aques Soldevila, & Galindo, 2008)

> Una vez descrito el marco jurídico en el cual se ajustan las consultas ilícitas relacionadas con el uso de las tecnologías de la información, se estudiaran brevemente las metodologías de trabajo que se pueden emplear, una vez ha sucedido el incidente, con la finalidad de averiguar que ha ocurrido y quien ha sido el presunto autor. Estas técnicas se recogen en una disciplina de reciente creación, situada a caballo entre el marco jurídico y la tecnología, denominada informativa forense, Las huellas que permiten reconstruir la ejecución de un hecho se encuentran almacenadas en apoyos digitales y se llaman genéricamente evidencias digitales. (p. 254)

La adquisición de evidencia es una de las partes más importantes den el proceso judicial pues deben de estar en condiciones similares a cuando se las recolectó para ello se sigue una cadena de custodia.

### 2.6.3 Importancia del Análisis Forense

La principal importancia de sistematizar los modos de reunir evidencia y realizar el proceso de análisis forense, es para evitar cometer equivocaciones que puedan colocar en riesgo a toda la investigación, tales como la duplicación de tareas, es decir, desperdicio de recursos humanos en una actividad que ya está siendo atendida por otra persona y

precisamente por esta desorganización de atribuciones especificas se puede excluir involuntariamente pruebas y evidencias cruciales para la investigación.

Acorde con (Unidas, 2009)

> La importancia de las buenas prácticas en la investigación de la escena del delito y sobre la índole y pertinencia de las pruebas materiales. Versa sobre cuestiones relativas a la labor que se lleva a cabo en la escena del delito, desde la actuación de los primeros en intervenir hasta la entrega de pruebas al laboratorio. Así pues, proporciona el fundamento mismo para permitir una reconstrucción de los hechos que se base con más solidez en las pruebas. (p.1)

La importancia de realizar análisis forenses en casos de delitos informáticos deviene de la necesidad de prevenir que se viole la seguridad de una red corporativa, así como también para determinar culpables en casos judiciales donde la evidencia son dispositivos móviles u ordenadores.

## 2.7 MARCO CONCEPTUAL

**Open source:** Open Source o Código abierto es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista

más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales las cuales destacan en el llamado software libre. (sites.google.com)

**Funciones Hash:** Las funciones Hash utilizan algoritmos criptográficos para crear un mensaje de los datos a los cuales fueron aplicados. Los Hashes representan grandes volúmenes de información en una relativamente pequeña porción de datos y debido a que su utilización no altera la información analizada, sino que la representan de una forma más pequeña, se las utilizan en la informática forense para comparar la información original con aquella resultante de haber aplicado un proceso de duplicación. (Computer Forensic, 2010)

**SIM:** La Tarjeta SIM (SIM son las siglas de Subscriber Identity Module (Módulo de identificación del Suscriptor), es una tarjeta que se utiliza en los teléfonos móviles en la que se almacena de forma segura la información del usuario del teléfono necesaria para identificarse en la red (clave de autenticación e identificación del área local). (masadelante.com)

**ME:** Equipo móvil y su configuración

**Jailbreak:** Proceso que permite posteriormente entrar en el sistema de archivos del iPhone o instalar aplicaciones desde un instalador como Cydia o Installer. (iBRICO, 2009)

**App Store:** La tienda oficial de Apple desde donde se es posible descargar aplicaciones para el iPhone. (iBRICO, 2009)

**Backup:** Es la copia total o parcial de información importante como respaldo frente a eventualidades. (Alegsa.com.ar, 2015)

**Delito Informático:** El delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad. (Alegsa.com.ar, 2015).

**Delito por medios informáticos:** Son delitos ya tipificados en la legislación vigente, que se cometen con el auxilio de medios físicos y/o lógicos, generalmente computacionales y excepcionalmente informáticos no computacionales. (Slideshare.net)

**Perito:** Persona que por su profesión tiene conocimientos sobre ciertos puntos e informa al juez bajo juramento. (The Free dictionary, 2015)

**Cadena de Custodia:** La cadena de custodia, se puede definir como una secuencia de actos llevados a cabo por el Perito, el agente del Ministerio Público o el Juez, mediante la cual los instrumentos del delito, las cosas objeto o producto de él, así como cualquier otra evidencia relacionada con éste, son asegurados, trasladados, analizados y almacenados para evitar que se pierdan, destruyan o alteren y así, dar validez a los medios de prueba. La cadena de custodia debe ser observada, mantenida y documentada. (García, 2009)

## 2.8.HERRAMIENTAS PARA EL ANÁLISIS FORENSE

Dentro de las herramientas utilizadas en análisis forense a teléfonos inteligentes se especifican una variación dependiendo de la cantidad de modelos celulares existentes en la actualidad.

> En el mercado existe una inmensa variedad de modelos de teléfonos celulares, con sistemas operativos propietarios, sistemas de archivos embebidos, así como también con disponibilidad de aplicaciones, servicios y periféricos. Se requiere conocimiento especializado en informática forense para poder contar el un mayor número de opciones de análisis sobre dichos dispositivos. (Gomez, 2013, pág. 2)

Entre las herramientas utilizadas tenemos:

- La herramienta **UFED** es una de las herramientas informáticas que se ajustan a una variedad de teléfonos celulares por lo que se constituye en una herramienta muy utilizada en las pericias informáticas. Se caracteriza por posibilitar la extracción lógica y física de información.

> UFED tiene como punto favorable una gran cobertura de modelos telefónicos, pero como toda herramienta de informática forense tiene limitaciones y no excluye la aplicación de otras técnicas especializadas y herramientas de informática forense durante la realización de una pericia informática sobre dispositivos de telefonía celular. (Gomez, 2013, pág. 5)

- Symbian OS esta herramienta es un sistema operativo que concuerda con una serie de teléfonos como SmartPhones, entre otros. De igual manera esta herramienta se caracteriza por ser un unificador para varios dispositivos.

  Dentro de esta diversidad, surge el Sistema operativo Symbian, como ente unificador para muchos dispositivos, en especial aquellos que tienen características asociadas a los SmartPhones (Symbian está presente en más del 60% de los teléfonos inteligentes del mercado actual. (Agualimpia & Hernández., 2012, pág. 4)

- **TULP2G** Este es un framework de software forense para adquisición y decodificación de datos almacenados en dispositivos electrónicos [15]. Esta herramienta desarrollada por el Netherlands Forensic Institute, es open source y como tal brinda unas ventajas y otras desventajas con respecto a otras herramientas licenciadas (…) El proceso de investigación es modelado con cuatro diferentes categorías de plug-in: dos para adquisición de datos y dos para convertir y exportar los datos. Una quinta categoría de plug-in ha sido definida para tareas relacionadas a casos. **(Agualimpia & Hernández., 2012, pág. 5)**

- **PARABEN** Este software es bastante robusto y está dirigido a múltiples plataformas computacionales. La versión para dispositivos móviles se denomina "Device Seizure" y permite hacer análisis forense de un gran número de dispositivos. El análisis se organiza por casos, aunque para poder efectuarlo requiere un cierto conocimiento del dispositivo móvil a analizar. (Agualimpia & Hernández., 2012, pág. 5)

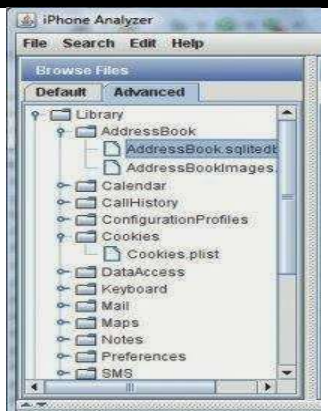
- **MOBILedit! FORENSIC.** Esta herramienta es bastante robusta y actualizada. Permite hacer un análisis forense diferenciado del SIM y del ME. Con este toolkit se analizó el SmartPhone Nokia N73. Una vez se efectúa la conexión (de forma casi automática, a diferencia de los dos toolkits analizados anteriormente), la herramienta muestra las principales características del teléfono: IMEI, revisión de Hardware, revisión de Software, red (GSM, para el caso de análisis), resolución de la pantalla, número de colores de la pantalla, soporte de Java, nivel de la batería y nivel de la señal. (Agualimpia & Hernández., 2012, pág. 5)

- ***Forensic Card Reader*** **(FCR)** es una herramienta forense de Becker & Partner que proporciona los medios para extraer los datos de SIMs. FCR no genera un archivo del caso, pero los resultados los datos adquiridos en un formato XML que puede ser visto con el editor correspondiente. FCR consiste en el software y un lector USB de tarjetas inteligentes. (Ocampo, 2009, pág. 2)

- ***Iphone Analyzer*** es una aplicación que trabaja principalmente con la importación de copias de seguridad producidos por iTunes o software de terceros, y que le proporciona una interfaz rica para explorar, analizar y recuperar datos en formatos legibles por humanos. Debido a que funciona desde la copia de seguridad de archivos de todo es seguro, y no se realizan cambios en los datos originales. **(Black, s.f.)**

## 2.9.CUADRO COMPARATIVO DE HERRAMIENTAS

**Tabla 2.**
CUADRO COMPARATIVO DE HERRAMIENTAS

| Nombre | Herramientas | Ventajas | Desventajas |
|---|---|---|---|
| **Iphone Analyzer** |  | Interfaz gráfica Q Multiplataforma (Linux, Mac OS, Windows)<br>Facilidad de manejo<br>Nos muestra un árbol con las aplicaciones que contiene el móvil<br>Software Libre | No elabora un reporte final del análisis<br>Pero con la información proporcionada se puede elaborar un informe final |
| **Oxygen Forensic** |  | Permite acceder a los archivos analizados<br>Nos muestra en iconos miniatura todos los archivos que han sido analizado | No es software libre<br>Su costo es demasiado alto<br>Es complicado manejar<br>Se debe realizar muchas configuraciones para poder empezar el análisis |

La herramienta a utilizarse en el presente trabajo investigativo de análisis forense a un teléfono inteligente con tecnología Iphone(IOS) es Iphone Analyzer herramienta open source, misma que permite realizar la extracción de datos y que cumple con lineamientos de cada fase de la cadena de custodia.

Entre las características que destacan de esta aplicación están:

- Soporta dispositivos iOS 2, iOS 3, iOS 4 y iOS 5
- Multi-plataforma (basado en Java), con el apoyo en Linux, Windows y Mac
- Búsqueda rápida y de gran alcance a través de dispositivo que incluye las expresiones regulares
- Mapeo integrado soporta la visualización de la información geo-etiquetado, incluyendo los mapas de google búsquedas, fotos y sitios celulares y lugares wifi observados por el dispositivo.
- Soporte integrado para mensajes de texto, correo de voz, las entradas de la libreta de direcciones, fotos (incluyendo metadatos), registros de llamadas y muchos más.
- Recuperación de registros sqlite "borrados" (registros que se han marcado como eliminado, pero aún no han sido purgados por el dispositivo a menudo se puede recuperar).
- Visualización integrada de archivos plist y SQLite
- Incluye soporte para la asignación fuera de línea, el apoyo a la cartografía en los ordenadores que no están conectados a Internet
- Apoyo a la exportación KML y exportación directa a Google Earth

- Examina que la estructura de archivos del dispositivo vaya directamente a los archivos de claves o explorar el dispositivo mediante conceptos tales como "quién", "cuándo", "qué" y "dónde". **(Black, Lydecker Black, 2013)**

## 2.10. METODOLOGÍA DE ANÁLÍSIS FORENSE

La metodología es aquella rama lógica que se encarga de realizar un estudio de diferentes métodos con la finalidad de llegar al conocimiento crítico y reflexivo que permita generar fundamentación de la ciencia y todo saber.

En el presente caso la metodología permitirá la construcción de la investigación como tal. Para realizar el análisis forense es necesario seguir un procedimiento ordenado siguiendo la precedente metodología conformada por 5 etapas.


**Figura 2.** Metodología de Análisis Forense
**Fuente: (Guaman, s.f.)**

### 2.10.1. Etapa de Identificación y Preparación:

Para alcanzar los resultados pretendidos es necesario realizar una adecuada planificación previa identificando los recursos, los roles y preparando la documentación adecuada para empezar con el análisis.

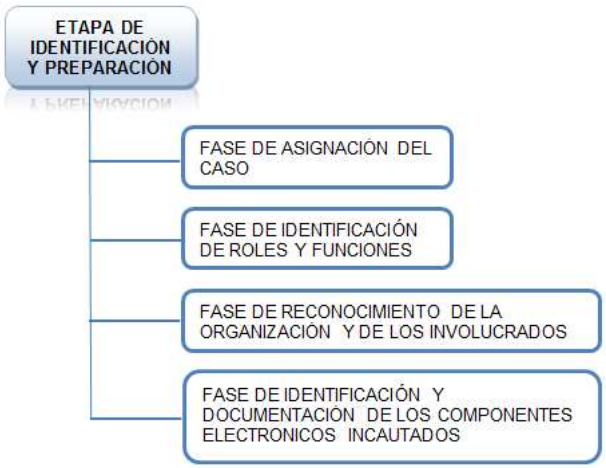



**Figura 3.** Etapa de Identificación y Preparación
**Fuente: (Guaman, s.f.)**

### 2.10.2. Etapa de Preservación y Adquisición:

En esta etapa se deberá tener definida la herramienta con la que vamos a realizar el análisis así como también la estación de trabajo en el cual se procederá almacenar lo analizado generando la evidencia que se busca en este trabajo de investigación.

Elena Darahuge aconseja que al realizar el peritaje con meticuloso cuidado y portando las herramientas necesarias para lo que recomienda:

- Al concurrir al lugar debe hacerlo con los elementos necesarios para realizar su tarea. Tenga en cuenta que debe detectar, documentar, preservar y trasladar la prueba.

- Respecto del punto anterior, lo ideal es el uso de una estación de trabajo informático forense portátil. (Un sistema basado en una notebook). Si debe decidir entre poseer un equipo de escritorio (desktop) o un equipo portátil, inclínese siempre por el portátil, ya que cumple ambas funciones. (Darahuge E. )

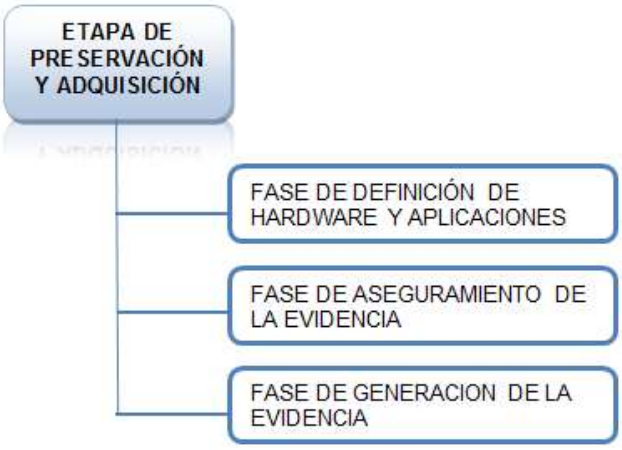



**Figura 4.** Etapa de Preservación y Adquisición

**Fuente: (Guaman, s.f.)**

### 2.10.3. Etapa de Análisis

En esta etapa se debe extraer la información, procesarla e interpretarla generando una informe accesible para entender los procesos realizados por el software forense y tener una clara idea de lo que se quiere analizar en el dispositivo.

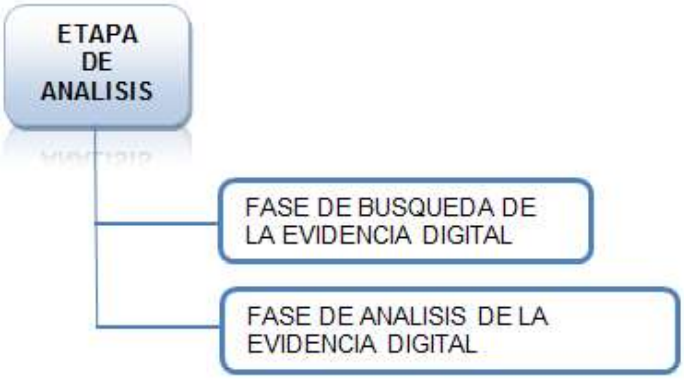



**Figura 5.** Etapa de Análisis.

**Fuente: (Guaman, s.f.)**

### 2.10.4. Etapa de Presentación

En la siguiente etapa se mostrara el informe detallado de todo lo que analizara en los puntos anteriores, presentando información verídica, clara y concisa del proceso que fue utilizado para la preservación y análisis de la evidencia.


**Figura 6.** Etapa de Presentación.
**Fuente: (Guaman, s.f.)**

### 2.10.5. Etapa de Entrega de Evidencia

Después de analizar la evidencia se realizarán hipótesis que se confirmarán o se eliminarán según los resultados del análisis realizado.

La demostración de las hipótesis deberá demostrarse mediante el razonamiento lógico de los resultados del proceso, de lo que arroja el estudio de la evidencia, debidamente tratada con las herramientas tecnológicas.

Cada análisis realizado conduce a conclusiones, las que deben referirse a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no será tomado en cuenta al momento de resolver el caso, y será tomado en consideración para la evaluación del perito. (funcionjudicial.gob.ec, pág. 2)


**Figura 7.** Etapa de Entrega de Evidencia.
**Fuente: (Guaman, s.f.)**

## 2.11. TÉCNICAS DE INVESTIGACIÓN

Las técnicas de investigación son procedimientos metodológicos y sistemáticos que se encargan de operar e implementar los métodos de Investigación y que tienen la facilidad de recoger información de manera inmediata (Eumed.net, 2010).

### 2.11.1. Observación

La observación es un proceso cuya función primera e inmediata es recoger información sobre el objeto que se toma en consideración. Esta recogida implica una actividad de codificación: la información bruta seleccionada se traduce mediante un código para ser transmitida a alguien (uno mismo u otros).

### 2.11.2. Cuestionario estructurado

El cuestionario estructurado es un listado de preguntas que se formulan al entrevistado tal y como están redactadas y en el orden que aparecen, la mayoría de respuestas que se puede obtener, están también contempladas en el cuestionario. (Hernández, 2001, pág.

241).

- **Encuesta:** La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador. (RRPPnet, 2001)
- **Entrevista.-** Es un dialogo entre dos personas (entrevistado y entrevistador), el instrumento será un cuestionario estructurado.

### 2.11.3. Fichaje bibliográfico

El fichaje es una técnica que toma notas importantes de la investigación, es una técnica que facilita la sistematización bibliográfica, la ordenación lógica de las ideas y el acopio de información, consiste en registrar los datos que se obtienen en los instrumentos llamados fichas. (Universidad César Vallejo, 2010).

## 2.12. PLAN PARA LA RECOLECCIÓN DE LA INFORMACIÓN

La recolección de la información y datos relevantes para realizar el presente estudio se fundamentara en las respuestas a las preguntas básicas de investigación, que a continuación se especifican:

**Tabla 3.**
Plan de recolección

| PREGUNTAS BÁSICAS | EXPLICACIÓN |
|---|---|
| 1. ¿Para qué? | Para comprobar la hipótesis |
| 2. ¿De qué personas u objetos? | Ciudadanos y especialistas en el tema. |
| 3. ¿Sobre qué aspectos? | Sobre afectación a partir de delitos informáticos y procedimientos en análisis forense. |
| 4. ¿Quién? ¿Quiénes? | El investigador: Mónica Gabriela Granda Velastegui |
| 5. ¿Cuándo? | año 2015 |
| 6. ¿Dónde? | Ciudad de "Quito" |
| 7. ¿Cuántas veces? | Uno |
| 8. ¿Qué técnicas de recolección? | Encuesta, entrevista, observación |
| 9. ¿Con qué? | Cuestionario, cuestionario estructurado, guía de observación. |
| 10. ¿En qué situación? | En la Universidad ESPE |

## 2.13. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

El procesamiento y análisis de la información se desarrollará siguiendo el presente esquema con el fin de procesar y tabular toda la información para finalmente realizar un análisis de los resultados.

### Fuentes primarias

- Encuesta: se realizará un formulario de encuesta que estará dirigida estudiantes de la universidad ESPE.
- Entrevista: se realizará un cuestionario estructurado dirigido a especialista en informática de la universidad ESPE.

**Fuentes secundarias**

- Revisión de la bibliografía
- Selección de la información

## 2.14. Análisis e Interpretación de datos

### 2.14.1. Análisis e Interpretación Encuesta

1. **¿Ha sido víctima por lo menos una vez, de pérdida, hurto o la sustracción de su teléfono celular o dispositivo móvil?**

**Tabla 4.**
Pérdida o sustracción del celular móvil.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 96 | 96% |
| **No** | 4 | 4% |
| Total | **100** | **100%** |

**Fuente:** Encuesta

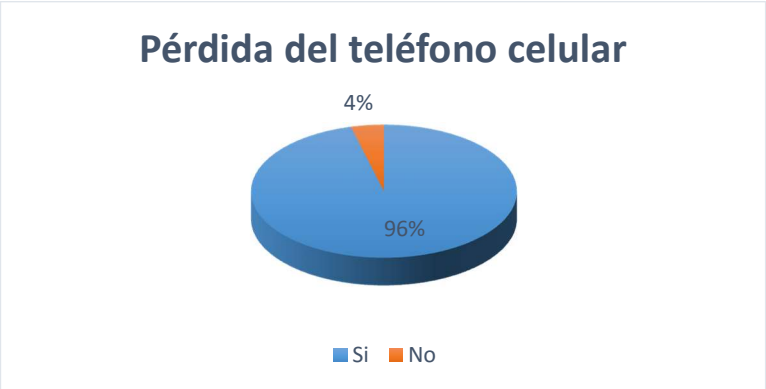



**Figura 8.** Análisis de personas que han perdido el teléfono móvil.

**Análisis e Interpretación de datos**

De 100 personas consultadas 96 respondieron que sí habían sufrido la sustracción de sus teléfono móvil por lo menos una vez, lo que corresponde al 96%, 4 personas respondieron que no, lo que corresponde al 4%.

Se concluye por lo tanto que a la mayoría de personas les han sustraído su teléfono celular por lo menos una vez en su vida, mientras que un porcentaje menor no ha sido víctima de sustracciones de sus móviles.

**2. ¿Ha sido víctima al menos una vez, de un ataque, delito virtual o tecnológico?**

**Tabla 5**.
Frecuencia Ataques virtuales.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 69 | 69% |
| **No** | 31 | 31% |
| Total | **100** | **100%** |

**Fuente:** Encuesta

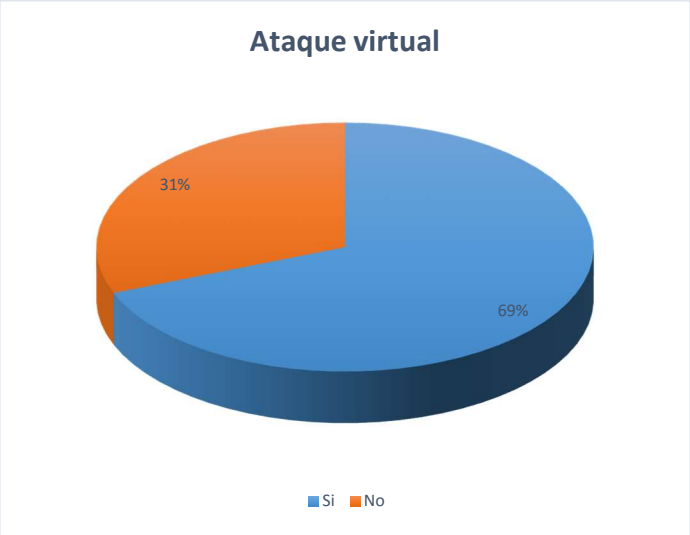



**Figura 9.** Frecuencia de ataque virtual.

**Análisis e Interpretación de datos**

De la muestra, 69 personas contestaron que sí habían sido víctimas de ataques virtuales, es decir el 69%, mientras que 31 personas es decir el 31% contestó que no.

De esto concluimos que un índice alto de personas han sido víctimas por lo menos una vez en sus vidas de algún ataque virtual.

### 3. ¿Cuál ha sido el medio por el cual se ha cometido el fraude o delito?

**Tabla 6.**
Frecuencia uso de dispositivos en delitos.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Teléfono** | 23 | 23% |
| **Computador** | 37 | 37% |
| **Cajeros automáticos** | 13 | 13% |
| **Dispositivos móviles** | 19 | 19% |
| **Otros** | 8 | 8% |
| Total | **100** | **100%** |

**Fuente:** Encuesta

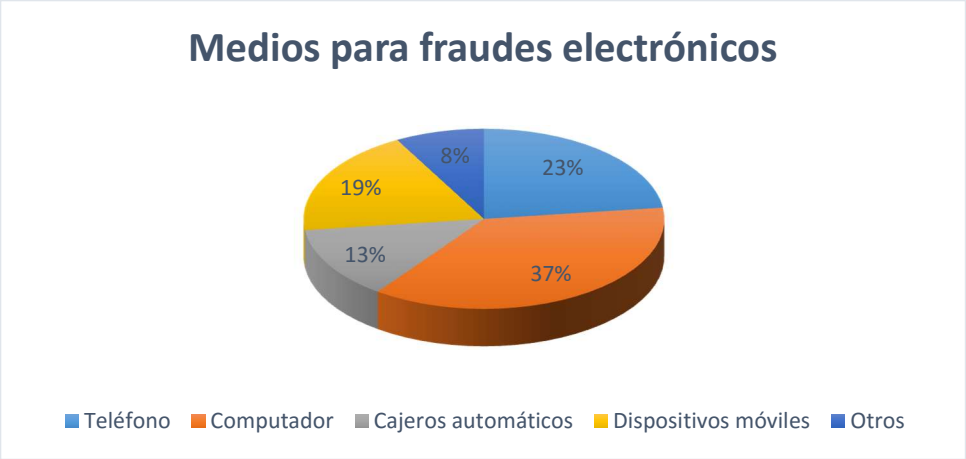



**Figura 10.** Tipo de medio usado en el ataque virtual

### Análisis e Interpretación de datos

Respecto al medio por el cual han sido víctimas de delito o fraude electrónico, los consultados respondieron un 23% que por teléfono, correspondiente a 23 consultados, otras

37 personas respondieron que por computador, correspondiendo a un 56%, mientras que 19 personas respondieron que por dispositivos móviles correspondiendo así a un 19%, un 8% es decir 8 personas respondieron que otros dispositivos fueron usados en el delito.

De estos resultados podemos deducir que la mayoría de fraudes electrónicos se comete utilizando como herramienta el computador, seguido por los teléfonos fijos, seguido de cerca por quienes prefieren los dispositivos móviles o celulares, es decir muchas personas utilizan esta opción para cometer un ilícito mientras que en menor medida lo hacen a través de cajeros automáticos u otros dispositivos electrónicos.

4. **¿Considera que el medio más frecuente y factible para incidentes como delitos son los dispositivos móviles?**

**Tabla 7.**
Frecuencia factibilidad de uso de dispositivos móviles en delitos.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 73 | 73% |
| **No** | 27 | 27% |
| Total | **100** | **100%** |

**Fuente:** Encuesta

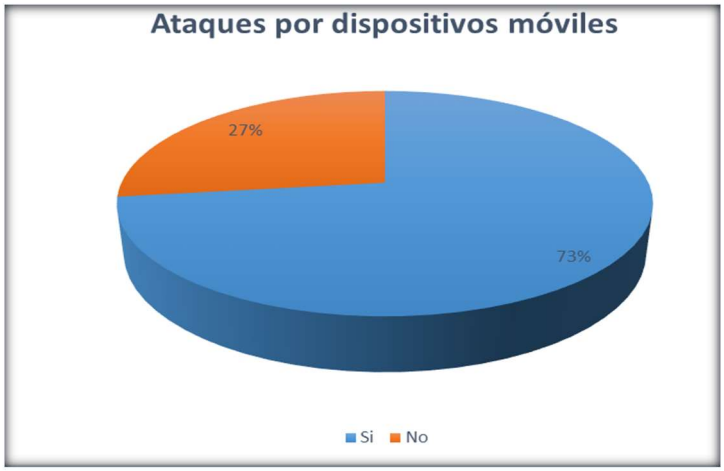



**Figura 11**. Frecuencia de factibilidad de uso de móviles en delitos.

## Análisis e Interpretación de datos

Del 100% de encuestados el 73 personas contestaron que sí, que el celular es el medio más frecuente y factible para cometer delitos, esto corresponde al 73% de la muestra, mientras que 27 personas respondieron que no, lo que corresponde a un 27%.

De esto podemos deducir que la mayoría de personas considera que los dispositivos móviles son los medios que con mayor frecuencia se utiliza para delitos u ocasionar incidentes y que son los más factibles, mientras que la minoría considera que no.

5. **¿Conoce a qué instancia o institución específica debe acudir si ha sido víctima de un fraude mediante dispositivos móviles?**

**Tabla 8.**
Conocimiento de instancias en caso de ser víctima de fraude electrónico.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 26 | 26% |
| **No** | 74 | 74% |
| Total | **100** | **100%** |

**Fuente:** Encuesta


**Figura 12.** Conocimiento de la gente en caso de ser víctima de delito electrónico

## Análisis e Interpretación de datos

En cuanto al conocimiento de instituciones e instancias a las cuáles las víctimas de fraude electrónico pueden acercarse, 26 personas respondieron que sí, lo que corresponde a un 26% y 74 personas respondieron que no, lo que corresponde al 74%

De estos resultados podemos deducir que la mayoría de personas desconoce las instituciones o estancias a las cuales puede acudir en caso de ser víctima de fraude virtual o electrónico.

**6. ¿Conoce qué es el análisis forense en teléfonos móviles?**

**Tabla 9.**
Conocimiento de análisis forense en móviles.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 21 | 21% |
| **No** | 79 | 79% |
| Total | **100** | **100%** |

**Fuente:** Encuesta

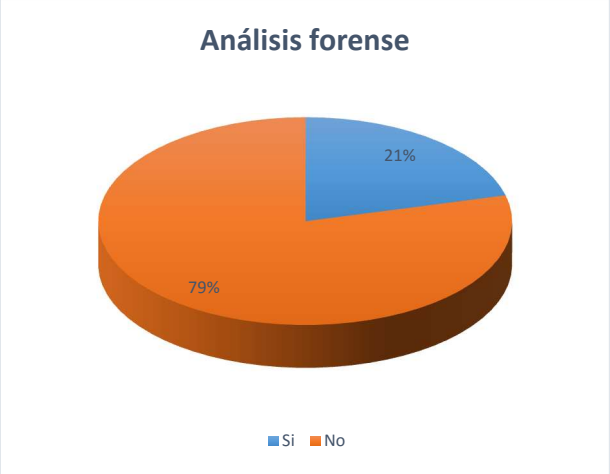



**Figura 13.** Conocimiento sobre análisis forenses en móviles.

## Análisis e Interpretación de datos

De las personas consultadas, 21 contestaron que sí saben qué son los análisis forenses que se realizan en los teléfonos móviles, es decir 21%, mientras que 79 personas respondieron que no, es decir 79%.

Se concluye que la mayoría de personas desconoce sobre el análisis forense que se realiza a los dispositivos móviles tras quedar como posibles pruebas de delito.

### 6. ¿Conoce sobre procedimientos formales para administración de evidencia digital?

**Tabla 10.**
Conocimiento para administración de evidencias digitales

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 8 | 8% |
| **No** | 92 | 92% |
| Total | **100** | **100%** |

**Fuente:** Encuesta


**Figura 14.** Frecuencia de conocimiento sobre administración de pruebas digitales.

## Análisis e Interpretación de datos

De las personas consultadas, 8 contestaron que sí conocen acerca de procedimientos formales para administración de evidencias digitales, es decir 8%, mientras que 92 personas respondieron que no, es decir 92%.

De estos resultados, se concluye que la mayoría de personas desconoce sobre los procedimientos que se siguen para la administración de pruebas digitales, mientras que muy pocas sí conocen sobre el tema.

**8. ¿Sabe o ha escuchado de alguna institución que aplique análisis forense sobre dispositivos móviles?**

**Tabla 11.**
Institución que aplique análisis forense

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 2 | 2% |
| **No** | 98 | 98% |
| Total | **100** | **100%** |

**Fuente:** Encuesta


**Figura 25.** Institución que aplique análisis forense

## Análisis e Interpretación de datos

De 100 personas consultadas 98 respondieron que no, es decir 98%, mientras que 2 personas respondieron que sí, es decir un 2%

Los resultados con muy claros respecto al desconocimiento de la gente sobre la aplicación de análisis forense y las instituciones que lo realizan, de tal manera que apenas dos de cien consultados sí tienen algún conocimiento de instituciones que realizan esos análisis un porcentaje realmente bajo.

**9. ¿Cree que es importante diseñar una metodología específica relacionada con informática forense para dispositivos móviles?**

**Tabla 12.**
Importancia del diseño de una metodología para análisis forense de dispositivos móviles.

| Alternativas | Frecuencia | Porcentaje |
|---|---|---|
| **Si** | 100 | 100% |
| **No** | 0 | 0% |
| Total | **100** | **100%** |

**Fuente:** Encuesta


**Figura 16.** Importancia de diseño para análisis forense en dispositivos móviles

**Análisis e Interpretación de datos**

De los consultados, 100 personas respondieron que sí es importante diseñar una metodología específica relacionada con informática forense para dispositivos móviles, es decir el 100% de la muestra.

Los resultados con muy claros respecto a la importancia que la gente considera que tiene el diseño de una metodología forense para los dispositivos móviles ya que todos consideran que es importante realizarlo.

### 2.14.2. Análisis e Interpretación de datos entrevista

**1. ¿Qué define usted por análisis forense digital?**

Los entrevistados respecto a la definición de análisis forense coinciden en que es una actividad que se realiza en medios informáticos, por tanto es un examen exhaustivo que se lleva a cabo para determinar varias cosas, entre estas saber el objetivo del análisis, de igual forma recalcan la diferencia existente al momento de realizar un análisis forense a un celular y a un Sistema Informático de una empresa, que generalmente se realiza bajo la petición de un juez o por requerimiento del gerente de la empresa.

Por otro lado, uno de los entrevistados menciona que el análisis forense es un tema que en la actualidad ha adquirido mayor importancia porque se cometen muchos delitos a

través de la tecnología. Por lo tanto, un análisis permite ingresar al sistema operativo sea de una computadora o de un celular, para extraer información importante a través del uso de técnicas especializadas y fases en el proceso que tienen por objetivo principalmente mantener la integridad de la información.

Además los entrevistados específica que un especialista al realiza un análisis forense digital sabe que debe mantener cierta rigurosidad para preservar el contenido. Por lo que es indispensable acatar medidas de protección tales como el uso de guantes, bolsas aislantes, entre otros, a fin de no alterar la evidencia como lo llamarían en un caso legal.

**2. ¿Por qué no es lo mismo realizar un análisis forense a un Sistema Informático que a un celular, cuál es la diferencia entre ambos?**

En relación a las diferencias entre un análisis forense a un sistema informático y un celular inteligente dos de los entrevistados determinaron que la diferencia radica en el hardware y software, ya que la información almacenada en un ordenador y un celular es diversa y diferente, por otro lado el software utilizado es especifico en cada caso, además, en el caso de los sistemas informáticos existen una variedad de softwares aplicables mientras que para teléfonos son escasos. También, una diferencia del software radica en la tecnología y el año de fabricación.

Por otro lado el tercer entrevistado señalo que la tecnología ha variado mucho por tanto las aplicaciones mantienen características diferentes entre sí, por lo que es imposible comprar la capacidad de almacenamiento de datos e información de un sistema informático

(ordenador) con un celular, de allí que la volatilidad de la información es más alta en un teléfono.

**3. ¿En qué casos considera usted que es necesario llevar a cabo un análisis forense a los dispositivos móviles?**

De acuerdo al siguiente cuestionamiento los entrevistados determinan que es imprescindible una orden, para que se realice este tipo de análisis, puesto que pocos son los casos en el que el dueño del dispositivo necesita recuperar información. Mencionan que por lo general el análisis se realiza porque el teléfono es evidencia de algún evento o un delito.

De tal manera se determina que el análisis forense en un celular se lo realizar cuando existe la petición de una autoridad judicial que considera que el teléfono encierra información importante para algún caso.

**4. ¿Cuáles han sido las principales dificultades que se le han presentado en el momento de realizar este tipo de análisis en un celular?**

Los entrevistados determinan que si existen varias dificultades en el proceso, especialmente relacionadas a la falta de aplicaciones desarrolladas que se adapten a la tecnología o tipo de teléfono que forma parte del análisis forense.

Sin embargo uno de los entrevistados afirma y ratifica que la principal dificultad es la falta de un manual específico, patentado que recopile toda la información que ayude en los procedimientos dentro del análisis.

**5. ¿Qué información es más relevante en el proceso de análisis forense?**

Los entrevistados determinan que no es posible especificar qué información es más relevante que otra, puesto que todo depende del caso estudiado, toda información en este sentido puede revelar historial de llamadas, hora exacta, lugar, entre otras.

Mencionan también que la determinación de la información más relevante lo define el juez dentro del proceso judicial y no en el análisis forense ya que el objetivo de este es recabar toda la información posible.

**6. ¿Qué delitos se pueden resolver a través de un análisis forense a un celular?**

Con respecto a esta indagación los entrevistados coinciden en que los delitos que se resuelven a través del análisis forense vara de acuerdo al tipi de delitos tipificados dentro de las normativas judiciales vigentes como por ejemplo extorsión, chantaje, acoso sexual, pornografía infantil, lavado de activos, contrabando, narcotráfico, fraudes, intromisión en un sistema informático, suplantación de identidad incluso, homicidio, entre otros.

**7. ¿Podría citar un caso en que un análisis forense haya permitido resolver un caso?**

Uno de los entrevistados menciono que existen muchos casos de ciber ataques, situaciones en que se vulnera la seguridad de un sistema para favorecer a determinadas personas en un concurso de mérito y oposición como ya ha sucedido en nuestro país.

El segundo entrevistado manifestó que un caso en el que el análisis forense fue utilizado fue para esclarecer el caso relacionado a las estafas realizadas en el BIESS cuando los empleados de esta institución realizaron préstamos tomando la base de datos de los afiliados y crearon claves, perjudicando a muchas personas.

Finalmente de manera general el tercer entrevistado menciono que el análisis forense es utilizado frecuentemente por los policías para desarticular y determinar bandas delictivas.

**8. ¿Qué recomendaciones daría usted a los peritos para realizar un análisis forense de evidencia digital?**

Los entrevistados determinaron que las recomendaciones más acertadas sería lograr preserven la evidencia, meticulosidad y cuidado en cada parte del proceso, para que las evidencias no sufran ningún tipo de alteración, así como también trabajar en copias para preservar los originales.

**9. ¿En qué casos, la evidencia digital corre riesgos de perderse?**

En relación a este cuestionamiento los entrevistados manifestaron que es posible perder información cuando no se asegura bien los bienes electrónicos, cuando no se sigue

el debido proceso, por lo tanto mencionan que es necesario recordar que le evidencia digital tiene sus características propias, por lo que se debe ser meticuloso a fin de que la información no pierda credibilidad en el proceso acusatorio.

**10. ¿Qué diferencia al Iphone de otros dispositivos móviles al momento de realizar en él un análisis forense?**

Los entrevistados determinan que el sistema operativo de un Iphone es exclusivo de la marca Apple. De igual forma se caracteriza porque el Sistema Operativo se destaca por la seguridad que brinda, ya que utiliza códigos cerrados, de difícil desciframiento. Además especifican que el sistema de Apple es más difícil y complicado para penetrar en relación a un Android o un GSM.

# CAPÍTULO III.

## 3. ANÁLISIS Y PRUEBAS

### 3.1.Especificación de los requerimientos del Análisis Forense.

Para poder realizar el análisis forense de un equipo Iphone, los requerimientos son:

- Que esté realizado el jailbreakque
- Que se tenga instalado en el ordenador la aplicación o herramienta open source, la versión mas actualizada.
- Disponer del dongle (dispositivo de seguridad para software)

- Tener instalados los drivers de conexión con el dispositivo a analizar
- Tener instalado el driver del cable.

### 3.1.1. Requerimientos de hardware.

Los requerimientos mínimos de hardware son:

- Procesador Intel Dual-Core o superior.
- Memoria RAM de 8Gb o superior.
- Disco Duro de 320 Gb o superior.
- Tarjeta de video, sonido.
- Parlantes.
- Lector de CD-ROM
- Monitor de 15 pulgadas.

### 3.1.2. Requerimientos de software.

Los requerimientos mínimos de Software son:

- Sistema Operativo Windows o IOS
- Navegador Web
- Aplicación open source

Para el estudio del análisis forense se sigue las siguientes etapas:

## 3.2. Desarrollo de la Metodología.

### 3.2.1. Etapa de Identificación y Preparación

#### a. Fase de Asignación del Caso:

**Escenario:** Universidad de las Fuerzas Armadas.

**Recepción de solicitudes de análisis forense:** Caso de estudio de tesis

**Revisión de políticas y legislación en el Ecuador y a nivel internacional:** Descrito en el capítulo del Marco legal de informática Forense en el Ecuador.

#### b. Fase de Identificación de Roles y Funciones

Formación del equipo para el análisis Forense a continuacion se detalla los roles de las personas que intervendran en este caso de estudio.

**Tabla 13.**
Roles de los encargados del caso.

| Nombres | Tipo |
|---|---|
| **Gabriela Granda** | Egresado de Sistemas e Informática |
| **Germán Ñacato** | Director de Tesis |

#### c. Fase de Reconocimiento de la Organización y de los Involucrados

**Reconocimiento de la organización:** ESPE, Departamento de Ciencias de la Computación.

**Reconocimiento del personal:** Alumno de 8vo.nivel de Ciencias de la Computación.

**Identificar y asegurar el escenario:** Aula 302 del edificio principal de la ESPE

**Identificar el incidente:** Análisis de información almacenada en dispositivo móvil

**Identificar cadena de custodia:** Garantizar el móvil bajo la custodia física en la respectiva caja y hoja de entrega-recepción del móvil.

### d. Fase de Identificación y documentación de los componentes electrónicos incautados.

Las fotografías del móvil para el respectivo análisis se muestran a continuacion se detalla mediante un formulario todo lo que se recepto:

**Tabla 14.**
Formulario de recepción de dispositivos móviles.

| DEPARTAMENTO DE INVESTIGACIÓN | | | | |
|---|---|---|---|---|
| **FECHA: dd/MM/YYYY** | | HORA: 5:00 (AM/PM) | | FORMULARIO: E1G41 |
| | | | | CODIGO CASO: IN-213 |
| **COMPONENTES ELECTRONICOS PARA LA INVESTIGACIÒN** | | | | |
| **Tipo de Accesorio** | Color | Marca | Numero Serial | Descripción |
| **Iphone** | Negro | Apple | 45637C238web | Dispositivo Utilizado para efecto del incidente |
| **Cable USB** | Blanco | Apple | N/A | Cable USB usado para la sincronización con la PC |
| **Cargardor** | Blanco | Apple | RT-985 | |
| **Manos Libres** | Blanco | Apple | N/A | |
| **Observaciones:** | | | | |
| **Los componentes recibidos se encuentran en buenas condiciones** | | | | |
| | | | | |
| **Receptado por:** | | | Revisado por: | Autorizado por: |
| | | | | |
| | | | | |

### 3.2.2. Etapa de Preservación y Adquisición

#### a. Fase de Definición de Hardware y Aplicaciones

Para el análisis se utilizó los recursos en el cual se detalla las características tanto del hardware como el software de la estación de trabajo y los dispositivos móviles en general.

**Tabla 15**:
Recursos de hardware

| HARDWARE | | | | |
|---|---|---|---|---|
| **Subtipo Activo** | Descripción | Marca | MODELO | COLOR |
| | | | | |
| **Portátil** | Intel Core I5 Inside 2,83 GHz 6GB RAM 330 GB HDD DVD-RW | SONY VAIO | SVF14C29U | Negro |
| **Celular** | Iphone IOS, 16 GB RAM | Apple | S5 | Negro |

**Tabla 16:**
Recursos de software

| SOFTWARE | | | |
|---|---|---|---|
| **NOMBRE** | SISTEMA OPERATIVO | VERSIÓN | INTERFAZ |
| **Iphone Analyzer** | Windows | 2 | GRAFICA |

Para cerciorarnos que la herramienta elegida Iphone Analyzer cumple con los requerimientos, se realizó un estudio con otras herramientas calificando 1 a 10 cada una de sus características utilizando criterios globales.

**Tabla 17**:
Matriz DAR

| Matriz DAR | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Criterios | | | | | | | | Total |
| | | Parametriz able | Para plataforma Windows | Para dispositivos móviles | Multiplataforma | Uso libre sin pago de licencia | Permiten actualización en línea | Tienen soporte | Existen manuales en español | |
| | **Weight** | 5 | 2 | 8 | 4 | 5 | 6 | 8 | 8 | |
| **Alternativas** | **Iphone Analyzer** | 2 | 3 | 3 | 4 | 3 | 3 | 3 | 3 | 134 |
| | **Oxygen Forensic** | 1 | 3 | 1 | 1 | 3 | 3 | 2 | 2 | 88 |
| | **Mobil Edit** | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 122 |

## b. Fase de Generación de la Evidencia

### Identificación de evidencias

Para el análisis se tomó en consideración los siguientes datos en el cual se describe todo lo que se encontró como evidencia en el dispositivo móvil.

**Tabla 18:**

Datos sobre el dispositivo a ser peritado

| Datos | Evidencia |
|---|---|

| | |
|---|---|
| **Evidencias:**<br><br>**Información Almacenada:** | Celular<br>Con estuche color café<br>Cable usb del dispositivo<br>Cargador<br>Audifonos<br>Archivos<br>SMS<br>Llamadas<br>Fotos<br>Música<br>Archivos PDF,Word<br>Navegación<br>Redes Sociales |
| **Lugar donde se encuentra:** | Aula 302 de la ESPE |
| **Como está almacenado el Móvil:** | El celular está en un estuche color café sin nada adicional |

### Recolección de evidencias

En esta fase se identifican, etiquetan, graban y recolectan los datos o información, preservando su integridad para su posterior estudio y análisis.

Para la recolección se utilizó el software de Iphone Analyzer por cuanto permite realizar un análisis exhaustivo del dispositivo. Se verifica la integridad del análisis que se realiza paso a paso por cada de las opciones que contiene este software ya que se la realiza de manera separa es decir llamadas, sms, archivos, fotos, etc.

Esta fase de recolección se realiza en la escena del hecho, se caracteriza por identificar el objeto de manera física de la escena para documentar todo los elementos encontrados. Y la preservación de la información se la efectúa para posteriormente realizar el análisis de la evidencia digital.

De manera general se pude definir estas actividades como el ejercicio aplicado en esta fase:

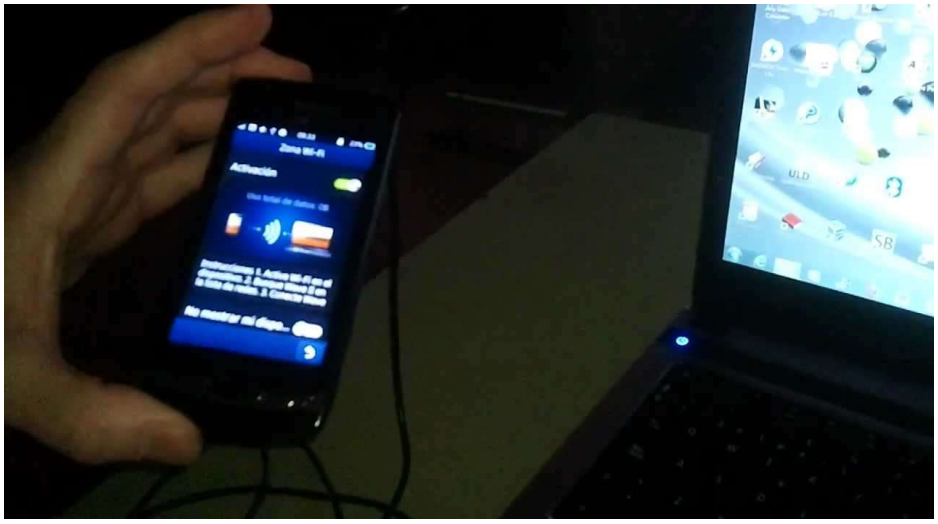


**Figura 37.** Estado del dispositivo y la herramienta
**Fuente:** Gabriela Granda

La adquisición de datos privados se realiza de manera física y lógica, de manera física hace referencia a las copias del dispositivo, su memoria RAM. Para las pericias la descarga de la memoria RAM será muy útil, es muy importante en esta instancia la evaluación de criticidad del incidente encontrado y los actores involucrados en él.

### 3.2.3. Etapa de Análisis

Se toman las medidas técnicas para conservar la evidencia de las copias generadas en el punto anterior, para su adecuada manipulación en el análisis forense.

El análisis de la evidencia digital es muy útil al reconstruir un delito porque puede proveer de detalles adicionales, los cuales pueden guiar al investigador hacia evidencia adicional, e inclusive hacia el mismo sospechoso del delito, para lo cual se utilizó los

siguientes pasos:

- Se verifica la información y se puede definir qué es lo que sucedió, para determinar la relación entre la información que se obtiene y el caso investigado.

- Establecemos una relación lógica entre los procesos realizados y las pruebas obtenidas, se documenta la información y se procede posteriormente a realizar un reporte.

- Se realiza un análisis de los archivos recibidos y se hace una correlación de eventos.

Los dispositivos IPhone se caracterizan por la alta seguridad que brindan, con claves de seguridad o passcode y aplicaciones que no permiten acceder a la información de manera fácil. El análisis forense era más sencillo hasta que Apple integró a estos dispositivos la herramienta Touch ID que permite desbloquear el contenido del celular únicamente con la huella digital del dueño, a partir de entonces se complicó la forma de realizar este proceso y lógicamente el análisis forense para estos dispositivos tuvo que buscar herramientas para poder realizar el respectivo análisis de evidencias.

A continuación se presenta el análisis que se realizó con el software forense Iphone Analyzer.

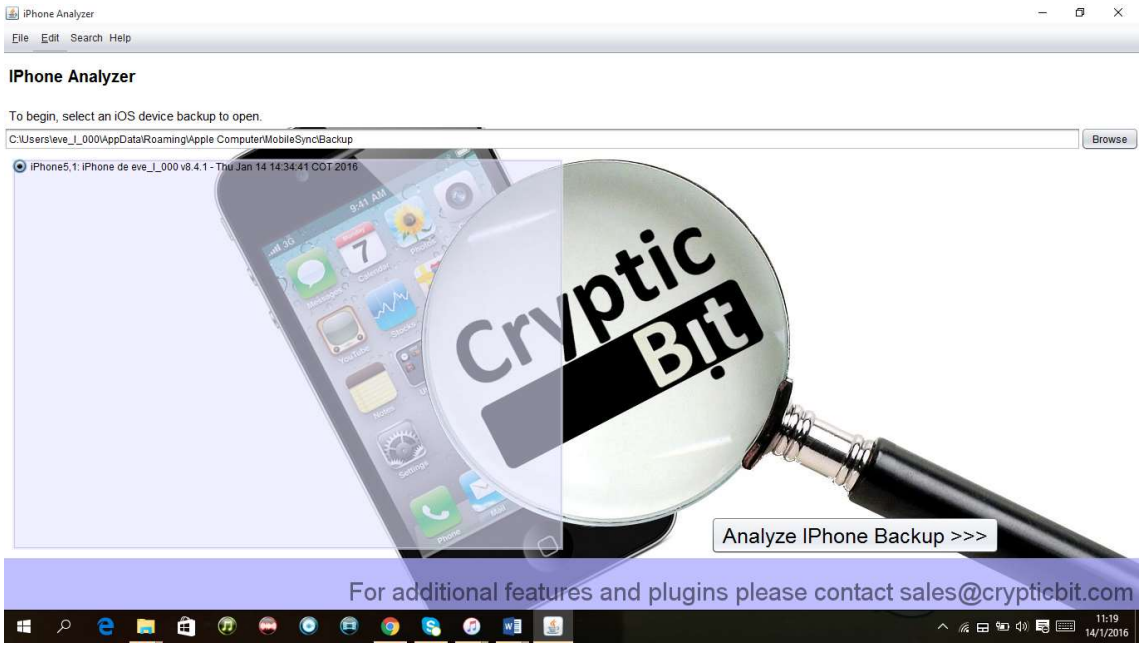



**Figura 18.** Pantalla Principal de iPhone Analyzer

A través de esta aplicación se puede analizar el Backup que genera iTunes en el ordenador. Existen otros métodos para la extracción de datos del iPhone como puede ser la copia íntegra del contenido mediante el uso del comando “dd” a través del ssh (requiere tener el jailbreak)


**Figura 19.** Extracción de datos

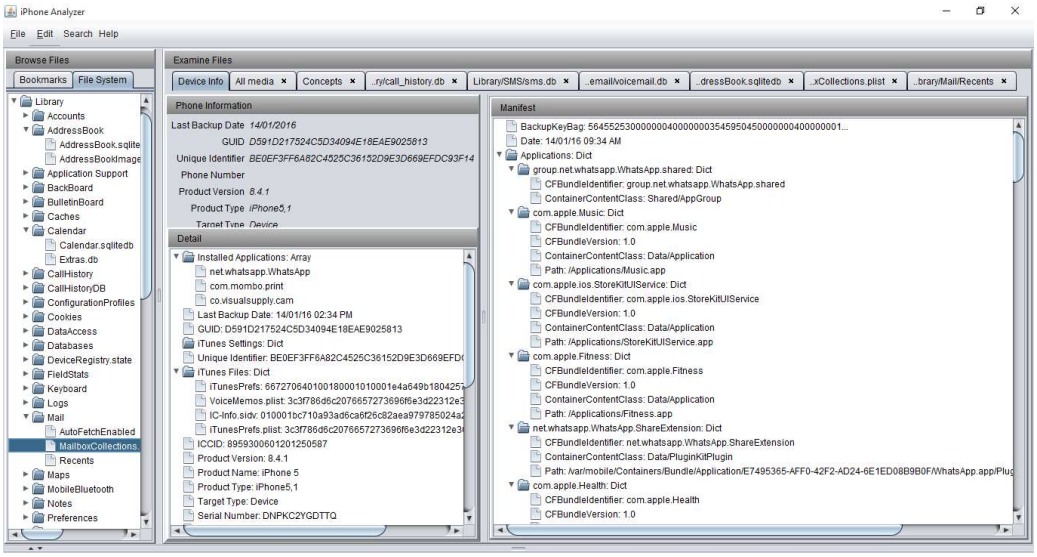



**Figura 20.** Pantalla para analizar datos a partir de backup

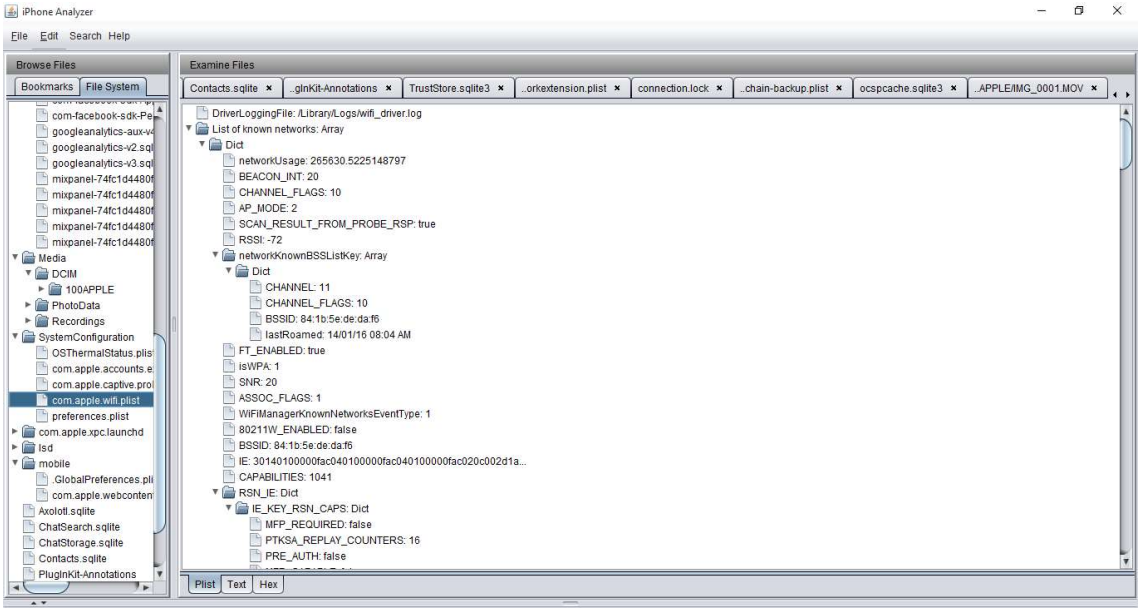



**Figura 41.** Pantalla para analizar la estructura del teléfono

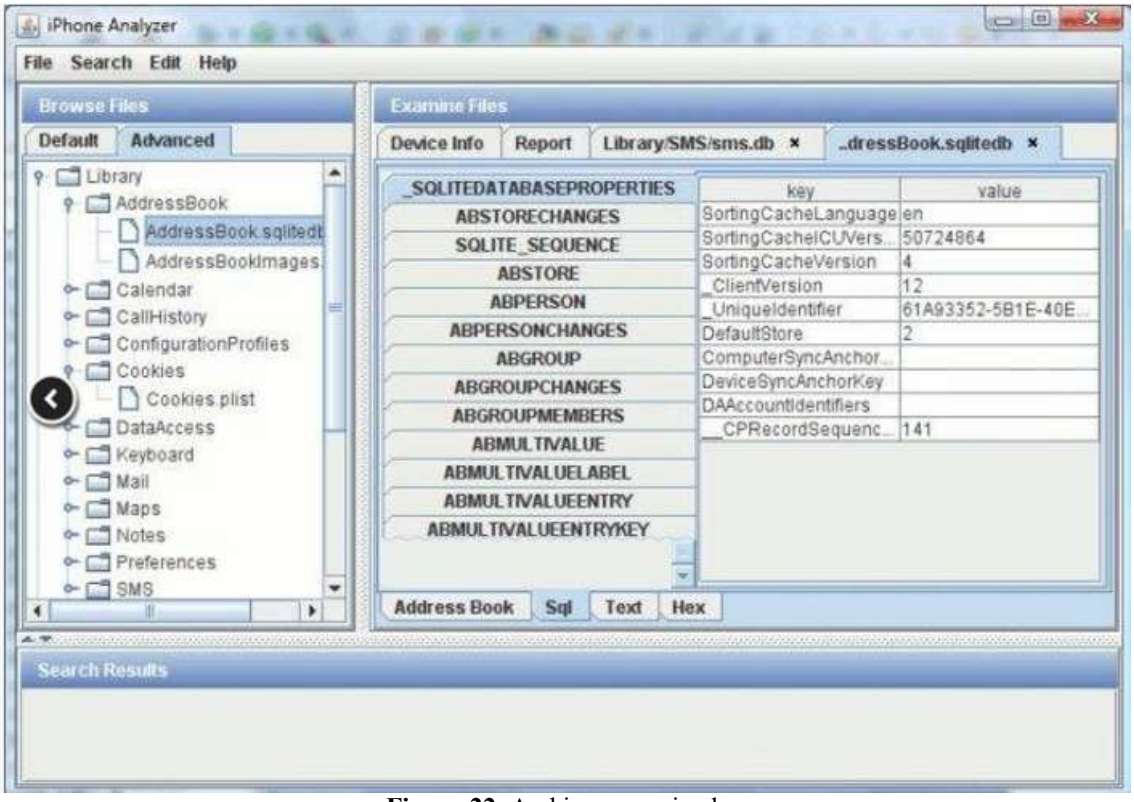



**Figura 22.** Archivos examinados

Muchos archivos personales se guarda en los dispositivos digitales, IPHONE incluye en los beneficios que da al comprador, la seguridad de la información con que cuentan estos dispositivos móviles, una de las aplicaciones que utiliza para esto es Touch ID que es una sencilla manera de utilizar la huella digital como código.

Para determinar que implicación existe entre la información que esta guardada en el equipo móvil y el delito, se habrá analizado información como el Sqlite, el que puede ser leído con aplicaciones Linux o Windows, de esta manera se obtiene las rutas de los archivos como los contactos, por ejemplo en un Backup de iOS en la versión 6.1. Una de las rutas para ingresar al historial de llamadas es /iOS Files/Library/CallHistory/call_history.db y dependiendo del modelo del celular con la aplicación de la herramienta adecuada, se obtendrá las rutas de los diferentes archivos almacenados en el equipo.

iPhone Analyzer permitirá visualizar información básica del dispositivo datos, mensajes, contactos, imágenes, correos, datos de navegación entre otros. De esta manera según la información que obtendremos podemos deducir si hubo o no participación del ususario del móvil en el caso investigado.

Para poder estudiar la información se trabaja en las copias dado que la información digital es bastante frágil, el sólo hecho de dar doble clic a un archivo modificaría la última fecha de acceso del mismo, es por ello que la importancia de las copias radica en que se debe preservar la integridad de la información, al tener copias, se mantiene intacta la información del archivo original.

Una vez establecidos los puertos de conexión con la herramienta determinada y el dispositivo móvil es posible realizar la navegación e indagación sobre los archivos instalados en el móvil.

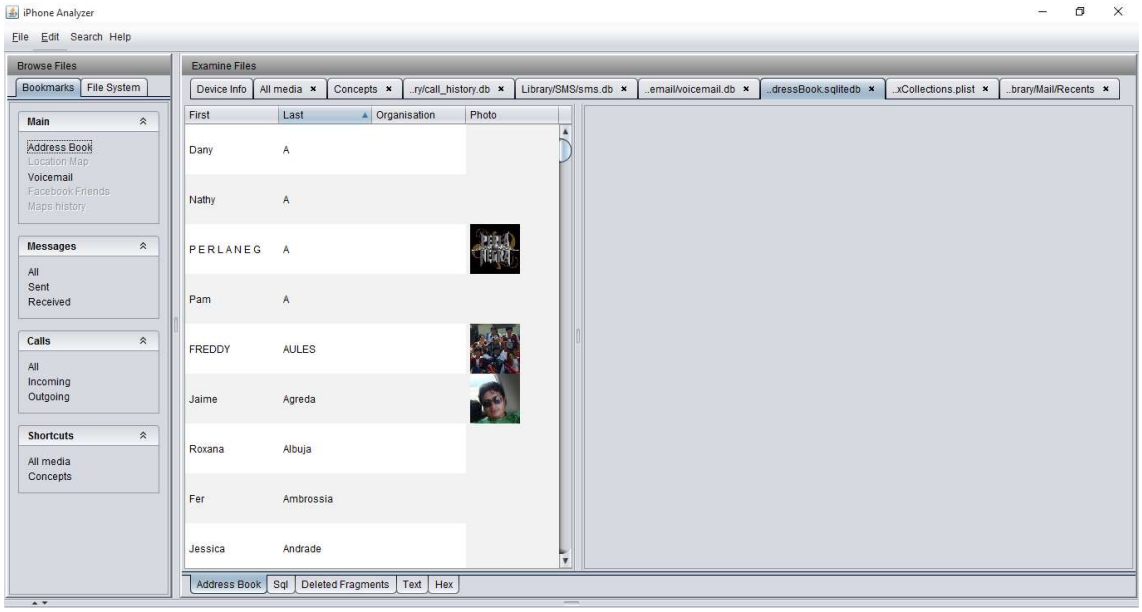



**Figura 23.** Interfaz de contactos personales del dispositivo.

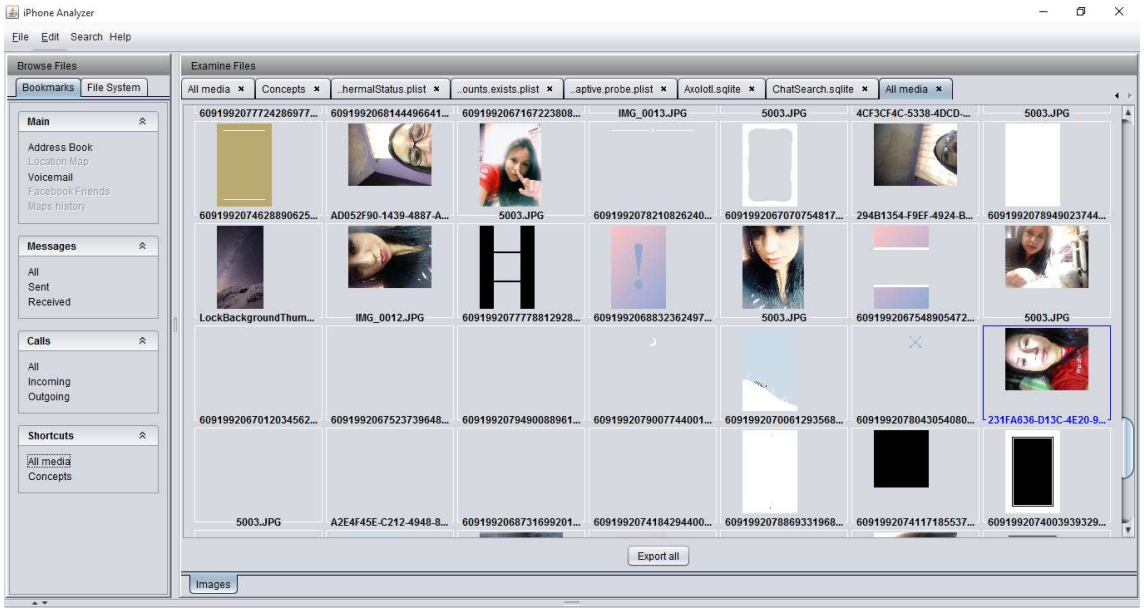



**Figura 54.** Interfaz de navegación de archivos instalados

Se deduce qué pasó según lo que se va obteniendo, se estudia la información que se obtiene para determinar la importancia de cada hallazgo en el dispositivo, como lo es el historial de llamadas.

Después de obtener el acceso a los datos del dispositivo, mediante iPhone Backup analizar se permite ingresar en el historial del dispositivo.

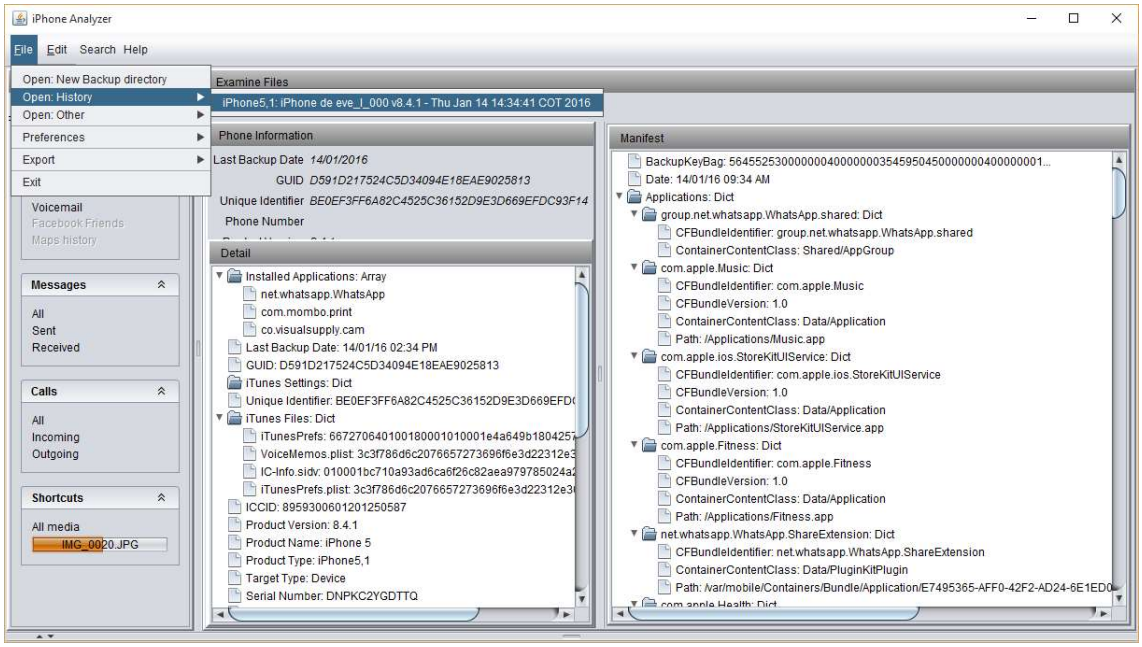



**Figura 6**. Pantalla de acceso al historial del dispositivo

También se puede revisar el historial de llamadas, ya en esta etapa debemos determinar la importancia de la información que el proceso de análisis arroja.

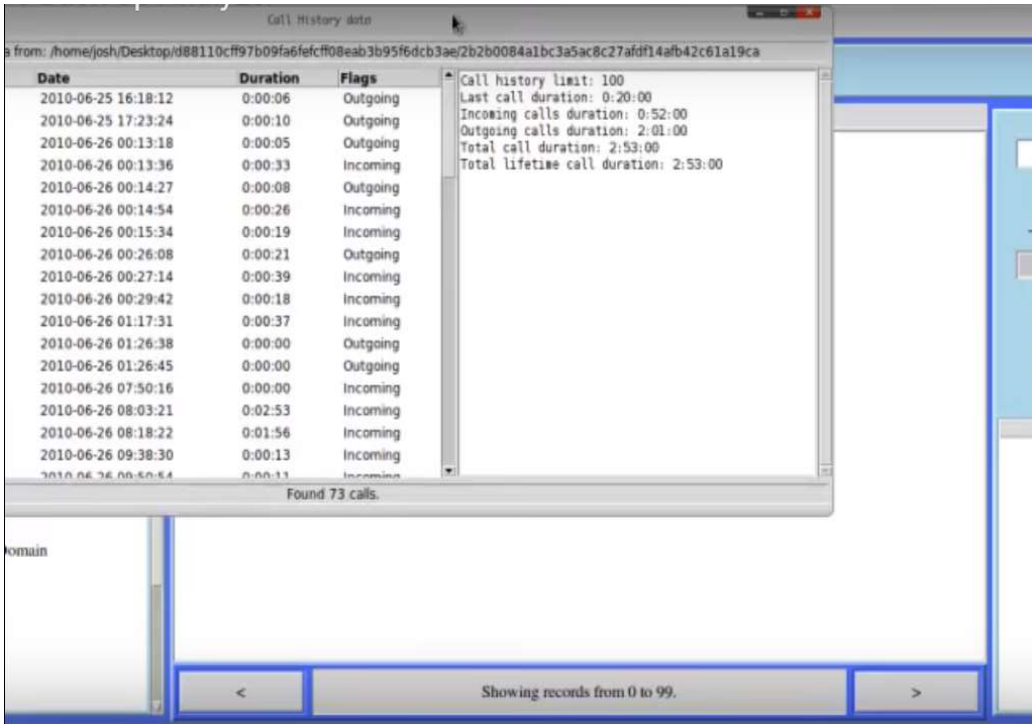



**Figura 7**. Historial de llamadas

Se puede revisar los mensajes enviados y recibidos:

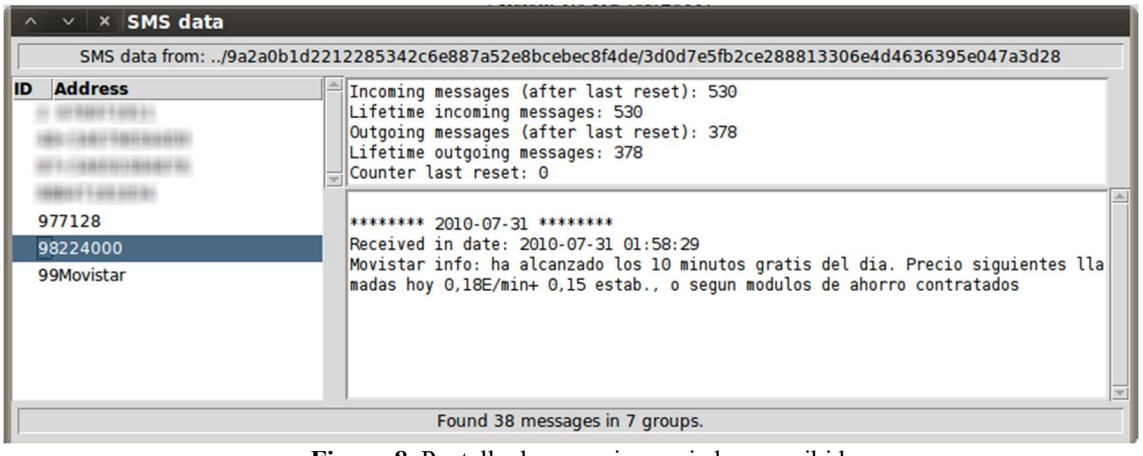



**Figura 8.** Pantalla de mensajes enviados y recibidos

Se analiza la lista de contactos registrados en el dispositivo

De acuerdo a la información que se verifica se puede definir qué es lo que sucedió, para determinar la relación entre la información que se obtiene y el caso investigado. Aquí se establece una relación lógica entre los procesos realizados y las pruebas obtenidas, se documenta la información y se procede posteriormente a realizar un reporte. Se realiza un análisis de los archivos recibidos y se hace una correlación de eventos.

### 3.2.4. Etapa de Presentación

Generalmente el reporte es obtenido de la aplicación utilizada, pero además de esto se debe realizar un informe en el cual se recopila la información de las otras fases, este informe se elabora de acuerdo a los criterios de:

- Solicitud de asignación de caso
- Roles y Funciones
- Información de los involucrados
- Componentes electrónicos incautados
- Información del dispositivo
- Software utilizado para el análisis
- Generación de código hash MDS
- Formulario de la fuente de información
- Reporte generado por la aplicación utilizada.

**Reporte del análisis forense**

El reporte del análisis forense es la presentación final de los resultaos así se determina y establece la documentación final de todas las acciones y eventos y hallazgos obtenidos durante la investigación.

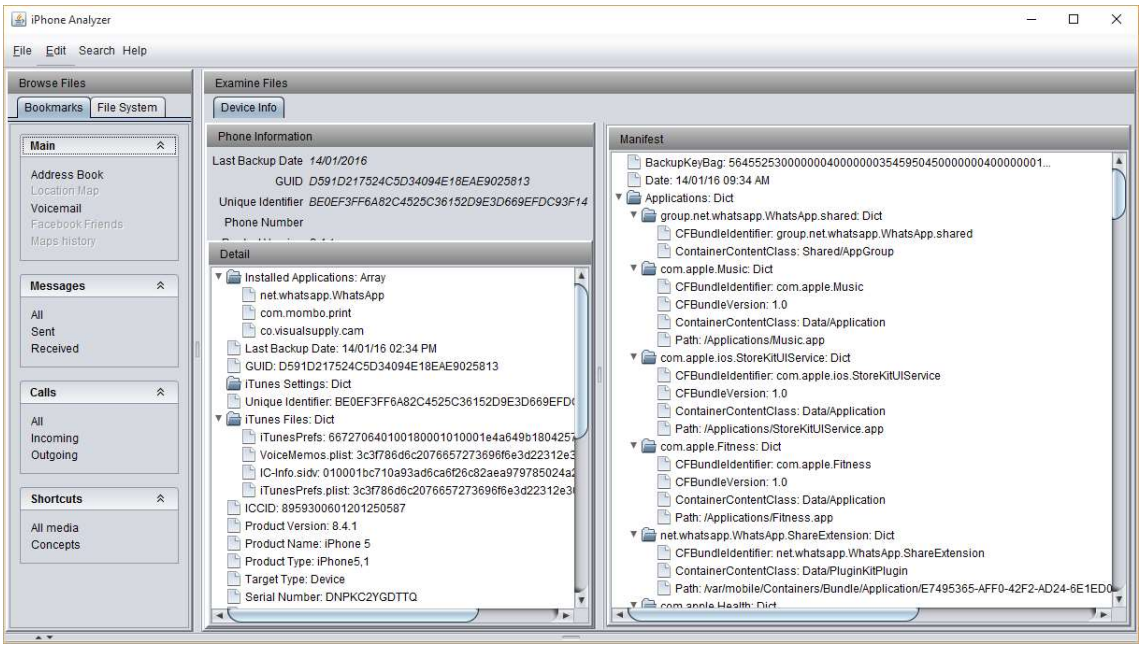



**Figura 98.** Log de Análisis Final

**Tabla 19:**
Reporte final


| Descripción del caso: Caso de prueba | | | |
|---|---|---|---|
| Descripción del teléfono celular: el celular corresponde a la marca IPhone 3G | | | |
| **Tipo fuente de información** | **Ruta** | **Fuente de información** | **Detalle** |
| .db | **Data/data/com.skype-files** | **Shared.xml** | **Se encuentra perfil de Skype** |
| .xml | **Data/data/com.android.contacts-databases** | **Preferences.xml** | **Se encuentra contactos guardados en correo gmail** |
| .db | **Data/data/com.twitter** | **Twitter.db** | **Se encuentra cuenta activa y contactos** |

| | | | |
|---|---|---|---|
| .db | **Data/data/com.facebook/profile** | **snsFacebook.db** | **Se encuentra inicio de sesión de esta red con conversaciones** |
| .key | **Data/data/systems** | **Gesture.key** | **Se encuentra patrón de seguridad para ingreso** |
| .db | **Data/data/com.calls-data** | **Datacalls.db** | **Se encuentran llamadas realizadas y recibidas** |

### 3.2.4.1. RESULTADOS OBTENIDOS

**Resultados con más dispositivos.**

De manera experimental se efectuó el procedimiento a 10 teléfonos móviles iphone, identificando toda la información almacenada en el dispositivo.

Se validaron los resultados usando diferentes herramientas tanto de software libre como de software propietario. La metodología permitió recolectar, manejar y analizar evidencias digitales almacenadas en el dispositivo móvil, garantizando el proceso forense. Para llevar a cabo éste proceso se identificaron varias herramientas, sin embargo ninguna de ellas resulta ser mejor que otra, incluso presentan deficiencias para interactuar con los dispositivos. Por lo tanto es importante utilizar varias de ellas para mejorar el proceso tanto de preservación, así como el de análisis.

Se analizó: Mobile Edit para preservar la información, Oxygen Forensic para la obtención del Hash que garantiza la integridad, y Iphone Analyzer para el análisis; esta herramienta nos permitio obtener un rendimiento promedio del 90% durante todo el proceso forense, sobre las otras herramientas analizadas y a continuación se muestra el resultado del análisis.


**Fig. 29:** Número de dispositivos analizados

A continuación se muestra los resultados luego de haber realizado el análisis de los dispositivos, cada opción ha sido calificada con un los siguientes valores.

1: No aplica
2: Deficiente
3: Bueno
4: Muy Bueno
5: Excelente

**Tabla 20:**
Análisis de Resultados de cada teléfono según su Sistema Operativo IOS

| S.O. | Rapidez | Eficacia | Capacidad de Respuesta | Compatibili-dad con la Interfaz | Tiempo de Análisis | Efectividad | Recupera-ción |
|---|---|---|---|---|---|---|---|
| **Iphone 4** | 2 | 4 | 4 | 5 | 4 | 5 | 4 |
| **Iphone 5** | 3 | 5 | 4 | 5 | 4 | 4 | 4 |
| **Iphone 5s** | 4 | 5 | 3 | 4 | 5 | 4 | 3 |
| **Iphone 6** | 4 | 5 | 3 | 4 | 5 | 4 | 3 |

Mediante estos resultados podemos observar que el software es aplicable para todos los Sistemas Operativos del Iphone IOS, tiene variaciones entre el Iphone 6 y el Iphone 5 debido a la limitante del open source hace que en el Iphone 6 no se registre mayor capacidad de respuesta que en los otros modelos, ya que en el software no habido más actualizaciones hasta el momento, pero tanto en efectividad y tiempo de análisis se llega a la conclusión de que el software cumple los objetivos planteados y se puede tener efectividad en la recuperación de los archivos almacenados en cada uno de los dispositivos analizados.

### 3.2.5. Etapa de Entrega de Evidencia

En esta última etapa una vez terminado el análisis se procede a devolver todo lo que se incautó para proceder con este caso, se detalla lo que se entrega para no tener problemas más adelante con el material presentado.

**Tabla 21:**
Entrega de material

| Tipo | Nombre | Identificador | Fecha de entrega | Fecha de recepción |
|---|---|---|---|---|
| **Celular** | Iphone IOS 4 | 45637C238web | 25/02/2016 | 25/02/2016 |
| **Cable USB** | Conector a pc | N/A | 25/02/2016 | 25/02/2016 |
| **Cargador** | Apple | RT-985 | 25/02/2016 | 25/02/2016 |
| **Manos libres** | Apple | N/A | 25/02/2016 | 25/02/2016 |

# CAPÍTULO IV

# 4. CONCLUSIONES Y RECOMENDACIONES

## 4.1.Conclusiones

- Tras el presente estudio investigativo se determina como conclusión que al realizar un análisis forense a dispositivos móviles con tecnología iPhone para la obtención de información almacenada y la posterior interpretación de los datos tras utilizar herramientas de análisis forense open source, se logró examinar la arquitectura de dispositivos iPhone.

- De igual forma se logró distinguir los diferentes mecanismos de almacenamiento de datos e información relevante almacenados en dispositivos móviles iPhone mediante las herramientas open source.

- Tras la aplicación de las herramientas open source fue posible identificar los mecanismos de seguridad de los dispositivos iPhone. De igual forma se definió que técnicas específicas necesarias a utilizar para la obtención de información en dispositivos móviles.

- Finalmente, se concluye que el presente estudio investigativo en su afán de indagar sobre el análisis forense si aplico herramientas de software forense open source para dispositivos iPhone.

- El empleo de las nuevas herramientas informáticas, incrementa las modalidades de delitos con el uso de la tecnología.

- Se requiere aplicar metodologías y procedimientos específicos en equipos con tecnología avanzada con el fin de asegurar integridad de las evidencias.

- El modelo propuesto brinda un orden durante todo el proceso de análisis, el cual facilita la obtención de la información, la adquisición de datos y su posterior estudio.

- Se concluye que la herramienta más eficaz para realizar análisis forense en open source, misma que permite realizar la extracción de datos y que cumple con lineamientos de cada fase de la cadena de custodia.

## 4.2.Recomendaciones

- Se recomienda contar con todos los requerimientos antes de realizar el análisis forense.

- Es necesario que se siga paso a paso los procedimientos del análisis para evitar alterar de alguna manera la evidencia

- Se recomienda trabajar en copias de la imagen digital generada en la fase de obtención de pruebas.

- El modelo propuesto que se ha aplicado es el resultado de un estudio para ver ventajas y desventajas en comparación a otros modelos, este estudio es necesario para elegir la herramienta que más se adecúe al proceso de análisis forense según el sistema operativo.

**BIBLIOGRAFÍA**

Agualimpia, C., & Hernández., R. (2012). *ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SYMBIAN OS.* Pontificia Universidad Javeriana.

Alegsa.com.ar. (2015, 07 31). *http://www.alegsa.com.ar*. Retrieved from http://www.alegsa.com.ar: http://www.alegsa.com.ar/Dic/backup.php

alkidia.com. (n.d.). *http://www.alkidia.com*. Retrieved 09 23, 2015, from http://www.alkidia.com: http://www.alkidia.com/informe/pericial/

Comisión Europea. (2014, 11 07). *http://science-girl-thing.eu*. Retrieved from http://science-girl-thing.eu: http://science-girl-thing.eu/es/jobs/analista-informatica-forense

compendium.com.ar. (n.d.). *http://www2.compendium.com.ar*. Retrieved 09 23, 2015, from http://www2.compendium.com.ar: http://www2.compendium.com.ar/juridico/peri2.html

Computer Forensic. (2010). *Investigating Network intrusions & Cyber Crime.*

Cuenca, A. (2013, 03). *http://oiprodat.com*. Retrieved 09 18, 2015, from http://oiprodat.com: http://oiprodat.com/2013/03/06/delitos-informaticos-y-comercio-electronico-ecuador/

Darahuge, E. (n.d.). *http://psicologiajuridica.org*. Retrieved 09 23, 2015, from http://psicologiajuridica.org: http://psicologiajuridica.org/psj181.html

Darahuge, M. (n.d.). *http://psicologiajuridica.org*. Retrieved 09 22, 2015, from http://psicologiajuridica.org: http://psicologiajuridica.org/psj181.html

Deconceptos.com. (n.d.). *http://deconceptos.com*. Retrieved from http://deconceptos.com: http://deconceptos.com/general/analista

definicionabc.com. (n.d.). *http://www.definicionabc.com*. Retrieved 09 23, 2015, from http://www.definicionabc.com: http://www.definicionabc.com/tecnologia/sistema-operativo.php

Echarri, A. (1999). *La Transferencia de Tecnología.* Fundación Confemetal.

educaweb.com. (2015). *http://www.educaweb.com*. Retrieved from http://www.educaweb.com: http://www.educaweb.com/profesion/analista-sistemas-informaticos-362/

eHow en Español. (n.d.). *http://www.ehowenespanol.com.* Retrieved 09 17, 2015, from http://www.ehowenespanol.com/: http://www.ehowenespanol.com/historia-informatica-forense-sobre_102525/

El telégrafo. (2012, 06 14). Hay 600 casos de delitos informàticos en 17 meses. *El Telégrafo*.

EUMED . (2010). *http://www.eumed.net*. Retrieved from http://www.eumed.net: http://www.eumed.net/libros-gratis/2010c/752/El%20Peritaje.htm

Eumed.net. (2010). *http://www.eumed.net*. Retrieved from http://www.eumed.net: http://www.eumed.net/libros-gratis/2010e/816/TECNICAS%20DE%20INVESTIGACION.htm

Fabri, S. (n.d.). *http://www.fhumyar.unr.edu*. Retrieved from http://www.fhumyar.unr.edu: http://www.fhumyar.unr.edu.ar/escuelas/3/materiales%20de%20catedras/trabajo%20de%20campo/solefabri1.htm

Ferro, J. (2002). *CYBERINVESTIGACIÓN.*

funcionjudicial.gob.ec. (n.d.). *http://www.funcionjudicial.gob.ec.* Retrieved 09 23, 2015, from http://www.funcionjudicial.gob.ec:

http://www.funcionjudicial.gob.ec/www/pdf/peritos/FORMATO%20DE%20INFORME%20PERICIAL%20OK.pdf

García, I. (2009). *http://www.diccionariojuridico.mx*. Retrieved from http://www.diccionariojuridico.mx: http://www.diccionariojuridico.mx/?pag=vertermino&id=1704

Gestiopolis.com Esperto. (2001, 04 08). *http://www.gestiopolis.com*. Retrieved 09 22, 2015, from http://www.gestiopolis.com: http://www.gestiopolis.com/que-es-el-estudio-de-factibilidad-en-un-proyecto/

Gomez, L. S. (2013). *Pericias informáticas sobre telefonía celular Laboratorio Pericial Informático.*

Google. (2012). *https://www.google.com.ec*. Retrieved 09 18, 2015, from https://www.google.com.ec: https://www.google.com.ec/search?q=imagenes+de+iphone+en+bolsa+antiest%C3%A1tica&biw=1366&bih=669&source=lnms&tbm=isch&sa=X&ved=0CAYQ_AUoAWoVChMIvL3K16mByAIVy6weCh0uGgC9#imgrc=GoA-Y-WLHvHemM%3A

Google.com. (n.d.). Retrieved 09 18, 2015, from https://www.google.com.ec/search?q=imagenes+de+un+celular+iphone+conectado+a+una+computadora&biw=1366&bih=669&tbm=isch&imgil=4qcMAI5eCy1q1M%253A%253BXTaHebTMKoFFAM%253Bhttp%25253A%25252F%25252Fwww.ajpdsoft.com%25252Fmodules.php%25253Fname%2525253DNews%252

Guamán, P. (2014, 09 09). *http://es.slideshare.net.* Retrieved 09 17, 2015, from http://es.slideshare.net: http://es.slideshare.net/PatoGuaman/modelo-de-anlisis-forense

Guevara, A. (2012). Dispositivos móviles. *Revista Seguridad*.

Hernández, B. (2001). *Técncias EStadísticas de investigación.* Madrid: Días de Santos.

iBRICO. (2009, 01 30). *http://www.ibrico.es*. Retrieved from http://www.ibrico.es: http://www.ibrico.es/2009/01/30/glosario-terminos-relacionados-con-el-desbloqueo-del-iphone/

IET. (2012, 05 19). *https://investigacionestodo.wordpress.com*. Retrieved from https://investigacionestodo.wordpress.com: https://investigacionestodo.wordpress.com/2012/05/19/clases-y-tipos-de-investigacion-cientifica/

INEC. (2014). *Encuesta de la Tecnologìa de Informaciòn y Comunicación.* Quito.

Instituto Tecnológico de Sonora. (n.d.). *http://biblioteca.itson.mx*. Retrieved from http://biblioteca.itson.mx: http://biblioteca.itson.mx/oa/educacion/oa3/paradigmas_investigacion_cuantitativa/p11.htm

Jorge, M., Karina, S., & Pablo, H. (2010). *ESTUDIO Y ANÁLISIS DE EVIDENCIA DIGITAL EN TELÉFONOS CELULARES CON TECNOLOGÍA GSM PARA PROCESOS JUDICIALES.* Escuela Politécnica Nacional.

Kendall & Kendall. (2011). *Análisis y Diseño de Sistemas.* México: SErvices of New England.

Laudon, J. (2004). *Sistemas de información gerencial: administración de la empresa digital.* Mexico, D.F.: Pearson Educación.

Maleza, J. (2011). *Estudio y Anàlisis de evidencia digital en telèfonos celulares.* Quito: EPN.

masadelante.com. (n.d.). *https://www.masadelante.com*. Retrieved 09 23, 2015, from https://www.masadelante.com: https://www.masadelante.com/faqs/tarjeta-sim

Medina, M. (2012). *Aplicabilidad metodològica de la informàtica forense en la obtenciòn de resultados.* El Salvador: Universidad El Salvador.

Ocampo, L. M. (2009). *Informatica Forense Para Moviles.* Universidad Mayor De San Andres .

RRPPnet. (2001). *http://www.rrppnet.com.ar*. Retrieved from http://www.rrppnet.com.ar: http://www.rrppnet.com.ar/tecnicasdeinvestigacion.htm

Sampieri, R. H. (2004). *Metodología de la Investigación.* Chile: Mc Grew Hill.

securitybedefault.com. (2010, 09 08). *http://www.securitybydefault.com*. Retrieved 09 22, 2015, from http://www.securitybydefault.com: http://www.securitybydefault.com/2010/09/forenses-en-iphoneitunes.html

sites.google.com. (n.d.). *https://sites.google.com*. Retrieved 09 23, 2015, from https://sites.google.com: https://sites.google.com/site/desarrollo2osti/tema-7/4

Slideshare.net. (n.d.). *http://es.slideshare.net*. Retrieved 09 23, 2015, from http://es.slideshare.net: http://es.slideshare.net/mquintabani/prueba-pericial-informatico-forense-presentation-653330

Smetoolkit. (2012). *http://mexico.smetoolkit.org*. Retrieved 09 18, 2015, from http://mexico.smetoolkit.org: http://mexico.smetoolkit.org/mexico/es/content/es/477/Gesti%C3%B3n-de-proyectos-de-inform%C3%A1tica

Suport Apple. (n.d.). *https://support.apple.com*. Retrieved 09 21, 2015, from https://support.apple.com: https://support.apple.com/kb/SP495?locale=es_ES&viewlocale=es_ES

The Free dictionary. (2015). *http://es.thefreedictionary.com*. Retrieved from http://es.thefreedictionary.com: http://es.thefreedictionary.com/perito

Toaza, J. (2011). *http://repositorio.cisc.ug.edu.ec.* Retrieved 09 18, 2015, from http://repositorio.cisc.ug.edu.ec: http://repositorio.cisc.ug.edu.ec/bitstream/123/61/2/TOMO%202.pdf

Tortosa, J. (n.d.). *http://www.antud.org.* Retrieved 09 23, 2015, from http://www.antud.org: http://www.antud.org/El%20informe%20pericial.pdf

Universidad César Vallejo. (2010). *http://intranet.ucvlima.edu.pe.* Retrieved from http://intranet.ucvlima.edu.pe: http://intranet.ucvlima.edu.pe/campus/file/6001213119/SEP%205%20-%20RU.pdf

Vera, L. (n.d.). *http://www.ponce.inter.edu*. Retrieved from http://www.ponce.inter.edu: http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html