UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

"ESTUDIO Y EVALUACIÓN DE APLICACIONES PARA EL ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES BAJO ANDROID EN LA CIUDAD DE AMBATO"

Proyecto de Trabajo de Graduación. Modalidad: Seminario de graduación presentado previo la obtención del título de Ingeniero Sistemas Computacionales e Informáticos

AUTOR: Yu Lung Li

TUTOR: Ing. Luis Solís

Ambato - Ecuador

Aprobación del tutor

En mi calidad de tutor del trabajo de investigación sobre el tema " ESTUDIO Y EVALUACIÓN DE APLICACIONES PARA EL ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES BAJO ANDROID EN LA CIUDAD DE AMBATO ", del señor LI YU LUNG, estudiante de la carrera de ingeniería en sistemas informáticos y computacionales, de la facultad de ingeniería en sistemas, electrónica e industrial, de la universidad técnica de Ambato, considero que le informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad el Art. 16 del capítulo II, del reglamento de graduación para obtener el Titulo Terminal de tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Febrero 2013

Ing. Luis Solís

Autoría

el presente trabajo de investigación titulado :" ESTUDIO Y EVALUACIÓN DE APLICACIONES PARA EL ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES BAJO ANDROID EN LA CIUDAD DE AMBATO ". Es absolutamente original, autentico y personal, en la virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor

_____

Li Yu Lung

C.C.: 171555942-1

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Clay Aldas, Ing. Galo López, revisó y aprobó el Informe Final del trabajo de graduación titulado **"ESTUDIO Y EVALUACIÓN DE APLICACIONES PARA EL ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES BAJO ANDROID EN LA CIUDAD DE AMBATO."**, presentado por el señor Yu Lung Li de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

_____

Ing. Edison Álvarez, Mg.

PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. Clay Aldas, Mg. Ing. Galo López, Mg.

DOCENTE CALIFICADOR DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo está dedicado a mis amados padres, hermana y a todas esas personas que incondicionalmente están junto a mí dándome ese apoyo infinito y palabras de aliento necesarias para seguir adelante y enfrentar los obstáculos de la vida diaria. Pero todo esto no se hubiese logrado sin las bendiciones de Dios, que siempre está conmigo guiándome por el camino del bien.

Li Yu Lung.

AGRADECIMIENTO

Primeramente a Dios que siempre ha sido mi guía, y por haberme bendecido con una familia única, que a pesar de todo obstáculo siempre estamos unidos y apoyándonos entre todos.

En especial al Ing. Luis Solis quien con su experiencia me ha sabido guiar y ayudar en todo lo necesario. También un eterno e infinito agradecimiento a las personas que me dieron su ayuda durante el desarrollo del proyecto, gracias por todo su apoyo.

Li Yu Lung.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La necesidad de comunicación del ser humano lo ha motivado a desarrollar sistemas o dispositivos altamente sofistificados, que incorporan conceptos inalámbricos y de movilidad para facilitar y mejorar la comunicación al desplazarse libremente.

Es de esta forma que el campo de las comunicaciones inalámbricas móviles representadas principalmente por las tecnologías celulares, se ha convertido en uno de los ejes más destacados de las telecomunicaciones a nivel global.

El origen del teléfono móvil fue en los inicios de la Segunda Guerra Mundial, donde vieron la necesidad de la comunicación a distancia, es por eso que la compañía Motorola creó un equipo llamado Handie Talkie H12-16, es un equipo que permite comunicarse con las tropas vía ondas de radio cuya banda de frecuencias en ese tiempo no superaban los 60 MHz.

Durante ese periodo y 1985 se comenzaron a perfeccionar y amoldar las características de este nuevo sistema revolucionario ya que permitía comunicarse a distancia. Fue así que en los años 1980 se llegó a crear un equipo que ocupaba recursos similares a los Handie Talkie pero que iba destinado a personas que por lo general eran grandes empresarios y debían estar comunicados, es ahí donde se crea el teléfono móvil y marca un hito en la historia de los componentes inalámbricos ya que con este equipo podría hablar a cualquier hora y en cualquier lugar.

En la actualidad, la mayoría de personas posee un teléfono celular sea para uso personal o laboral, tanto fue la acogida que se ha convertido en una herramienta

indispensable para las personas. por tal motivo desde hace aproximadamente diez años, el uso de dispositivos móviles se ha incrementado notablemente por las funcionalidades que brinda para poder mantenerse en contacto con las personas y otros servicios más.

Pero algo que debemos tomar en cuenta que mientras haya más servicios que nos facilita las cosas pero de igual forma va incrementado el peligro, es decir al proporcionar tantas facilidades también proporciona más facilidades para cometer algún delito o crimen, por tal motivo aparece el termino de **Análisis Forense** el cual sirve para poder detectar y recolectar toda información necesario para documentarla y llevar a la corte.

CAPÍTULO I

EL PROBLEMA

1.1. Tema:

Estudio y evaluación de aplicaciones para el análisis forense de dispositivos móviles bajo Android en la ciudad de Ambato.

1.2. Planteamiento del problema

1.2.1. Contextualización

Android es un sistema operativo basado en el núcleo Linux diseñado originalmente para dispositivos móviles, tales como teléfonos inteligentes, pero que posteriormente se expandió su desarrollo para soportar otros dispositivos tales como tablets, reproductores MP3, netbooks, PCs, televisores e incluso, se han llegado a ver en el CES, microondas y lavadoras.

Android tiene una gran comunidad de desarrolladores el cual desarrollan aplicaciones para los dispositivos móviles, actualmente ha alcanzado más de 250.000 aplicaciones el cual está disponible para todas las personas.

En el Ecuador, el uso de los celulares también se ha incrementado

considerablemente sin embargo Android todavía no es un sistema muy conocido, ya que son sistemas nuevos y no hay muchas personas que sepa bien de la sobre esa tecnología.

El primer móvil bajo Android llega a Ecuador, casi dos años después de que sus similares hicieran su aparición en el mercado de Smartphone con el HTC Dream con la empresa Telefónica Movistar.

En la ciudad de Ambato las personas ya adquieren los teléfonos inteligentes con sistema de Android pero se desconoce las aplicaciones del sistema por lo que no es correctamente utilizado desperdiciando de esta manera los beneficios que presta este tipo de teléfono inteligente.

1.2.2. Análisis Critico

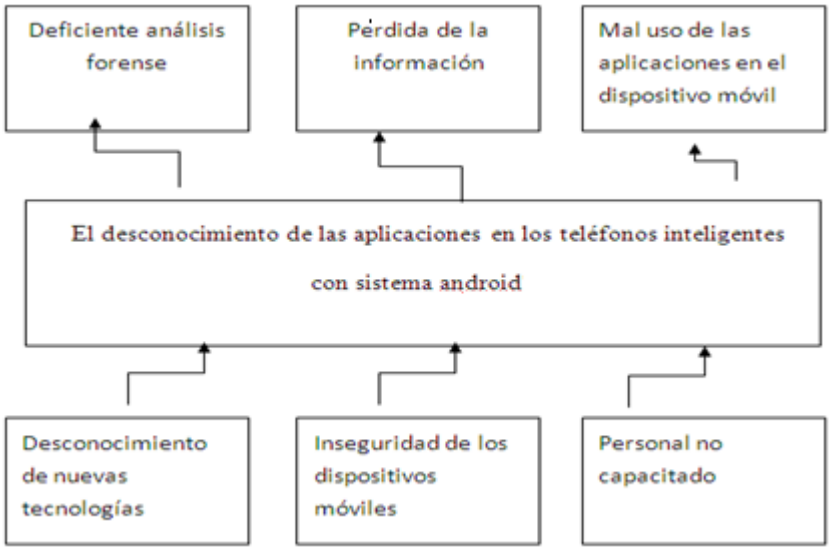


Figura1. 1 Árbol del Problema

Al utilizar los teléfonos inteligentes con sistema Android, se lo realiza muy superficialmente esto se debe a que existe un desconocimiento por parte de los usuarios de nuevas tecnologías que se está aplicando en los actuales sistemas de los teléfonos Android lo que ocasiona que al realizar un análisis forense del

mismo este sea deficiente.

Actual mente los teléfonos inteligentes son modificados constantemente lo que ocasiona que haya una inseguridad en los dispositivos lo que con lleva a perdida de la información siendo afectado el usuario.

Las personas que actualmente utilizan sistemas android no están debidamente capacitado en el manejo de este sistema lo que hace que se dé un mal uso de las aplicaciones en los dispositivos móviles.

Además como el análisis forense es un tema nuevo el cual no hay muchas personas que sepan o tengan conocimientos de esto y no hay personas capacitadas referente al tema de análisis forense por eso no le pueden dar el uso correcto a las aplicaciones existentes.

1.2.3. Prognosis

La deficiente utilización de las aplicaciones de los teléfonos inteligentes con sistema Android haría que este tipo de teléfonos no sea muy apreciado dentro de los usuarios por el desconocimiento del manejo del mismo por lo que podría traer problemas principalmente cuando se realice análisis forense lo que producirá descontento de quienes hayan adquirido este tipo de tecnología produciéndose reclamos a la empresa distribuidora la misma que podría sufrir pérdidas económicas así como un desprestigio.

Si no se puede conocer y saber más sobre las aplicaciones de los celulares inteligentes con sistema Android entonces no podríamos mejorar el análisis forense a este dispositivo y a futuro las personas no sabría cómo usar las aplicaciones de análisis forense a ese tipo de celulares inteligentes.

1.2.4. Formulación del problema

¿Cómo influye el desconocimiento de aplicaciones en el análisis forense de los dispositivos móviles bajo Android?

1.2.5. Preguntas y directrices

- ¿Cuáles son las aplicaciones más adecuadas para el análisis forense del estudio de la funcionalidad de los programas siguientes: Bitpim, Oxigen Forensics, Device Seizure, MOBILedit y SDK

- ¿Cómo analizar el uso de los dispositivos móviles de los usuarios?

- ¿ Que características debe tener la propuesta que mejore el análisis forense de los dispositivos móviles con S.O. de Android mediante la aplicación del software más adecuado como el resultado de estudio y evaluación del programa

1.2.6. Delimitación

Campo: Seguridad Informática
Área: Análisis forense
Aspecto: Metodología de la seguridad informática.
Tiempo: Para el investigador la información será tomada del año 2009 al año 2010.
Lugar: usuarios de la ciudad de Ambato

1.3. Justificación

Actualmente la tecnología está avanzando a pasos agigantados, Ahora toda la información es almacenada en los ordenadores de manera automática, a diferencia de épocas anteriores en donde la información se almacenaba de manera manual y en papel. Esto conlleva cierto tipo de ventajas y desventajas.

Las ventajas son evidentes, mayor facilidad en el manejo de la información, rapidez en la recolección y análisis de la misma, alta disponibilidad tanto en tiempo como en localidad. Sin embargo, las desventajas y riesgos en los que se incurre no son tan obvios. Entre estos, la vulnerabilidad de la información a ser borrada, la fácil replicación de la información, la explotación de la información por vulnerabilidades en el sistema.

Con todo el riesgo que se corre al manejar información debemos de tener una manera de protegernos y de proteger a las personas de las que mantenemos información. Para poder mejorar las políticas de seguridad y la protección de la información y las tecnologías que facilitan la gestión de la información surge la informática forense.

Porque La información es el activo más valioso que poseemos en la sociedad actual. Ésta es cada vez más importante para el desarrollo de las empresas y de negocios exitosos a través de la implementación de sistemas de información. Para mejorar la protección de la información surge una nueva Ciencia, la Informática Forense; ésta persigue objetivos preventivos así como reactivos, una vez se ha dado una infiltración en el sistema. La Informática forense es una ciencia relativamente nueva y no existen estándares aceptados.

El análisis forense consiste en investigar sistemas de información con el fin de detectar evidencias en los mismos. La finalidad del análisis forense es para perseguir objetivos preventivos (anticipándose al posible problema) u objetivos correctivos (para una solución favorable una vez que la vulnerabilidad y las infracciones ya se han producido).

Y como es un tema nuevo no existe mucha información sobre la informática forense mucho más si se trata del análisis forense de los dispositivos móviles ya que es algo nuevo y novedoso, pero en la actualidad acorde las necesidades de las personas poco a poco está apareciendo aplicaciones donde nos permite sacar información, y gracias a esto la seguridad informática va mejorando cada vez más,

para que todos los sistemas de información sea más seguros, concisos y pueda disponer de ella en cualquier momento.

En el presente trabajo investigativo se pondrá en práctica los conocimientos teóricos adquiridos para solucionar problemas referentes a la seguridad de información aplicando nuevas tecnologías esto será una aporte hacia el uso de la tecnología.

El proyecto es factible de realizarse porque se cuenta con personal especializado en el área de seguridad informática en la FISEI y contamos con las herramientas necesarias para realizar esta investigación.

La investigación a realizarse es de gran impacto a la sociedad, al campo informático y para la provincia de Tungurahua será de gran ayuda para todas las personas para que puedan proteger más a su información.

1.4 Objetivos

1.4.1. Objetivo General

- Determinar las aplicaciones forenses para el análisis forense de los dispositivos móviles bajo Android.

1.4.2. Objetivos Específicos

- Diagnosticar las aplicaciones más adecuadas para el análisis forense en el estudio de la funcionalidad de los programas siguientes: Bitpim, Device Seizure, Oxigen Forensic, MOBILedit y SDK

- Analizar el uso de los dispositivos móviles en los usuarios.

- Plantear una propuesta que mejore el análisis forense de los dispositivos móviles con S.O. de Android mediante la aplicación del software más adecuado como el resultado de estudio y evaluación de programa.

CAPÍTULO II

MARCO TEORICO

2. Marco Teórico

2.1. Antecedentes Investigativos

No se encontró trabajos similares que se refieran al tema.

2.2. Fundamento Legal

Sección Tercera
Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

Sección Novena

Personas Usuarias y Consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características. La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

Sección octava

Ciencia, Tecnología, Innovación y Saberes Ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Sección Novena

Gestión del Riesgo

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza

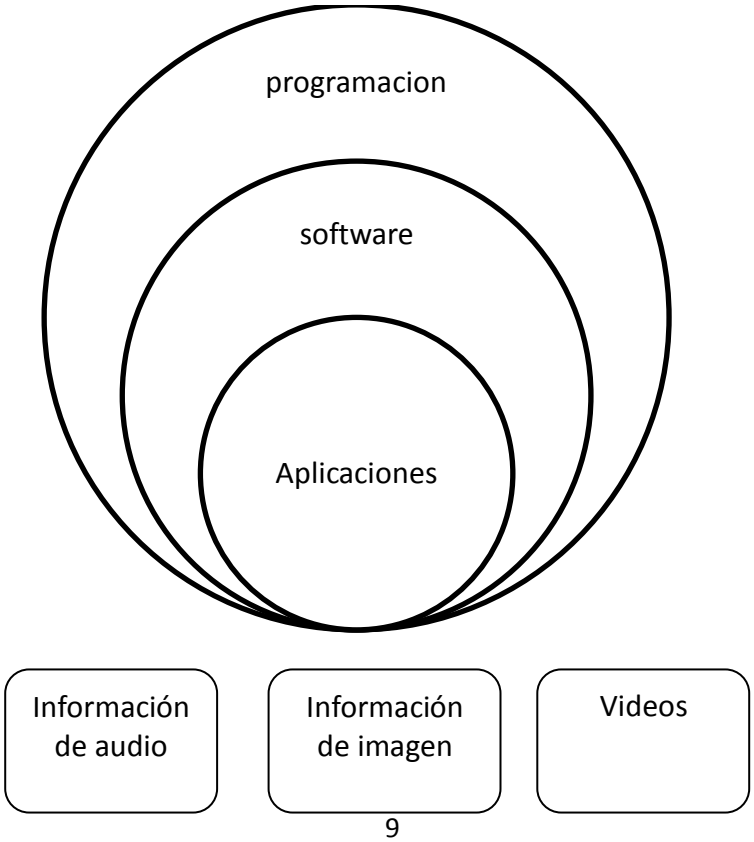
frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

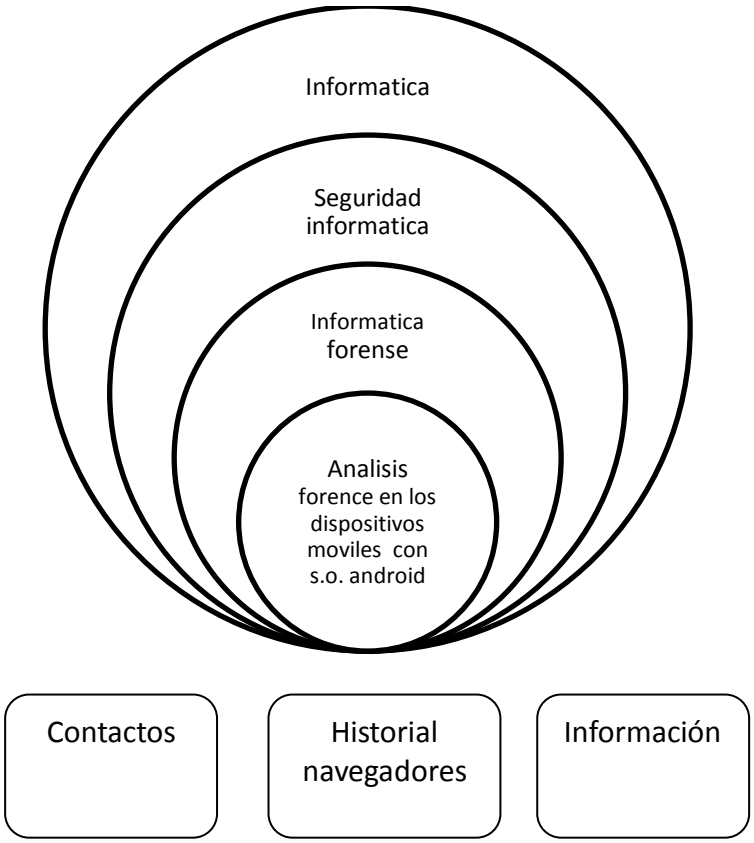
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.

4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.

2.3. Categorías Fundamentales

Es proponer un sistema de categorías que permitan acercarse al problema, describirlo y analizarlo, relación entre variables y posteriormente comprobar esa relación





Programación

Para GUSTAVO FABIÁN TORREALDAY (Internet; desconocido; 22, 10,2011; 20h00 pm) dice: Un lenguaje de programación es una serie de comandos que nos permiten codificar instrucciones de manera que sean entendidas y ejecutadas por una computadora. de la misma forma GUS WOLVERING dice que: símbolos y reglas que permite la construcción de programas con los que la computadora puede operar así como resolver problemas de manera eficaz. También LISANDRO PERALTA MURUA dice: que es un conjunto de instrucciones que nos permiten realizar operaciones de entrada/salida. Calculo, manipulación de texto, lógica/comparación y almacenamiento/recuperación.

Programación es una serie de instrucciones donde construimos el comportamiento o las operaciones que debe que hacer para poder resolver el problema con el

computador.

Software

Según KERVIN VERGARA dice: El software es un conjunto de programas elaborados por el hombre, que **controlan la actuación del computador**, haciendo que éste siga en sus acciones una serie de esquemas lógicos predeterminados.

(Internet; 21, 10, 2011; 27,10 ,2011; 19h05 pm)Se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.
Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas; tales como el procesador de textos, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el software de sistema, tal como el sistema operativo, que, básicamente, permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz para el usuario.

El software se compone se secuencias de órdenes que indica al hardware que debe realizarse, es decir seguir las instrucciones programadas.

Software de Seguridad

(Internet; desconocido; 30,10,2011; 20h10 pm)Siempre que utilicemos un sistema informático, sin importar cuál sea la razón, es importante que tengamos como prioridad la instalación de un software de seguridad, teniendo en cuenta la cantidad de riesgos que corremos con un sistema informático sin protección. Justamente por la importancia acerca de lo que es un software de seguridad para cualquier usuario, la mayoría de los sistemas operativos con los que podemos

trabajar suelen traer incorporado en ellos un software de seguridad básico, pero es importante que sepamos ante todo qué es un software de seguridad y la diferencia entre éste software y uno que es especialmente desarrollado para prevenir problemas en el funcionamiento del sistema, es que el mismo, simplemente nos advierte cuando estamos frente a algún riesgo.

(Internet; desconocido; 20,10,2011; 20h40 pm)**Es importante que sepamos ante todo qué es un software de seguridad y la diferencia entre éste software y uno que es especialmente desarrollado para prevenir problemas** en el funcionamiento del sistema, es que el mismo, simplemente nos advierte cuando estamos frente a algún riesgo.

Aplicaciones de Seguridad

Son Programas informáticos ayuda a proteger el equipo que lo tenga instalado contra virus, robo de información, o ataques informáticos que se pueda tener en una computadora

Información de Audio

(Internet; desconocido; 22,01,2012; 16:34pm) es un contenedor multimedia que guarda una grabación de audio (música, voces, etc.). Lo que hace a un archivo distinto del otro son sus propiedades; cómo se almacenan los datos, sus capacidades de reproducción, y cómo puede utilizarse un archivo en un sistema de administración de archivos (etiquetado).

La manera general de almacenar audio digital es maestreando el voltaje de audio, que al reproducirlo, corresponde a un nivel de señal en un canal individual con un cierto resolución -el número de bits por muestreo - en intervalos regulares (creando la frecuencia de muestreo). Estos datos después pueden ser almacenados sin comprimir o comprimidos para reducir el tamaño del formato.

Información de Imagen

(Internet; desconocido; 25,01,2012; 17:00pm) es un archivo donde se almacena una copia o imagen exacta de un sistema de ficheros, normalmente un disco compacto, un disco óptico, como un CD, un DVD..., pero también soportes USB. Una imagen Iso es la elección más común que se adopta en memorias extraíbles. Como usa el protocolo ISO 9660 o el protocolo UDF que es compatible con el ISO 9660, es útil a la hora de distribuir por Internet, archivos que necesitan evitar en la transferencia la pérdida de cualquier información o la modificación de la estructura original, necesaria muchas veces para el correcto funcionamiento del programa. Aunque la ISO 9660 lo especifica como formato de *sólo lectura* es posible modificarlos con algunos programas.

Videos

(Internet; desconocido; 01,11,2011; 16:44pm) Modo en el que los vídeos guardan los datos de un archivo de vídeo con el fin de que puedan ser interpretados por el ordenador. Normalmente, un vídeo es una colección de imágenes acompañada de sonido; la información de uno y otro tipo se suele grabar en pistas separadas que luego se coordinan para su ejecución simultánea.

Informática

(Internet; desconocido; 25,10,2011; 21h10 pm)JHON DILAS dice: La informática es la ciencia que estudia todo tipo de procesos. Y que está hecha para solucionar problemas de la vida. También ANALÍA LANZILLOTTA dice : La informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora. Esta definición, si bien es bastante amplia, se debe a que el concepto de informática también es amplio. Para referirse a esta ciencia, también suele utilizarse el término Computación o Ciencia de la Computación, con la diferencia de orígenes. El término informática proviene de la conjunción de las palabras francesas “information” y “automatique” que derivaron

en la palabra “informatique”, creada por el ingeniero Dreyfus. Mientras que computación es de origen inglés, refiriéndose a ella como Computer Science.

Informática es la ciencia que estudia la automatización de la información y también del manejo de los datos.

Seguridad Informática

(Internet; desconocido; 23,10,2011; 20h48 pm)La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos.

(Internet; desconocido; 20,10,2011; 20h40 pm)La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

la seguridad informática se enfoca a la protección de las infraestructura computacional y la información que está dentro de ella para dar integridad y consistencia en los datos.

Análisis Forense

(Internet; 28,10,2011; 20h00 pm)Rodney McKennish, dice "Es la técnica de capturar, procesar e investigar información procedente de sistemas informáticos utilizando una metodología con el fin de que pueda ser utilizada en la justicia". Ángel Alonso Párrizas, Roberto Gutiérrez tambien dice: El uso de métodos científicamente probados y derivados hacia la conservación, la recogida, validación, identificación, análisis, interpretación, documentación y la presentación de evidencia digital derivada de cámaras digitales fuentes con el fin de facilitar o promover la reconstrucción de los hechos del criminal, o ayudar a anticipar las acciones no autorizadas demostrado ser perjudicial para las operaciones previstas

Análisis Forense de los Dispositivos Móviles

(Internet; desconocido; 30,10,2011; 22h40 pm)Según MARCELO RODRÍGUEZ Uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal (Digital Forensic Research Workshop DFRWS).

El análisis forense de los dispositivos móviles es uno de los métodos forenses informáticos que se aplica a los dispositivos móviles para poder sacar evidencia del dicho dispositivo, como el acceso a la información, lista de contactos, llamadas... etc.

Contactos

Son las listas de personas que se tiene registrado en el celular con su respectiva información: numero, cumpleaños ..etc.

Historial de Navegadores

son todos los lugares o sitios que has visitado o navegado y eso se va registrando dentro de los archivos temporales para luego poder listar todos los sitios ordenado con las fechas de navegación.

Información

(Internet; desconocido; 01,12,2011; 17h02 pm)La **información** es un **conjunto organizado de datos**, que constituye un **mensaje** sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento**.**

(Internet; desconocido; 01,12,2011; 17h02 pm)Según Idalberto Chiavenato, **información** "es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones"

2.4. Hipótesis

Afirmación en presente

El uso de las aplicaciones influirá en el análisis forense de los dispositivos móviles con S.O. Android.

2.5. Señalamiento de variables

Variable independiente: Aplicaciones

Variable dependiente: Análisis forense de los dispositivos móviles con S.O. Android

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Enfoque

El presente trabajo investigativo tomara un enfoque cuali-cuantitativo por las siguientes consideraciones

Siempre se debe considerar en un entorno natural; se considerará mucho la participación de las personas de cada lugar de la ciudad dentro del problema;

Interna:

Nos permite realizar un análisis de los resultados obtenidos en la ciudad de Ambato; se considerara a las personas de los diferentes lugares o áreas de Ambato en el cual nos permitirá estudiar el tema.

Normativo: se regirá a través de normas y reglas de estudio; se tomara una sola dirección por lo que nos llevará a un solo fin; se explicará lo realizado

3.2. Modalidades Básicas de la Investigación

La presente investigación tiene las siguientes modalidades:

- **Modalidad bibliográfica o documentada:** Se ha considerado esta modalidad porque se ha tomado información del internet, libros virtuales, tesis de grados, videos, informes, proyectos, revistas, informes.

- **Modalidad experimental:** Se ha considerado la relación de la variable independiente las vulnerabilidades del reloj biométrico y su influencia y relación de la variable dependiente registros del personal para considerar sus causas y efectos.

- **Modalidad de campo:** Se ha considerado esta modalidad ya que el investigador ira a recoger la investigación primaria directamente de los involucrados a través de encuestas.

3.3. Tipos de Investigación

Se ha realizado la investigación *Exploratoria*, ya que permitió plantear el problema de la investigación como influye el desconocimiento de las aplicaciones para el análisis forense en la detección del mal uso de los dispositivos móviles en las oficinas comerciales en la zona del centro de la ciudad de Ambato como de la misma manera nos ayudó a plantear la hipótesis Es posible El uso de las aplicaciones forenses para realizar el análisis forense de los dispositivos móviles detecta el mal uso de los dispositivos móviles con S.O. Android en usuarios de la ciudad de Ambato.

Se ha considerado la investigación *Descriptiva*, por que permitió analizar el problema en sus partes como delimitar en tiempo y espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación *Correlacional*, ya que ha permitido medir la compatibilidad de la variable independiente las vulnerabilidades del reloj biométrico con la dependiente registros de personal.

3.4. Población y Muestra

La población que se va a considerar en la presente investigación será la totalidad del personal que usan dispositivos móviles bajo Android que vive en la ciudad de Ambato.

3.5. Operación de Variables

Variable independiente: aplicaciones				
Concepto	**Categoría**	**Indicadores**	**Ítems**	**Técnicas e instrucciones**
Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de actividades.	Programas informáticos	Tipo	¿Qué tipos de programas informáticos tiene los celulares móviles?	-Ficha de observación
		características	¿Qué tipo de herramientas existe para crear programas?	- Ficha de observación
	herramienta	tipos	¿Qué tipos de actividades puede hacer?	- Ficha de observación
	actividades	tipo		

Tabla 3.1 Tabla de operacionalización de la variable independiente

Variable dependiente: Análisis forense de los dispositivos móviles bajo Android				
Concepto	**Categoría**	**Indicadores**	**Ítems**	**Técnicas e instrucciones**
El análisis forense son los métodos informáticos que se aplica a los dispositivos que tenga memoria para extraer evidencia digital.	métodos informáticos	Herramientas informáticas	¿Qué métodos informáticos existe para el análisis forense de los dispositivos móviles?	Ficha de observación
			¿Qué tipos de S.O. tiene los teléfonos inteligentes?	
			¿Qué evidencia se puede sacar a través del análisis forense de los dispositivos móviles i	
	Dispositivos móviles	Android		Ficha de observación
		iphone		
	evidencia	Información		Ficha de observación

Tabla 3.2 Tabla de operacionalización de la variable dependiente

3.6. Técnicas de Investigación

Bibliográficas	De campo
● El análisis de documentos (lectura científica) ● El fichaje	● observación

Tabla 3.3 Tabla de técnicas de investigación1

Preguntas	Explicación
1. ¿Para que ?	Recolectar información primaria para comprobar la hipótesis
2. ¿A qué personas o sujetos?	Usuarios
3. ¿sobre qué aspectos?	VI: Aplicaciones forenses VD: Análisis forense de dispositivos móviles con S.O. android
4. ¿Quién?	Li Yu Lung
5. ¿Cuándo?	De acuerdo con el cronograma establecido
6. ¿Lugar de recolección de la información	FISEI

7. ¿Cuántas veces?	Una sola vez
8. ¿qué Técnicas de recolección?	Observación
9. ¿Con que ?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiano

Tabla 3.4 Tabla de técnicas de investigación 2

3.7 Procesamiento y análisis de la información

Categorización y tabulación de la información

- tabulación manual
- tabulación computarizada (programa spss)

Análisis de los datos

- La presentación de los datos se hará a través de los gráficos, cuadros para analizar e interpretarlos

Interpretación de los resultados

- describir los resultados
- estudiar cada uno de los resultados por separado
- redactar una síntesis general de los resultados

CAPÍTULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de Resultados

4.1.1 Fichas de Observación

	Si	No
El uso del Smartphone para todas edades?	X	
Se puede acceder a las cuentas personales?	X	
Se tiene el conocimiento sobre aplicaciones de análisis forense?		X
Se puede guardar datos personales ?	X	
Se puede usar para cometer delitos ?	X	

Tabla 4.1 Tabla de Ficha de observación

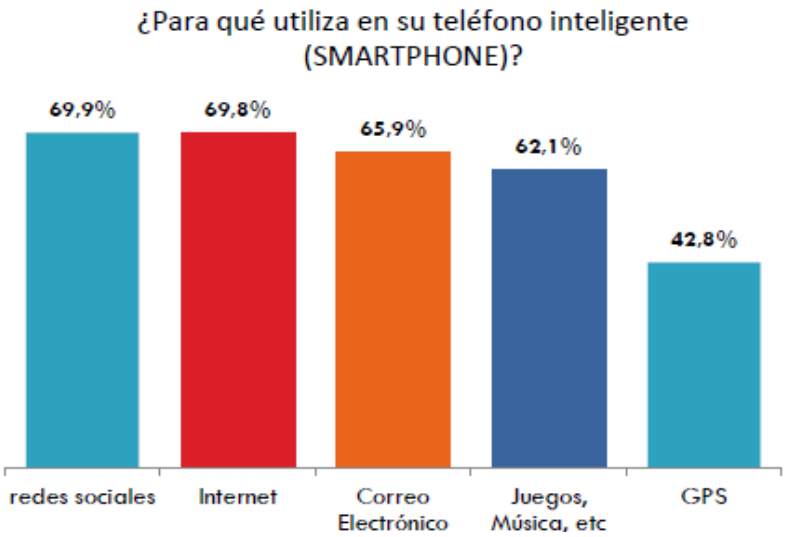


Figura 4. 1 Ficha de observación1

http://www.inec.gob.ec/sitio_tics/presentacion.pdf

Mediante los estudios de INEC (Instituto Nacional de Estadística y Censos) sobre el uso de los Smartphone, con el grafico obtenido podemos darnos cuenta que la mayoría de personas usan el Smartphone para acceder a redes sociales, internet o correo electrónico en donde tenemos nuestros datos y cuentas personales.

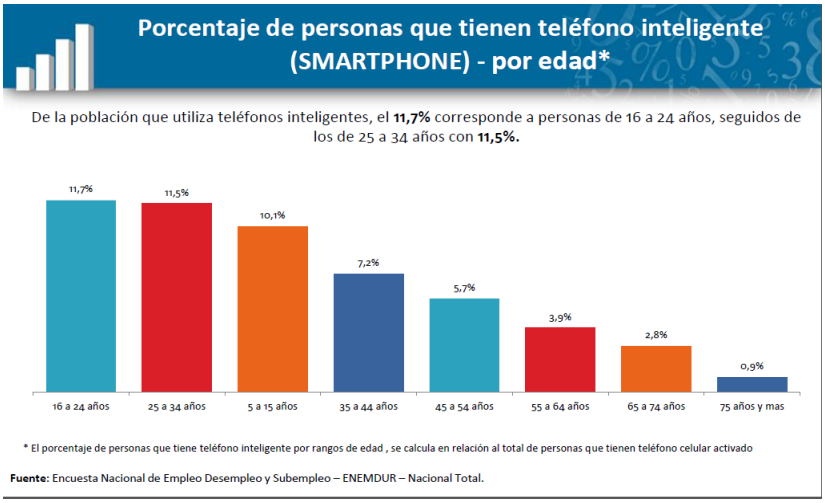


Figura 4. 2 Ficha de observación1

http://www.inec.gob.ec/sitio_tics/presentacion.pdf

Con los datos que proporciona INEC sobre las personas que tienen los Smartphone diferenciando por edades, podemos ver que todos tienen y usan el

celular sin importar la diferencia de edades.

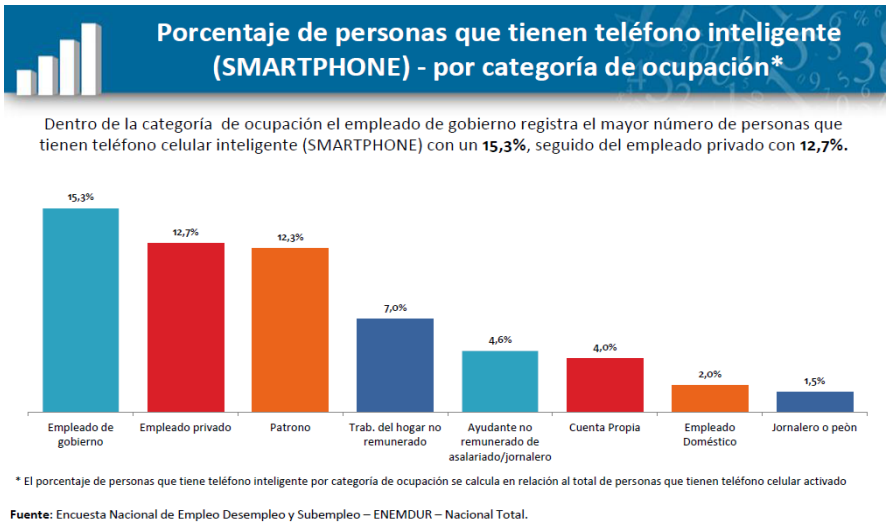


Figura 4. 3 Ficha de observación1
http://www.inec.gob.ec/sitio_tics/presentacion.pdf

Con el grafico podemos darnos cuenta que la mayoría de personas que usan el Smartphone están trabajando

4.2 Interpretación de Resultados

Tomando en base a la ficha de observación se ha podido determinar el incremento del uso de los Smartphone y la falta de conocimiento sobre el análisis forense en los dispositivos móviles, además con el incremento de los delitos informáticos se requiere hacer un manual para mejorar el uso de las aplicaciones de análisis forense en la ciudad de Ambato.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Los datos proporcionado por la INEC nos muestra que hubo un gran incremento en el uso de los Smartphone.

- En la ficha de observación se pudo notar que la mayoría de personas no conocen sobre el concepto de análisis forense.

- No todas las personas que usen el Smartphone saben del análisis forense y tampoco ha usado aplicaciones de ese tipo.

- Según los estudios de INEC nos muestra que la mayoría de personas usan el Smartphone para acceder a las redes sociales y el uso del internet

5.2 RECOMENDACIONES

- En la actualidad los delitos informáticos cada vez se hace más comunes, ya que conforme avanza la tecnología, también lo hacen en la forma de cometer delitos informáticos y se recomienda estar al día con los conocimientos tecnológicos para que no seamos victimas de dichos delitos

- Se recomienda saber sobre la seguridad que tiene el Smartphone para que los datos personales estén seguros.

- Se recomienda usar las aplicaciones forenses para dispositivos móviles mediante un manual para que podamos mejorar el Análisis forense en dispositivos móviles.

CAPÍTULO VI

PROPUESTA

6.1.Datos Informativos

- **Titulo**

"Estudio Y Evaluación De Aplicaciones Para El Análisis Forense De Dispositivos Móviles Bajo Android En La Ciudad De Ambato"

- **Institución ejecutora**

Ciudad de Ambato

- **Director de Tesis**

Ing. Luis Solis

- **Beneficiario**

Ciudadanos de la ciudad de Ambato

- **Ubicación**

Ambato, Provincia de Tungurahua

- **Tiempo estimado para la ejecución**

  - **Fecha de inicio:** Enero de 2012
  - **Fecha de Finalización:** Julio de 2012

- **Equipo técnico responsable**

  - **Investigador:** Li Yu Lung

6.2 Justificación

En la actualidad, la mayoría de personas posee un teléfono celular sea para uso personal o laboral, tanto fue la acogida que se ha convertido en una herramienta indispensable para las personas. por tal motivo desde hace aproximadamente diez años, el empleo o el uso de dispositivos móviles se ha incrementado notablemente por las facilidades que brinda para poder mantenerse en contacto con las personas que desea y otros servicios más.

pero algo que debemos tomar en cuenta que mientras haya más servicios que nos facilita las cosas pero de igual forma va incrementado el peligro, es decir al

proporcionar tantas facilidades también proporciona más facilidades para cometer algún delito o crimen, por tal motivo aparece el termino de **Análisis Forense** el cual sirve para poder detectar y recolectar toda información necesario para documentarla y llevar a la corte.

6.3 Objetivos de la Propuesta

6.3.1 Objetivo General

Determinar la aplicación más adecuada para mejorar el análisis forense de los dispositivos móviles bajo Android

6.3.2 Objetivos Específicos

- Definir las aplicaciones a usar en el análisis forense de los dispositivos móviles bajo Android
- Seguir los procesos existentes para poder realizar el análisis forense a los dispositivos móviles.
- Realizar un manual para mejorar el análisis forense a los dispositivos móviles bajo Android.

6.4 Análisis de Factibilidad

6.4.1. Factibilidad Política

Garantizar la seguridad de los datos e información que fluyen dentro de los dispositivos móviles.

6.4.2. Factibilidad Socio Cultural

El análisis forense ayuda a la integridad de los datos e información de todos los usuarios que usan dispositivos móviles .

6.4.3. Factibilidad Tecnológica

En aspectos tecnológicos es factible porque si se puede encontrar información referentes al tema.

6.4.4. Factibilidad Equidad de Género

El análisis forense a los dispositivos móviles se puede aplicar para todas las personas, sin discriminar el género.

6.4.5. Factibilidad Ambiental

El desarrollo del proyecto no afectará al medio ambiente en ningún sentido.

6.4.6. Factibilidad Económica Financiera

El proyecto de investigación en el ámbito económico es factible de realizarlo; porque también se puede emplear herramientas de software libre.

6.4.7. Factibilidad Operativa

Con el Análisis forense, se puede recuperar y extraer las informaciones existentes el cual es una ayuda a todos los usuarios que tengo un dispositivo móvil.

6.4.8. Factibilidad Legal

El desarrollo del proyecto no infringe ninguna ley o norma establecida a nivel local, ni estatal.

6.5 Fundamentación Teórica

6.5.1 Qué es Análisis Forense

"Es la técnica de capturar, procesar e investigar información procedente de sistemas informáticos utilizando una metodología con el fin de que pueda ser utilizada en la justicia".

El análisis forense de sistemas tiene como objetivo averiguar lo ocurrido durante un incidente de seguridad. Buscamos dar respuesta a los interrogantes que normalmente envuelven a todo incidente: quién es el origen del problema, qué activos de información se vieron afectados y en qué grado, cuándo tuvo lugar, dónde se originó y contra qué objetivos se dirigió, cómo fue llevado a cabo y por qué.

Es decir que son técnicas o métodos que se aplican, para poder dar una respuesta o

evidencia del cómo se realizó el delito, que hicieron, y que puede pasar o qué efecto puede haber después del incidente para luego documentarlos y presentar dicha información cómo evidencia para la corté

La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas que luego serán analizadas para recobrar los registros y mensajes de datos existentes dentro de un equipo informático, y si es necesario reconstruir los mismos con la finalidad de obtener información digital que pueda servir como prueba en un proceso judicial.

Existen modos de Análisis para la Informática Forense, estos son:

• Análisis post-mortem: se realiza con un equipo dedicado específicamente para fines forenses para examinar discos duros, datos o cualquier tipo de información recabada de un sistema que ha sufrido un incidente. En este caso, las herramientas de las que se puede disponer son aquellas que existan en el laboratorio destinado al análisis de discos duros, archivos de logs de firewalls, etc.

• Análisis en caliente: se lleva a cabo cuando un sistema presume que ha sufrido un incidente o está sufriendo un incidente de seguridad. En este caso, se debe emplear un CD con las herramientas de Respuesta ante Incidentes y Análisis Forense compiladas de forma que no realicen modificaciones en el sistema. Una vez hecho este análisis en caliente, y confirmado el incidente, se realiza el análisispost-mortem.

La Informática Forense es la ciencia de: **identificación preservación, recolección, análisis, presentación.**

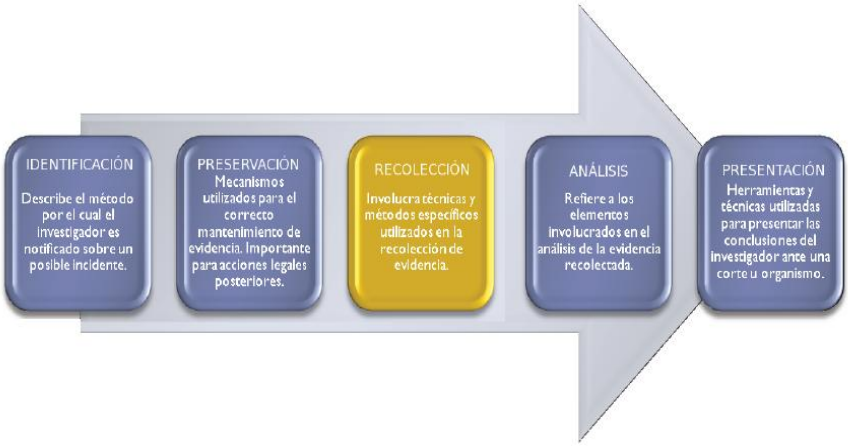


Figura 6. 1 Procesos de la informática forense

- **Identificación:** Se trata de identificar si hubo algún tipo de ataque, si en caso de haber existido algún ataque también debe identificar la forma y el método como se realizó el ataque, aparte de eso también identificar las evidencias o los rastros que existen para poder proseguir con el siguiente paso que es la preservación.
- **preservación:** Es la protección necesaria que se le da a los dispositivos o medios de almacenamiento para luego poder sacar la información.
- **Recolección:** Aquí es donde empezamos a recolectar la información a través del análisis forense puede ser a través de software o hardware para poder extraer toda información que haya para su posterior uso.
- **Análisis:** Es el análisis que se le da a la documentación recolectada validando que cual de todos los documentos o datos es útil para luego poder sacar reportes y su presentación.
- **Presentación:** Es la fase final en la cual se presenta el documento recopilado

y resumido de la documentación de los pasos anteriores.

Metodología Básica de Análisis Forense

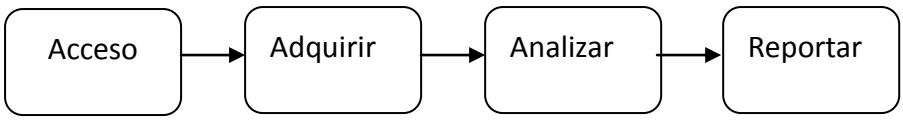


Figura 6. 2 Metodología básica de análisis forense

- **Acceso:** El primer paso que hay que hacer es pedir la autorización para que de esta forma no se vaya en contra de las políticas y leyes, luego de tener la autorización empezamos a evaluar cuales son los datos principales a extraer
- **Adquirir:** aquí empieza la investigación y el acceso a los datos para poder extraerlos y almacenarlos.
- **Analizar:** se trata de analizar toda la información recopilada dependiendo el tipo de datos el análisis es diferente como archivos que se envía a través de la red, videos, mensajes.
- **Reportar:** Aquí se organiza toda la información que se analizo y evaluó para poder presentar.

Aspectos útiles de una investigación Forense

- El método utilizado por el atacante para introducirse en el sistema
- Las actividades ilícitas realizadas por el intruso en el sistema.
- El alcance y las implicaciones de dichas actividades.
- Las "puertas traseras" (backdoors) instaladas por el intruso.

- Otras actividades realizadas por el sistema.

Preguntas Fundamentales de un análisis forense

- ¿En qué momento exacto se ha producido el daño?
- ¿Quien ha sido el sujeto que ha realizado la acción?
- ¿Qué metodología o técnica se ha utilizado para ello?
- ¿Qué daños y modificaciones ha producido en el sistema?

Dispositivos a analizar

La infraestructura informática que puede ser analizada puede ser toda aquella que tenga una Memoria (informática), por lo que se pueden analizar los siguientes dispositivos:

- Disco duro de una Computadora o Servidor
- Teléfono Móvil o Celular, parte de la telefonía celular
- Agendas Electrónicas (PDA)
- Dispositivos de GPS
- Impresoras
- Memorias USB

6.5.2 Computación Anti Forense

Es un término para describir las técnicas que se utilizan para contrarrestar el análisis forense.

La computación anti forense es un conjunto de métodos de levantamiento de evidencias con el objetivo de debilitar los resultados de la computación forense,

utilizando ciertas herramientas con las cuales se obtiene información confiable para crear insolvencias en la evidencia y el proceso forense.

Clasificación De Métodos Anti-Forenses

A medida que se explora y se investiga más sobre las técnicas anti-forenses se han generado varias clasificaciones y del mismo modo se han definido varios métodos. Para efectos de este trabajo se tomará la clasificación planteada por (Harris 2006)

- Destrucción de la evidencia.
- Ocultar la evidencia.
- Eliminación de las fuentes de la evidencia.
- Falsificación de la evidencia.

Existen dos niveles de destrucción de la evidencia:

- Nivel Físico: A través de campos magnéticos.
- Nivel Lógico: Busca reinicializar el medio, cambiar la composición de los datos, sobrescribir los datos o eliminar la referencia a los datos.

6.5.3 Evidencia Digital

De acuerdo con el HB:171 2003 Guidelines for the Management of IT evidence, la evidencia digital es: "cualquier información, que sujeta a una informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".

La evidencia computacional es única, cuando se la compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original.

Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia.

Categorías de la Evidencia Digital

1. Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos de aplicaciones de ofimática, imágenes, videos, Audio... etc.)

2. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).

3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

Procesos de la Evidencia Digital.

- diseño de la evidencia
- Generación de la evidencia

- Recolección de la evidencia
- Análisis de la evidencia
- Reporte y presentación
- Determinar la relevancia de la evidencia

Condiciones para considerar los documento como evidencia digital.

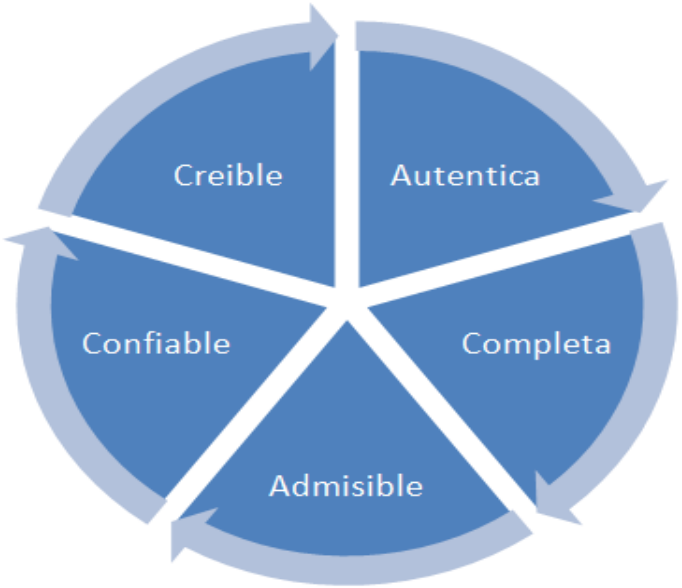


Figura 6. 3 Condiciones de la Evidencia

Información que se puede realizar el análisis forense

- -Mensajes
- -Agendas
- -Llamadas entrantes y salientes
- -Contraseñas, Pin
- -Sitios web visitados
- -Correos
- -Chats

6.6 Manual para análisis forense de los dispositivos móviles

6.6.1 Objetivos del Manual

General:

- Mejorar el análisis forense de los dispositivos móviles mediante la utilización de las aplicaciones forenses.

Específicos :

- Proporcionar los pasos necesarios para poder utilizar y manejar las aplicaciones de análisis forenses

- Identificar los procesos para realizar el análisis forense en los dispositivos móviles.

6.6.2 Alcance del Manual

El manual tendrá como principales componentes los pasos para la conexión de los Smartphone con las aplicaciones y la utilización de los programas forenses para mejorar y facilitar el proceso de análisis forense de los dispositivos móviles.

Son herramientas utilizadas en el ámbito de la informática forense para la recuperación de los datos borrados o recolección de evidencia digital como.

6.6.3 BitPim

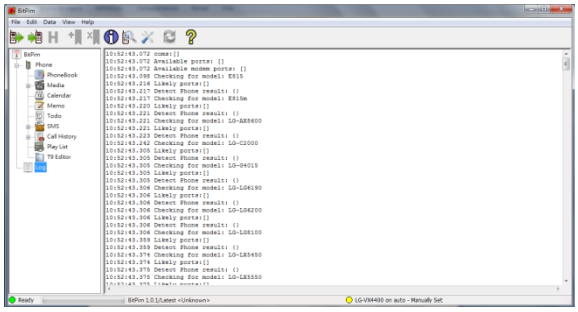


Figura 6. 4 Bitpim1

Es un código abierto programa diseñado para administrar el contenido de CDMA dispositivos. La mayoría de los teléfonos móviles con un Qualcomm CDMA fabricado chips son compatibles. El programa también es multi-plataforma , que opera en el Microsoft Windows , Mac OS X y Linux sistemas operativos.

Aunque BitPim puede ser tomado por un administrador de información personal (PIM) , su nombre deriva de "bitpym", una sugerencia generada por un generador de pronouncable-password , la "y" se sustituye por una "i", simplemente para eliminar la ambigüedad en la pronunciación. Anteriormente, el programa había sido nombrado "Entrocul" por el mismo método.

Características

Funciones varían según el modelo del dispositivo. Las siguientes funciones de gestión son compatibles actualmente con BitPim:

- Guía telefónica
- Calendario
- Fondos de pantalla
- Ringtones
- Sistema de archivos
- Medios de comunicación
- Memorándum

- Todo
- Historial de llamadas
- SMS
- T9 editor

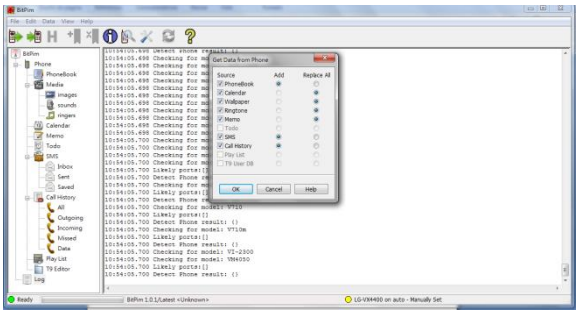


Figura 6. 5 Bitpim2

Los datos pueden ser importados y exportados desde diversas fuentes, tales como Microsoft Outlook y Google Calendar .

6.6.4 Device Seizure

Figura 6. 6 Device Seizure

Es una herramienta forense de mano que permite la recuperación de datos eliminados, volcados de datos completas de ciertos modelos de teléfonos celulares,

las adquisiciones lógicas y físicas de PDA, acceso a datos por el cable, e informes avanzados. La cantidad y calidad de los datos que puede obtener de una adquisición física completa sobrepasa la información que puede obtener de una adquisición de lógica simple. Incautación dispositivo no cambia los datos en el dispositivo.

Marcas apoyados por fabricantes de teléfonos celulares

- LG
- Motorola - incluyendo iDen
- Nokia
- Siemens
- Samsung
- Sony-Ericsson

Incautación paraben dispositivo compatible con PDAs con los siguientes sistemas operativos:

- Palm handhelds a 5.4
- Windows CE / Pocket PC / Mobile 5.0 y anteriores
- BlackBerry 4.xy versiones anteriores
- Symbian 6.0, 6.1, 7.x, 8.x, y 9.X
- EPOC 16/32 (dispositivos Psion)

Incautación paraben dispositivo compatible con tarjetas SIM GSM con el uso de un lector de tarjetas SIM (que se encuentra en Herramientas de dispositivo convulsiones).

Incautación paraben dispositivo también es compatible con los siguientes tipos de dispositivos GPS con más fabricantes a seguir:

- Garmin

Proceso para conectar el dispositivo

Conectar Dispositivo

Figura 6. 7 Datos de adquisicion (Seizure)

Iniciamos la aplicacion Device Seizure y nos mostrara una ventana de bienvenida para empesar a crear un caso forense con respecto al dispositivo que se va a analizar para ello pulsaremos el boton de **Data Acquisition** para poder empezar el proceso de analisis forense.

Figura 6. 8 Asistente para la conexion al dispositivo (Seizure)

Despues de dar clic en la adquisicion de datos se abrira una ventana que explica del proceso que se va a realizar y que las acciones lo que se vaya a hacer lo haga con precauchion.

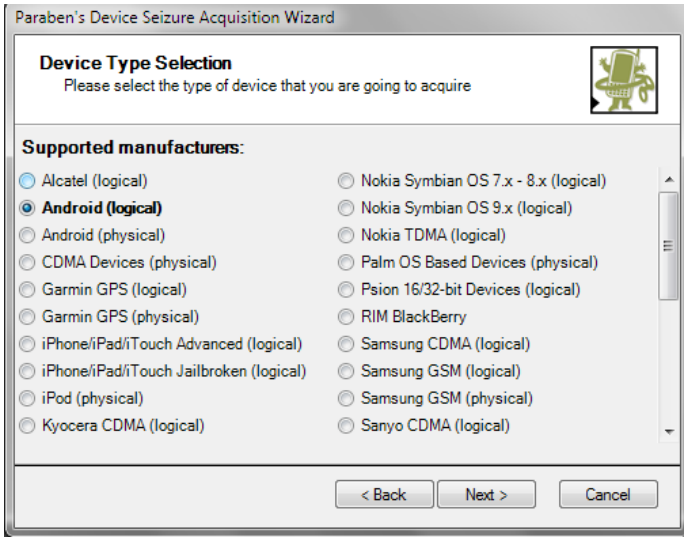


Figura 6. 9 Seleccion del tipo de dispositivo (Seizure)

Ahora habra que seleccionar el tipo de dispositivo que tenemos por tal motivo escogeremos la opcion **Android(logical)** ya que el dispositivo que se va a analizar

es del tipo android, cada opcion que aparece en la ventana se puede definir como los tipos de accesos al dispositivo movil si en caso de no escoger la opcion correcta la aplicacion no podra detectar el dispositivo hasta que la seleccion sea la correcta.

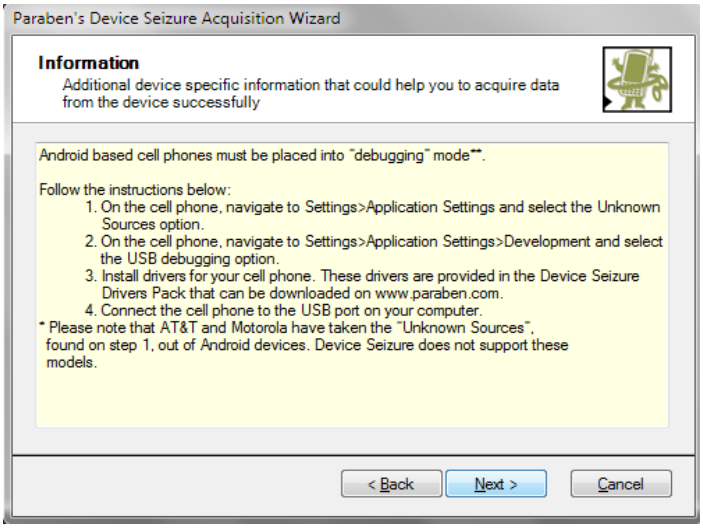


Figura 6. 10 Informacion especifica para la adquisicion del dato (Seizure)

Luego de seleccionar el tipo de dispositivo empezara a establecer la conexión al dispositivo, pero para poder establecer coneccion primero se debe instalar los controladores del dispositivo y tambien los controladores para el puerto usb porque sino no se podra conectarse, luego tenemos que activar la opcion **Usb debugging,** para esto podemos ir al dispositivo MENU -> configuraciones -> Aplicaciones -> Desarrollo -> USB debugging, después de activar la opción debugging podemos pulsar **Next** para ir al siguiente paso.

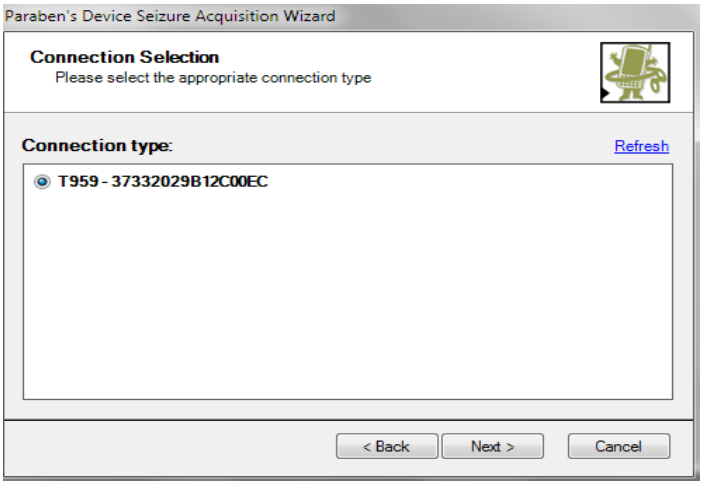


Figura 6. 11 Seleccion de conexión (Seizure)

Ahora se define el tipo de conexión que se va a utilizar para conectar con el dispositivo, en nuestro caso es por el cable USB, hay que tomar en cuenta que si no se instalo correctamente los controladores mencionados anteriormente en la ventana no aparecerá ningún tipo de conexión ya que no puede identificar el dispositivo, pero si está instalado correctamente aparecerá la conexión y podrá seguir al siguiente paso.

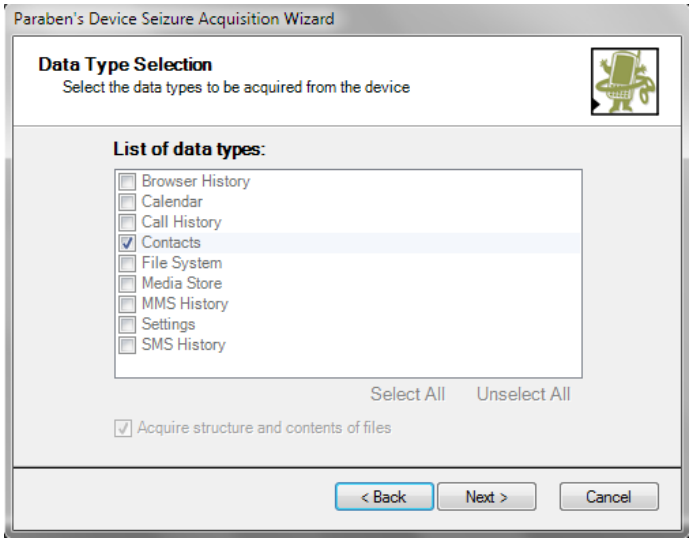


Figura 6. 12 Datos a extraer (Seizure)

Luego de escoger el tipo de conexión hay que escoger los datos que se va a extraer como lo vemos en la figura 6. 12, por tal motivo solo habrá que activar las opciones para extraer los datos.

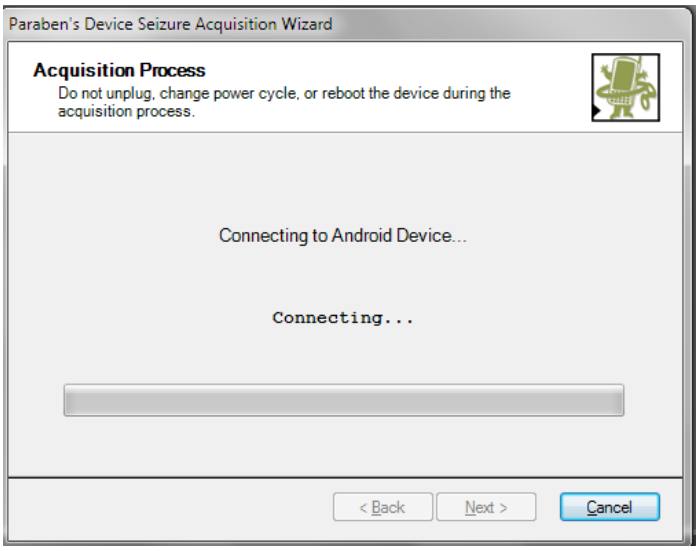


Figura 6. 13 Conexion con el dispositivo (Seizure)

Luego de seleccionar todas las opciones que se menciona anteriormente la aplicación empezara a establecer la conexión con el dispositivo para poder empezar a extraer los datos que se selecciono.

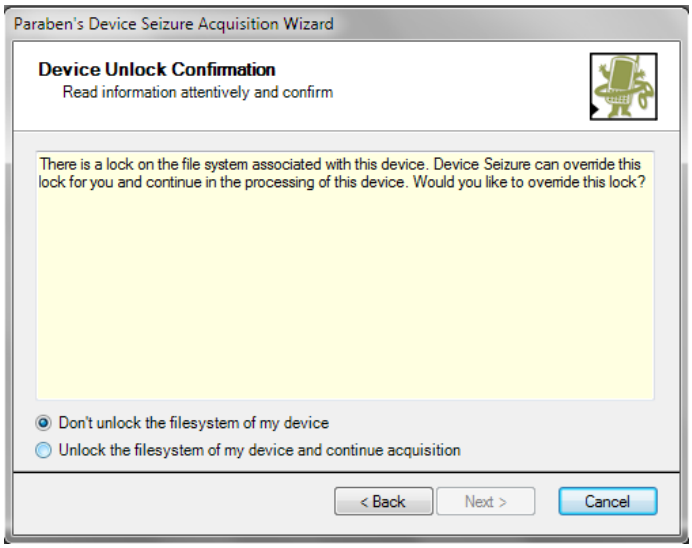


Figura 6. 14 Confirmacion de desbloqueo (Seizure)

Un punto importante es que la aplicación pide la confirmación para poder desbloquear el dispositivo que podemos decir como tener el permiso de root para poder acceder a las carpetas y poder extraer la información deseado.

Figura 6. 15 Extracion de datos (Seizure)

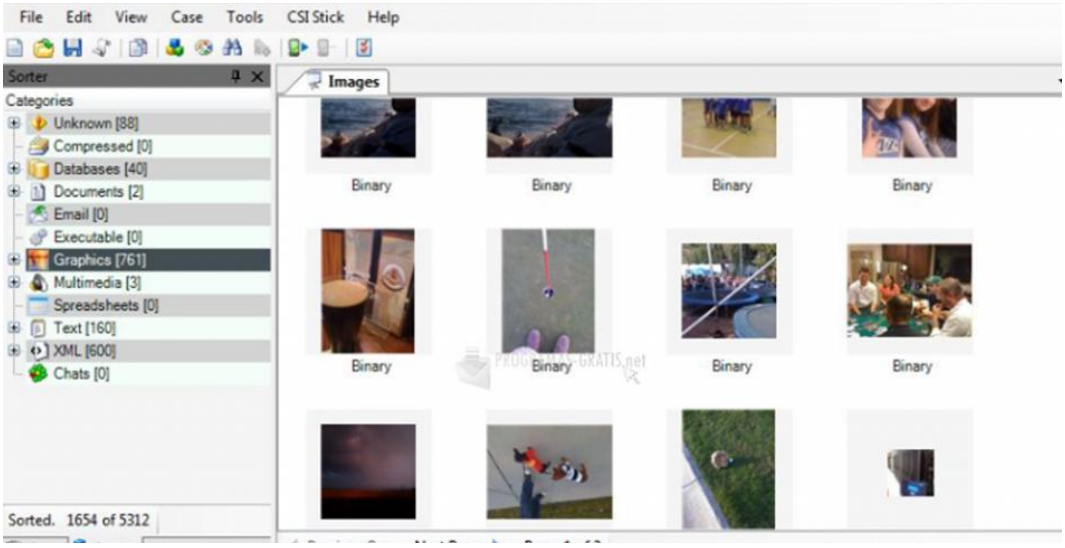


Figura 6. 16 Extracion de datos2 (Seizure)

Luego de extraer los datos podremos ver las carpetas con los datos como el calendario, categorias ..etc.

Despues de la extracion de datos se podra empezar con el estudio y analisis de toda la informacion extraido para finalmente poder validar cuales son los datos utiles y podra organizar la documentacion y presentarla.

6.6.5 Oxygen forensic suite

Figura 6. 17 Oxygen1

Es una aplicación o un software forense que sirve para realizar el análisis lógico de los teléfonos celulares , teléfonos inteligentes y PDAs desarrollado por Oxygen Software . La suite puede extraer información del dispositivo, los contactos, eventos del calendario, SMS mensajes, registros de eventos, y los archivos. Además, el vendedor afirma la suite puede extraer metadatos relacionados con los anteriores. A partir de septiembre de 2011, la suite de apoyo a más de 2300 dispositivos, incluyendo Nokia , Apple iPhone series, Apple iPod Touch , iPad Vertu, Sony Ericsson , Samsung, Motorola, Blackberry , Panasonic, Siemens, HTC, HP, E-Ten, Gigabyte , i-Mate y otros teléfonos móviles. El programa también soporta dispositivos con Symbian OS , Windows Mobile 6.5 y los dispositivos Android OS

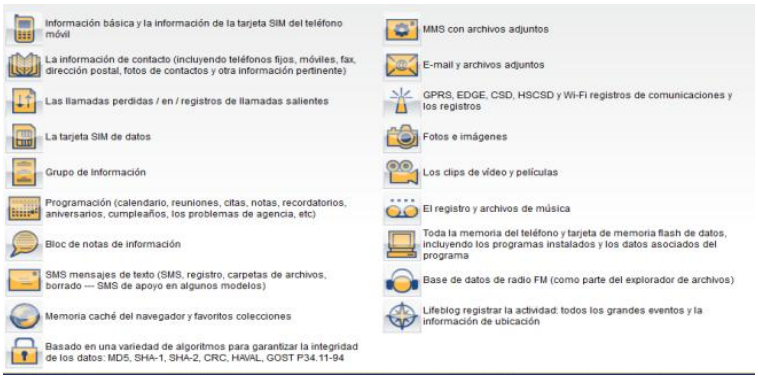


Figura 6. 18 Items del Programa Oxygen

Proceso para conectar el dispositivo

Conectar el dispositivo

damos clic en el boto de conectar a un dispositivo nuevo para poder empezar a identificar el dispositivo a analizar.

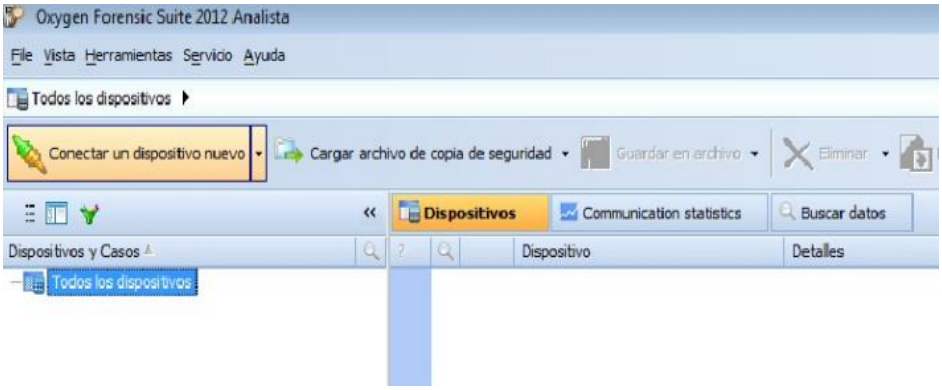


Figura 6. 19 Conexión a un nuevo dispositivo móvil (Oxygen)

Luego nos aparecerá una ventana de bienvenida y le damos clic en siguiente para poder entrar al asistente de conexión con el dispositivo móvil.

Figura 6. 20 Asistente de conexión al dispositivo (Oxygen)

Tipos de conexión

Aquí podremos ver qué tipo de conexión tiene nuestro dispositivo móvil de Android.

- **Cable:** es la conexión con un cable físico, y se necesita la instalación del cable (si fuera necesario).

- **Bluetooth:** sirve para los dispositivos que tenga bluetooth tanto para el equipo analizador y el dispositivo a analizar
- **Infrarrojo:** es para los dispositivos que tenga el hardware para Infrarrojo.

Figura 6. 21 Tipos de conexión (Oxygen)

Luego de conocer los tipos de conexión podremos seguir con la instalación de la aplicación en el dispositivo para que a través de ella se pueda acceder a los datos del dispositivo móvil.

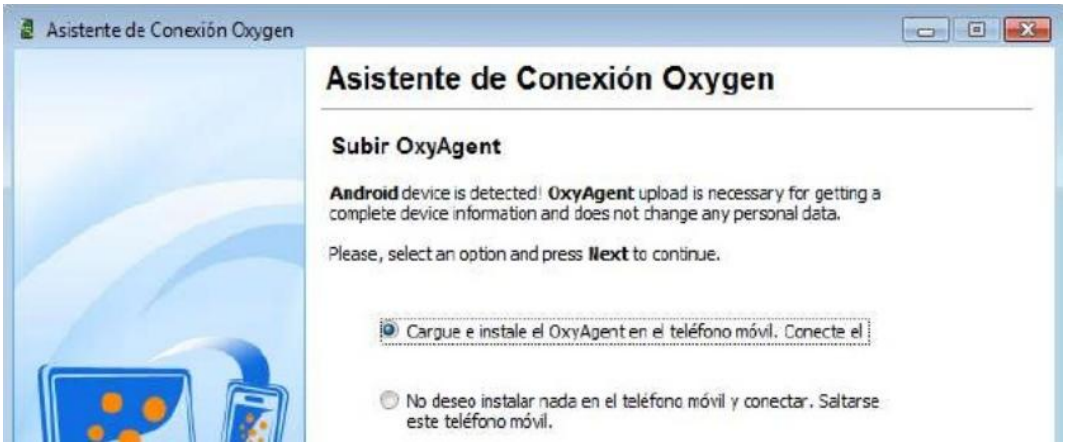


Figura 6. 22 Detección del dispositivo (Oxigen)

Nota: Antes tenemos que tener activado la opción **depuración USB** para que

pueda reconocer el dispositivo móvil y tener espacios en la misma.

Figura 6. 23 Identificación del dispositivo (Oxygen)

En el instante de establecer conexión con el dispositivo móvil también lo da un ide para identificar el celular dentro del programa.

Figura 6. 24 Conexión al dispositivo (Oxygen)

Después de tener identificado el celular y asignado el identificador del dispositivo móvil, la aplicación procederá a crear el número de caso (forense) y receptar los

comentarios que tienen con respecto al caso que se va a crear.

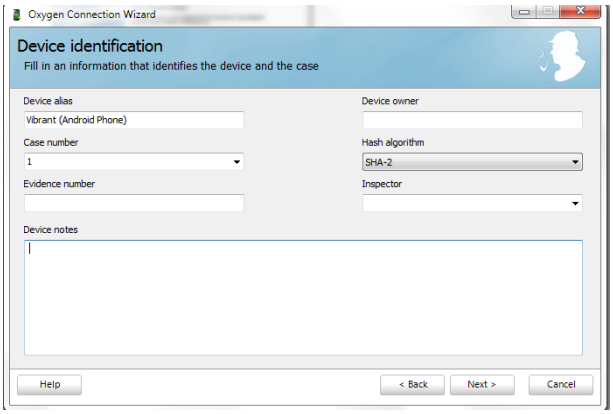


Figura 6. 25 Asignación del número de caso (Oxygen)

Antes extraer la información hay que Rootear al dispositivo para que tenga los permisos totales en el celular y pueda acceder a todas las carpetas necesarias asi que para ellos se utiliza la aplicación: GalaxyS_Vibrant_One-Click_Root y a nivel del celular también tienen que activar la opcion usb-debugging del dispositivo (MENU -> configuraciones -> Aplicaciones -> Desarrollo -> USB debugging), luego ejecutamos el T-Mobile Vibrant One-Click Root.exe y le damos clic en el boton “One-Click Root” se rooteara el dispositivo.

Figura 6. 26 Rooteando al dispositivo

Luego de rootear el Dispositivo podemos seguir con el procedimiento de la extracción de la información.

Figura 6. 27 Verificación del rooteo del dispositivo (Oxygen)

Luego de establecer la conexión e identificar el dispositivo empezara a extraer los datos del dispositivo móvil, lo primero que hace es instalar la aplicación en el dispositivo para poder acceder a los datos del celular y después de eso la aplicación generara un archivo .OFB donde se encuentra todos los datos extraídos desde el celular como los: contactos, calendario, eventos, llamadas ..etc.

En la página principal se visualizara un resumen general de las características del dispositivo móvil.

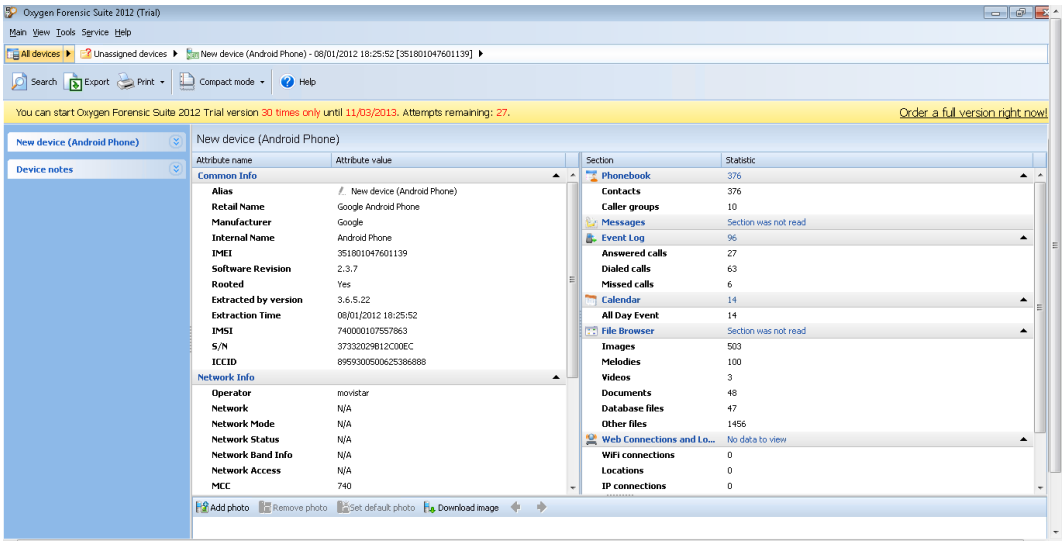


Figura 6. 28 Información general del dispositivo (Oxygen)

Y también tenemos como un tipo de menú de todos los datos que se ha podido extraer del dispositivo móvil donde podemos acceder a los contactos, mensajes llamadas..etc.

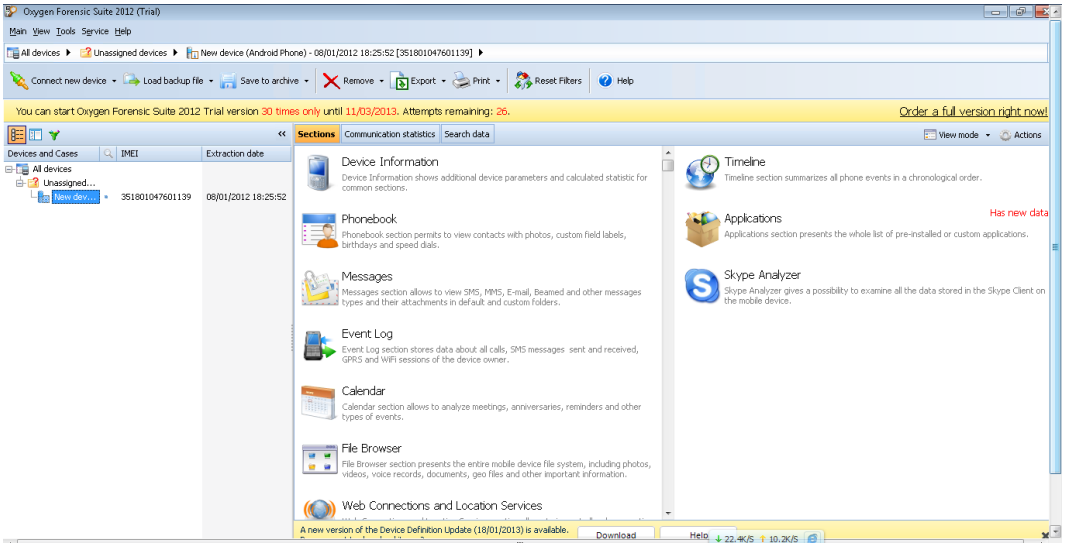


Figura 6. 29 Vista general de la información extraída del dispositivo (Oxygen)

También se puede ir a la pestaña de los contactos para tener una vista general de todos los contactos del dispositivo móvil o incluso podemos posicionar el cursor

en unos de los contactos para poder ver más detalladamente.

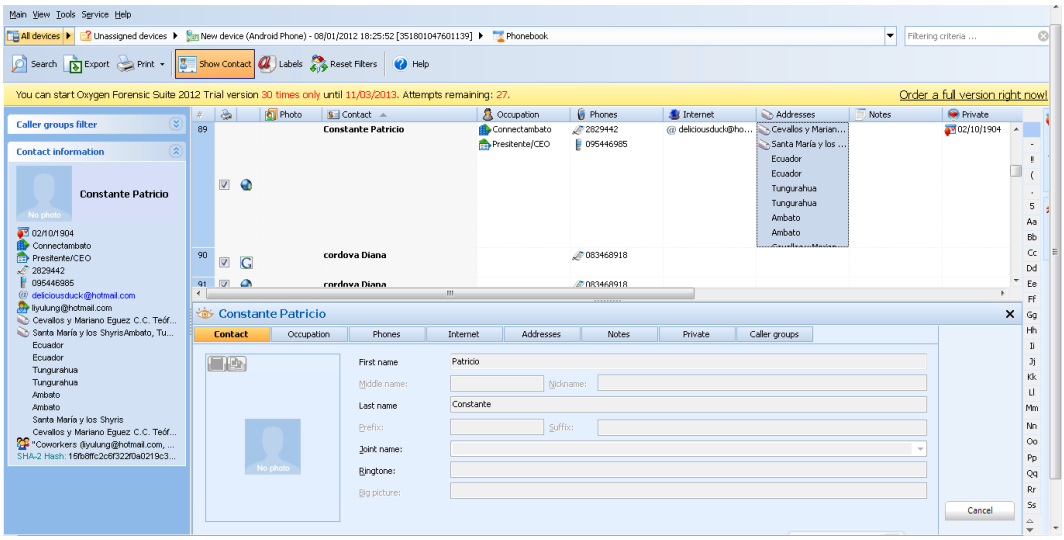


Figura 6. 30 Información extraída - Contactos (Oxygen)

Al dar clic en los eventos de llamadas o el log de llamadas, se visualizara un registro donde esta las llamadas entrantes y salientes incluso la duración de las llamadas también la fecha y la hora de la llamada.

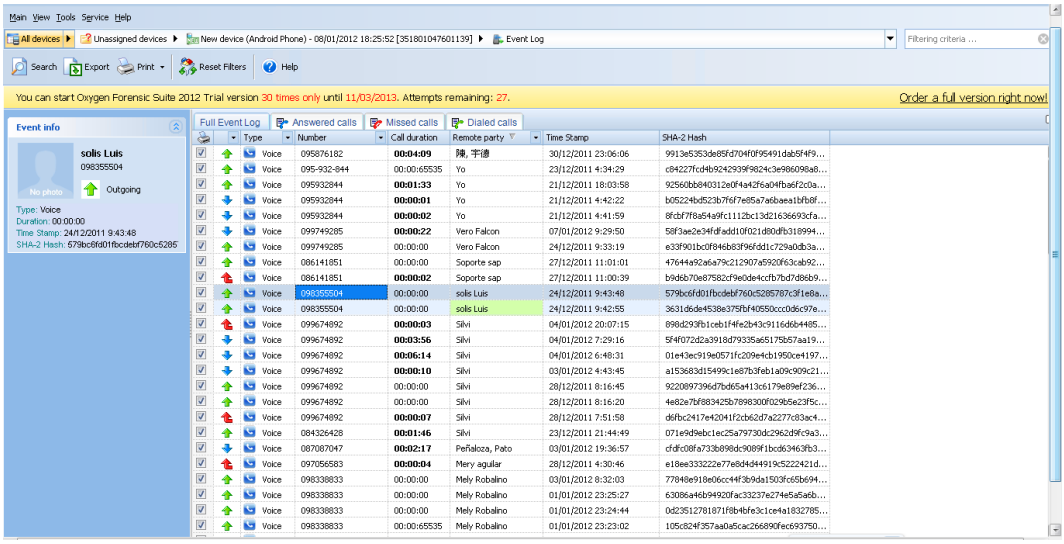


Figura 6. 31 Información extraída - evento de llamadas (Oxygen)

También podemos entrar al calendario del celular donde va se visualizara en los eventos que tiene programado la persona

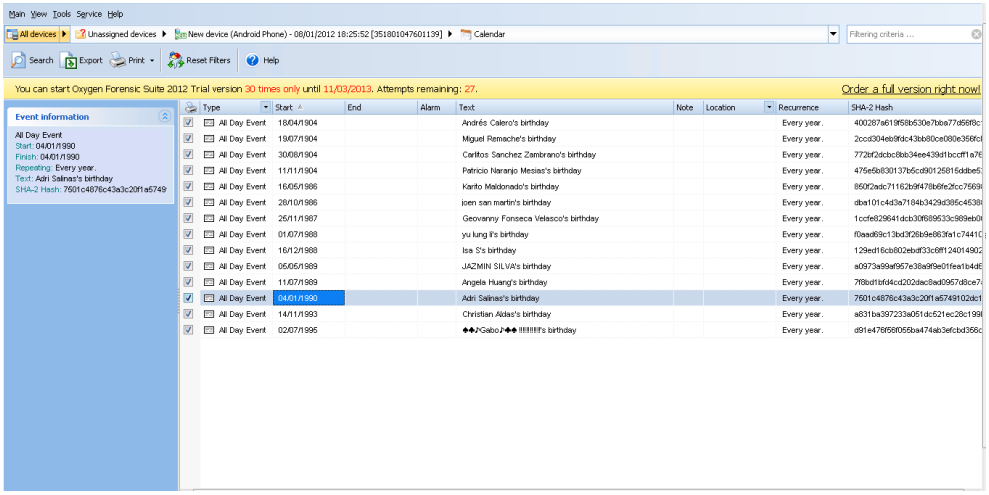


Figura 6. 32 Información extraída - calendario (Oxygen)

Otros de los puntos importantes es que en el programa permite sacar como una copia de la estructura de los archivos del dispositivo movil.

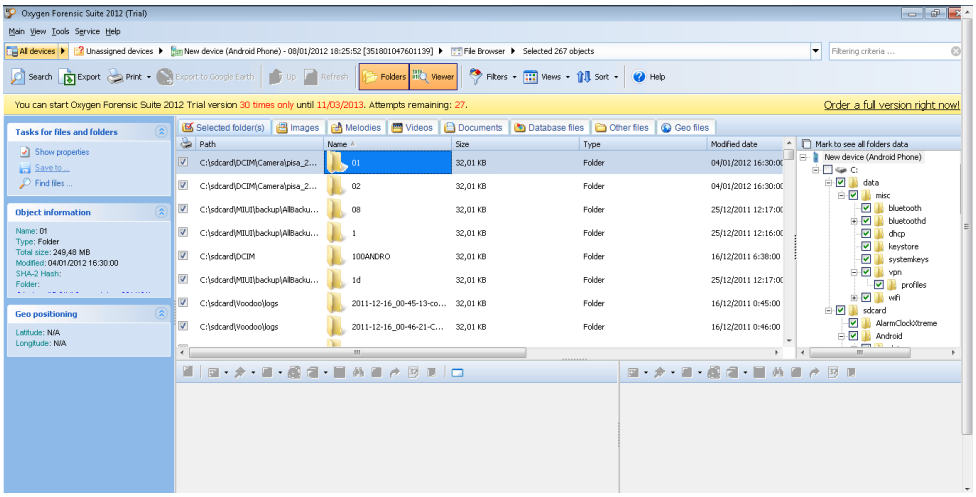


Figura 6. 33 Información extraída - estructura de archivos (Oxygen)

Como podemos ver en la figura 6.33 que se puede navegar por el sistema de

archivo extraído.

También podemos acceder a revisar a las imágenes o videos que tiene el dispositivo móvil, incluso la aplicación permite hacer una visualización previa de las imágenes y los videos existentes, algo que podemos tomar en cuenta es que la aplicación hacer una copia de los archivos y lo guarda dentro del archivo .OFB

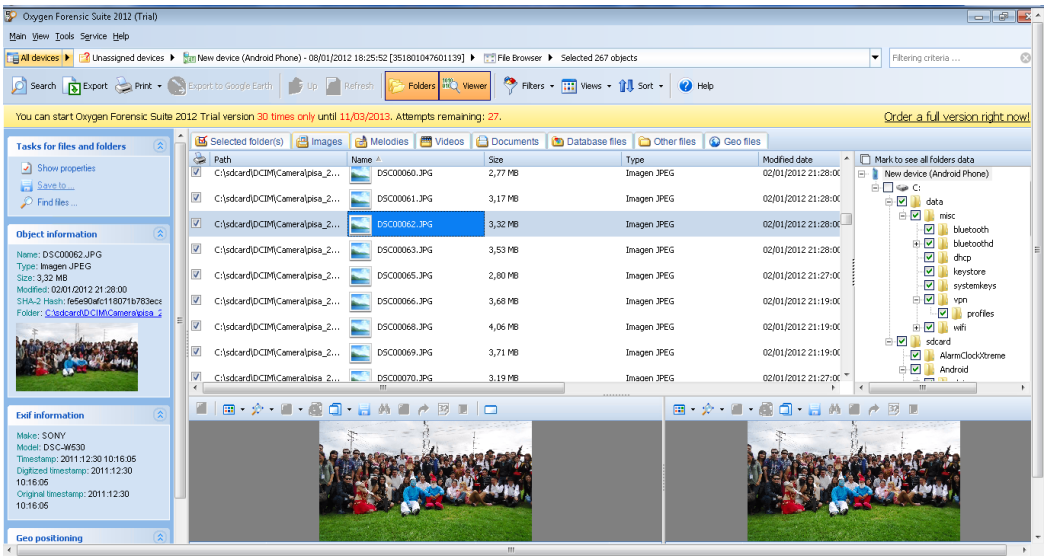


Figura 6. 34 Información extraída - imágenes (Oxygen)

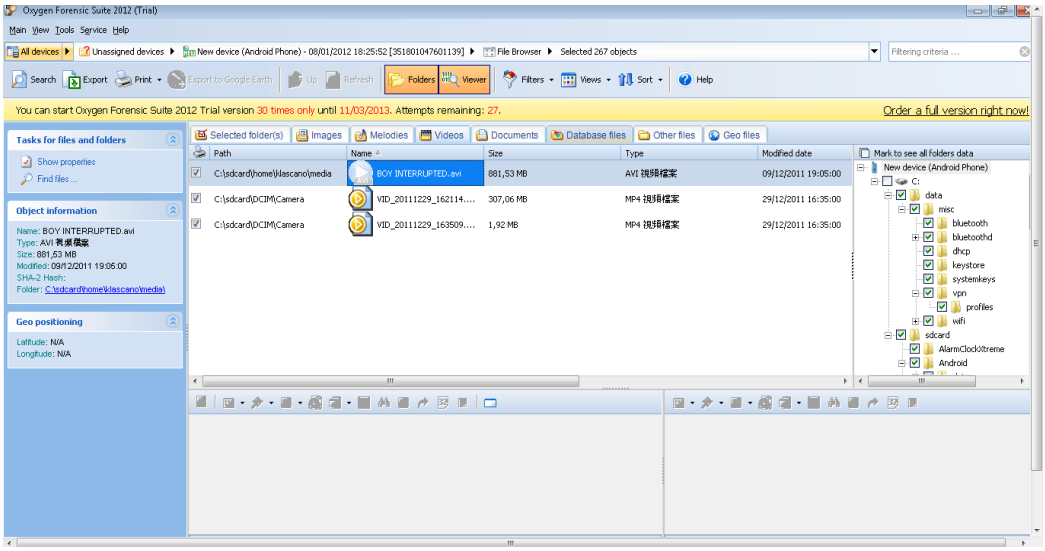


Figura 6. 35 Información extraída - Videos (Oxygen)

También podemos acceder a revisar a las imágenes o videos que tiene el dispositivo móvil, incluso la aplicación permite hacer una visualización previa de las imágenes y los videos existentes, algo que podemos tomar en cuenta es que la aplicación hacer una copia de los archivos y lo guarda dentro del archivo .OFB

La aplicación también hace una copia de los archivos **.DB** los archivos .db podemos definir como la base de datos que usa en sistema de archivos del dispositivo móvil Android el cual puede ser abierto a través de un browser de SQLITE.

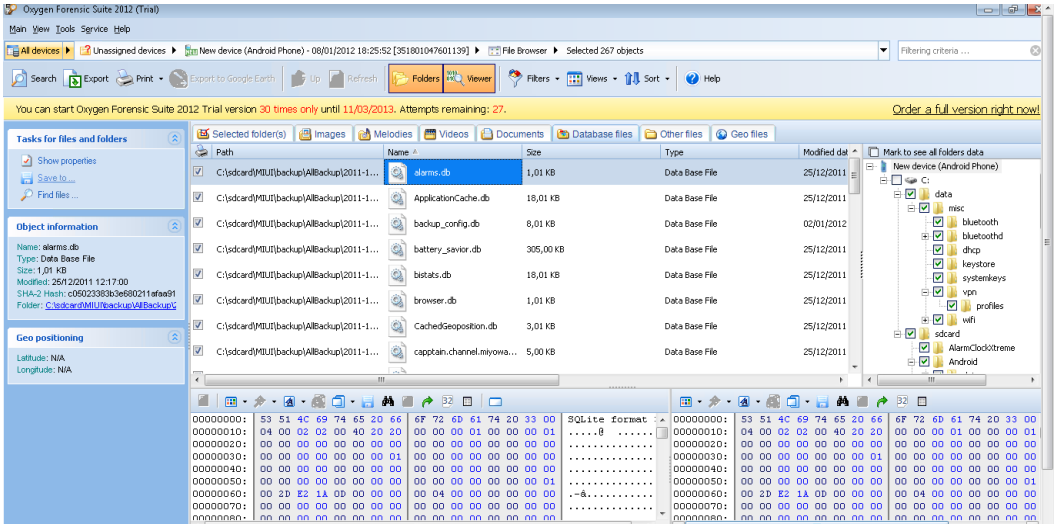


Figura 6. 36 Información extraída - archivos .db (Oxygen)

6.6.6 MOBILedit

Es una herramienta confiable de análisis forense en celulares utilizada en más de 70 países y reconocida por el Instituto Nacional de Estándares y Tecnología página oficial

Permite extraer todo el contenido del teléfono y genera un reporte (en cualquier idioma) listo para su presentación en una audiencia.

Entre sus principales características se puede mencionar:

- ✓ Análisis de teléfonos vía cable USB, Bluetooth e Infrarrojo.
- ✓ Compatibilidad con una gran cantidad de teléfonos.
- ✓ Recuperación de mensajes borrados de tarjetas SIM.
- ✓ Exportación a Word, Excel / XLS, navegador, XML / XSL.

Los datos adquiridos o extraidos desde el dispositivos de telefonía celular están almacenados en el formato de archivo. Med. Después de una exitosa adquisición lógico, los siguientes campos se rellenan con los datos: información de suscriptores, dispositivos específicos, Contactos, Agenda SIM, Llamadas perdida, últimos números marcados, llamadas recibidas, Bandeja de entrada, Elementos enviados, Borradores, carpeta de archivos. Elementos presentes en la carpeta de archivos, que van desde archivos gráficos para cámara de fotos y tonos, dependen de las capacidades del teléfono. Las características adicionales incluyen el servicio myPhoneSafe.com, que proporciona acceso a la base de datos de IMEI para registrar y comprobar para teléfonos robados.

Proceso para conectar el dispositivo

Conectar Dispositivo

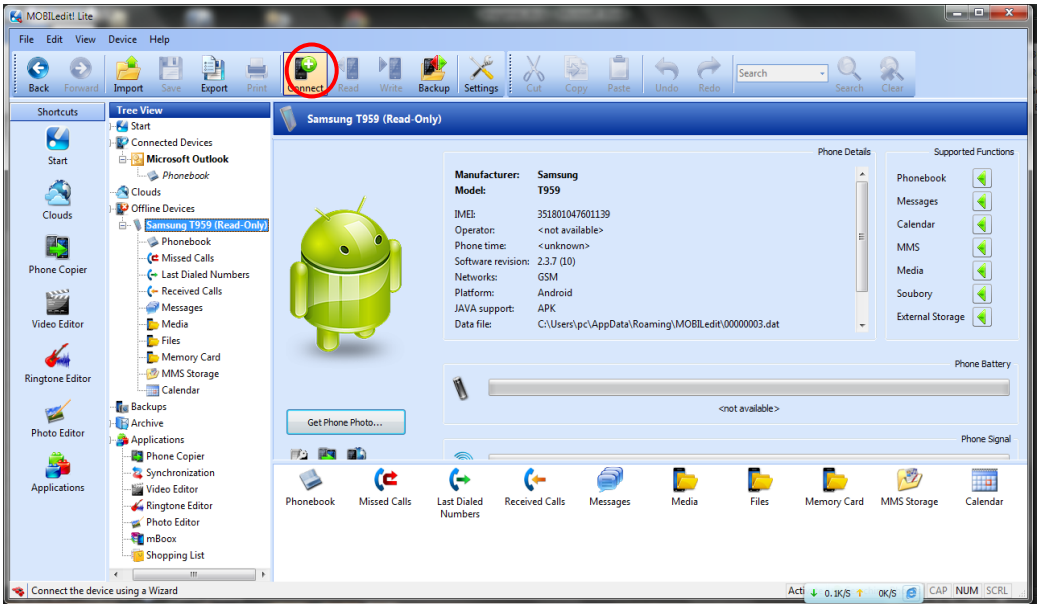


Figura 6. 37 Conectar Dispositivo (MOBILedit)

Para conectar el dispositivo podemos pulsar el botón de **conectar** para empezar con el análisis forense y la correspondiente extracción de los datos del dispositivo móvil.

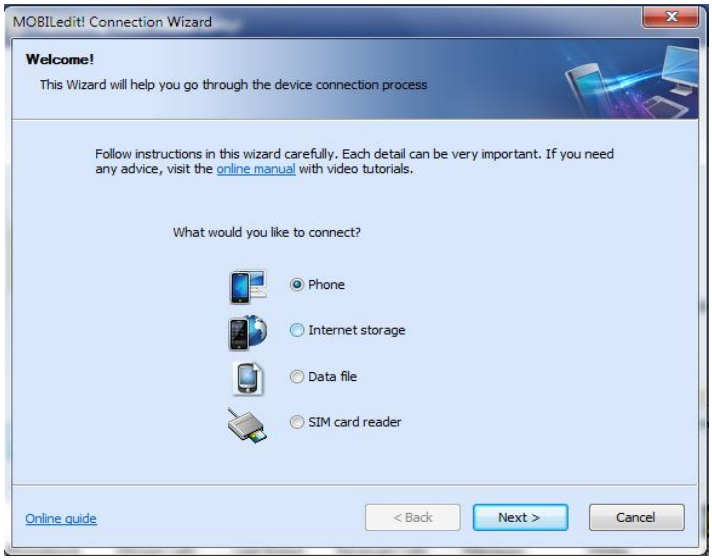


Figura 6. 38 Dispositivo a conectar (MOBILedit)

Aquí escogemos al dispositivo que vamos a analizar, la cual escogeremos la opción teléfono.

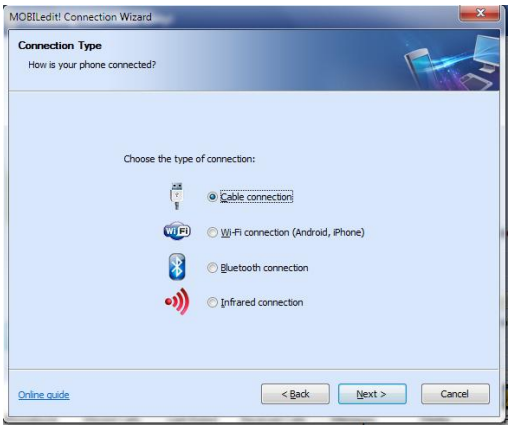


Figura 6. 39 Tipo de conexion (MOBILedit)

Luego de escoger el tipo de dispositivo a analizar tendremos que selecciona el tipo de conexión que tendrá en dispositivo, para MOBILedit puede conectarse de 4 formas: Conexión por Cable, Conexión WIFI, Conexión Bluetooth, Conexión infrarrojo en nuestro caso usaremos la **Conexión por cable**.

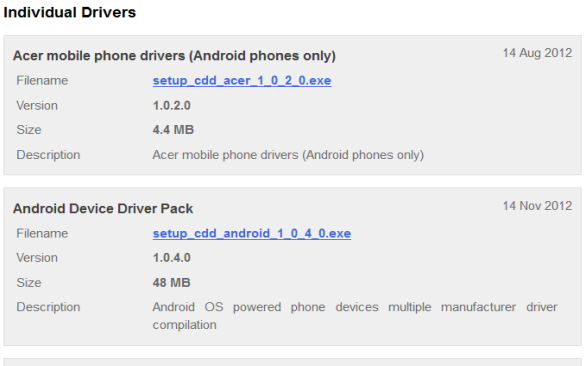


Figura 6. 40 Instalación de los controladores (MOBILedit)

Para que la aplicación pueda reconocer el dispositivo tenemos que instalar el controlador del cable USB y el controlador del dispositivo móvil en la cual podemos encontrarla en la página web de MOBILedit.

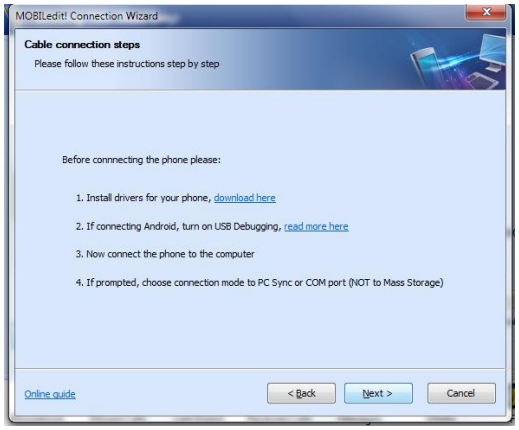


Figura 6. 41 Pasos para la conexión por cable (MOBILedit)

Para que el dispositivo sea detectado tenemos unos pasos que seguir como nos muestra en la figura 6.41 primero tener instalado los controladores del dispositivo móvil luego activar la opción de USB debuggin (MENU -> configuraciones -> Aplicaciones -> Desarrollo -> USB debugging) en el celular luego de activar la opción podemos proceder a conectar el dispositivo en el computador pero no tenemos que conectar el celular como un dispositivo de almacenamiento para que pueda detectar el dispositivo móvil.

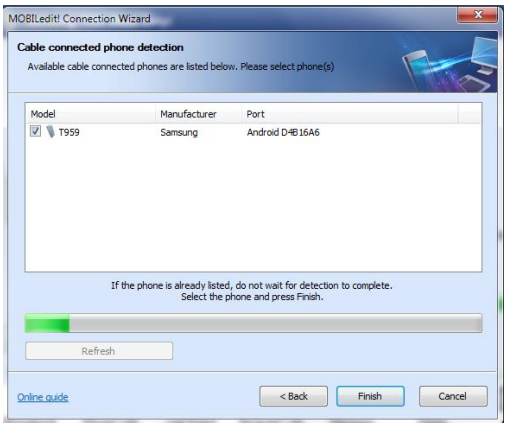


Figura 6. 42 Detectar la conexión (MOBILedit)

Después de realizar los pasos para la conexión la aplicación podrá detectar el dispositivo que se va a analizar cómo se visualiza en la figura 6. 42. que ya tiene

identificado el dispositivo y el modelo del celular.

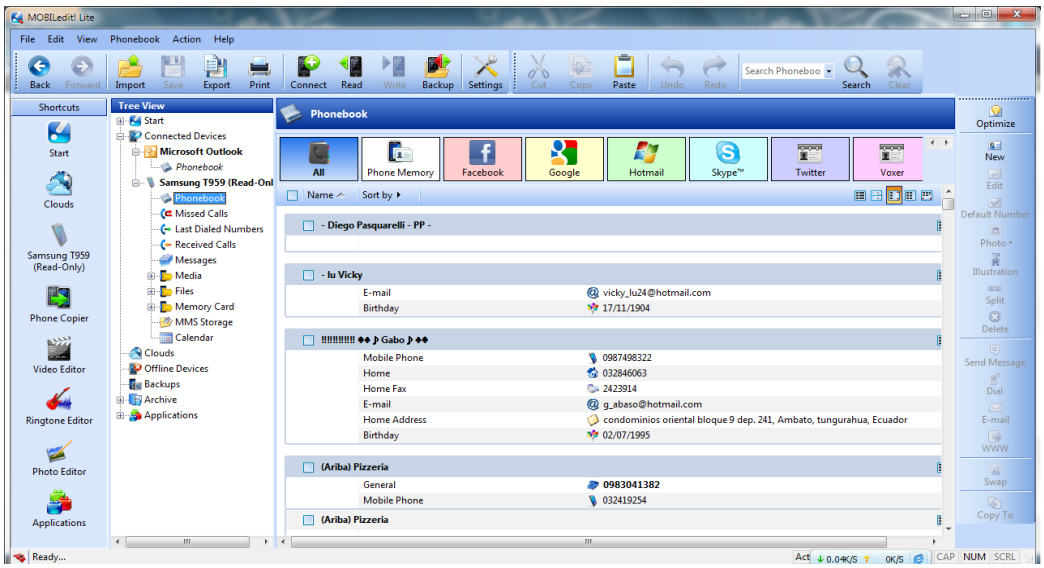


Figura 6. 43 Extracción de datos - Contactos (MOBILedit)

Después de tener la conexión de la aplicación con el dispositivo se podrá visualizar los datos extraídos como los contactos del celular con toda la información detallada que tenga en el celular como : correos, números de teléfono ...etc.

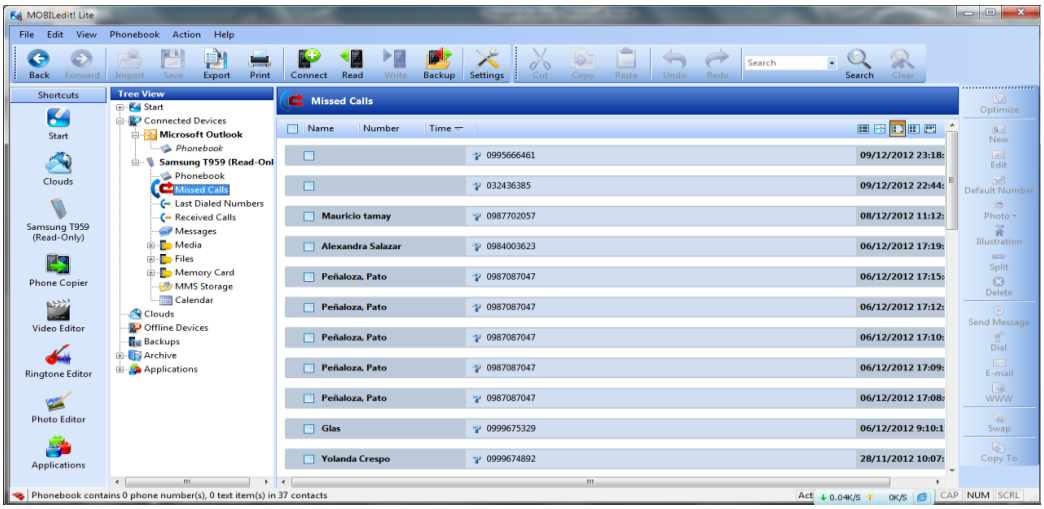


Figura 6. 44 Extracción de datos - llamadas (MOBILedit)

Podemos ir a los ítems de las llamadas perdidas o las llamadas recibidas o llamadas hechas para ver todos esos registros extraídos desde el celular.

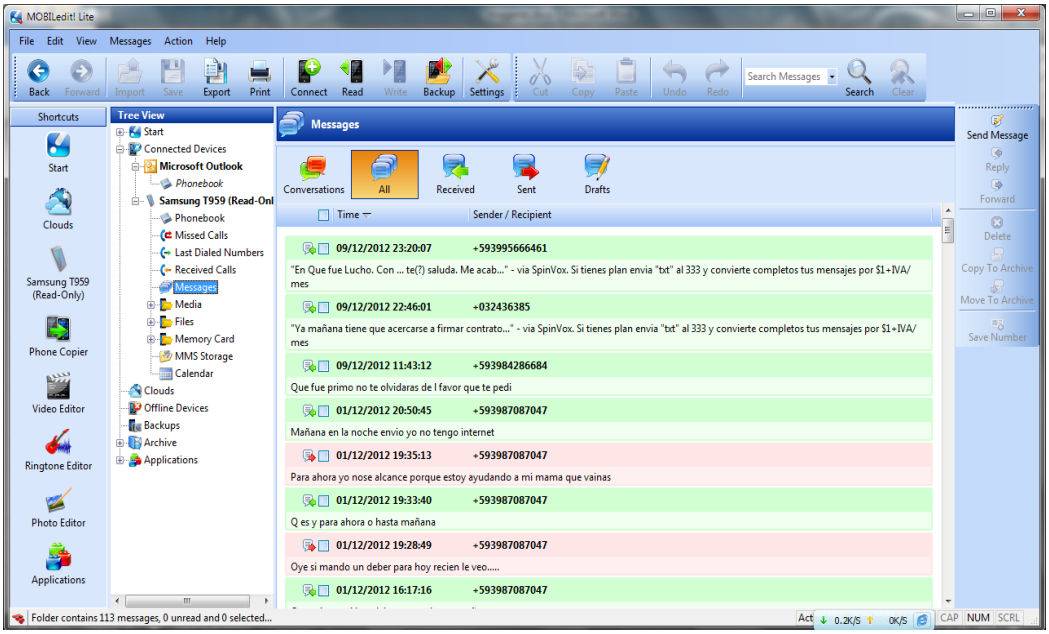


Figura 6. 45 Extracción de datos - Mensajes (MOBILedit)

También podemos entrar al ítem de mensajes donde podremos ver todos los mensajes hecho desde el dispositivo móvil incluso el día y la hora que se envió o recibió, también podemos ver el contenido del mensaje aparte de eso también podemos ver el numero celular al que se envió el mensaje.

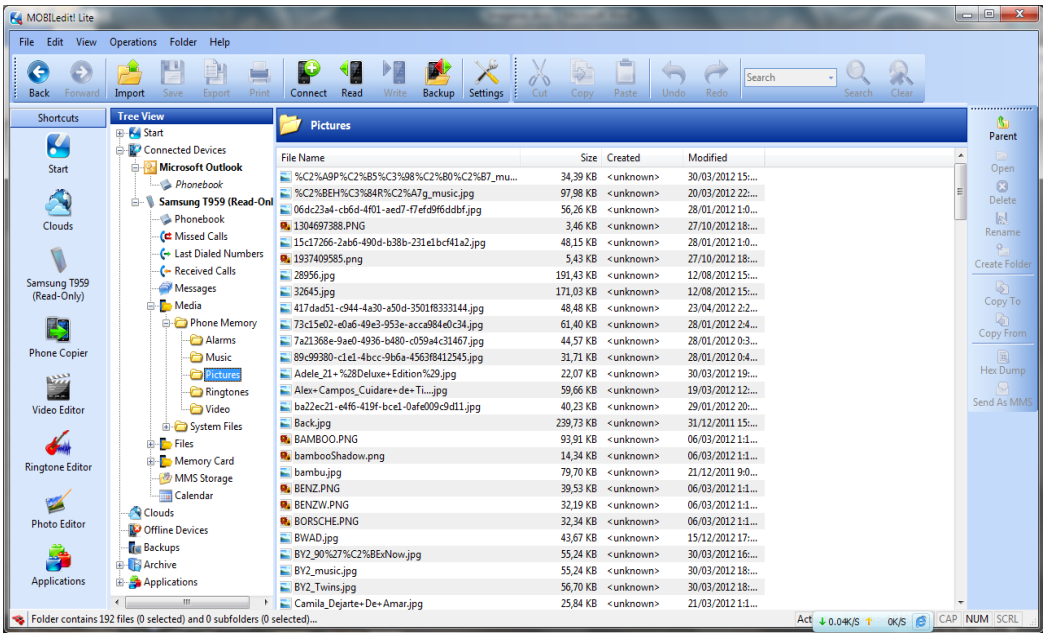


Figura 6. 46 Extracción de datos - Multimedia (MOBILedit)

En el ítem de media se encuentra toda la información extraída del dispositivo móvil como: música, imágenes, ringtones o videos y se puede visualizar todos los archivos en listados a lado derecho de la ventana.

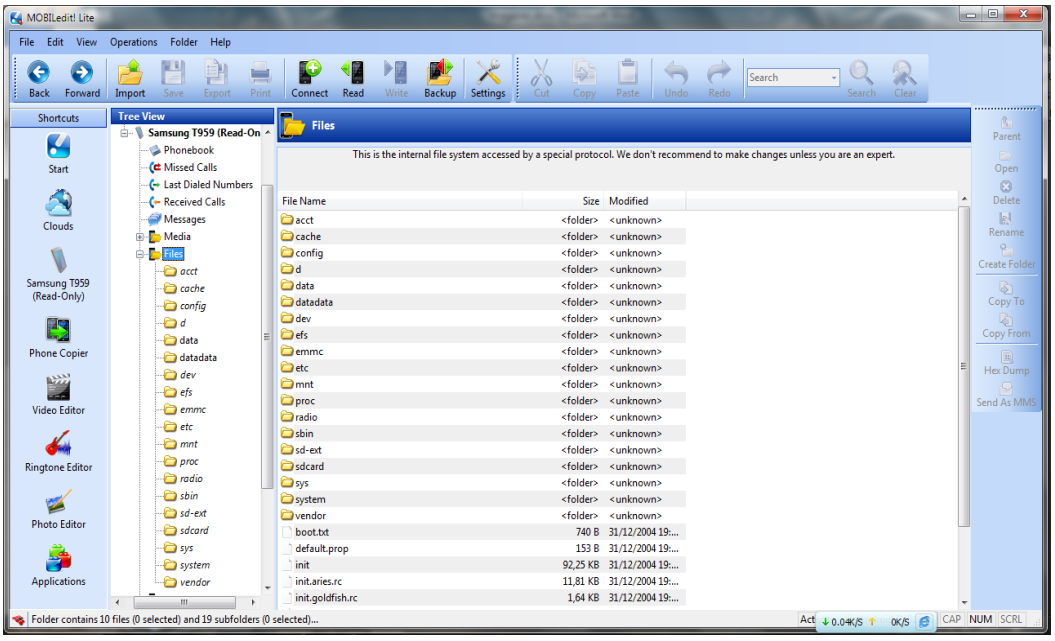


Figura 6. 47 Extracción de datos - Sistema de archivos (MOBILedit)

En la aplicación también podemos ver la estructura del sistema de archivos del dispositivo.

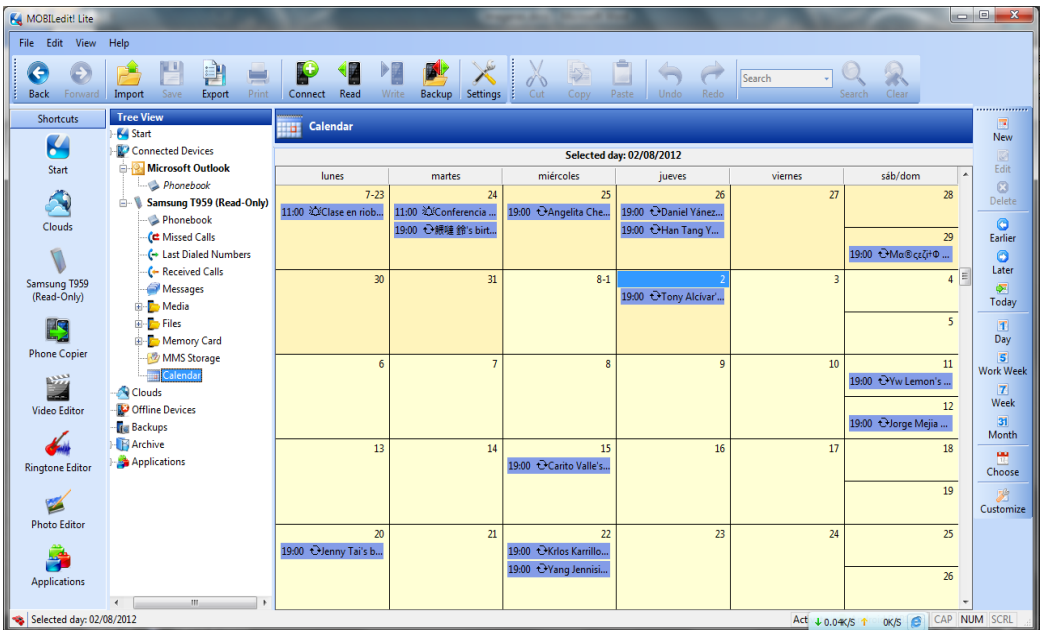


Figura 6. 48 Extracción de datos - Calendario (MOBILedit)

También se puede visualizar el calendario del dispositivo móvil y podremos ver toda la programación que tiene el celular.

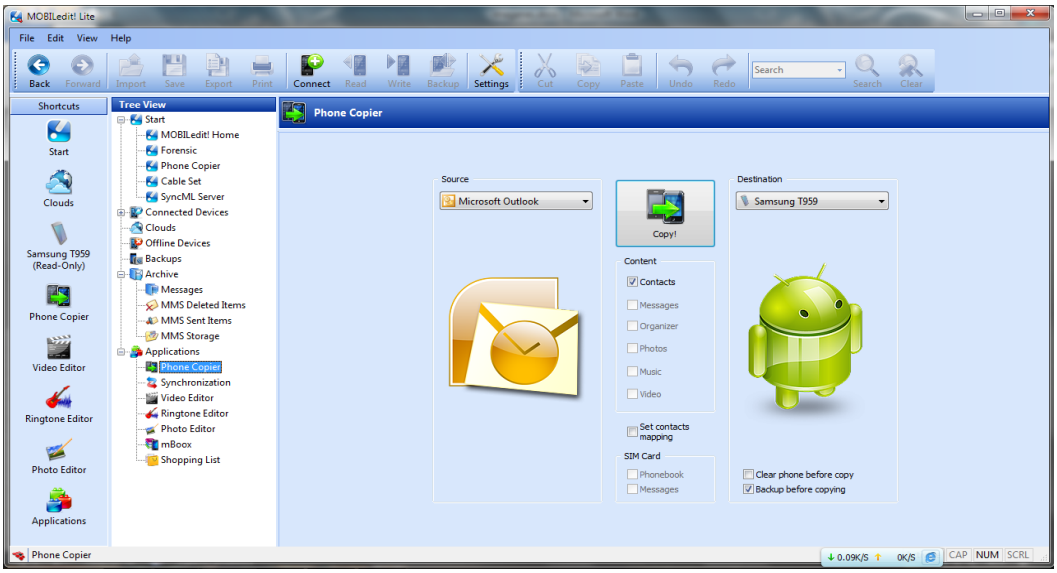


Figura 6. 49Copiar archivos (MOBILedit)

Dentro de la aplicación también nos ofrece una opción que puedes copiar datos de un archivo extraído y pasarlo al dispositivo móvil o copiar de un dispositivo.

6.6.7 SDK (kit de desarrollo de software)

Es generalmente un conjunto de herramientas de desarrollo de software que le permite al programador crear aplicaciones para un sistema concreto, por ejemplo ciertos paquetes de software, frameworks, plataformas de hardware, computadoras, videoconsolas, sistemas operativos, etc.

La manera natural de interactuar con el teléfono a nivel consola es lanzar comandos mediante Android Debug Bridge (ADB). ADB es parte del SDK de Android y nos permite conectar al dispositivo estando esté conectado vía USB en la máquina que queramos analizar. si vamos a usar ADB en Windows, ya que tenemos que tener el driver USB instalado (consultar SDK). En cualquiera de los casos, tanto Windows como Mac o Linux, la depuración USB tiene que estar activada en el teléfono.

Se puede hacer un análisis forense al celular ya que podemos interactuar con el teléfono a través de los comandos ADB que está integrada en el SDK, porque al poder acceder al celular podemos para copiar a la base de datos donde están registradas todos los datos como: contactos, llamadas, historiales de navegación, masajes.. etc.

Proceso para conectar el dispositivo

Conectar al teléfono

Para poder conectar al teléfono a través del ADB, primero tenemos que instalar la aplicación java en nuestro caso usaremos Ubuntu 12.04

Abrimos el terminal y pones el siguiente comando para instalar la aplicación java

```
sudo add-apt-repository ppa:webupd8team/java
sudo apt-get update
sudo apt-get install oracle-java7-installer
```

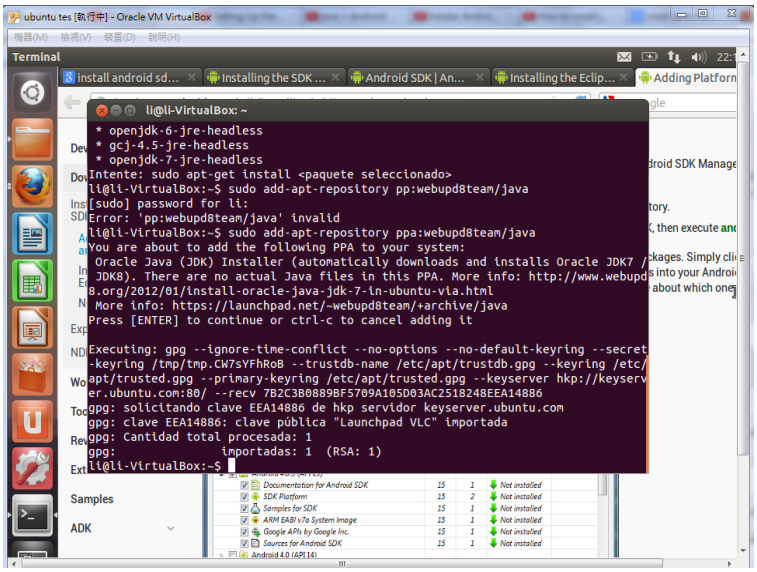


Figura 6. 50 Instalación de java

Luego de eso instalaremos el SDK para ellos tenemos que ir a la pagina para descargarnos el archivo de instalación

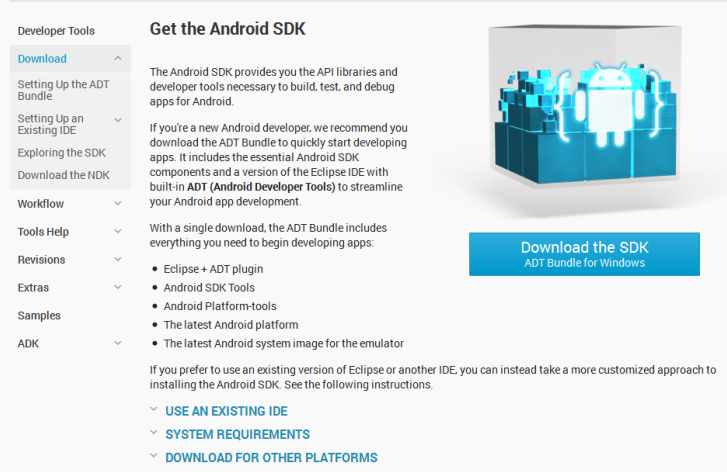


Figura 6. 51 Pagina de descarga SDK

Luego de descargar el SDK abriremos un terminal y entraremos por medio de comandos para ejecutar y tenemos que navegar hasta donde está la carpeta **tools** y luego instalaremos el SDK con el comando **./android**

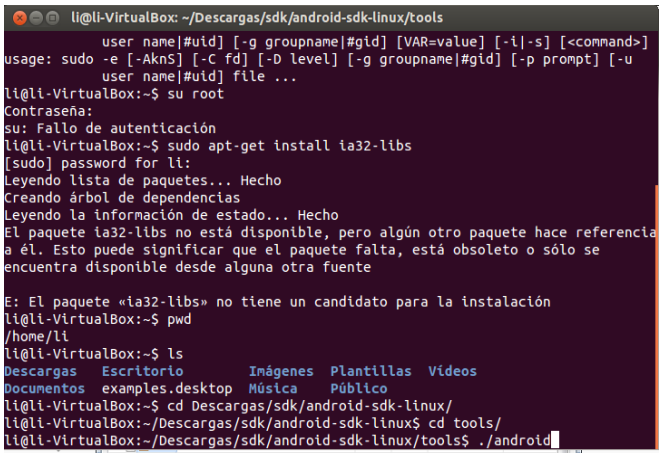


Figura 6. 52 Instalando SDK

Luego de ejecutar el comando aparecerá el listado de paquetes de Android que podemos instalar, el paquete representan las versiones de Android que se pueden instalar.

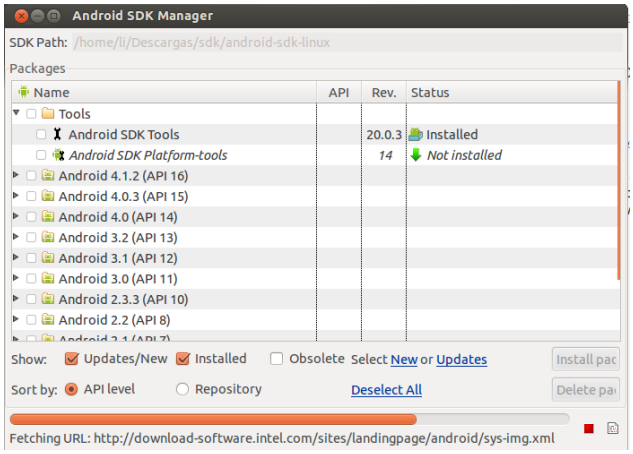


Figura 6. 53 Android SDK Manager

Luego de seleccionar el paquete que se quiera instalar, empezara a descargar el paquete y luego procederá su instalación.

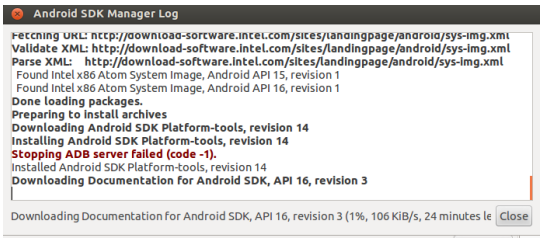


Figura 6. 54 Android SDK Manager2

El proceso tardara varios minutos cuando termine de instalar los paquetes y podrá cerrar el Android Manager.

Crear variable del sistema

Para poder crear el variable del sistema tenemos que editar el fichero **.bashrc** y dentro del archivo podemos poner las variables para que de esta forma el comando ADB pueda ser reconocido.

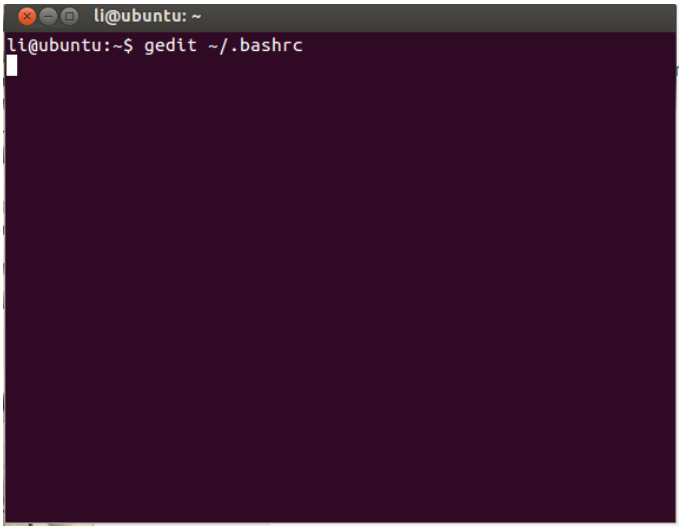


Figura 6. 55 Editando ~/.bashrc

El comando para editar el archivo ~/.bashrc podemos usar el siguiente comando:

gedit ~/.bashrc

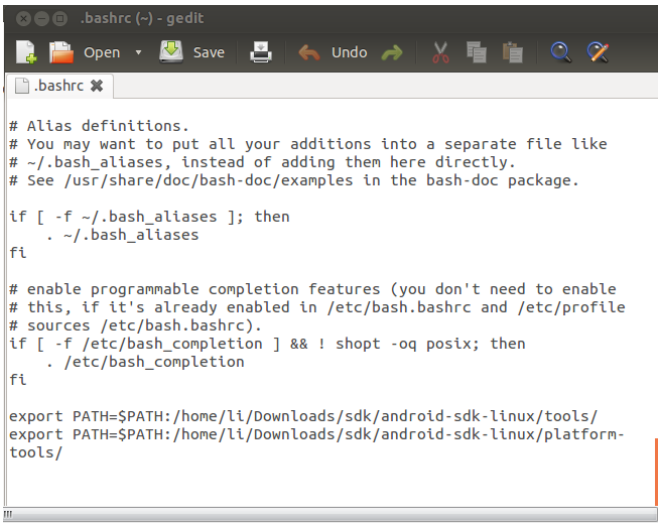


Figura 6. 56 Editando2 ~/.bashrc

Ya cuando hayamos abierto el archivo podemos poner las variables del sistema:

export PATH=$PATH:/home/li/Downloads/sdk/android-sdk-linux/tools/
export PATH=$PATH:/home/li/Downloads/sdk/android-sdk-linux/platform-tools/

Luego de poner las variables lo guardamos y lo cerramos, pero hay que tomar algo en cuenta la ruta depende del usuario y de donde estén los directorios.

Crear los perfiles USB para cada dispositivo Android

Hay que crear el perfil de USB para que pueda reconocer el dispositivo y para crear el dicho perfil se debe crear un archivo en la ruta **/etc/udev/rules.d/**

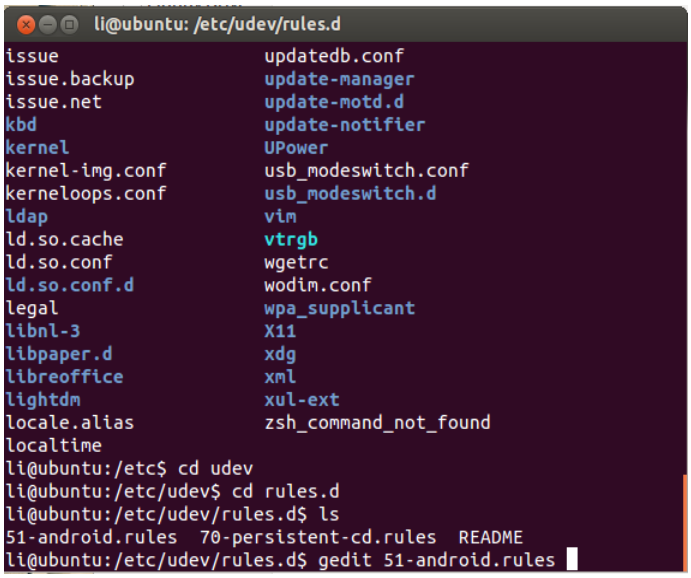


Figura 6. 57 Ruta para la creación de perfil

y ponemos el siguiente código en el archivo

#Acer
SUBSYTEM=="usb", SYSFS{idVendor}=="502", MODE="0666"
#ASUS
SUBSYTEM=="usb", SYSFS{idVendor}=="0b05", MODE="0666"
#Dell
SUBSYTEM=="usb", SYSFS{idVendor}=="413c", MODE="0666"
#Foxconn
SUBSYTEM=="usb", SYSFS{idVendor}=="0489", MODE="0666"
#Fujitsu
SUBSYTEM=="usb", SYSFS{idVendor}=="04c5", MODE="0666"
#Garmin-Asus
SUBSYTEM=="usb", SYSFS{idVendor}=="091e", MODE="0666"

```
#Google
SUBSYTEM=="usb", SYSFS{idVendor}=="18d1", MODE="0666"
#Hisense
SUBSYTEM=="usb", SYSFS{idVendor}=="109b", MODE="0666"
#HTC
SUBSYTEM=="usb", SYSFS{idVendor}=="0bb4", MODE="0666"
#Huawei
SUBSYTEM=="usb", SYSFS{idVendor}=="12d1", MODE="0666"
#K-Touch
SUBSYTEM=="usb", SYSFS{idVendor}=="24e3", MODE="0666"
#KT Tech
SUBSYTEM=="usb", SYSFS{idVendor}=="2116", MODE="0666"
#Kyocera
SUBSYTEM=="usb", SYSFS{idVendor}=="0482", MODE="0666"
#Lenovo
SUBSYTEM=="usb", SYSFS{idVendor}=="17ef", MODE="0666"
#LG
SUBSYTEM=="usb", SYSFS{idVendor}=="1004", MODE="0666"
#Motorola
SUBSYTEM=="usb", SYSFS{idVendor}=="22b8", MODE="0666"
#NEC
SUBSYTEM=="usb", SYSFS{idVendor}=="0409", MODE="0666"
#Nook
SUBSYTEM=="usb", SYSFS{idVendor}=="2080", MODE="0666"
#Nvidia
SUBSYTEM=="usb", SYSFS{idVendor}=="0955", MODE="0666"
#OTGV
SUBSYTEM=="usb", SYSFS{idVendor}=="2257", MODE="0666"
#Pantech
SUBSYTEM=="usb", SYSFS{idVendor}=="10a9", MODE="0666"
#Pegatron
SUBSYTEM=="usb", SYSFS{idVendor}=="1d4d", MODE="0666"
#Philips
SUBSYTEM=="usb", SYSFS{idVendor}=="0471", MODE="0666"
#PMC-Sierra
SUBSYTEM=="usb", SYSFS{idVendor}=="04da", MODE="0666"
#Qualcomm
```

```
SUBSYTEM=="usb", SYSFS{idVendor}=="05c6", MODE="0666"
#SK Telesys
SUBSYTEM=="usb", SYSFS{idVendor}=="1f53", MODE="0666"
#Samsung
SUBSYTEM=="usb", SYSFS{idVendor}=="04e8", MODE="0666"
#Sharp
SUBSYTEM=="usb", SYSFS{idVendor}=="04dd", MODE="0666"
#Sony
SUBSYTEM=="usb", SYSFS{idVendor}=="054c", MODE="0666"
#Sony Ericsson
SUBSYTEM=="usb", SYSFS{idVendor}=="0fce", MODE="0666"
#Teleepoch
SUBSYTEM=="usb", SYSFS{idVendor}=="2340", MODE="0666"
#Toshiba
SUBSYTEM=="usb", SYSFS{idVendor}=="0930", MODE="0666"
#ZTE
SUBSYTEM=="usb", SYSFS{idVendor}=="19d2", MODE="0666"
```

Una vez terminado, grabar y cerrar el fichero. Damos permiso de lectura a todos los usuarios:

```
$ sudo chmod a+r /etc/udev/rules.d/51-android.rules
```

Después de guardar los archivos podemos empezar a probar el comando ADB para ver si ya reconoce el comando

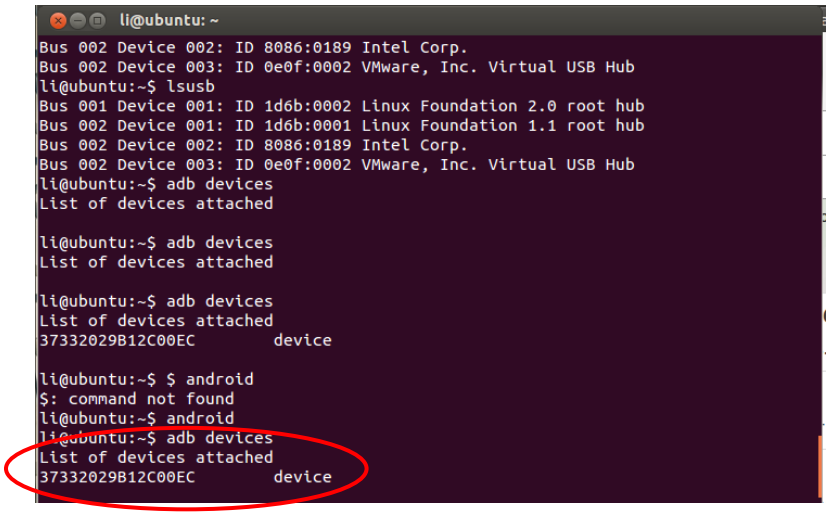


Figura 6. 58 Comando ADB

Como podemos ver el ADB ya reconoció los dispositivos que están conectados a través del comando:

-adb devices

Después de comprobar que el comando ADB funciona empezaremos entraremos en modo root al celular para copiar los datos (archivos .db)

- adb shell (entrar en modo root)

- find / -name *.db (busca todos los archivos .db)

y vamos a la carpeta /data/system y copiamos el archivo al escritorio.

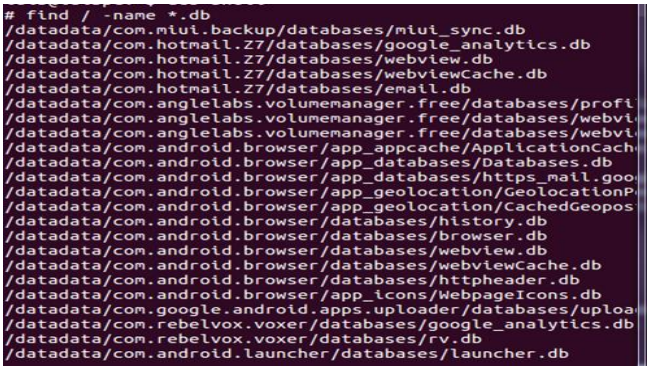


Figura 6. 59 Archivos .db

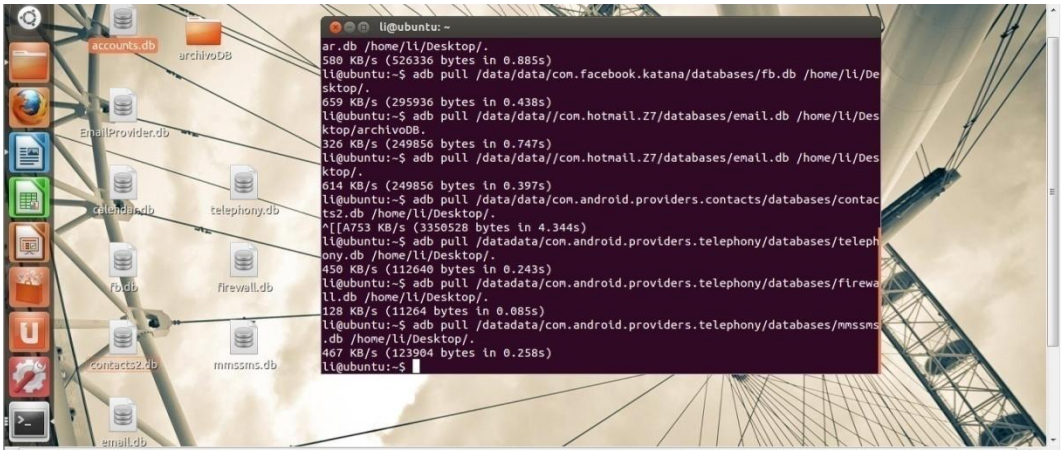


Figura 6. 60 Copiando Archivos

Copiamos los ficheros que tengan la extensión .db:

$ adb pull /data/system/accounts.db

Para poder visualizar el archivo copiado como ejemplo **accounts.db** que contienen las bases de datos se puede usar varias herramientas, sqlite3, sqliteview..etc. pero para este caso usamos un plugin de firefox llamado SQLite Manager.

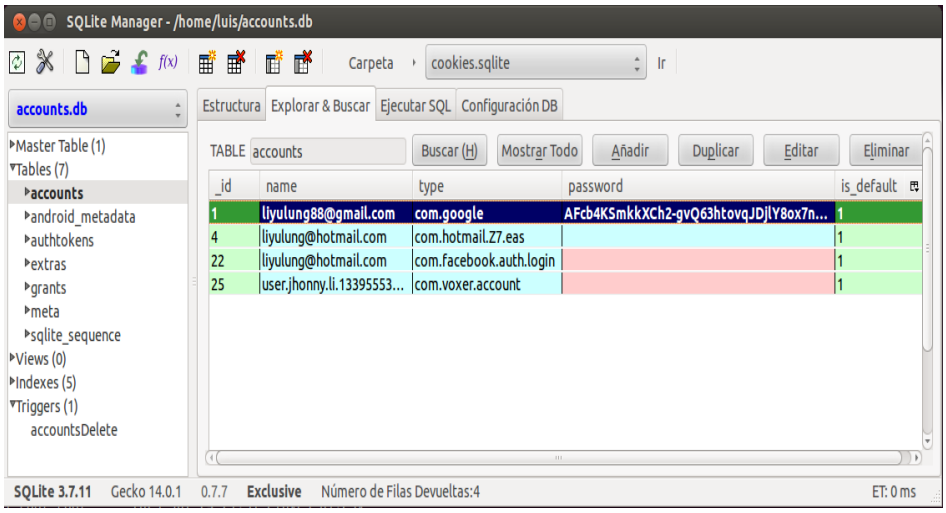


Figura 6.61 Account - SQLite

Los registros de las llamadas se encuentra en la tabla calls, que está dentro de la bases de datos contacts2.db, la misma que está en la ruta /data/com.android.providers.contacts/databases/contacts2.db

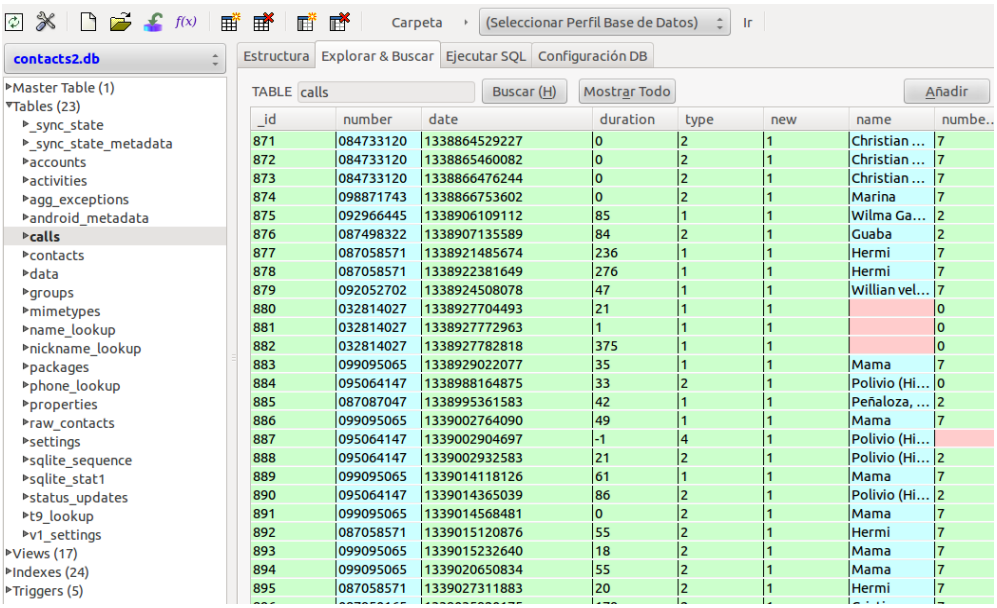


Figura 6. 62 Contacts – SQLite

6.7 Evaluación de las aplicaciones

	Recuperación de datos	Extracción de datos	Imágenes	Dump en la ram
Seizure	0	60	20	20
Bitpim	0	20	0	0
Oxygen/ MOBILedit	0	70	20	10
Otros	0	50	25	25

Tabla 6. 1 Tabla de Evaluación

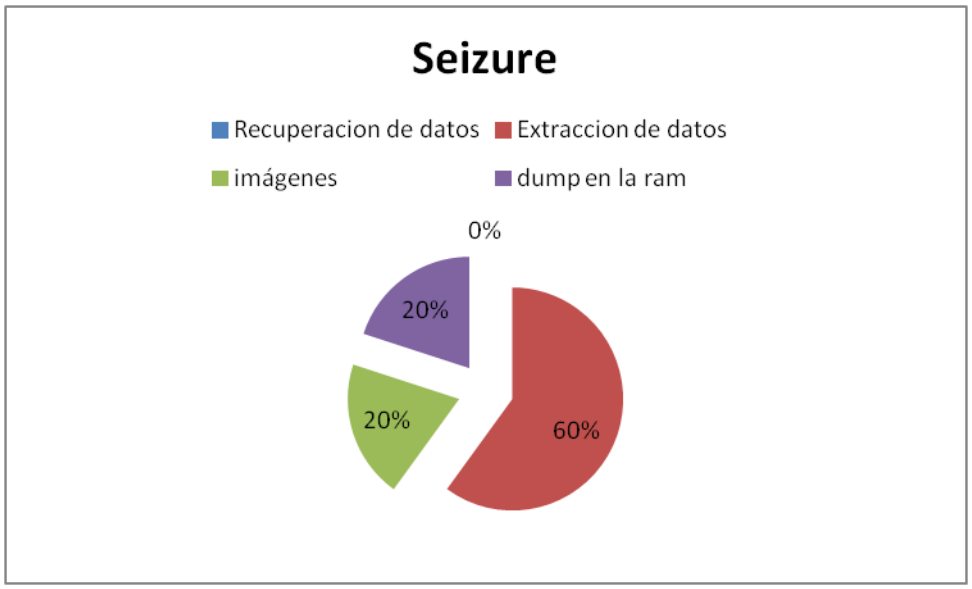


Figura 6. 63 Evaluación1

A través de las pruebas podemos ver que el programa SEIZURE no tienen la funcionalidad de recuperación de datos pero tiene un 60% en la extracción de datos y un 20% para las imágenes y en Dump tiene también un 20%.

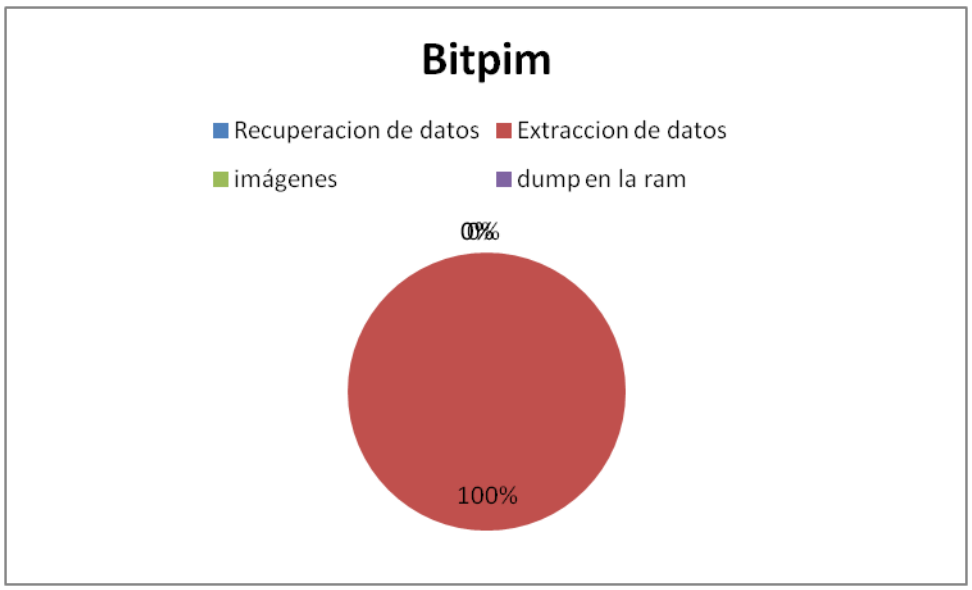


Figura 6. 64 Evaluación 2

A través de las pruebas podemos ver que el programa BITPIM no tienen la funcionalidad de recuperación de datos tampoco la de imágenes ni el de dump y solo tiene un 20% para la extracción de datos

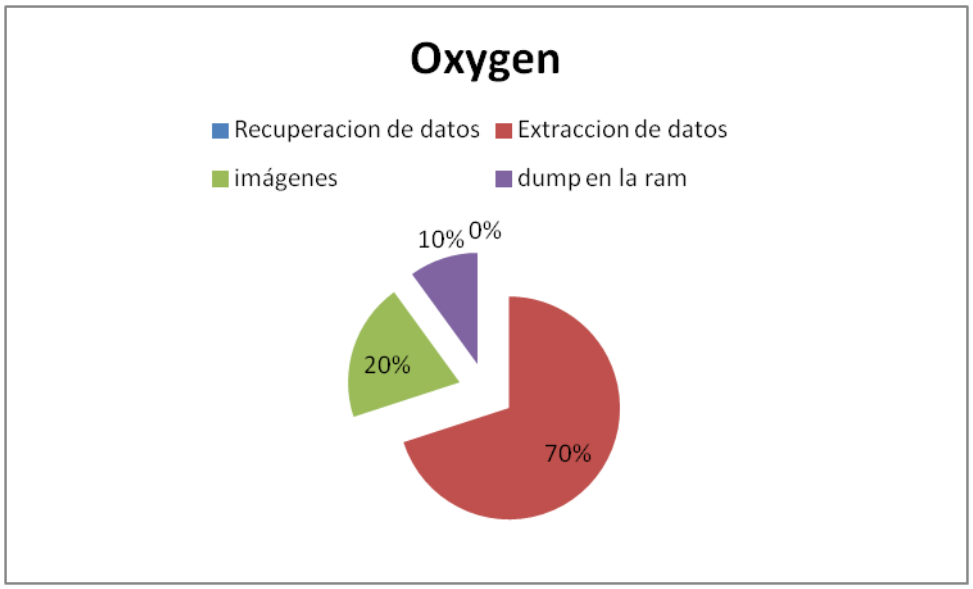


Figura 6. 65 Evaluación 3

A través de las pruebas podemos ver que el programa OXYGEN no tienen la funcionalidad de recuperación de datos pero tiene un 70% en la extracción de datos y un 30% para las imágenes y en Dump tiene también un 10%.

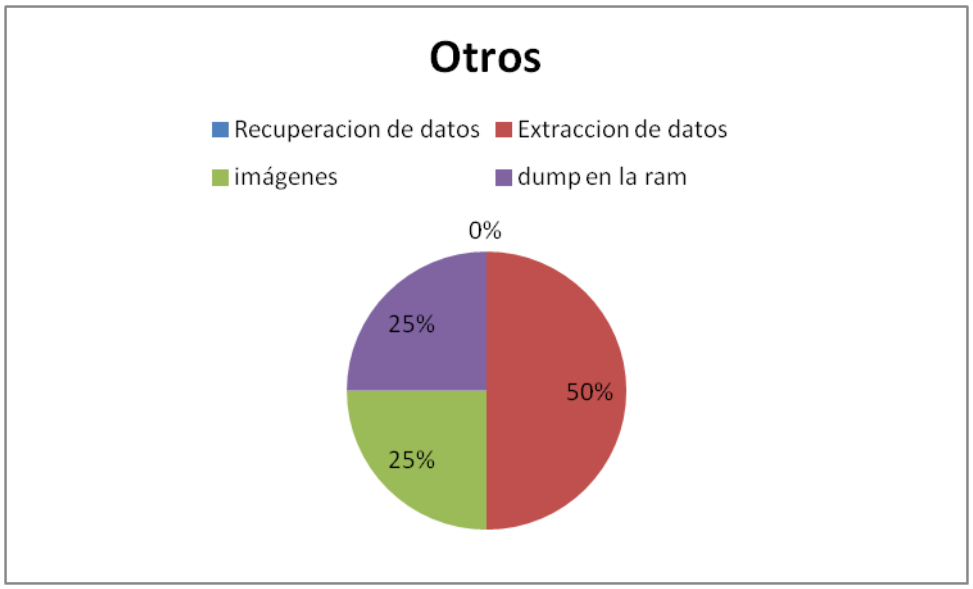


Figura 6. 66 Evaluación 4

A través de las pruebas de otro tipo de programas no tienen la funcionalidad de recuperación de datos pero tiene un 50% en la extracción de datos y un 25% para las imágenes y en Dump tiene también un 25%.

	Cable	**Bluetooth**	**Wifi**
Bitpim	X		
Seizure paraben	X		
Oxygen	X	X	X
Mobiledit	X	X	X
Otros	X	X	X

Tabla 6. 2 Tipos de conexión

Con la siguiente tabla se puede ver las aplicaciones de análisis forense que tipos de conexiones soportar y podemos ver que Bitpim y Seizure paraben no soporta las Bluetooth y WIFI.

	Velocidad de Extracción / Minutos
Bitpim	5
Seizure paraben	20
Oxygen	40
Mobiledit	60
Otros	30

Tabla 6. 3 Velocidad de extracción de información

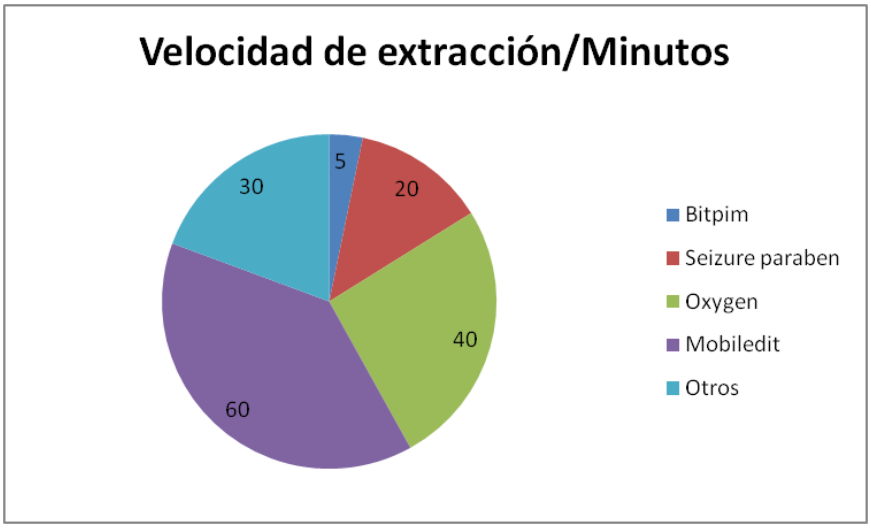


Figura 6. 67 Velocidad de extracción por minutos

Mediante el grafico podemos ver el tiempo que se requiere para las aplicaciones de análisis forense en extraer la información del dispositivo móvil.

Se ha tomado en cuenta las fichas de observación y se a determinado que el programa OXYGEN cumple mas las expectativas para realizar el análisis forense ya que permite sacar más la información en los dispositivos móviles.

6.8 Conclusiones y Recomendaciones de la Propuesta

6.8.1 Conclusiones

- Las aplicaciones OXYGEN y MOBILET pudieron extraer más datos del dispositivo móvil que las otras aplicaciones.

- La Velocidad de extracción de datos depende de la cantidad de datos que tiene en el Smartphone.

- En algunas aplicaciones forenses nos permite generar un reporte acerca de los datos extraídos del dispositivo como contactos, mensajes, llamadas ... etc.

- Con el manual de la propuesta se mejoro el manejo y la utilización de los aplicaciones forenses para dispositivos móviles.

- Con el manual facilita la instalación de las aplicaciones de análisis forense del dispositivo móvil.

- En base al estudio y evaluación de las aplicaciones de análisis forense para los dispositivos móviles, se ha podido determinar que la aplicación OXYGEN permite extraer mas información y el tiempo de extracción es mucho mejor comparando con las otras aplicaciones y no requiere características especiales a nivel de hardware del computador para poder instalarla.

6.8.2 Recomendaciones

- Se recomienda estar al tanto de las nuevas aplicaciones forense y las nuevas metodologías para mejorar el análisis forense de los dispositivos móviles bajo Android.

- Para poder acceder al dispositivo móvil de Android hay que activar la opción de debugging USB para que las aplicaciones pueda acceder a los datos del celular.

- Se recomienda antes de usar las aplicaciones Forenses se rootear el dispositivo móvil para que las aplicaciones tenga permisos de extraer los archivos.

- Se recomienda el uso de la Aplicación OXYGEN porque según los estudios y la evaluación realizada es más eficiente y rápida que otras aplicaciones.

6.9 Bibliografía

- Andorid, Recuperado en 10-12-2011 y disponible en http://es.wikipedia.org/wiki/Android

  Sitio Web donde explica lo que es Android
- Que es android, Recuperado en 10-12-2011 y disponible en http://www.configurarequipos.com/doc1107.html

  Sitio Web donde explica lo que es Android.
- Android llega a Ecuado, Recuperado en 09-10.2011 y disponible en http://tecnodatum.com/2010/06/exclusivo-android-llega-oficialmente-a-ecuador-con-movistar/

  Sitio Web que habla del primer Android llega al Ecuado
- Primer teléfono con sistema operativo Android en Ecuador, Recuperado en 09-10-2011 y disponible en http://www.eluniverso.com/2010/06/25/1/1431/primer-telefono-sistema-operativo-android-ecuador.html

  Sitio Web donde esta un reporte del primer celular android en Ecuador
- Informatica Forense, Recuperando en 01-10-2012 y disponible en http://laconsigna.files.wordpress.com/2008/05/informatica-forense.pdf

  Sitio Web que tiene un pdf sobre la informática forense
- Multimedia Recuperado en 10-10-2012 y disponible en

http://es.wikipedia.org/wiki/Multimedia

Sitio Web que habla sobre la multimedia y sus caracteristicas

- Análisis forense con oxygen forensics suite 2012 analyst Recuperado en 29-12-2012 y disponible en http://www.slideshare.net/eventoscreativos/anlisis-forense-con-oxygen-forensics-suite-2012-analyst

  Sitio Web que trata de la aplicación oxygen

- Root Samsung Galaxy S, Captivate y Vibrant, Recuperado el 16-05-2012 y disponible en: http://www.poderpda.com/plataformas/root-samsung-galaxy-s-captivate-y-vibrant/

  Sitio web donde se describe como rootear al Dispositivo móvil Android

- Como abrir bandas y rutear a Samsung Galaxy S1 Captivate SGH I 897, Recuperado el 16-05-2012 y disponible en http://www.youtube.com/watch?v=Y5wtugN6NUA

  Sitio web donde esta un video de como rootear al Dispositivo móvil Android

- Análisis forense de dispositivos Android 02, Recuperado 20-05-2012 y disponible en http://www.slideshare.net/eventoscreativos/anlisis-forense-de-dispositivos-android-02-13580763

  Sitio Web que trate sobre el análisis forense - sistema de ficheros.

- Android Forensics Android Forensics Android Forensics, Recuperado 20-05-2012 y disponible en http://www.slideshare.net/peterbuck/android-forensics-android-forensics-android-forensics

  Sitio web que explica la informática en los dispositivos moviles bajo Android

- Metodologías, estrategias y herramientas de la informática forense aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional Recuperado 17-02-2013 y disponible en http://dspace.ups.edu.ec/bitstream/123456789/546/2/CAPITULO1.pdf

  Sitio web que describe la informática forense

- Metodologías, estrategias y herramientas de la informática forense aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional Recuperado 17-02-2013 y disponible en http://dspace.ups.edu.ec/bitstream/123456789/546/3/CAPITULO2.pdf

  Sitio web que describe la informática forense

- Metodologías, estrategias y herramientas de la informática forense aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional Recuperado 17-02-2013 y disponible en http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf

  Sitio web que describe la informática forense

- Metodologías, estrategias y herramientas de la informática forense aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional Recuperado 17-02-2013 y disponible en http://dspace.ups.edu.ec/bitstream/123456789/546/5/CAPITULO4.pdf

  Sitio web que describe la informática forense

- Metodologías, estrategias y herramientas de la informática forense aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional, Recuperado 17-02-2013 y disponible en http://dspace.ups.edu.ec/bitstream/123456789/546/6/CAPITULO5.pdf

  Sitio web que describe la informática forense

- Informática Forense, Recuperado 17-02-2013 y disponible en http://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDYQFjAB&url=http%3A%2F%2Fauditoriasistemasucb.pbworks.com%2Ff%2FINFORMATICA%2BFORENSE.ppt&ei=bzYhUYbq

Eeq-0QH19YGwDQ&usg=AFQjCNEHhSAsemVh8OqTUYFXNj5whrPgCg&bvm=bv.42553238,d.eWU

Sitio web que tiene un archivo .PPT el cual explica sobre la informática forense

- Técnicas Anti Forenses en informática, Recuperado 17-02-2013 y disponible en http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6%283%29.pdf

  Sitio Web que describe sobre las técnicas de anti forense

- Análisis forense de dispositivos Android 03, Recuperado 03-03-2012 y disponible en http://www.slideshare.net/eventoscreativos/anlisis-forense-de-dispositivos-android-03

  Sitio web que describe del análisis forense android

Referencias

- Gustavo Fabián Torrealday artículos lenguaje de programación (http://www.torrealday.com.ar/articulos/articulo006.htm)
- Gus wolvering Conceptos básicos de programación (http://www.monografias.com/trabajos38/programacion/programacion.shtml)
- LISANDRO PERALTA MURUA analisis de lenguaje (pag 1) (http://enriquebarrueto0.tripod.com/algoritmos/algor01.pdf)
- KERVIN VERGARA conceptos y tipos de software (http://www.bloginformatico.com/concepto-y-tipos-de-software.php)
- Jhon Dilas (http://www.universidadperu.com/ingenieria-informatica-peru.php)

- http://forogrupo38.foro-colombia.net/t3-definicion-software#13
- http://www.alegsa.com.ar/Dic/seguridad%20informatica.php
- ANALÍA LANZILLOTTA

(http://www.mastermagazine.info/termino/5368.php)

- Rodney McKennish (http://www.scribd.com/doc/37134020/Analisis-forense)
- Ángel Alonso Párrizas, Roberto

Gutiérrez(http://www.angelalonso.es/doc-presentaciones/AF_v3.pdf)