ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSTITUTO DE POSTGRADO Y EDUCACIÓN CONTINUA

MAESTRÍA EN INTERCONECTIVIDAD DE REDES

GUÍA DE PROCEDIMIENTOS PARA EL MANEJO DE INCIDENTES EN DISPOSITIVOS MÓVILES MEDIANTE ANÁLISIS FORENSE

TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN INTERCONECTIVIDAD DE REDES

MARIANELA DE JESÚS INCA CHUNATA

RIOBAMBA – ECUADOR

2014

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TESIS, CERTIFICA QUE:

El trabajo de investigación titulado: "GUÍA DE PROCEDIMIENTOS PARA EL MANEJO DE INCIDENTES EN DISPOSITIVOS MÓVILES MEDIANTE ANÁLISIS FORENSE", de responsabilidad de la Ingeniera Marianela de Jesús Inca Chunata, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal de Tesis

Ing. MsC. Fernando Proaño	_____
PRESIDENTE	**FIRMA**
Ing. Ms.C. Diego Ávila Pesantez	_____
DIRECTOR	**FIRMA**
Ing. MsC. Gloria Arcos	_____
MIEMBRO	**FIRMA**
Dra. MsC. Narcisa Salazar	_____
MIEMBRO	**FIRMA**

DERECHOS DE AUTORÍA

Yo, Marianela de Jesús Inca Chunata, soy la responsable de las ideas, doctrinas y resultados expuestos en esta Tesis; y, el patrimonio intelectual de la misma pertenece a la Escuela Superior Politécnica de Chimborazo.

ÍNDICE DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

DEDICATORIA

Este trabajo de Tesis se lo dedico:

A Dios por llenar mi vida de dicha y bendiciones.
A mis padres por su amor, cariño y comprensión;
por ayudarme a ser una mejor persona cada día.
A mis hermanos por brindarme su apoyo en todo momento.

AGRADECIMIENTO

A Dios quien ha guiado mis pasos
a lo largo de mi vida, y me ha dado la fortaleza
para continuar y alcanzar la metas que me he trazado.

A mis padres y hermanos por haberme brindado
su comprensión y apoyo incondicional.

A los ingenieros. Diego Ávila, Gloria Arcos y
Dra. Narcisa Salazar, por estar siempre dispuestos a
compartir sus conocimientos y por sus comentarios en
todo el proceso de esta investigación.

RESUMEN

La presente investigación es proponer una guía de procedimientos para el manejo de incidentes en dispositivos móviles mediante análisis forense, aplicado a teléfonos celulares incautados en la ciudad de Riobamba a personas que se dedican a la compra y venta de estos equipos.

La metodología utilizada para obtener evidencia digital en los dispositivos celulares bajo la plataforma Symbian, Android versión 2.3.4/2.3.6, y sistema operativo propietario Sony Ericsson, que pudieran estar relacionados con algún incidente de seguridad como: pérdida o robo del dispositivo celular, fraude o extorsión, se fundamenta en el método científico e inductivo, se investigó los conceptos, herramientas, procedimientos de la informática forense, se realizaron experimentos en 50 dispositivos móviles Nokia, Samsung, LG, Sony Ericsson, el uso de estos métodos permitió construir la guía de procedimientos que integra cuatro fases: identificación del problema, recolección de la evidencia digital, análisis forense de la información recuperada, creación de un reporte.

Se aplicó la técnica estadística ji cuadrado para comprobar la obtención de evidencia digital, se generó el valor de 21,04. Se recuperó: mensajes de texto en un 75%, 60% de llamadas telefónicas, se ha logrado generar un 60% de reportes, imágenes, agenda telefónica; evidencia digital que puede ser utilizada en una corte de justicia, en caso de iniciarse un proceso legal.

Con los resultados obtenidos se concluye que la guía de procedimientos propuesta ayuda a obtener información de los teléfonos móviles celular. Se recomienda a la ciudadanía usar adecuadamente políticas de seguridad en los dispositivos móviles así evitaremos robos, fraudes o extorsiones.

SUMMARY

This research is to propose a guide of procedures for incident management in mobile devices using forensics analysis, applied to cell phones confiscated in Riobamba to people engaged in the buying and selling these devices.

The methodology used to obtain evidence digital cellular devices under the Symbian, Android platform version 2.3.4/2.3.6, and Sony Ericsson proprietary operating system, which could be related to an incident as: loss or theft of the mobile device, fraud or extortion, is based on the scientific and inductive method, it was investigated the concepts, tools and procedures for computer forensics, experiments were conducted on 50 mobile devices, Nokia, Samsung, LG, Sony Ericsson, the use of these methods allowed to build procedures guide comprising four phases: problem identification, digital evidence collection, forensic analysis of the retrieved information, creation of a report.

Chi-square statistical technique was applied to check the obtaining of digital evidence, getting a value of 21.04. Recovered: text messages in a 75%, 60% of phone calls, it has been able to generate 60% of reports, images, phonebook, digital evidence that can be used in a court of law, in the event of a legal process.

With the obtained results it is concluded that the proposed procedures guide helps to get information from cell phones. It is recommended to properly use the public security policies on mobile devices to avoid theft, fraud and extortion.

CAPITULO I
INTRODUCCIÓN

1.1. PROBLEMATIZACIÓN

Los teléfonos celulares, así como todos los dispositivos móviles, son aparatos que en la actualidad utiliza la mayoría de la gente. Al igual que las computadoras, estos artefactos han dejado de ser un lujo, pues se han convertido en una necesidad. Además de cumplir con la función básica de un celular, la mayoría de ellos cuentan con funciones especiales: el envío de mensajes de texto cortos (SMS), mensajes de texto multimedia (MMS), mensajes instantáneos (IM), correos electrónicos, navegar en Internet y administrar información personal (PIM) [1].

Casi todos los celulares permiten a los usuarios la instalación de ciertas aplicaciones, así como el almacenamiento de información personal y confidencial, sin importar el sistema operativo, la forma en la que se sincroniza la información o cómo se conectan con los equipos de cómputo [2].

De la misma forma que ocurre con un equipo informático, cuando un celular es analizado, servirá para redactar un reporte detallado de las actividades realizadas, incluyendo fechas, con la finalidad de buscar evidencias que revelen la causa y forma en la que se llevó a cabo un delito o se violó una política.

Por lo tanto la inseguridad informática es mucho más latente y como si fuera poco, más vulnerable gracias a la movilidad que puede poseer un atacante a la hora de violentar alguna plataforma bien sea esta del tipo móvil o fija por medio del uso de estos dispositivos móviles.

---

[1] **BECERRIL, I.,** Análisis forense en dispositivos móviles., Estados Unidos., 2008., pp. 4-5. E-book: http://www.revista.unam.mx/vol.9/num4/art26/int26.htm

[2] **BECERRIL I.,** Análisis forense en dispositivos móviles., Estados Unidos., 2008., pp. 6-7. E-book: http://www.revista.unam.mx/vol.9/num4/art26/int26.htm

Hay que tener en cuenta, que no únicamente se trata de los posibles riesgos que genera un atacante, sino de la importancia de poder examinar detalladamente la información que sea relevante y que pueda estar almacenada, escondida, cifrada o suprimida en un dispositivo móvil, como llamadas realizadas o perdidas, imágenes, videos, mensajes de texto, ya que por medio de estos, muy seguramente se logrará encontrar evidencia y conectar al sospechoso de algo, con la o las personas afectadas [3].

De esta forma surge la necesidad de tener técnicas forenses, que involucran procedimientos, métodos herramientas, con el fin de poder interactuar de una manera más directa dando así la posibilidad que a partir de esa evidencia digital se puedan plantear hipótesis concretas que indaguen sobre respuestas a un acto delictivo que bien puede tocarnos directa o indirectamente a nosotros. Las actividades deben investigarse contestando posibles preguntas: ¿qué se hizo?, ¿cómo se hizo? y ¿en qué orden se hizo? [4].

Para dar solución al problema planteado se propone una metodología para realizar el manejo de incidentes en dispositivos móviles mediante análisis forense, para poder obtener un reporte detallado de las actividades realizadas.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Proponer una guía de procedimientos para el manejo de incidentes en dispositivos móviles mediante análisis forense.

1.2.2. OBJETIVOS ESPECÍFICOS

- Realizar una revisión de los conceptos fundamentales, herramientas y procedimientos de la informática forense en general y su aplicación en dispositivos móviles con tecnología GSM.

---

[3] **HERNÁNDEZ R.,** Análisis forense en dispositivos móviles con Symbian OS., Bogotá – Colombia, 2008., pp. 1-6. E-book: http://www.criptored.upm.es/guiateoria/gt_m142e1.htm

[4] **AYERS R.,** Guidelines on Cell Phone Forensics., Estados Unidos., 2007., pp. 14-64., E-book: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

- Analizar las herramientas de software que permitan realizar análisis forense en dispositivos móviles GSM.
- Aplicar la guía de procedimientos propuesta para poder recopilar y analizar información de un incidente ocurrido en un dispositivo celular GSM.

1.3. JUSTIFICACIÓN

La informática forense sobre dispositivos móviles es la ciencia que se encarga de recuperar y recolectar evidencia digital de un teléfono móvil bajo una serie de condiciones forenses usando métodos aceptados. Para entender los numerosos aspectos que se relacionan con el proceso de un análisis forense en dispositivos móviles, es necesario entender los conceptos de la informática forense en general y aplicada a dispositivos móviles, los modelos de investigación que existen en la actualidad, las herramientas, procedimientos y estándares los cuales permiten que el análisis se realice con éxito sin pérdida o alteración de la potencial evidencia que pudiera llevarse a un proceso legal.

Es necesario realizar una investigación en este nuevo campo que es poco explorado. Esta investigación tiene como objetivo avanzar en el estudio y análisis de la informática forense en dispositivos móviles GSM, para ampliar este conocimiento y contribuir con el entendimiento de los incidentes.

Además de esto, es necesario comprender los dispositivos móviles, sus características, su funcionamiento, los problemas de seguridad que tienen estos, debido a que sobre ellos se realizará el análisis forense.

Siendo las vulnerabilidades informáticas frecuentes en la computación de oficina y las prácticas propias de los usuarios de los hogares, ahora el nuevo escenario de inseguridad informática está en la telefonía móvil y la integración de servicios que avanza rápidamente en este tipo de dispositivos. En consecuencia, los incidentes de seguridad que se presenten en este tipo de escenario, requiere un entendimiento más detallado de dichas tecnologías que permitan comprender las conductas de los atacantes en este tipo de comunicaciones inalámbricas.

El reto de la tecnología no sólo será innovar sobre dispositivos móviles que sean de dimensiones pequeñas para que sea fácil portarlos, o crear dispositivos con materiales que alarguen su vida útil, sino también deberá innovarse para crear dispositivos móviles que brinden seguridad a sus usuarios, esto es: que puedan almacenar información sin la incertidumbre de que cualquier persona en alguna parte del mundo pueda acceder, crear o modificar dicha información. Además otra de las ventajas que ofrece la informática forense es la facilidad en el manejo de la información, rapidez en la recolección y análisis de la misma.

El Análisis Forense orientado a incidentes se realizará en dispositivos móviles celulares con tecnología GSM con sistema operativo Symbian OS, este sistema brinda un nivel medio de desempeño, en procesamiento, multimedia, servicios para aplicaciones del sistema, comunicaciones, y de seguridad. Es importante resaltar este último elemento, el de seguridad, debido a la vital importancia que tiene para la investigación el poder trabajar con un sistema operativo que brinde ciertas facilidades y niveles de confianza a la hora de realizar un análisis forense debido a la complejidad de este campo y al elevado costo de las herramientas.

Todo lo mencionado anteriormente conlleva a realizar una incursión en el novedoso mundo del análisis forense orientado a incidentes ocurridos sobre dispositivos móviles, ya que un buen análisis forense ayudara a identificar las causas y si es viable identificar a los posibles atacantes mediante la evidencia digital obtenida.

Con la investigación realizada se podrá recopilar y analizar información para poder diseñar una guía de procedimientos que permita realizar un análisis forense orientado a incidentes sobre teléfonos celulares GSM, proporcionando los procedimientos necesarios para obtener la mayor cantidad de detalles posibles de un incidente ocurrido en un dispositivo celular y, de esta manera, fortalecer la base científica del campo de informática forense en dispositivos móviles.

El escenario será diseñado exclusivamente para simular cierto tipo de incidente de seguridad en el que pueda estar afectado un ciudadano y/o propietario del equipo celular, de esta forma se va a explorar y probar la efectividad de la metodología que se va a proponer frente a la evidencia encontrada y a los reportes generados por las herramientas usadas dentro del análisis forense.

1.4. HIPÓTESIS

La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense permitirá la obtención de evidencia digital frente a posibles ataques.

CAPITULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES Y ESTUDIOS PREVIOS

Las Ciencias Forenses han sido desarrolladas desde hace mucho tiempo atrás; uno de los primeros textos y estudios en este campo lo podemos ubicar en el año de 148 D.C, cuando el médico chino HI DUAN YU, escribió el libro "COMO CORREGIR LOS ERRORES", en el cual se explica las diferencias entre una muerte por ahogamiento y otra por una herida de cuchillo al igual que la muerte por causas naturales [5].

Posteriormente con el avance de la ciencia y la tecnología, las ciencias forenses han alcanzado un desarrollo inconmensurable, pero ese desarrollo a veces no ha ido de la mano del avance de la legislación penal.

Esto en razón del retraso en la incorporación de nuevos elementos de prueba y medios probatorios y sobre todo en la demora de la admisibilidad de nuevas evidencias o pruebas. Este es el caso por ejemplo de la prueba de ADN que fue admitida en un juicio en el año de 1996, pero su desarrollo y comprensión se logró desde la década de los ochenta [6].

Las ciencias forenses siempre están en constante cambio, siempre buscando nuevos métodos y procesos para encontrar y fijar las evidencias [7].

---

[5] **ACURIO S.,** Delitos Informáticos: Generalidades., 2011., pp. 6-8., E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[6] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 15., E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[7] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 33., E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

Gracias a estas ciencias se han podido emplear procedimientos y conocimientos científicos para encontrar, adquirir, preservar y analizar las evidencias de un delito y presentarlas apropiadamente a una Corte de Justicia siempre y cuando las leyes estén regularizadas en cada país.

2.2. FUNDAMENTACIÓN TEÓRICA

2.2.1. LA INFORMÁTICA FORENSE

La informática forense es el vehículo idóneo para localizar y presentar de forma adecuada los hechos jurídicos informáticos relevantes dentro de una investigación, ya sea de carácter civil o penal [8].

La ciencia forense es sistemática y se basa en hechos premeditados, permitiendo de esta forma recabar pruebas para luego analizarlas. La tecnología en caso de la identificación, recolección y análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y los elementos de convicción necesarios [9].

Históricamente la ciencia forense ha basado su experiencia y su accionar en estándares de práctica y entrenamiento, por lo tanto no solo es necesaria la incautación y recolección de evidencias digitales, sino también en su procesamiento cumpliendo siempre con los principios para el debido proceso; es decir *no alterando la evidencia* [10].

Como disciplina, la informática forense tiene como fin el aplicar los estándares y procedimientos; estándar que se utilizan en una investigación de crímenes e incidentes, para enfocarlos hacia el análisis de datos y evidencia digital, todo esto soportado por herramientas tecnológicas de extracción y análisis de datos [11].

---

[8] ACURIO S., Introducción a la Informática Forense., 2008., pp. 8., E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[9] ACURIO S., Delitos Informáticos: Generalidades., 2011., pp. 9., E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[10] ACURIO S., Introducción a la Informática Forense., 2008., pp. 9., E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[11] CASTILLO C., Dispositivos móviles. iPhorensics., 2010., pp. 1., E-book: http://www.carlosacastillo.com/2010/01/iphorensics/

La informática forense busca estudiar, entender, analizar y enfocar los conceptos referentes a esta ciencia, para poder llevar a cabo la construcción de una base sólida de conocimiento en la materia, de tal forma que esto es mi base principal para la construcción de la guía de procedimientos propuesta en este documento.

2.2.2. PROCESO FORENSE EN EQUIPOS INFORMÁTICOS Y/O DE TELECOMUNICACIONES

Un proceso Forense puede ser llevado a cabo, tanto en los sistemas informáticos, como en los de telecomunicaciones; la segunda es considerada como parte del tema de investigación en el presente trabajo. En este proceso se consideran dos aspectos.

El primero tiene que ver con el manejo de los incidentes informáticos producidos por la vulnerabilidad del sistema o por la participación de algún agente intruso. El manejo de incidentes persigue objetivos diferentes en comparación con aquellos que persigue la Informática Forense.

Sin embargo, también pueden ser aprovechados por esta última, ya que permite reconocer las fuentes de evidencia digital que contribuyen a determinar los responsables de un incidente.

El segundo aspecto está relacionado con la realización de una investigación digital sobre un sistema, ya sea informático o de telecomunicaciones, que bajo condiciones normales o no de operación ha sido utilizado dentro un delito. Con esta investigación se busca determinar quiénes fueron los responsables y cuál fue su proceder, a partir de evidencias digitales contundentes que pudieran presentarse, con carácter factual inobjetable, ante alguna instancia jurídica, administrativa o civil con la autoridad suficiente para determinar responsables y sanciones, en función de los daños producidos.

En el Ecuador los Delitos Informáticos se encuentran sancionados por el Código Penal; dentro de la Función Judicial los jueces y magistrados no cuentan con la

preparación necesaria, haciendo que estos delitos sean confundidos como delitos tradicionales [12].

La Asamblea en el Ecuador propone una clasificación de los delitos que permita su juzgamiento adecuado. Por lo cual dentro del código penal se está implementando un Plan Operativo de creación para la Unidad de Delitos Informáticos, con la única finalidad de proteger a los usuarios de la red frente a la emergente criminalidad informática, que aprovecha las vulnerabilidades de los sistemas informáticos y el desconocimiento generalizado de la mayoría de usuarios de la cultura digital [13].

Entre las secciones que forman parte de esta unidad esta la Técnica Forense, la misma que se encarga de brindar apoyo técnico y realizar el análisis forense de las evidencias encontradas en la escena del delito, esta sección la integran el grupo de apoyo técnico y un grupo de analistas forenses, en el Ecuador aún no existe el Departamento de Ciencias Forenses.

Dentro de las infracciones Informáticas tenemos [14]:

- Daños informáticos (CPP Art. 415), la represión va desde 6 meses a 5 años.
- Apropiacion ilícita (CPP Art. 553), la represión va de 6 meses a 5 años.

Phil Williams [15] manifiesta que es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura, como con el recurso humano científico, técnico, ético calificado para hacerle frente a este tipo de delitos transnacionales [16].

---

[12] ACURIO S., Delitos Informáticos: Generalidades., 2011., pp. 54., E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[13] ACURIO S., Plan Operativo de creación de la Unidad de delitos Informáticos del Ministerio Público., 2002., pp. 3., E-book: http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

[14] ACURIO S., Perfil sobre delitos Informáticos: Generalidades., 2012., pp. 3-68., E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[15] PHIL W., Crimen Organizado y Cibernético, sinergias, tendencias y respuestas., 2006., pp. 2-10., E-book: http://www.pitt.edu/~rcss/toc.html

[16] ACURIO S., Perfil sobre delitos Informáticos: Generalidades., 2009., pp. 34., E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Por lo tanto con la finalidad de precautelar los derechos de las víctimas y llevar a los responsables a juicio, se debería poseer un cuerpo especializado para combatir esta clase de criminalidad, los estados del mundo no debería olvidarse de los graves problemas que ocasionan la violación a la información privada por ende estos delitos deben ser penalizados.

2.2.3. LA INVESTIGACIÓN DIGITAL

La investigación digital consiste en la aplicación de técnicas forenses para extraer datos que sirvan como evidencia digital y para ello utiliza herramientas que permitan asegurar la integridad; por ejemplo, la creación y verificación de la imagen, y la prevención de la modificación de la evidencia original. Se debe tener cuidado con la evidencia, esta debe ser recolectada y guardada de tal forma que no sea alterada por la afectación accidental o intencional. Si la evidencia digital no se maneja adecuadamente, su validez puede ser cuestionada, e incluso anulada.

2.2.3.1. Casos típicos objeto de una investigación digital

Los casos típicos donde un análisis forense digital puede resultar de gran utilidad suelen estar relacionados con conflictos como, por ejemplo [17]:

a. Envío de amenazas, insultos o información confidencial mediante correo electrónico, SMS o publicación en internet
b. Uso malintencionado de los sistemas de la empresa: borrado masivo o sobreescritura de información, sabotaje de los sistemas, modificación no autorizada de páginas web, suplantación de identidad
c. Fraude
d. Conflictos laborales

2.2.3.2. Aspectos a analizar para realizar una investigación digital

Se puede realizar una investigación digital sobre casi cualquier dispositivo o medio que contenga información digital, por ejemplo [18]:

[17] REVISTA Evidentia., Informática Forense., Barcelona – España., 2008., pp. 1-2., E-book: http://www.evidentia.biz/informatica_forense.html

- Páginas web, foros de internet
- Redes sociales (como facebook, tuenti, etc.)
- Correo electrónico
- Ordenadores personales y portátiles
- Teléfonos móviles (dispositivo de estudio en mi investigación), PDA's y smartphones
- Memorias USB, discos duros externos, CDs, DVDs, ...
- Servidores de empresa
- Sistemas de almacenamiento corporativos
- Sistemas de software comerciales o desarrollados propios

2.3. EVIDENCIA DIGITAL

La evidencia digital es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales [19].

2.4. EVIDENCIA DIGITAL EN UN DISPOSITIVO MÓVIL

Los fabricantes de los equipos de telefonía celular normalmente ofrecen un conjunto de características similares para el manejo de información, incluyendo aplicaciones orientadas a la administración de información PIM, mensajería y correo electrónico, así como para el uso de Internet. Estas características pueden variar según el modelo, la versión de firmware que está ejecutándose, modificaciones realizadas por un proveedor de servicios determinado, y cualquier tipo de modificaciones o aplicaciones instaladas por el usuario. De manera general, la evidencia potencial de estos dispositivos incluye [20]:

- Identificadores del suscriptor y equipo
- Fecha – hora, idioma, y otras configuraciones

---

[18] REVISTA Evidentia., Informática Forense., Barcelona–España., 2008., pp. 2-4., E-book: http://www.evidentia.biz/informatica_forense.html

[19] CASEY E., Digital Evidence and Computer crime, Forensic science computers and the Internet., Tercera Edición., San Diego-California., 2011., pp. 12., E-book: http://www.amazon.com/Digital-Evidence-Computer-Crime-Edition/dp/

[20] SANTES L., Análisis Forense para dispositivos de telefonía., México., 2009., pp. 47., E-book: http://tesis.ipn.mx:8080/xmlui/bitstream/handle/123456789/3730

- Información de directorio
- Citas calendarizadas
- Correo electrónico
- Fotos
- Grabaciones de audio y video
- Mensajes multimedia
- Mensajería instantánea y Web
- Documentos electrónicos
- Información de ubicación

Además de los anteriores, existen datos adicionales en un teléfono móvil que pudieran corroborar algunos aspectos de investigación. Por ejemplo, material que pareciera sin importancia tal como tonos de teléfono pudieran tener cierta relevancia, dado que el usuario de un teléfono móvil a menudo agrega tonos particulares para distinguirlos de otros equipos.

Un testigo de algún incidente podría recordar el haber escuchado un tono determinado del dispositivo de un sospechoso, lo cual contribuiría a la identificación de un individuo. Incluso información relacionada con la red encontrada en una tarjeta SIM aportaría datos útiles. Por ejemplo, si una red rechaza una actualización de localización en un teléfono al intentar registrarse, la lista de entradas prohibidas en el archivo elemental PLMNs Prohibidos (Forbidden PLMN) es actualizado con el código del país y la red involucrada [21].

El equipo de cierto usuario que se encuentre bajo sospecha, si viaja a un área vecina puede ser confirmado a través de esta información. Los datos presentes en un dispositivo son dependientes no solo de las características y posibilidades del equipo, sino también de los servicios de voz y datos a los cuales el usuario se encuentra suscrito.

Por ejemplo, el servicio de prepago normalmente no incluye servicios de datos y elimina la posibilidad el uso de mensajes multimedia, correo electrónico y la navegación de Internet.

[21] 3GPP., Specification of the Suscriber Identity Module – Mobile Equipment (SIM-ME) interface., 2005., E-book: http://www.3gpp.org/FTP/Specs/html-info/1111.htm

La Tabla I. muestra una relación de fuentes de evidencia comunes encontradas en equipos de telefonía celular. En muchas instancias, estas fuentes proporcionan datos que pudieran estar involucrados en la investigación, convirtiéndolos en piezas clave para consolidar o refutar las acusaciones sobre el sospechoso.

TABLA I.
Relación entre fuentes de evidencia y objetivos

	¿Quién?	¿Qué?	¿Dónde?	¿Cuándo?	¿Por qué?	¿Cómo?
Id Suscriptor / Dispositivo	x					
Registro de llamadas	x			x		
Directorio telefónico	x					
Calendario	x	x	x	x	x	x
Mensajes	x	x	x	x	x	x
Ubicación			x	x		
Web URL/Contenido	x	x	x	x	x	x
Imágenes/Video	x	x	x	x		x
Contenido de otros archivos	x	x	x	x	x	x

Fuente: Análisis Forense para dispositivos de telefonía celular. Lucio Santes. Diciembre 2008.

La mayoría de las fuentes de evidencia provienen de los datos PIM, datos de llamadas, mensajes e información relacionada con Internet. Algunas otras aplicaciones instaladas en el dispositivo pudieran convertirse en fuentes de evidencia adicionales.

Los archivos de usuario, almacenados en el dispositivo con el fin de realizar diversas operaciones sobre ellos (edición, visualización, etc.), también constituyen una fuente importante de evidencia. Además de los archivos de gráficos, son importantes las grabaciones de audio y video, hojas de cálculo, diapositivas para presentaciones, así como otros documentos electrónicos similares [22].

[22] SANTES L., Análisis Forense para dispositivos de telefonía celular., México., 2009., pp. 31., E-book: http://tesis.ipn.mx:8080/xmlui/bitstream/handle/123456789/3730/PROPUESTAMETODFORENSE.pdf?sequence=1

Los programas instalados, en ciertas circunstancias, también podrían ser importantes. Sin embargo, los datos que podrían considerarse más importantes corresponden a aquellos que puedan vincular al proveedor del servicio.

Estos proveedores almacenan información mediante bases de datos, las cuales utilizan para facturar o realizar cargos a cuentas de usuario basados en los registros de llamadas, estas bases de datos pueden ser consultadas utilizando los datos del suscriptor o mediante los identificadores del equipo.

De forma similar, los mensajes de texto no entregados, los mensajes de voz o multimedia también podrían recuperarse.

2.5. TECNOLOGÍA GSM Y LOS PROBLEMAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES

En los años 80, la industria de teléfonos móviles en Europa comenzó a presentar un crecimiento importante, lo cual trajo como consecuencia la aparición de diferentes estándares en la industria por parte de diferentes fabricantes. Estos sucesos plantearon la necesidad de crear una unificación de tecnologías, para así generar una especificación estándar sobre la cual se pudiera trabajar de manera conjunta y beneficiosa.

Los teléfonos celulares se encuentran expuestos a problemas y amenazas, para conocer en detalle cuales son estos, es necesario conocer de forma general las características y funcionalidades de estos dispositivos, logrando de esta manera diseñar la guía de procedimientos la misma que va a permitir obtener evidencia digital de incidentes ocurridos en teléfonos celulares GSM.
En el mercado existe gran variedad de dispositivos, sin embargo, dado que el enfoque de la investigación en curso está dirigido a los teléfonos móviles GSM, sólo se presentará una breve reseña de dispositivos como BlackBerrys, Pocket PC y Palm Handheld.

2.5.1. BlackBerrys

Los BlackBerrys inicialmente fueron una solución que se dio a la necesidad de interconexión entre personal de empresas para el uso de mensajes instantáneos, voz, e-mail, agenda de contactos, etc., de manera instantánea a través del uso de redes inalámbricas y la característica de portabilidad del dispositivo [23].

En el transcurso de los años, las funcionalidades de estos dispositivos fueron aumentando gracias a los avances tecnológicos crecientes, añadiendo funcionalidades como mapas, GPS, organizador, aplicaciones, juegos, cámara integrada, etc.[24].

Figura 2.1. Blackberry [25]

Entre las características de estos dispositivos entre sus diferentes modelos, se encuentran [26]:

- Bluetooth 2.0
- Media player, MP3/AAC/MPEG4/
- Ranura de expansión de memoria MicroSD
- Pantallas de alta resolución
- Soporte para redes GSM/GPRS y redes EDGE

---

[23] GSM Association., BlackBerrys., Barcelona – España., 2007., pp. 1-2., E-book: http://www.gsmworld.com/news/press_2007/press07_03.shtml

[24] APPLEWHITE A., The BlackBerry Business., Estados Unidos., 2002., E-book: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1012329

[25] TIEMPO DE EQUILIBRIO., BlackBerry., México., 2011., E-book: http://www.tiempodeequilibrio.com/blackberry-despide-a-decenas-de-empleados-en-eu/

[26] BLACKBERRY., Devices., Estados Unidos., 2013., E-book: http://na.blackberry.com/eng/devices/

- Soporte para redes Wireless RIM

2.5.2. Pocket PCs

Estos dispositivos fueron concebidos por empresas como Compaq, HP, entre otros, para suplir necesidades de organización, agenda, conexión inalámbrica redes, correo, y demás funcionalidades estándar de una PDA.

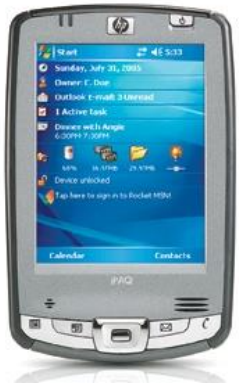


Figura 2.2. Pocket PCs [27]

Entre las características de hardware que estos dispositivos manejan se encuentran:

- Bluetooth
- Reproducción de contenido multimedia
- Ranura de expansión de memoria SD
- Pantallas de alta resolución
- Soporte para redes GSM/GPRS en dispositivos con teléfono integrado.
- Soporte de Wi-Fi en sus diferentes estándares.

2.5.3. Palm Handhelds

Al igual que las Pocket PC, las Palm Handhelds son dispositivos portátiles de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de

[27] PDA Palm y Pocket PC., Revista Ordenadores y portátiles., 2014., E-book: http://www.ordenadores-y-portatiles.com/pda-palm.html

red, ofrece además servicios de información a personas y empresas de manera portátil, dadas sus características de conectividad y estación móvil de trabajo [28].

Figura 2.3. Palm Handhelds [29]

En estos equipos se puede disponer de aplicaciones de oficina, agenda, correo electrónico, navegación por internet, reproductores multimedia, además utilizan sistemas operativos como Palm OS y Windows Mobile, Mac Os, conectividad hacia otros dispositivos por medio de un puerto infrarrojo, Bluetooth o conexión por sincronía hacia una PC por medio de un puerto USB.

2.6. ANÁLISIS FORENSE SOBRE TELÉFONOS CELULARES GSM

La informática forense aplicada a dispositivos móviles es una ciencia que a diferencia de la informática forense clásica, la cual comprende en general todo lo referente a computadoras de escritorio y servidores, es bastante nueva, dado que la popularización de dispositivos móviles, puntualmente GSM con capacidades de comunicación modernas, como Bluetooth y Wi-Fi, ha venido ocurriendo en los últimos años de manera masiva, lo cual ha dado paso a muchos fenómenos, como la portabilidad de la información, vulnerabilidades de seguridad dado el acelerado desarrollo de nuevas versiones de las tecnologías de comunicación en estos

[28] OLVERA C., Tipos de Computadoras, PDA's, Smartphone, Handheld a Detalle. Guanajuato - México., 2010., E-book: http://tiposdecomputadora.wordpress.com/2010/10/27/pdas-smarphone-handheld-a-detalle/
[29] CHRISTENSEN J., Palm Introduces Three Handhelds., Estados Unidos., 2003., E-book: http://multivu.prnewswire.com/mnr/palm/11277/

dispositivos, realización de crímenes a través de esta clase de dispositivos de manera inalámbrica dada su naturaleza, entre otros [30].

Se hace necesario realizar una investigación en este campo que ha sido poco explorado. Esta investigación tiene como objetivo el estudio y análisis de la informática forense en dispositivos móviles GSM, para ampliar los conocimientos que guarda esta ciencia.

El objetivo de la informática forense radica en el mismo objetivo de la informática forense clásica, la cual se basa en la búsqueda y recolección de información en donde un incidente concerniente a esta ciencia ocurra, a través de herramientas tecnológicas especializadas para este fin.

Logrando principalmente que la información recolectada en estos dispositivos se mantenga consistente, es decir, de manera inalterada respecto a la información que estaba presente en el medio involucrado en la investigación, intentando de esta manera, darle un carácter legal valido a dicha información.

2.6.1. Modelos de investigación

Los modelos de investigación forenses en el campo digital, varían tanto en hardware como en software.

2.6.2. Procedimientos y estándares

Los dispositivos móviles GSM, varían de otros sistemas digitales, como por ejemplo, los PC, tanto en su configuración de hardware, como en su sistema operativo y el tipo de aplicaciones que manejan.

Según [29] [42], investigadores de la Fuerza Aérea de Estados Unidos identificaron las características comunes en varios procesos de modelos e incorporaron otros en

---

[30] ARIZA A., Análisis forense orientado para dispositivos móviles inteligentes., Bogotá – Colombia., 2009., pp. 64., E-book: http://pegasus.javeriana.edu.co/~CIS0910SD01/Documentos/TG_IPHORENSICS_corto.pdf

un modelo de procesos abstracto. Este modelo consta de 9 componentes, que conducen una investigación forense [31]:

- **Identificación:** Consiste en reconocer y determinar el tipo de incidente.

- **Preparación:** En este paso se preparan las herramientas, técnicas, se buscan garantías, autorizaciones y la aprobación de los superiores para realizar la investigación.

- **Estrategia de acercamiento:** Consiste en maximizar la recolección de la evidencia minimizando el impacto en la victima.

- **Preservación:** En esta fase se asegura el aislamiento, seguridad y preservación del estado de la evidencia física y digital.

- **Recolección:** Consiste en registrar la escena física y duplicar la evidencia digital.

- **Examinación:** En esta fase se busca evidencia sospechosa relacionada con el crimen cometido.

- **Análisis:** Esta fase consiste en determinar el significado de la evidencia recolectada, reconstruir fragmentos de datos y obtener conclusiones sobre la evidencia encontrada.

- **Presentación:** Consiste en resumir y proveer una explicación de las conclusiones obtenidas.
- **Devolver la evidencia:** Se debe asegurar que la propiedad física y digital sea devuelta a su propietario

[31] MARK Reith., An Examination of Digital Forensic Models., Vol. 1., 2002., California–Estados Unidos., E-book: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

De la diversidad de modelos que existe y de los que se debe seguir se propone una guía de procedimientos para realizar análisis forenses orientados a incidentes en dispositivos móviles GSM, la misma que incluye cuatro fases para realizar el proceso de análisis forense a equipos de telefonía celular, basado en los principios que rige el análisis forense clásico. Esta guía de procedimientos está orientada a ser empleada en aquellos incidentes en los que se requiera obtener evidencia digital de un equipo de telefonía celular que estuviera involucrado, estas fases son:

- Fase Preliminar
- Fase de Recolección de Información
- Fase de Análisis
- Reporte

2.6.2.1. Fase Preliminar

Dentro de esta fase se propone realizar las siguientes tareas:

- ✓ Identificación del problema
- ✓ Etapa de preparación
- ✓ Investigación preliminar del Problema
- ✓ Aseguramiento de la escena
- ✓ Exploración y reconocimiento
- ✓ Protección de las comunicaciones
- ✓ Recolección y preservación física

2.6.2.2. Fase de Recolección de Información de la evidencia

El objetivo de ésta fase es localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales no han sido alterados. Esta fase se relaciona con la primera parte de esta sección la cual habla de los principios que se deben tener en cuenta para manipular evidencia digital.

Dentro de esta etapa se definen las siguientes sub-etapas:

- ✓ Recolección de evidencia digital

- ✓ Determinación de las herramientas forenses a utilizar
- ✓ Aplicación de la cadena de custodia a la evidencia recolectada

2.6.2.3. Fase de Análisis de la evidencia

Esta fase consiste en realizar el ensamble, análisis y articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis.

Dentro de esta etapa se definen las siguientes sub-etapas:

- ✓ Inspección de la información recuperada
- ✓ Identificación del autor o autores del incidente

2.6.2.4. Reporte y Presentación

El objetivo de ésta fase consiste en generar toda la documentación concerniente a los hallazgos, resultados, actividades, cadena de custodia de la evidencia y, en general, de todo lo realizado en el proceso de investigación.

Dentro de esta etapa se definen las siguientes sub-etapas:

- ✓ Revisión del proceso forense
- ✓ Elaboración de un informe o documento de la investigación forense realizada

2.6.3. Herramientas forenses para teléfonos celulares GSM

La situación con las herramientas forenses para teléfonos celulares es considerablemente diferente a la relacionada con las computadoras personales. Mientras que las que son para computadores personales son diseñadas para sistemas de propósito general, las que son para teléfonos celulares son diseñadas, generalmente, para propósitos específicos las cuales realizan un conjunto de tareas predefinidas. La razón de esto radica en que mientras las computadoras personales, generalmente, utilizan un sistema operativo más estandarizado, los

fabricantes de teléfonos celulares prefieren, en su mayoría, utilizar sistemas operativos propietarios.

Es por lo anterior que existen en la actualidad una gran variedad de herramientas forenses, por las distintas plataformas del fabricante, por la familia del sistema operativo o por el tipo de arquitectura del hardware del dispositivo. Sin embargo, dichas herramientas son difíciles de utilizar ya que, si no son confidenciales, su código fuente no es abierto y no existe documentación de su funcionamiento interno.

Por otro lado, la herramienta exige que el investigador tenga completo acceso al dispositivo, es decir, que el dispositivo no esté protegido por ningún mecanismo de autenticación.

Debido a los cortos ciclos de lanzamiento de nuevos dispositivos de los fabricantes de teléfonos celulares, los productores de las herramientas forenses deben actualizar continuamente sus productos para mantenerlos vigentes; sin embargo, esto no ocurre siempre y varias veces el soporte para los nuevos modelos de dispositivos se demoran significativamente.

Las herramientas forenses, en general, pueden adquirir datos de un dispositivo de dos maneras diferentes:

1. **Adquisición física:** Implica copiar bit a bit el almacenamiento físico entero, por ejemplo, un chip de memoria. Este procedimiento se puede realizar tanto con herramientas de software como mediante métodos más avanzados como el acceso físico a la memoria flash.

2. **Adquisición lógica:** Implica copiar bit a bit el almacenamiento lógico de los objetos, por ejemplo directorios y archivos, que residen en el almacenamiento lógico del dispositivo, por ejemplo una partición del sistema de archivos.

Las imágenes obtenidas de los archivos, ya sean físicas o lógicas, deben ser comprendidas, decodificadas y traducidas para obtener los datos. Este trabajo consume mucho tiempo si se realiza manualmente. Imágenes físicas de los

dispositivos pueden ser importadas en una herramienta para su examen automático el cual genera un reporte con estos datos.

2.7. HERRAMIENTAS PARA REALIZAR EL ANÁLISIS FORENSE DE SIM Y GSMS

La mayoría de las herramientas de software de análisis forense para teléfonos celulares adquieren los datos de modo lógico porque los datos adquiridos comúnmente se encuentran codificados de manera poco convencional, como texto representado en 7-bits del alfabeto GSM; una vez decodificado se facilita la interpretación. En ocasiones la información encontrada está codificada en código binario, como los códigos de país o el proveedor de servicio, y puede ser traducida y procesada usando una base de datos [32].

Los tipos de software utilizados para realizar el análisis forense incluyen software comercial, programas de fuente abierta (open-source), herramientas de diagnóstico y hasta herramientas que pueden ser consideradas para realizar un tipo de hacking.

Dentro del software comercial se encuentran herramientas que no son para el uso forense, es decir, cualquier persona tiene acceso a ellos para transferir archivos; para utilizarlos en un análisis se debe tener mucho cuidado para no alterar la evidencia digital.

Una forma de no alterar la evidencia es utilizando un monitor de puertos que monitorea la comunicación del dispositivo móvil con la computadora; este software puede bloquear los intentos de escritura sobre el dispositivo móvil además de crear filtros si es necesario, haciendo confiable el análisis y la extracción de información.

El software utilizado en el análisis forense puede manejar diferentes tipos de interfaces, como bluetooth, infrarrojo o cable serial. La adquisición por medio de cable serial es la manera más confiable ya que se puede evitar la escritura sobre el

[32] LÓPEZ M., Análisis forense digital. Segunda Edición., 2007., E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

dispositivo y no requiere una contraseña como con algunas configuraciones de bluetooth.

Algunas de estas herramientas utilizadas para el análisis forense en telefonía celular son:

- **TULP2G.**

  Es una herramienta sólo para plataformas Windows y para poder funcionar requiere .NET 2.0. fue desarrollada por Netherlands Forensic Institute (NIS) y se encuentra implementada en C#. Es considerada como una herramienta forense que no automatiza todo el proceso de análisis forense. El beneficio que ofrece esta herramienta es la de poder extraer datos de equipos móviles así como en la tarjeta SIM [33].

- **Mobiledit Forensic.**

  Es una herramienta forense desarrollada por Laboratorios Compelson. Su origen proviene de una aplicación diseñada para funcionar como administrador de equipos móviles. Es una herramienta que permite la extracción de datos y puede trabajar con varios modelos de telefonía celular. Permite extraer datos de la tarjeta SIM como datos del equipo móvil [34].

- **Device Seizure.**

  Desarrollada por la empresa Paraben Forensics. La herramienta tiene la capacidad de extraer datos contenidos en dispositivos de telefonía móvil sin afectar la integridad de los datos. Entre los datos que puede extraer se encuentran los números telefónicos, fechas, tiempos, fotos, registro de llamadas, etc. Fue diseñado tomando en cuenta las marcas más comunes de teléfonos Nokia, Siemens, Motorola y Sony Ericson. Esta herramienta produce informes en formatos. La salida verifica usando funciones MD5 [35].

---

[33] TULP2G., Forensic framework for extracting and decoding data., 2007., E-book: http://tulp2g.sourceforge.net/

[34] MOBILEDIT! FORENSIC., San Francisco – Estados Unidos., 2009., E-book: http://www.mobiledit.com

[35] PARABEN CORPORATION., Mobile Forensics., 2013., E-book: http://www.paraben-forensics.com/catalog/product_info.php?products_id=342

2.8. ANÁLISIS COMPARATIVO DE LAS HERRAMIENTAS MÁS UTILIZADAS PARA REALIZAR ANÁLISIS FORENSE

Las herramientas forenses están destinadas a facilitar el trabajo de los investigadores forenses, como es la adquisición y análisis de forma oportuna y estructurada de la información del equipo móvil. Pero hay que considerar que cada teléfono posee diversas características en relación a su fabricante, lo cual dificulta la adquisición de estos datos; puesto que cada fabricante de herramientas forenses mantiene una lista de teléfonos y características compatibles con su software, ocasionando que la recuperación de los datos se lo realice con herramientas especializadas, todo dependerá del modelo y características del equipo que deberá ser compatible con la herramienta, lo cual involucra costos en la herramienta a adquirir para efectuar el análisis forense.

Por lo tanto el investigador forense al iniciar su trabajo para la adquisición de datos sobre el equipo móvil determinará que teléfonos soportan las herramientas, características de los equipos móviles y el costo que implica la adquisición de las mismas.

La Tabla II muestra las características y el valor representativo que tiene la evidencia digital, parámetros utilizados dentro de la guía de procedimientos a desarrollar dentro de esta investigación.

TABLA II
Características de los datos/ valor evidencia digital

	CARACTERÍSTICAS	DESCRIPCIÓN	VALOR
1	**Fabricante**	La herramienta puede presentar el nombre del fabricante del teléfono celular	2
2	**Modelo**	La herramienta puede presentar el nombre del modelo de teléfono móvil.	2
3	**IMEI**	La herramienta presenta el número de serie de un teléfono móvil.	2
4	**ESN**	La herramienta presenta el número Serial Electrónico del teléfono móvil que es compatible con CDMA	2
5	**IMSI**	La herramienta presenta el número de serie de una tarjeta SIM	2
6	**Phonebookmem**	La herramienta presenta la agenda que reside en la memoria interna del teléfono móvil.	2
7	**Lastdialedmem**	La herramienta presenta los últimos números marcados en la memoria del teléfono móvil.	2
8	**Receivedmem**	La herramienta presenta llamadas recibidas desde la memoria del teléfono móvil.	2
9	**Archivos**	La herramienta presenta una vista jerárquica del contenido del sistema de ficheros del teléfono.	2
10	**Eventos**	La herramienta presenta una vista jerárquica del contenido de eventos de teléfono.	2
11	**Tareas**	La herramienta presenta una vista jerárquica del contenido de las tareas telefónicas.	2
12	**Hex Dump/ Extracción lógica**	La herramienta puede realizar una extracción lógica o volcado de memoria.	2
13	**Captura de datos básicos**	La herramienta puede capturar del usuario: IMSI, ICCID	2
14	**Conectividad y recuperación**	La herramienta puede conectarse correctamente al dispositivo y recuperar el contenido del mismo.	2
15	**Llamadas marcadas / recibidas**	La herramienta encuentra llamadas telefónicas marcadas, recibidas y perdidas	2
16	**Análisis de mensajes**	La herramienta encuentra los SMS/MMS realizados, recibidos	2
17	**Análisis de contactos**	La herramienta presenta lista de contactos.	2
18	**Tarjetas de memoria**	La herramienta puede adquirir, identificar y evaluar archivos almacenados en una tarjeta de memoria insertada en el dispositivo.	2
19	**Análisis de backups**	La herramienta realiza backups para su posterior análisis.	2
20	**Formato de archivos de texto, gráficos y archivos comprimidos**	La herramienta puede buscar y mostrar una recopilación de archivos de texto, gráficos y archivos comprimidos, que residen en el teléfono	2
21	**Pérdidas de energía**	La herramienta puede adquirir información del dispositivo después de que haya perdido su energía, mientras esté conectado vía cable o se cambie de bateria	2
22	**Información de geolocalización**	La herramienta puede recuperar información como LOCI y LOCIGPRS en la tarjeta SIM.	2
23	**Generación de informes**	La herramienta genera reportes en formato: .xml, .xls, .rtf, html.	2

Fuente: Maleza Jorge

En la tabla III se muestra la evaluación realizada con las herramientas forenses que permiten la extracción de evidencia digital, de acuerdo a los parámetros establecidos en este tema de investigación.

TABLA III
Características para obtención de evidencia mediante herramientas forenses

	Oxigen Forensic Suit	BitPim	Cellebrite	Zdiarski Techniqu	ParabenDevice Seizure	TULP2G	Mobiledit
Fabricante	*	*	*	*	*	*	*
Modelo	*		*	*	*	*	*
IMEI	*	*	*	*	*	*	*
ESN							*
IMSI							*
Phonebookmem	*		*	*	*	*	*
Lastdialedmem	*		*	*	*	*	*
Receivedmem	*		*	*	*	*	*
Archivos	*						*
Eventos	*						*
Tareas	*						*
Hex Dump/ Extracción lógica	*						*
Captura de datos básicos	*				*		*
Conectividad y recuperación	*				*		*
Llamadas marcadas / recibidas	*	*	*	*	*	*	*
Análisis de mensajes	*	*	*	*	*	*	*
Análisis de contactos	*		*	*	*	*	*
Tarjetas de memoria	*				*	*	*
Análisis de backups							*
Formato de archivos de texto, gráficos y archivos comprimidos	*				*		*
Pérdidas de energía							*
Información de geolocalización							*
Generación de informes	*	*	*	*	*	*	*
TOTAL	36	10	20	20	28	22	46

Fuente: Maleza Jorge

*: valor de 2, asignado a las características de la evidencia digital que puede ser extraída de un equipo móvil (celular)

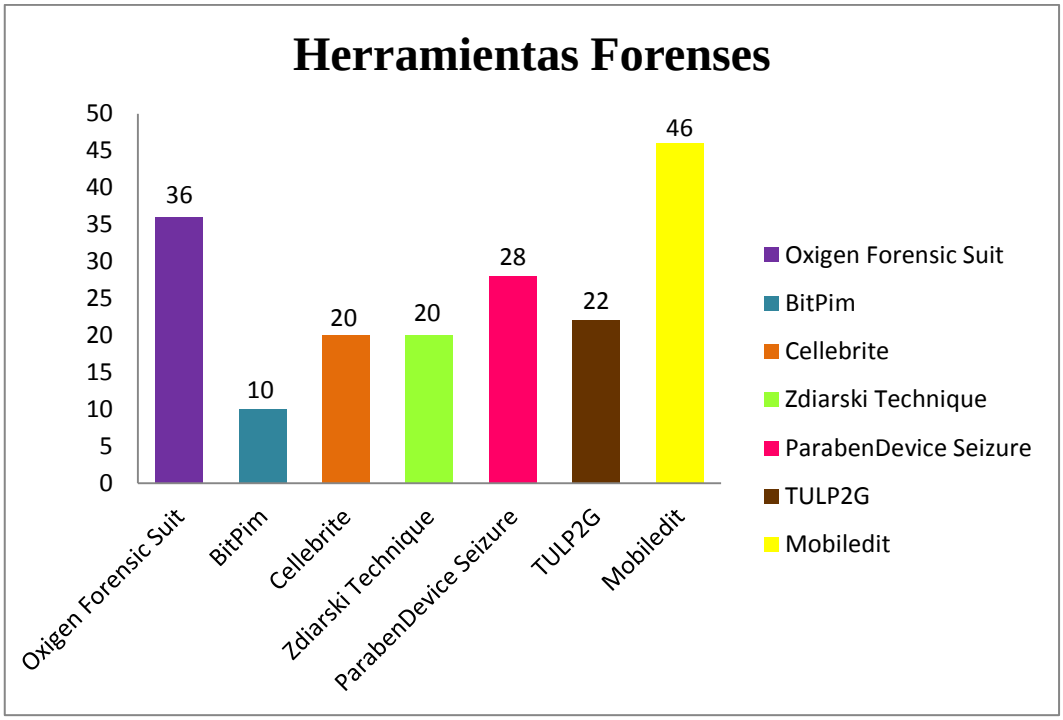


Figura 2.4. Análisis comparativo herramientas forenses

Resumen: La Tabla III muestra herramientas forenses utilizadas en el campo de la forensia digital. Las herramientas: Mobiledit, Oxigen Forensic Suit y Paraben Device Seizure presentan mayor porcentaje y serán utilizadas en esta investigación, como se puede visualizar en la figura 2.4, herramientas que soportan la mayor parte de parámetros establecidos en la Tabla II para la extracción de evidencia digital.

2.9. LIMITACIONES PARA PRACTICAR ANÁLISIS FORENSE EN TELÉFONOS CELULARES

La aplicación de técnicas de computación forense en teléfonos celulares es un área que está creciendo rápidamente en la actualidad. Durante los últimos años, las funcionalidades de los teléfonos celulares se han venido incrementando, tanto en desempeño como en variedad, aumento en la capacidad de almacenamiento, nuevas aplicaciones que permiten el manejo de documentos y multimedia.

Además del avance tecnológico de los teléfonos celulares en la actualidad, dichos dispositivos tienen una característica que los diferencia de los computadores de

escritorio convencionales: Emplean una gran variedad de sistemas operativos propietarios y estructuras de almacenamiento de datos. Lo anterior representa una limitación para realizar análisis forense en los dispositivos debido a que las herramientas que realizan dichos procedimientos usan protocolos de sincronización, de interfaz de comandos y de diagnósticos, todos propietarios de cada fabricante.

Adicionalmente, el número de modelos de teléfonos celulares que son lanzados en el mercado mundial cada año es considerable, dificultando el área de la informática forense aplicada en teléfonos celulares.

Lo expuesto es una limitación debido a que los nuevos teléfonos celulares incluyen frecuentemente nuevas funcionalidades que los diferencian de los modelos anteriores, lo cual hace necesario actualizar las herramientas forenses para que soporten las nuevas características y puedan tomarlas en cuenta para recuperar y reportar los datos correctamente.

Cuando un teléfono nuevo aparece, el fabricante de la herramienta debe decidir si adapta su producto al nuevo teléfono celular. Para ello es necesario comprar ejemplares para su estudio, crear las actualizaciones correspondientes para la herramienta y finalmente distribuir la actualización entre los usuarios.

Lo anterior representa tiempo, dinero y esfuerzo por parte de la compañía fabricante y es por esto que cada vez es más complicado obtener herramientas forenses para teléfonos celulares al día con los teléfonos celulares más recientes en el mercado.

2.10. CONCEPTUALIZACIONES

2.10.1. Los Delitos Informáticos. Son aquellos actos delictivos que en su realización hacen uso de las tecnologías electrónicas ya sea como método, medio o fin y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos [36].

---

[36] HUILCAPI A., El delito informático., 2011., Quito-Ecuador., E-book: http://www.slideshare.net/JorgeFernandoCruz/el-delito-informtico

2.10.2. El objetivo de la Informática Forense. 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 [37].

2.10.3. Aspectos de la informática forense. Posee aspectos positivos y negativos tales como [38]:

Positivos: Replantean y validan: procesos forenses, herramientas forenses y habilidades.

Negativos: Pueden exonerar a un culpable, pueden inculpar a un inocente, afectar al proceso forense.

2.10.4. Principios forenses

Existe un número de principios básicos que son necesarios al examinar un computador o un cadáver. Estos principios son [39]:

- Evitar la contaminación
- Actuar metódicamente
- Controlar la cadena de evidencia, es decir, conocer quien, cuando y donde ha manipulado la evidencia

Evitar la contaminación. En televisión salen los examinadores forenses ataviados con batas blancas y guantes, cogiendo todas las pruebas con pinzas y poniéndolas en bolsa de plástico selladas. Todo ello es para prevenir la "contaminación". Aquí es donde las evidencias se pueden echar a perder, por ejemplo, si alguien coge un cuchillo y deja sus huellas digitales en la hoja del cuchillo.

Actuar metódicamente. En cualquier cosa que se haga, si tuvieras que ir a un juicio, necesitarías justificar todas las acciones que hayas tomado. Si actúas de una

[37] ACURIO S., Introducción a la Informática Forense., 2008., pp. 33., E-book: http://www.egov.ufsc.br/portal/sites/default/files/9.pdf

[38] DELGADO C., Análisis Anti-Forense., 2004., pp. 1-14., E-book: http://dspace.ups.edu.ec/bitstream/123456789/546/2/CAPITULO1.pdf

[39] VILLACÍS M., Características y principios de la informática forense., 2011., pp. 1-7., E-book: https://docs.google.com/document/d/1hiIZdtTFPlz5c5940iCSL0N8bTa8ncJzGVzGw1w8PnA/edit

manera científica y metódica, tomando cuidadosas notas de todo lo que haces y cómo lo haces, esta justificación es mucho más fácil. También permite a cualquier otra persona poder seguir tus pasos y verificar que tú no has cometido ningún error que pueda poner en duda el valor de tu evidencia.

Cadena de Evidencias. Siempre se debe mantener lo que se denomina la “Cadena de Evidencias”. Esto Significa que, en cualquier momento del tiempo, desde la detección de la evidencia hasta la presentación final en el juicio, puedes justificar quién ha tenido acceso y dónde ha sido. Esto elimina la posibilidad de que alguien haya podido sabotearlo o falsificarlo de alguna manera.

2.11. EVIDENCIA DIGITAL

La evidencia digital puede definirse como "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio 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 [40].

La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad [41]:

a) Volátil
b) Anónima
c) Posible duplicarla
d) Alterable y modificable
e) Susceptible de ser eliminada

[40] VILLAMIZAR C., Delitos Informáticos., Colombia., 2013., E-book: https://www.delitosinformaticos.com/01/2013/paises-delitos-informaticos/delitos-informaticos-colombia/vision-de-delitos-informaticos-en-colombia#.Uq4p8-Qszec

[41] CARPIO P., Evidencia digital., 2011., E-book: http://repositorio.utn.edu.ec/bitstream/123456789/539/7/04%20ISC%20157%20CAPITULO%20II.pdf

2.12. DIFICULTADES DEL INVESTIGADOR FORENSE

El investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes [42]:

1. Carencia de software especializado para buscar la información en varios.
2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.
3. Será difícil encontrar toda la información valiosa.
4. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.
5. Los errores cometidos pueden costar caro para la persona o la organización que representa.
6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.
7. Falta de experiencia para mostrar, reportar y documentar un incidente.
8. Dificultad para conducir la investigación de manera objetiva.

[42] VIRTUALCLASS., Dificultades del Investigador Forense., 2011., E-book: http://problemasconlatecnologia.blogspot.com/2011/03/if-dificultades-del-investigador.html.

CAPITULO III
MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN

Los tipos de investigación utilizados en el desarrollo de la tesis son: Descriptiva y Experimental.

Investigación Descriptiva.- La investigación descriptiva, trabaja sobre realidades de hecho y su característica fundamental es la de presentar una interpretación correcta.

La informática forense poco a poco ha ido evolucionado gracias a los aportes realizados por entidades que cada cierto tiempo formulan modelos o metodologías para la mejora en las fases que la componen. La importancia de la investigación en este tema de tesis se fundamenta en el interés de aportar en el tema relacionado con análisis forense en telefonía celular, investigando características de la telefonía celulares, métodos y técnicas empleadas por la ciencia forense por descubrir y brindar la información necesaria y útil que pueda ser utilizada en aspectos legales y judiciales; gracias a este tipo de investigación se ha logrado construir la guía de procedimientos.

Investigación Experimental.- La investigación de enfoque experimental consiste en hacer un cambio en el valor de una variable (variable independiente) y observar su efecto en otra variable (variable dependiente).

Una vez construida la guía de procedimientos y aplicando cada una de las fases que posee esta guía a teléfonos celulares de tecnología GSM se ha podido recuperar evidencia en formato digital tanto de mensajes SMS, imágenes guardadas en el equipo, llamadas entrantes y salientes, y que en el caso de ser

presentados en materia del código penal como pruebas, como evidencia en caso de haberse efectuado un fraude. Los teléfonos celulares analizados son:

- Nokia N95 8GB
- Nokia E6
- Nokia C2
- LG KP520
- Samsung Star S5230
- Samsung DUOS
- Samsung GT S 5830
- Samsung Galaxy Ace s5830i
- Samsung GT – S5302
- Sony Ericsson W395
- Sony Ericsson W810i
- Sony Ericsson K550i
- Sony Xperia E10a
- Sony Ericsson 580i
- Sony Ericsson W200
- Celular BLU

Pero se debe tener en cuenta que no todo celular puede ser analizado, ya que no todos los modelos de teléfonos celulares poseen la misma arquitectura, por ende no permitirán la recuperación de mensajes, imágenes, llamadas.

3.2. DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación utilizada en la tesis es experimental.

Investigación Experimental.- En una investigación experimental, se lleva a cabo experimentos con la finalidad de analizar si una o más variables independientes afectan a una o más variables dependientes y por qué lo hacen.

Por lo tanto aplicando la guía de procedimientos que es la variable independiente y siguiendo cada una de las fases que se establecen en esta guía se ha podido recuperar información la misma que puede ser utilizada como evidencia, este experimento se lo ha realizado a 50 celulares con tecnología GSM.

3.3. MÉTODOS

Los métodos utilizados en el desarrollo de la tesis son los métodos:

- Método científico, y
- Método inductivo

Método Científico es una serie ordenada de pasos a seguir para la resolución de un problema determinado.

El Método Científico consta de varios pasos, estos pasos se describen a continuación:

a. Observación.

Los dispositivos móviles son capaces de almacenar información digital.

b. Problema

¿Cómo recuperar la información digital?

c. Hipótesis

Incidentes ocurridos a través de teléfonos celulares GSM las herramientas de análisis forense permite analizar los teléfonos vía Bluetooth, IrDA o cable de conexión, analiza la agenda, los últimos números marcados, llamadas perdidas, llamadas recibidas, mensajes SMS.

d. Experimentación

Para demostrar que se puede recuperar la información de los teléfonos celulares se sigue cada una de las fases que se establece en la guía de procedimientos como es: identificación del problema, recolección de la

evidencia digital, análisis forense de la información recuperada, creación de un reporte describiendo los datos. Se analizó varios teléfonos celulares con tecnología GSM. Siguiendo cada una de las etapas de la guía de procedimientos se analiza el teléfono celular Sony Ericsson W580i, mediante puerto BluetoothMS, se realiza en una de las fases el backup de la información que posee el teléfono celular para no modificar la información como es mensajes SMS, Contactos, llamadas; aplicando las herramientas forenses como Mobiledit Forensics, y Device Seizure se procede con el análisis de la información, la información no es totalmente recuperada, se emite un informe con la información recuperada que es proporcionada por las herramientas forenses; esta información puede ser utilizada como evidencia en el caso de haber ocurrido algún tipo de fraude.

Método Inductivo.- El método inductivo es aquel método científico que obtiene conclusiones generales a partir de premisas particulares.

Una vez realizada la investigación sobre los conceptos fundamentales, analizadas las herramientas y procedimientos de la informática forense se pudo construir la guía de procedimientos propuesta en esta tesis.

Esta Guía de Procedimientos está integrada por 4 fases dentro de cada fase se realiza actividades, siguiendo cada una de ellas se logra recopilar la información básica necesaria para poder establecerla como evidencia en caso de presentarse algún incidente en un dispositivo celular GSM.

Con la guía de procedimientos se puede analizar la información, previo a este análisis y para no alterar la evidencia se prepara una copia de la evidencia digital, se examina la copia obtenida con la finalidad de recuperar la información, se analiza la información recuperada, y se crea un reporte describiendo los datos recuperados en todo el procedimiento de análisis.

3.4. TÉCNICAS

Las técnicas empleadas en el tema de tesis es la técnica documental, se ha procedido a la revisión documentos, observación mediante las pruebas realizadas, con estas técnicas se ha podido recopilar la información necesaria para poder construir la guía de procedimientos que plantea este tema de tesis, y con las fases que posee esta guía obtener la evidencia necesaria en caso de ocurrir fraudes (incidente).

La guía de procedimientos construida en base a estándares analizados en la informática forense ha permitido establecer las siguientes fases:

- Identificación del problema
- Recolección de la evidencia digital
- Análisis forense de la información recuperada
- Creación de reporte de la descripción de datos recuperados

3.5. HERRAMIENTAS

Los teléfonos móviles contienen algunas de las pruebas más importantes en las investigaciones policiales y judiciales, las fuerzas de seguridad en todo el planeta precisan todas las ventajas probables para apoyar a solucionar crímenes o fraudes.

Por lo tanto para poder registrar información y que la misma sea tratada como evidencia frente a evento delictivos es fundamental y como parte del desarrollo aplicar y seguir una metodología, ya que para obtener estas evidencias es necesario seguir estándares, junto a ello se debe utilizar herramientas, por ende las herramientas usadas en el desarrollo de la tesis y que forman parte del desarrollo de la guía de procedimientos propuesta se presentan a continuación:

3.5.1. MOBILEDIT FORENSICS

Características. Es un programa utilizado para la gestión de teléfonos móviles al PC a través de Bluetooth, infrarrojos o cable.

- Permite hacer un análisis forense diferenciado del SIM. Con este toolkit se analizó el teléfono celular Sony Ericsson W580i, y más modelos y marcas de teléfonos celulares
- Una vez que se efectúa la conexión, la herramienta muestra las principales características del teléfono: IMEI, revisión de Hardware, revisión de Software, red (GSM, para el caso de análisis), resolución de la pantalla, nivel de la batería y nivel de la señal.
- Las principales evidencias digitales a analizar por parte de la herramienta son: el directorio telefónico, gestión de SMS (incluye inbox, items enviados), calendario, notas, tareas.
- Adicionalmente la herramienta permite exportar cualquier archivo o dato del teléfono.
- Finalmente se tuvo una dificultad, esta fue la generación de reportes en diferentes formatos, sólo se pueden realizar si se compra el toolkit.

3.5.2. PARABEN FORENSIC SOFTWARE - DEVICE SEIZURE

Permite hacer análisis forense a dispositivos móviles. El análisis se organiza por casos.

Con este toolkit se analizó el teléfono celular Sony Ericsson W580i, obteniéndose información del mismo. La información es organizada en múltiples logs. Las características en este análisis forense, a recuperar son: archivos de usuario dentro del móvil: directorio telefónico, SMS, archivos de sonido, archivos de aplicaciones, etc.

3.5.3. OXIGEN FORENSIC SUITE

Para realizar el análisis forense con esta herramienta, debemos encender el dispositivo (equipo celular) y conectarlo al equipo (computador). Se ha conectado el teléfono celular Sony Ericsson W580i, y accedemos para la extracción de evidencia a través del asistente '*Tools / Oxygen Connection Wizard'*. La información recuperada fue: directorio telefónico, mensajes, etc.

3.6. VALIDACIÓN DE LAS HERRAMIENTAS

Dado la dificultad que implica el análisis forense a un dispositivo móvil, las herramientas utilizadas en el desarrollo de la tesis son: Mobiledit, Oxigen Forensic Suite y Paraben Forensic Software - Device Seizure, estas herramientas han sido empleadas ya que abarca diversos dispositivos de diferentes fabricantes y numerosos modelos, lo contrario a otras herramientas que limitan a ciertos modelos y marcas de teléfonos celulares.

Estas herramientas son comerciales, pese a los problemas de licenciamientos en versión trial las herramientas permiten recuperar la siguiente información útil y requerida para realizar un análisis forense:

- Fecha, hora y recurso que se accedió
- Registro de los parámetros de la petición realizadas.
- Comprobación de integridad (lo hace con MD5 y SHA1).
- Permite recuperar archivos de usuario dentro del móvil: directorio telefónico, SMS, archivos de sonido, archivos de aplicaciones, etc.

3.7. POBLACIÓN Y MUESTRA

Conjunto de mediciones que son de interés, la cual se efectúa sobre una característica común de un grupo de seres o conjuntos de objetos.

La población a analizar son los teléfonos celulares con tecnología GSM.

Muestra: Colección de mediciones seleccionadas de una población de interés.

La cantidad de teléfonos analizar son 50, los mismos que se muestran a continuación; y se ha considerado solamente este tipo de teléfonos por la facilidad de prestación que se tuvo al momento de realizar el análisis forense. Es decir esto representa una muestra no aleatoria, escogida de acuerdo a los siguientes criterios de selección como es sistema operativo, marca, modelo, tipo de cable que utiliza, modo de conexión del equipo móvil, aplicaciones instaladas en el equipo.

- Nokia N95 8GB

- Nokia E6
- Nokia C2
- LG KP520
- Samsung Star S5230
- Samsung DUOS
- Samsung GT S 5830
- Samsung Galaxy Ace s5830i
- Samsung GT – S5302
- Sony Ericsson W395
- Sony Ericsson W810i
- Sony Ericsson K550i
- Sony Xperia E10a
- Sony Ericsson 580i
- Sony Ericsson W200
- Celular BLU

De estos teléfonos se podrá analizar agenda, los últimos números marcados, llamadas perdidas, llamadas recibidas, mensajes SMS, mensajes multimedia, fotos, archivos, detalles básicos del teléfono.

3.8. OPERACIONALIZACIÓN DE VARIABLES

TABLA IV.
Operacionalización de variables

VARIABLES	CATEGORÍA	INDICADORES	TÉCNICA	FUENTE/INSTRUMENTO
Independiente: Guía de procedimientos para el manejo de incidentes en dispositivos móviles mediante análisis forense.	Porcentaje de información recuperada	1. Fases 2. Formularios 3. Cadena de custodia	• Observación • Revisión de documentos	• Investigación bibliográfica • Internet
Dependiente: Obtención de evidencia		**I1:** Porcentaje de mensajes SMS de información recuperada. **I2:** Porcentaje de contactos de información recuperada. **I3:** Porcentaje de llamadas de información recuperada. **I4:** Porcentaje de tipos de reportes de información recuperada.	• Observación • Pruebas	Herramientas forenses utilizadas: • MobilEdit Forensic • Oxigen Forensic Suite • Paraben Forensic software - Device Seizure • Ambiente de prueba

3.9. AMBIENTE DE PRUEBA

Para la validación de la propuesta denominada Guía de procedimientos para el manejo de incidentes en dispositivos móviles mediante análisis forense, se utilizó el siguiente escenario:

Escenario:

Incautación de equipos celulares a personas que se dedican a la compra y venta de dispositivos móviles de dudosa procedencia (escenario ficticio para la puesta en marcha de la guía de procedimientos planteada). Para la adquisición de evidencia digital frente a este incidente se deberá poseer el hardware y software básico para la adquisición de evidencia digital: teléfonos celulares, computador, adaptador USB, herramientas forenses instaladas en el equipo portátil, examinador forense.

Figura 3.1. Escenario Parque San Francisco de Riobamba

Figura 3.2. Adquisición evidencia digital

CAPITULO IV
RESULTADOS Y DISCUSIÓN

Ante el manejo de evidencias sobre un crimen o delito informático cometido, se debe actuar como en cualquier proceso criminal, como primer paso de la guía de procedimientos que se desarrolla como tema de investigación es asegurar la escena del delito restringiendo el acceso a la misma para no modificar la evidencia.

Debido a que el análisis forense presenta carencias en cuanto a la asignación de recursos como es tecnología, y al no existir especialistas se hace difícil el tener y poder utilizar procedimientos adecuados que lleven a la toma de decisiones al momento de enfrentarse con una investigación forense en nuestro entorno.

Por lo tanto la investigación efectuada en esta tesis permitirá y servirá de guía para la adquisición y manejo de la evidencia digital.

A continuación se presenta un esquema general de las fases que tiene la Guía de Procedimientos planteada como tema de tesis:

4.1. VARIABLE INDEPENDIENTE: GUÍA DE PROCEDIMIENTOS PARA OBTENCIÓN DE EVIDENCIA DIGITAL

La variable independiente es la Guía de procedimientos para el análisis forense orientado a incidentes en dispositivos móviles GSM, la misma que se presenta a continuación:

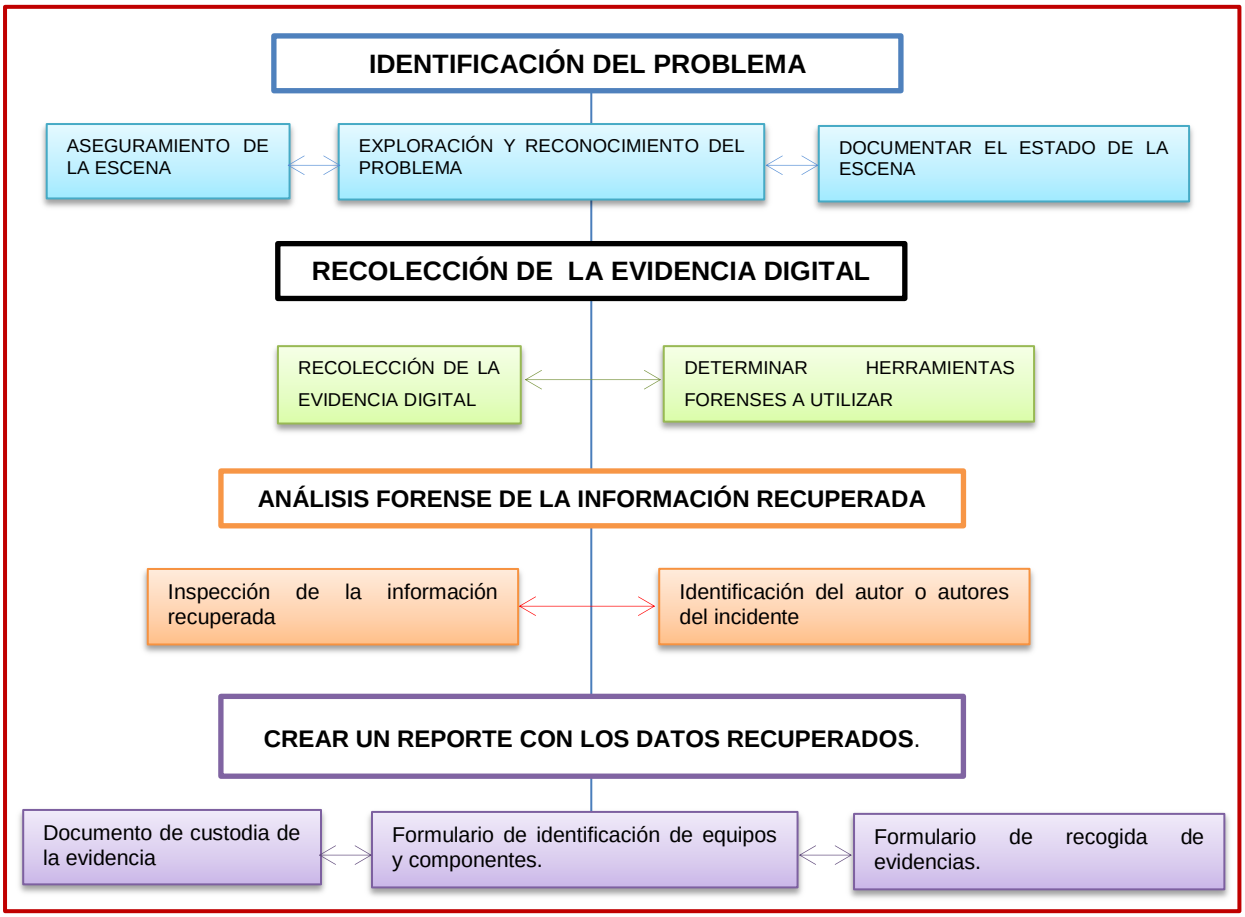


Figura 4.1. Guía de procedimientos

La Guía de procedimientos propuesta para el Análisis Forense Orientado a Incidentes en dispositivos móviles GSM, planteada como tema de investigación se divide en cuatro fases principales: Identificación del problema, Recolección de la evidencia digital, Análisis forense de la información recuperada, Reporte de la evidencia. Para poder aplicar la guía de procedimientos se procederá a montar un escenario ficticio, el cual está integrado de los teléfonos celulares incautados, computador portátil HP Pavilion tx2000 con un sistema operativo Windows 7 de 32 bits.

4.1.1. FASE 1: IDENTIFICACIÓN DEL PROBLEMA

Teléfonos celulares incautados a un sospechoso que intentaba venderlos, se presumen de dudosa procedencia al no disponer factura de los mismos; en la parroquia Maldonado parque de San Francisco, dispositivos sobre los cuales se va

a realizar el análisis forense, el croquis *Anexo A*, muestra la escena para la posterior documentación y para la preservación física de los dispositivos, así como la incautación de estos equipos, para su posterior análisis.

Figura 4.2. Parque San Francisco

Se identificó la extensión y perímetro del incidente (escenario ha sido fabricado para propósitos del trabajo de investigación), el cual se reduce al mercado San Francisco lugar donde se dedican a la venta de todo tipo de productos. Se evitó que personas ajenas a la escena entraran en contacto con ella.

Asegurar la preservación de la evidencia

Los dispositivos y accesorios son colocados en una envoltura y sellados antes de colocarlos dentro de las bolsas antiestáticas como evidencia.

- **Aislar el dispositivo de la red GSM:** Esto se logró utilizando una bolsa anti-estática.

Identificación y documentación de los componentes electrónicos que no se van a incautar.

TABLA V.
Componentes electrónicos que no se van a incautar

TIPO	MARCA	NUMERO DE SERIE
Computador portátil	Notebook HP Pavilion tx2110us	CWF8201L55

Recolección de los elementos no electrónicos relacionados con el dispositivo.

TABLA VI.
Componentes no electrónicos

TIPO	MARCA	NUMERO DE SERIE
Cargador	Sony Ericsson	9207w30610727
Cable USB	Sony Ericsson	DCU-65

Figura 4.3. Escenario de Análisis

En el *Anexo A* y en la *figura 4.3* son establecidos los componentes necesarios para la obtención de evidencia digital, *Anexo A* lugar donde ciertos ciudadanos se dedican a la compra y venta de diferentes productos, figura 4.3 hardware y software para la adquisición de evidencia.

CONCLUSIÓN: Se ha detenido a una persona que se dedicada a la venta ilegal de celulares.

DOCUMENTO: Croquis_Escena. *Anexo A*

4.1.2. FASE 2: RECOLECCIÓN DE LA EVIDENCIA DIGITAL

INSPECCIÓN INICIAL: El equipo de telefonía celular solo muestra el nombre de la marca Sony Ericcson, el equipo presenta un estado que presumía estar apagado.

Instalación de los componentes de software necesarios. Se instaló el programa del proveedor denominado Sony Ericsson PC. Gracias a la herramienta se obtuvo archivos que se encontraba almacenada en la tarjeta externa, que las herramientas forenses utilizadas en este caso no pudieron acceder.

Preparar las herramientas forenses de telefonía celular. Se instalaron las aplicaciones para la extracción de los datos. Estas herramientas fueron MobilEdit!, Oxigen Forensic Suite y Device Seizure (como se puede observar la obtención de la evidencia digital en el *Anexo C Herramientas Forenses*) hay que tomar en cuenta que las herramientas a utilizar son herramientas comerciales y por su elevado costo, se realizará el análisis con la versión de prueba.

Una vez realizado el análisis la herramienta proporciono los siguientes datos:

- Historial SMS
- SMS
- Agenda de contactos
- Historial de llamadas: Llamadas recibidas, números marcados, llamadas perdidas, datos de las llamadas
- Agenda
- Calendario
- Lista de tareas
- Sistema de archivos: Archivos del sistema, archivos multimedia, notas rápidas
- E-mail

Posterior a esto se realiza un registro de la cadena de custodia, como se muestra en la tabla VII, este formulario recolecta información básica, evitando que se rompa la cadena de custodia:

TABLA VII.
Formulario de registro de la cadena de custodia [43]

Entidad:			Tipo del elemento físico:		
Fecha(DD/MM/AA)			IMEI:		
Ciudad:			Numero Serial:		
Sitio Exacto del hallazgo:			Marca y referencia:		
Descripción del elemento físico de prueba:					
Fecha	Hora	Nombre completo de quien recibe el elemento físico de prueba.	Propósito del traspaso de cadena de custodia.	Observaciones	Firma

Posterior a este proceso se realizó una copia de la evidencia digital, esto es útil si el dueño del dispositivo desea iniciar un proceso judicial contra sus atacantes y en tal caso deberá documentar y acudir donde un abogado para realizar el proceso respectivo.

Los archivos guardados fueron almacenados en una unidad de memoria externa, bajo la carpeta Datos Forenses. Además se hicieron copias de respaldo en CD y en el disco duro de la computadora.

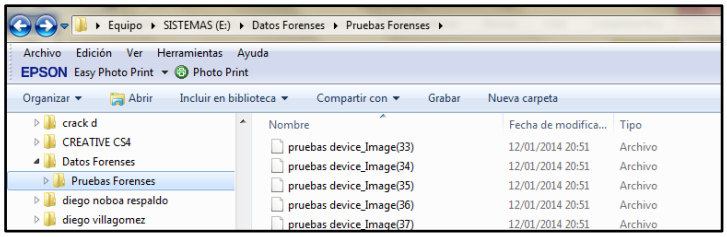


Figura 4.4. Evidencia digital

[43] BARYAMUREEBA V., The Enhanced Digital Investigation Process Model., 2004., pp. 1-4., E-book: http://www.forensicfocus.com/enhanced-digital-investigation-model

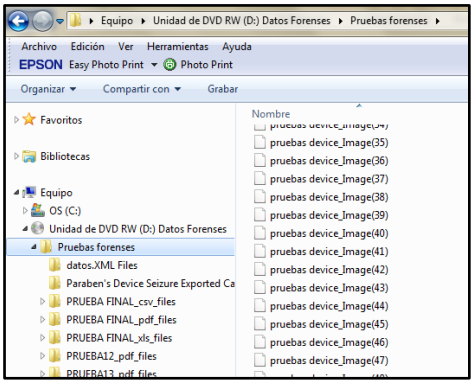


Figura 4.5. Pruebas Forense

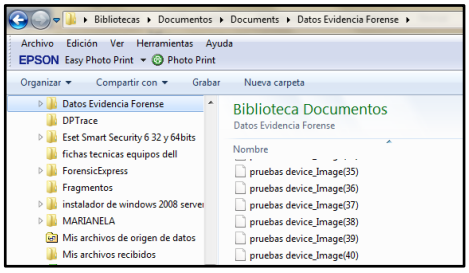


Figura 4.6. Almacenamiento evidencia digital

RESUMEN: Se obtuvo la información básica necesaria para poder trabajar correctamente con el dispositivo, esto es, se identificó el modelo, y de esta manera, sus características técnicas principales. Además se identificó las posibles fuentes de evidencia, se realizó la recolección y preservación de datos mediante las herramientas forenses, aplicaciones del fabricante y se recurrió a las fotografías digitales para aquello elementos que no pudieron extraerse mediante estas aplicaciones.

Recomendaciones:

- Obtener el modelo del equipo de telefonía celular
- En base al modelo obtener el manual del equipo

Documentos obtenidos: Manuales digitales, aplicaciones del fabricante (Sony Ericsson PC Suite, imágenes digitales, archivos digitales de audio, contenido de mensajes, registro de llamadas, reportes sobre la evidencia extraída.)

4.1.3. FASE 3: ANÁLISIS FORENSE DE LA INFORMACIÓN RECUPERADA

La información recuperada del dispositivo, se detalla a continuación con cada una de las herramientas utilizadas.

DEVICE SEIZURE

Figura 4.7. Herramienta Forense Device Seizure
Fuente: http://www.paraben.com/device-seizure.html

Esta herramienta proporcionó información sobre:

- **Directorio.** En cuanto a la información sobre el directorio almacenado en el equipo de telefonía celular modelo w810i. Se tiene el siguiente resumen:
  - Presenta 29 contactos almacenados en la memoria interna del teléfono
  - Presenta 20 contactos almacenados en la tarjeta SIM
- **Registro de llamadas.** En cuanto al registro de llamadas el equipo presenta al momento de la extracción de datos poca actividad. El programa solo recuperó tres registros correspondientes a las llamadas perdidas.
- **Tareas programadas:** El programa no encontró ningún evento programado.
- **Historial SMS.** El programa logró extraer datos relacionados con la actividad de mensajes SMS. El historial se compone de 30 mensajes de texto.
- **Detalles del equipo w810i.** Además de haberse identificado el modelo comercial del equipo w810i, el programa logró identificar diferentes clasificaciones de modelo del equipo asegurado.

MOBILEDIT FORENSIC

Figura 4.8. Herramienta Forense Mobiledit Forensic
Fuente: http://www.mobiledit.com/forensic

- **Directorio:**
  - Presenta 50 contactos almacenados en la memoria interna del equipo.
  - Presenta 120 contactos almacenados en la tarjeta SIM
  - Esta herramienta obtuvo un contacto más que Device Seizure.
- **Registro de llamadas:** Similar al programa Device Seizure pues solo se pudo extraer información sobre tres llamadas perdidas.
- **Tareas programadas:** No se encontraron datos sobre esta categoría.
- **Historial SMS.** MobilEdit! logró extraer información sobre mensajes SMS. Al igual que Device Seizure, el historial está compuesto de 100 mensajes de texto.
- **Detalles del equipo w810i:** MobilEdit! también logró identificar diferentes clasificaciones de modelo del equipo asegurado.

OXIGEN FORENSIC SUIT

Figura 4.9. Herramienta Forense Oxigen Forensic Suite
Fuente: http://www.oxygen-forensic.com/en/

- **Directorio:**
  - Presenta 40 contactos almacenados en la memoria interna del equipo.
  - Presenta 90 contactos almacenados en la tarjeta SIM
  - Esta herramienta al igual que Mobiledit Forensic obtuvo más contactos que Device Seizure.
- **Registro de llamadas: S**e pudo extraer información sobre dos llamadas perdidas.
- **Tareas programadas:** No se encontraron datos sobre esta categoría.
- **Historial SMS. H**istorial compuesto de 90 mensajes de texto.
- **Detalles del equipo w810i:** Se logró identificar diferentes clasificaciones de modelo del equipo asegurado.

PC SUITE

Figura 4.10. Herramienta Sony Ericsson PC Suite
Fuente: http://www.sonymobile.com/es/tools/sony-ericsson-pc-suite-16/

Con esta aplicación se accedió a una tarjeta de memoria externa que acompañaba al dispositivo. Se obtuvieron los siguientes elementos:

- **Se obtuvo un álbum de imágenes digitales.** El álbum se compone de 54 archivos
- **Imágenes adicionales.** Una carpeta que contiene 6 imágenes
- **Archivo de audio:** Se encontraron archivos de tipo mp3, m4a, .mid, 3gp.

RESUMEN: Luego de haber realizado la inspección sobre el equipo celular se pudo identificar información un poco relevante al incidente, además las herramientas forenses Mobiledit Forensic, Device Seizure y Oxigen Forensic Suite generan reportes forenses de la información extraída en ciertos formatos (.xml, .html, .pdf, .xls, .rtf) dependiendo de la selección del investigador forense.

4.1.4. FASE 4: REPORTE DESCRIBIENDO LOS DATOS

El **Anexo D** muestra un reporte, resumen de la obtención de la evidencia digital extraída por el examinador forense y que puede formar parte del documento de un proceso judicial.

4.2. VARIABLE DEPENDIENTE: OBTENCIÓN DE EVIDENCIA

INDICADOR 1: *Porcentaje de mensajes SMS de información recuperada*

TABLA VIII.
Información SMS

HERRAMIENTAS	CON GUÍA DE PROCEDIMIENTOS	CON CONOCIMIENTOS GENERALES (SIN GUÍA DE PROCEDIMIENTOS)
MobilEdit Forensic	90 %	15 %
Device Seizure	60 %	5 %
Oxigen Forensic Suite	75 %	10 %
Promedio	75 %	10 %

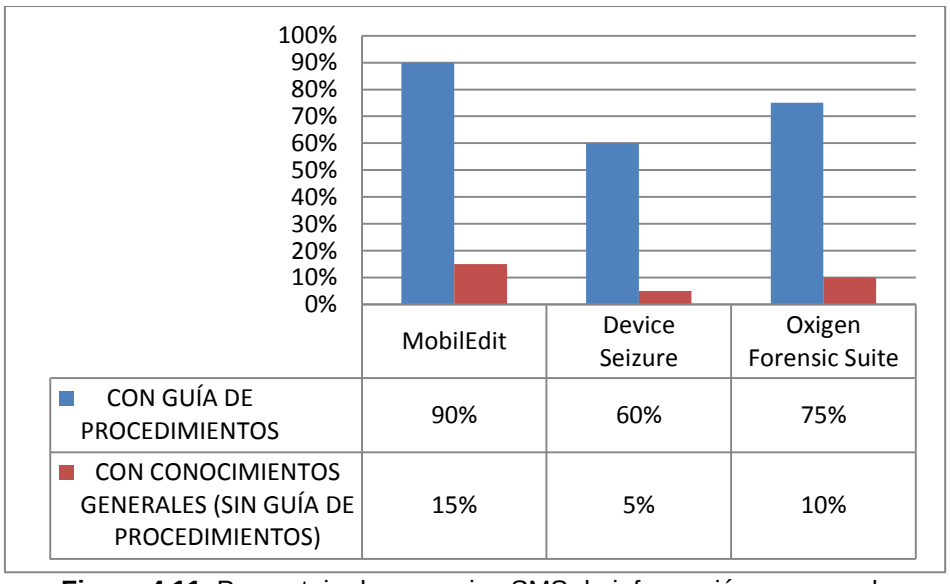


Figura 4.11. Porcentaje de mensajes SMS de información recuperada

Resultado: Se puede concluir que utilizando la guía de procedimientos propuesta en esta Tesis, y utilizando las herramientas forenses se ha logrado recuperar con la herramienta MobilEdit Forensic información el 90%, con la herramienta Device Seizure 60%, con la herramienta Oxigen Forensic 75% de mensajes SMS; en cambio al no seguir cada una de las fases que involucra una guía de procedimientos solo se ha podido recuperar 10% de información.

INDICADOR 2: *Porcentaje de contactos de información recuperada*

TABLA IX.
Información Agenda

HERRAMIENTAS	CON GUÍA DE PROCEDIMIENTOS	CON CONOCIMIENTOS GENERALES (SIN GUÍA DE PROCEDIMIENTOS)
MobilEdit Forensic	85%	10 %
Device Seizure	65%	10 %
Oxigen Forensic Suite	75%	10 %
Promedio	75%	10 %

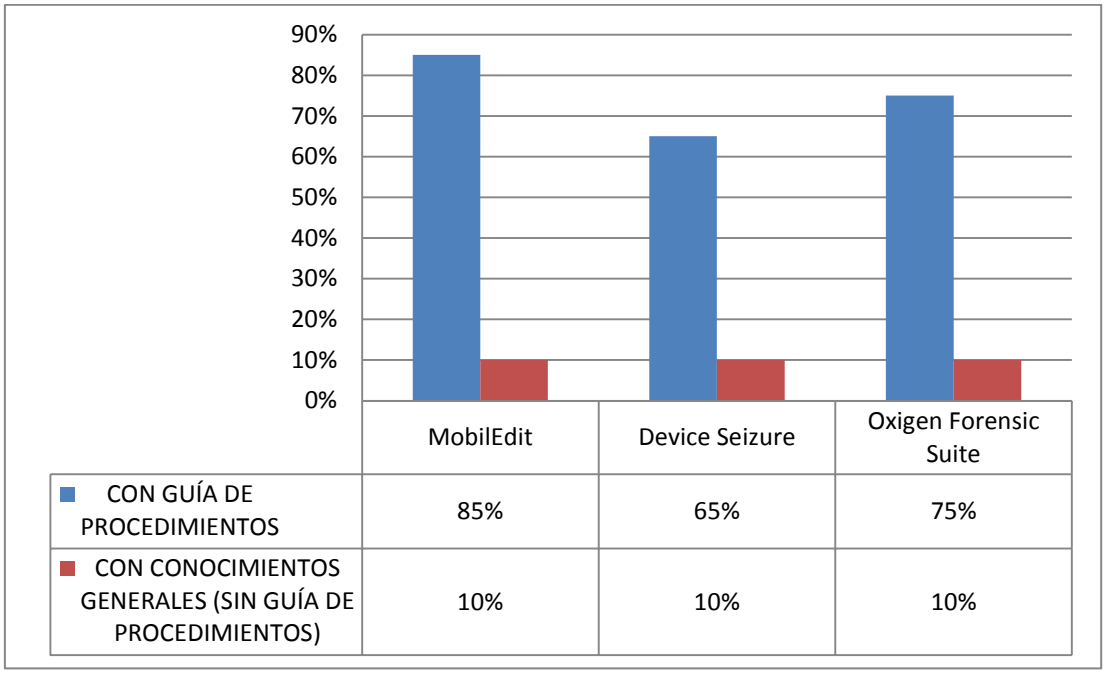


Figura 4.12. Porcentaje de contactos de información recuperada

Resultado: Se puede concluir que utilizando la guía de procedimientos propuesta en esta Tesis, y utilizando las herramientas forenses se ha logrado recuperar contactos de información con la herramienta MobilEdit Forensic el 85%, con la

herramienta Device Seizure 65%, con la herramienta Oxigen Forensic 75% de contactos; en cambio al no seguir cada una de las fases que involucra una guía de procedimientos solo se ha podido recuperar 10% de contactos.

INDICADOR 3: *Porcentaje de llamadas de información recuperada*

TABLA X.
Información llamadas

HERRAMIENTAS	CON GUÍA DE PROCEDIMIENTOS	CON CONOCIMIENTOS GENERALES (SIN GUÍA DE PROCEDIMIENTOS)
MobilEdit Forensic	70%	15 %
Device Seizure	50%	10 %
Oxigen Forensic Suite	60%	5 %
Promedio	60%	10 %

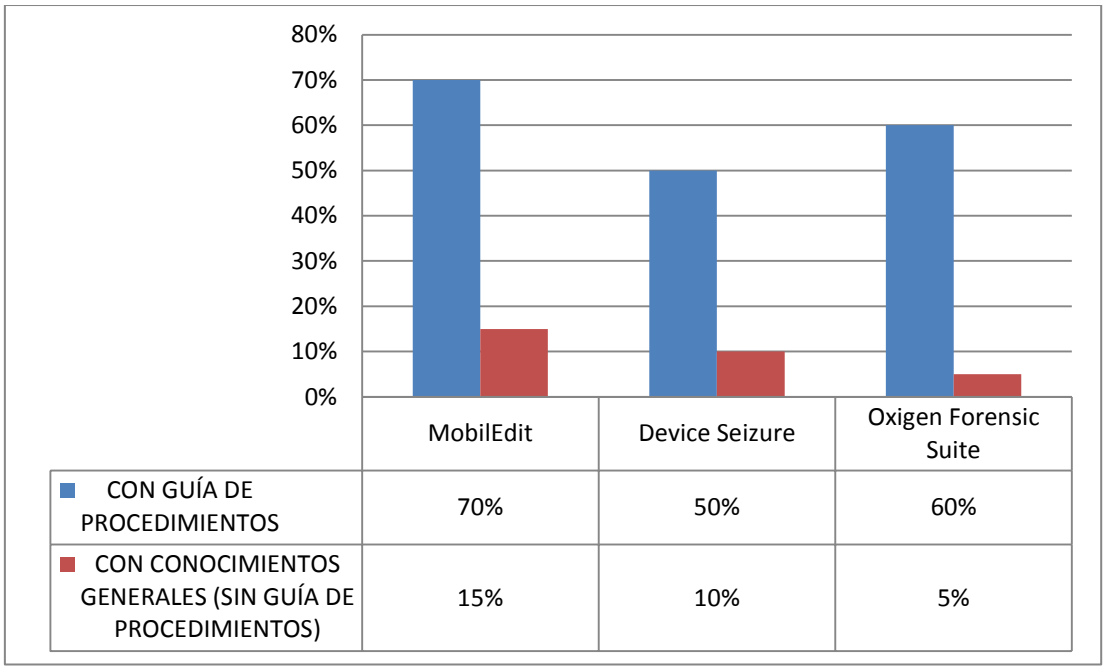


Figura 4.13. Porcentaje de llamadas de información recuperada.

Resultado: Se puede concluir que utilizando la guía de procedimientos propuesta en esta Tesis, y utilizando las herramientas forenses se ha logrado recuperar llamadas de información con la herramienta MobilEdit Forensic el 70%, con la herramienta Device Seizure 50%, con la herramienta Oxigen Forensic 60% de llamadas; en cambio al no seguir cada una de las fases que involucra una guía de procedimientos solo se ha podido recuperar 10% de llamadas.

INDICADOR 4: *Porcentaje de tipos de reportes de información recuperada generada.*

TABLA XI.
Información Reporte

HERRAMIENTAS	CON GUÍA DE PROCEDIMIENTOS	CON CONOCIMIENTOS GENERALES (SIN GUÍA DE PROCEDIMIENTOS)
MobilEdit Forensic	90%	2 %
Device Seizure	4%	0 %
Oxigen Forensic Suite	5%	1 %
Promedio	33%	1 %

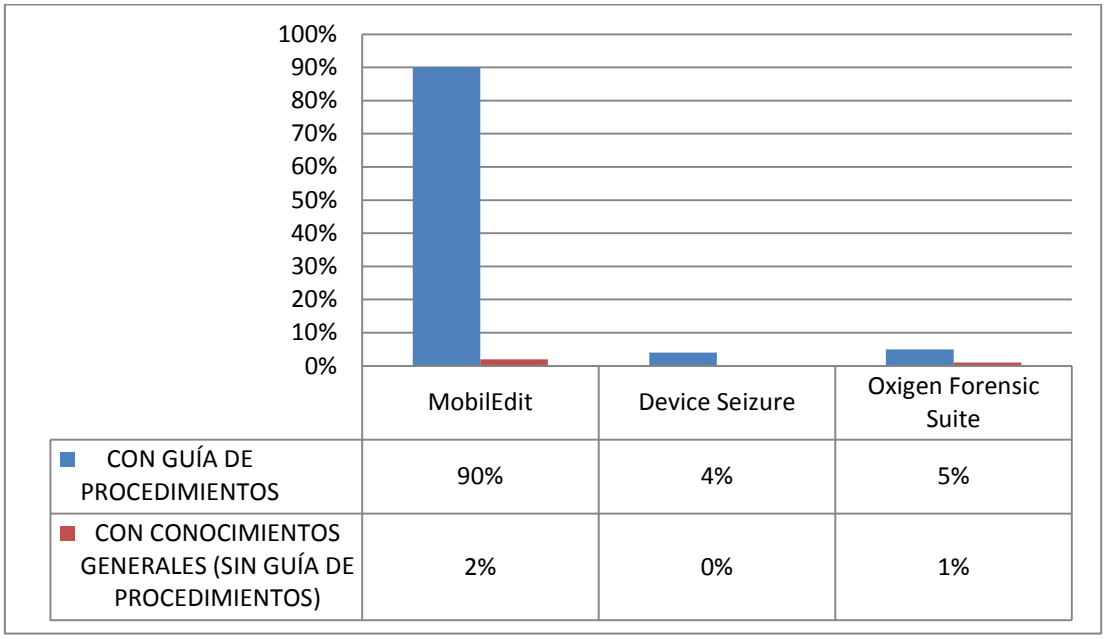


Figura 4.14. Porcentaje de tipos de reportes de información recuperada generada

Resultado: Se puede concluir que utilizando la guía de procedimientos propuesta en esta Tesis, y utilizando las herramientas forenses se ha logrado generar reportes de información con la herramienta MobilEdit Forensic el 90%, con la herramienta Device Seizure 4%, con la herramienta Oxigen Forensic 5% de tipos de reportes generados; en cambio al no seguir cada una de las fases que involucra una guía de procedimientos se ha podido generar 1% de reportes.

4.3. RESUMEN DE RESULTADOS

En base a la variable Dependiente y sus indicadores se realizó la comprobación de la hipótesis basándose en los resultados obtenidos con herramientas forenses realizados en 50 teléfonos celulares objeto de análisis para la construcción de la Guía de procedimientos, demostrando que la hipótesis planteada es significativa para la investigación.

TABLA XII. RESUMEN DE RESULTADOS

	INDICADOR	**Variable Independiente:** Con Guía de procedimientos	Con conocimientos generales
Variable Dependiente: Obtención de evidencia digital mediante el empleo de herramientas forenses	**I1:** Porcentaje de mensajes SMS recuperados	75	10
	I2: Porcentaje de contactos de información recuperada.	75	10
	I3: Porcentaje de llamadas de información recuperada.	60	10
	I4: Porcentaje de tipos de reportes de información recuperada generada.	33	1

4.4. COMPROBACIÓN DE HIPÓTESIS

4.4.1. PLANTEAMIENTO DE LA HIPÓTESIS

Para la prueba de la hipótesis planteada se utilizó la prueba ji cuadrado, que es una prueba no paramétrica a través de la cual se midió la relación entre la variable dependiente e independiente. Además se consideró la hipótesis nula Ho y la hipótesis de investigación Hi.

a) Hipótesis Nula, H_o

H_o: La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense no permitirá obtención de evidencia digital frente a posibles ataques.

b) Hipótesis Alternativa, H_1

H_1: La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense permitirá la obtención de evidencia digital frente a posibles ataques.

4.4.2. NIVEL DE SIGNIFICANCIA

El nivel de significancia utilizado es 0,050.

4.4.3. TAMAÑO DE LA MUESTRA

Se utilizó una muestra intencionada basándose en los resultados obtenidos con los herramientas empleadas para la obtención de evidencia digital, 50 celulares escogidos de acuerdo a los siguientes criterios de selección como es sistema operativo, marca, modelo, tipo de cable que utiliza, modo de conexión del equipo móvil, aplicaciones instaladas en el equipo.

4.4.4. ESPECIFICACIONES DE LAS REGIONES DE ACEPTACIÓN Y RECHAZO

En la Figura 4.15 se visualiza la región de aceptación de la hipótesis nula H_O que es 5%. Por lo tanto si:

$$X_i > X_T$$

Se rechazará la Hipótesis Nula y se aceptará la Hipótesis Alternativa.

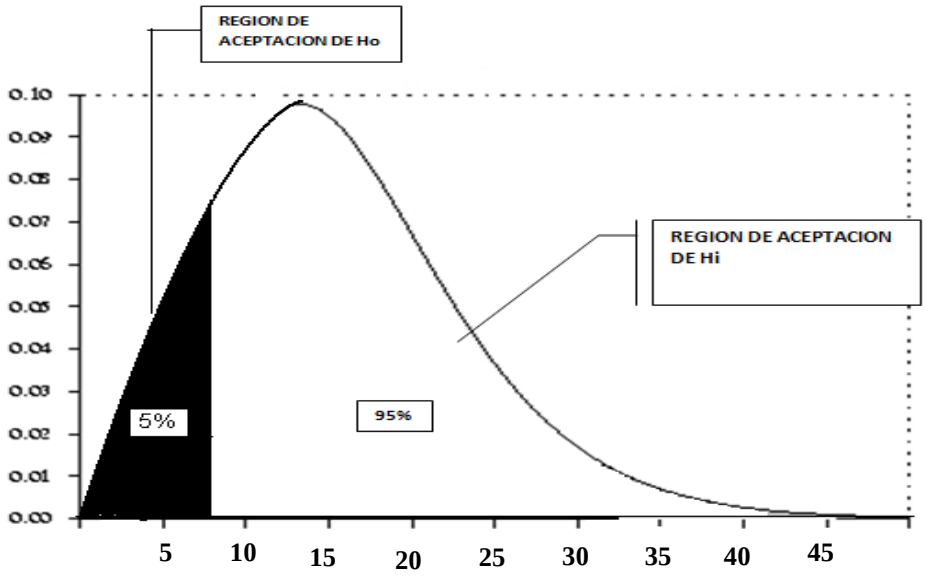


Figura 4.15. Región de aceptación y rechazo Hipótesis Nula

4.4.5. ESPECIFICACIÓN DEL ESTADÍSTICO CHI CUADRADO

$$\chi^2 = \sum \frac{(O-E)^2}{E}$$

4.4.6. CÁLCULO ESTADÍSTICO CHI CUADRADO

La tabla de contingencia creada para el cálculo de **ji** cuadrado, contiene los indicadores que determinarán si la construcción de la Guía de Procedimientos permite la obtención de evidencia digital, mediante la utilización de herramientas forenses.

4.4.6.1. FRECUENCIAS OBSERVADAS

Las frecuencias observadas se encuentra de las sumas del valor obtenido en la Tabla XII, de cada indicador con los valores de las variables que permite la obtención de evidencia digital y los valores de la variable que no permite obtención de evidencia digital tomando como referencia la utilización de 50 celulares de la muestra intencionada.

Tabla XIII.
Frecuencias Observadas-Tabla de contingencia

Variable Dependiente: Obtención de evidencia digital mediante el empleo de herramientas forenses	**Variable Independiente:** Guía de procedimientos para el manejo de incidentes en dispositivos móviles mediante análisis forense.		
	Utilizando herramientas forenses permite obtención de datos	**Sin utilizar herramientas forenses no permite obtención de datos**	**TOTAL**
H_1: La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense permitirá la obtención de evidencia digital frente a posibles ataques.	61,25	0	61,25
H_o: La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense no permitirá la obtención de evidencia digital frente a posibles ataques.	0	7,75	7,75
TOTAL	61,25	7,75	69,00

4.3.6.2. FRECUENCIAS ESPERADAS

Las frecuencias esperadas de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$fe = \frac{(total\_de\_fila)(total\_de\_columna)}{N}$$

Ecuación 2: Fórmula para calcular la frecuencia esperada

$$fe = \frac{(total\_de\_fila)(total\_de\_columna)}{N}$$

$$fe = 61,25*61,25/69$$

$$fe= 1,11$$

Donde **N** es el número total de frecuencias observadas

Nota: el valor ***fe*** es el valor de la primera operación de la tabla, se debe realizar las demás operaciones para llenar la tabla en mención.

Tabla XIV.
Frecuencias Esperadas de la investigación

Variable Dependiente: Obtención de evidencia digital mediante el empleo de herramientas forenses	**Variable Independiente:** Guía de procedimientos para el manejo de incidentes en dispositivos móviles mediante análisis forense.		
	Utilizando herramientas forenses permite obtención de datos	**Sin utilizar herramientas forenses no permite obtención de datos**	**TOTAL**
H_1: La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense permitirá la obtención de evidencia digital frente a posibles ataques.	43,49	6,88	61,24
H_o: La guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense no permitirá la obtención de evidencia digital frente a posibles ataques.	6,88	0,87	7,75
TOTAL	50,37	7,75	68,99

4.4.7. SUMATORIA DE X^2

Una vez obtenidas las frecuencias esperadas, se aplica la fórmula de ji cuadrado para cada una de las celdas de la tabla:

$$\chi^2 = \sum \frac{(O-E)^2}{E}$$

Dónde:

O es la frecuencia observada en cada celda

E es la frecuencia esperada en cada celda

X^2= (61,25-43,49)^2/43,49

X^2=7,25

Nota: el valor X^2 es el valor de la primera operación de la tabla, se debe realizar las demás operaciones para llenar la tabla en mención.

Tabla XV.
Sumatoria de X^2

OBSERVADAS	ESPERADAS	O-E	(O-E)^2	(O-E)^2/E
61,25	43,49	17,76	315,42	7,25
0	6,88	-6,88	47,33	6,88
0	6,88	-6,88	47,33	6,88
7,75	7,25	0,50	0,25	0,03
			TOTAL	21,04

4.4.8. INTERPRETACIÓN

Para saber si el valor de X^2 es o no significativo, se debe determinar los grados de libertad mediante la siguiente fórmula:

Gl *= (r-1) (c-1)*

Dónde:

r: es el número de filas de la tabla de contingencia

c: es el número de columnas de la tabla de contingencia

$$Gl = (2-1)\ (2-1)$$

$$Gl = 1$$

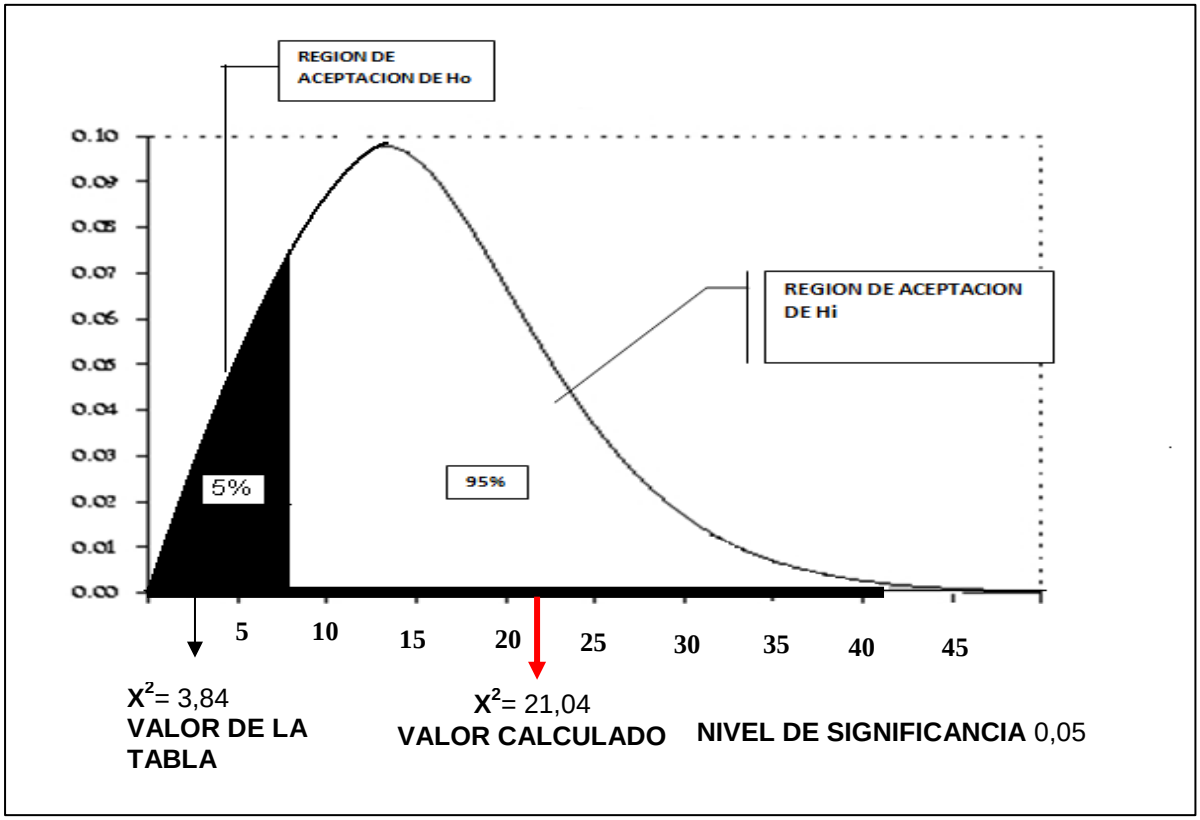


Figura 4.16. Ji Cuadrado

4.4.9. DECISIÓN

Dado la condición:

$$X^2_i > X^2_T$$

$$\boldsymbol{21,04 > 3,84}$$

Se rechaza la Hipótesis Nula y se acepta la Hipótesis Alternativa

Por lo tanto: *De la tabla de distribución de X^2 que se encuentra en el Anexo B, eligiendo como nivel de significancia= 0,050 se obtiene que X^2 =3,84, el valor de X^2 calculado en esta investigación es de 21,04 que es muy superior a la tabla de distribución por lo que X^2 está en la zona de rechazo de la hipótesis nula, y se acepta la hipótesis de la investigación.*

CONCLUSIONES

1. Se realizó un estudio de las metodologías de la Informática forense y como cada análisis es único, se planteó para este tema de investigación una guía de procedimientos la cual consta de las siguientes fases: Identificación del problema, Recolección de la evidencia digital, Análisis forense de la información recuperada, Creación de un reporte describiendo los datos recuperados; fases que permitieron la recuperación de la evidencia digital, la cual pueda ser utilizada como parte del proceso judicial en una corte de justicia, en caso de iniciarse un proceso legal.

2. Las herramientas forenses utilizadas sobre la muestra de 50 teléfonos celulares Nokia, Samsung, LG, Sony Ericsson, BLU son: Paraben Device Seizure, Oxigen Forensic Suit y Mobiledit, instaladas sobre la plataforma Windows XP, Windows 7 de 32 y 64 bits, fueron elegidas de acuerdo a los 23 parámetros establecidos (fabricante, modelo, IMEI, captura de datos básicos, conectividad y recuperación, llamadas marcadas / recibidas, mensajes, etc.) en este tema de investigación para lograr la extracción de evidencia digital básica y necesaria en toda investigación forense.

3. Para la comprobación de la hipótesis se utilizó la prueba ji cuadrado, con una muestra de 50 teléfonos celulares escogidos de acuerdo a los siguientes criterios de selección como es: sistema operativo, marca, modelo, tipo de cable que utiliza, modo de conexión del equipo móvil, aplicaciones instaladas en el equipo, por lo tanto, utilizando la guía de procedimientos para el manejo de incidentes en dispositivos móviles con tecnología GSM mediante análisis forense se pudo recuperar la siguiente evidencia digital: 75% de mensajes SMS, 75% de información de contactos, 60% de llamadas telefónicas realizadas y recibidas y se ha logrado generar en un 60% reportes de la información recuperada. Además se concluye para esta investigación que la herramienta MobilEdit es más efectiva en comparación a Oxigen Forensic Suite y Device Seizure; Mobiledit recupera el 83.75% de evidencia digital, Oxygen Forensic Suite logra recuperar el 53.75% de evidencia digital y Device Seizure recupera el 44.75% de evidencia digital.

RECOMENDACIONES

1. Profundizar en el tema de la ciencia forense, la falta de conocimiento delimita y restringe a la ciudanía, a recurrir a aspectos legales, en caso de ocurrir robos, fraudes, amenazas, y otras clases de incidentes de seguridad que puede ocurrir cuando se utiliza tecnología celular.

2. Se debe concientizar a las personas en el buen uso de la tecnología, y más aún usar adecuadamente políticas de seguridad en los dispositivos con eso evitaremos incidentes de seguridad y sobre todo fraudes y estafas.

3. Se recomienda a las autoridades judiciales profundizar y tipificar un departamento de investigación sobre análisis forense; donde la información recuperada de los equipos celulares sea tratada de forma correcta para evitar la degradación o el borrado de datos, logrando de esta forma la integridad de todas las pruebas en caso de ser utilizado en un proceso judicial.

CAPITULO V
BIBLIOGRAFÍA

[1] **BECERRIL, I.,** Análisis forense en dispositivos móviles., Estados Unidos., 2008., pp. 4-5.
E-book:
http://www.revista.unam.mx/vol.9/num4/art26/int26.htm

[2] **BECERRIL I.,** Análisis forense en dispositivos móviles., Estados Unidos., 2008., pp. 6-7.
E-book:
http://www.revista.unam.mx/vol.9/num4/art26/int26.htm

[3] **HERNÁNDEZ R.,** Análisis forense en dispositivos móviles con Symbian OS., Bogotá – Colombia, 2008., pp. 1-6.
E-book:
http://www.criptored.upm.es/guiateoria/gt_m142e1.htm

[4] **AYERS R.,** Guidelines on Cell Phone Forensics., Estados Unidos 2007., pp. 14-64.
E-book:
http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

[5] **ACURIO S.,** Delitos Informáticos: Generalidades., 2011., pp. 6-8. E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[6] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 15. E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[7] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 33. E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[8] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 8. E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[9] **ACURIO S.,** Delitos Informáticos: Generalidades., 2011., pp. 9. E-book: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[10] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 9. E-book: http://www.criptored.upm.es/guiateoria/gt_m592b.htm

[11] **CASTILLO C.,** Dispositivos móviles. iPhorensics., 2010., pp. 1.
E-book:
http://www.carlosacastillo.com/2010/01/iphorensics/

[12] **ACURIO S.,** Delitos Informáticos: Generalidades., 2011., pp. 54.
E-book:
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[13] **ACURIO S.,** Plan Operativo de creación de la Unidad de delitos Informáticos del Ministerio Público., 2002., pp. 3.
E-book:
http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

[14] **ACURIO S.,** Perfil sobre delitos Informáticos: Generalidades., 2012. pp. 3-68.
E-book:
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[15] **PHIL W.,** Crimen Organizado y Cibernético, sinergias, tendencias y respuestas., 2006., pp. 2-10.
E-book:
http://www.pitt.edu/~rcss/toc.html

[16] **ACURIO S.,** Perfil sobre delitos Informáticos: Generalidades., 2009 pp. 34.
E-book:
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[17] **REVISTA Evidentia.,** Informática Forense., Barcelona – España. 2008., pp. 1-2.
E-book:
http://www.evidentia.biz/informatica_forense.html

[18] **REVISTA Evidentia.,** Informática Forense., Barcelona - España 2008., pp. 2-4.
E-book:
http://www.evidentia.biz/informatica_forense.html

[19] **CASEY E.,** Digital Evidence and Computer crime, Forensic science computers and the Internet., Tercera Edición., San Diego - California., 2011., pp. 12.
E-book:
http://www.amazon.com/Digital-Evidence-Computer-Crime-Edition/dp/0123742684#reader_0123742684

[20] **SANTES L.,** Análisis Forense para dispositivos de telefonía., México., 2009., pp. 47
E-book:
http://tesis.ipn.mx:8080/xmlui/bitstream/handle/123456789/3730/PROPUESTAMETODFORENSE.pdf?sequence=1

[21] **3GPP.,** Specification of the Suscriber Identity Module - Mobile Equipment (SIM-ME) interface., 2005.
E-book:
http://www.3gpp.org/FTP/Specs/html-info/1111.htm

[22] **SANTES L.,** Análisis Forense para dispositivos de telefonía celular., México., 2009., pp. 31.
E-book:
http://tesis.ipn.mx:8080/xmlui/bitstream/handle/123456789/3730/PROPUESTAMETODFORENSE.pdf?sequence=1

[23] **GSM Association.,** BlackBerrys., Barcelona – España., 2007., pp. 1-2.
E-book:
http://www.gsmworld.com/news/press_2007/press07_03.shtml

[24] **APPLEWHITE A.,** The BlackBerry Business., Estados Unidos., 2002.
E-book:
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1012329

[25] **TIEMPO DE EQUILIBRIO.,** BlackBerry., México., 2011
E-book:
http://www.tiempodeequilibrio.com/blackberry-despide-a-decenas-de-empleados-en-eu/

[26] **BLACKBERRY.,** Devices., Estados Unidos., 2013.
E-book:
http://na.blackberry.com/eng/devices/

[27] **PDA Palm y Pocket PC.,** Revista Ordenadores y portátiles., 2014.
E-book:
http://www.ordenadores-y-portatiles.com/pda-palm.html

[28] **OLVERA C.,** Tipos de Computadoras, PDA's, Smartphone, Handheld a Detalle. Guanajuato - México., 2010.
E-book:
http://tiposdecomputadora.wordpress.com/2010/10/27/pdas-smarphone-handheld-a-detalle/

[29] **CHRISTENSEN J.,** Palm Introduces Three Handhelds., Estados Unidos., 2003.
E-book:
http://multivu.prnewswire.com/mnr/palm/11277/

[30] **ARIZA A.,** Análisis forense orientado para dispositivos móviles inteligentes., Bogotá – Colombia., 2009., pp. 64.
E-book:
http://pegasus.javeriana.edu.co/~CIS0910SD01/Documentos/TG_IPHORENSICS_corto.pdf

[31] **MARK Reith.,** An Examination of Digital Forensic Models., Vol. 1., 2002., California – Estados Unidos
E-book:
www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

[32] **LÓPEZ M.,** Análisis forense digital. Segunda Edición., 2007.
E-book:
http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[33] **TULP2G.,** Forensic framework for extracting and decoding data., 2007.
E-book:
http://tulp2g.sourceforge.net/

[34] **MOBILEDIT! FORENSIC.,** San Francisco – Estados Unidos., 2009.
E-book:
http://www.mobiledit.com

[35] **PARABEN CORPORATION.,** Mobile Forensics., 2013.
E-book:
http://www.paraben-forensics.com/catalog/product_info.php?products_id=342

[36] **HUILCAPI A.,** El delito informático., 2011., Quito-Ecuador.
E-book:
http://www.slideshare.net/JorgeFernandoCruz/el-delito-informtico

[37] **ACURIO S.,** Introducción a la Informática Forense., 2008., pp. 33.
E-book:
http://www.egov.ufsc.br/portal/sites/default/files/9.pdf

[38] **DELGADO C.,** Análisis Anti-Forense., 2004., pp. 1-14.
E-book:
http://dspace.ups.edu.ec/bitstream/123456789/546/2/CAPITULO1.pdf

[39] **VILLACÍS M.,** Características y principios de la informática forense., 2011., pp. 1-7.
E-book:
https://docs.google.com/document/d/1hiIZdtTFPlz5c5940iCSL0N8bTa8ncJzGVzGw1w8PnA/edit

[40] **VILLAMIZAR C.,** Delitos Informáticos., Colombia., 2013.
E-book:
https://www.delitosinformaticos.com/01/2013/paises-delitos-informaticos/delitos-informaticos-colombia/vision-de-delitos-informaticos-en-colombia#.Uq4p8-Qszec

[41] **CARPIO P.,** Evidencia digital., 2011.
E-book:
http://repositorio.utn.edu.ec/bitstream/123456789/539/7/04%20ISC%20157%20CAPITULO%20II.pdf

[42] **VIRTUALCLASS.,** Dificultades del Investigador Forense., 2011.
E-book:
http://problemasconlatecnologia.blogspot.com/2011/03/if-dificultades-del-investigador.html.

[43] **BARYAMUREEBA V.,** The Enhanced Digital Investigation Process Model., 2004., pp. 1-4.
E-book:
http://www.forensicfocus.com/enhanced-digital-investigation-model

[44] **LÓPEZ M.,** Análisis forense digital. Segunda Edición., 2007., pp. 13-20.
E-book:
http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[45] **LÓPEZ M.,** Análisis forense digital. Segunda Edición., 2007., pp. 20-30.
E-book:
http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[46] **LÓPEZ M.,** Análisis forense digital. Segunda Edición., 2007., pp. 31-35.
E-book:
http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[47] **LÓPEZ M.,** Análisis forense digital. Segunda Edición., 2007., pp. 21-28. E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[48] **LÓPEZ M.,** Análisis forense digital. Segunda Edición., 2007., pp. 35-37. E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

ANEXOS

Anexo A.

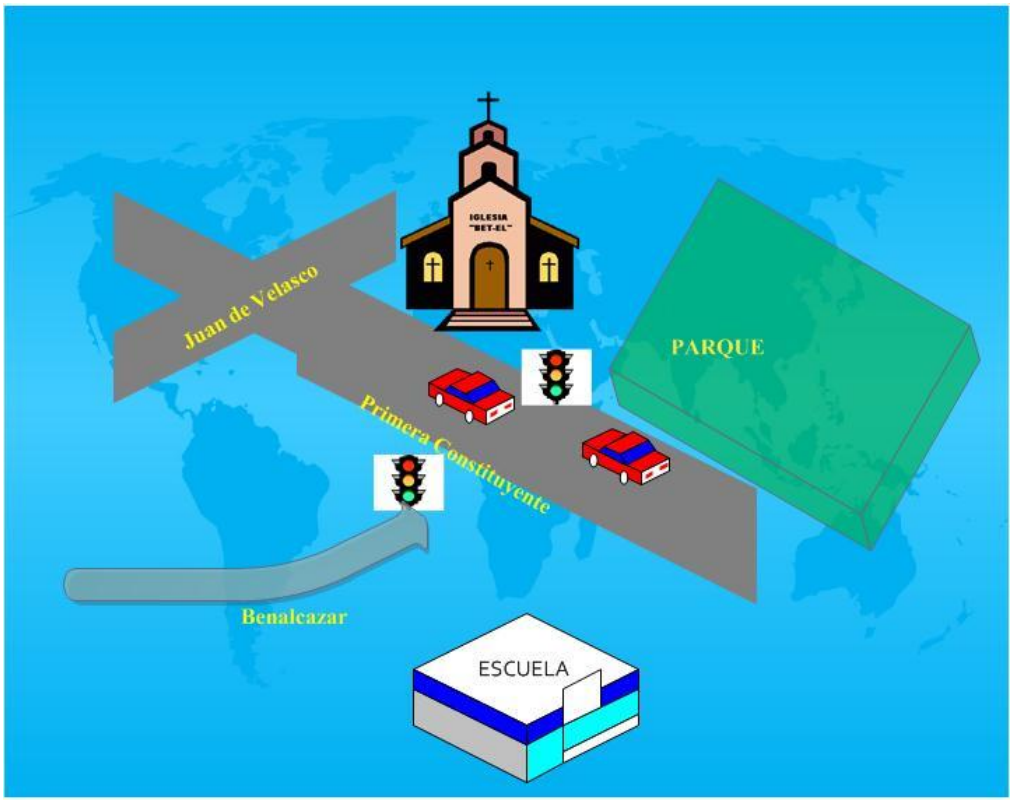


Figura 4.17. Croquis compra – venta de celulares

ANEXO B.

DISTRIBUCION DE χ^2

Grados de libertad	Probabilidad										
	0,95	0,90	0,80	0,70	0,50	0,30	0,20	0,10	0,05	0,01	0,001
1	0,004	0,02	0,06	0,15	0,46	1,07	1,64	2,71	3,84	6,64	10,83
2	0,10	0,21	0,45	0,71	1,39	2,41	3,22	4,60	5,99	9,21	13,82
3	0,35	0,58	1,01	1,42	2,37	3,66	4,64	6,25	7,82	11,34	16,27
4	0,71	1,06	1,65	2,20	3,36	4,88	5,99	7,78	9,49	13,28	18,47
5	1,14	1,61	2,34	3,00	4,35	6,06	7,29	9,24	11,07	15,09	20,52
6	1,63	2,20	3,07	3,83	5,35	7,23	8,56	10,64	12,59	16,81	22,46
7	2,17	2,83	3,82	4,67	6,35	8,38	9,80	12,02	14,07	18,48	24,32
8	2,73	3,49	4,59	5.53	7,34	9,52	11,03	13,36	15,51	20,09	26,12
9	3,32	4,17	5,38	6,39	8,34	10,66	12,24	14,68	16,92	21,67	27,88
10	3,94	4,86	6,18	7,27	9,34	11,78	13,44	15,99	18,31	23,21	29,59
	No significativo								Significativo		

Figura 4.18. Distribución de X^2

ANEXO C.

HERRAMIENTAS FORENSES

REQUERIMIENTOS DEL SOFTWARE:

- MOBILedit Forensic
- Paraben Device Seizure
- Oxygen Forensic

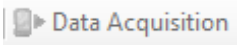
Las características que debe tener el equipo donde se instalará estas aplicaciones son:

- Procesador Pentium IV o superior
- Mínimo 1 GB de RAM
- 40 GB en disco duro
- Windows XP, 7 de 64 y 32 bits
- Adobe Reader
- Microsoft Office

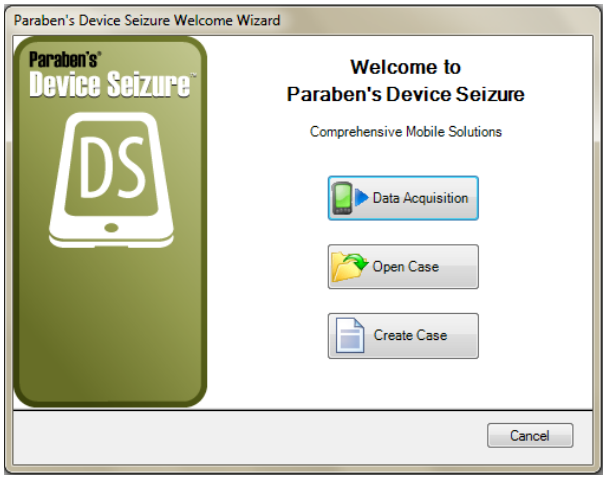
PANTALLAS DE OBTENCIÓN DE EVIDENCIA DIGITAL CON LA HERRAMIENTA DEVICE SEIZURE.

Dispositivo celular a analizar: Samsung GT-S5830i

1. Iniciar la herramienta, clic botón Inicio / Todos los Programas / Paraben Corporation / Device Seizure / Device Seizure

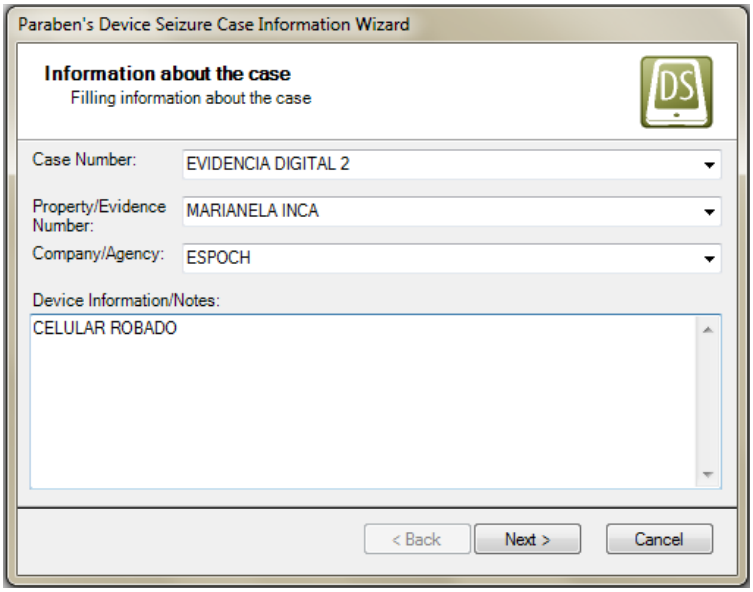
2. Conectar el teléfono celular a través del puerto USB o encender el bluetooth del equipo celular
3. Clic sobre el botón 

(Data Acquisition) de la barra de herramientas, se visualizará la siguiente ventana

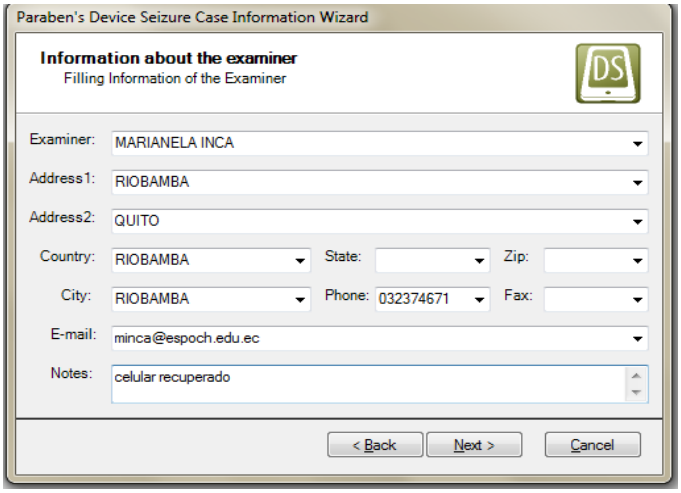


4. Clic sobre la opción Data Acquisition
5. Clic sobre el botón siguiente

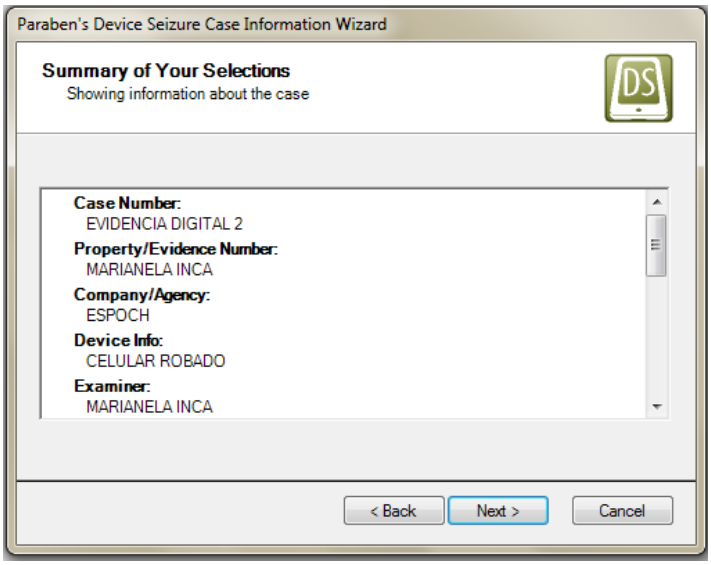
6. Llenar la información solicitada en la siguiente ventana, que hace referencia a la información a extraer del teléfono celular y que será considerada como evidencia digital



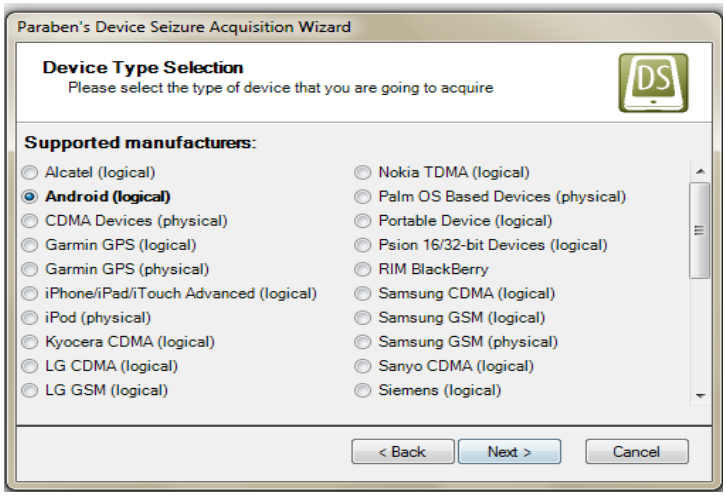
7. Clic en el botón siguiente, y proceder al llenado de la información solicitada en la siguiente ventana



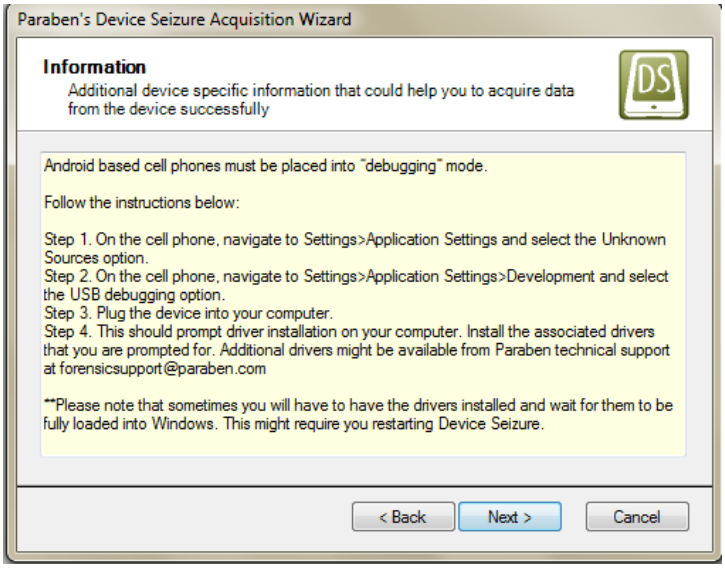
8. Clic sobre el botón siguiente, visualizá un resumen de la información colocada en las ventanas anteriores



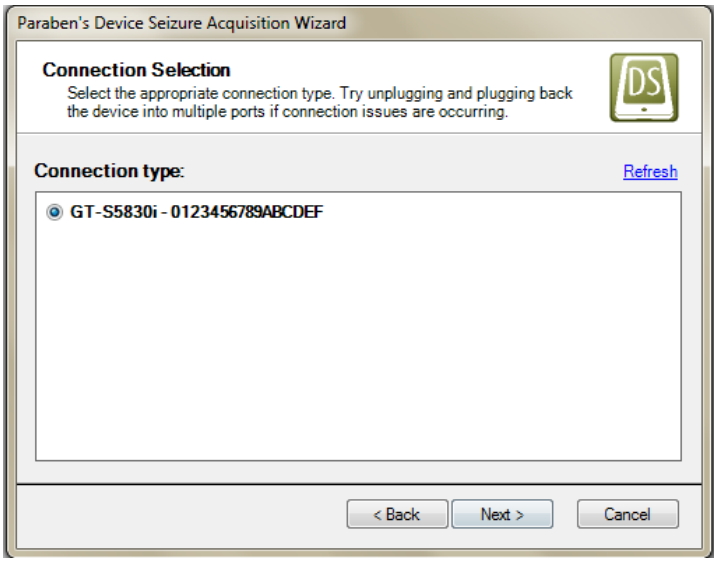
9. Seleccionar el tipo de dispositivo del que se va extraer la información de la lista que se presenta a continuación:



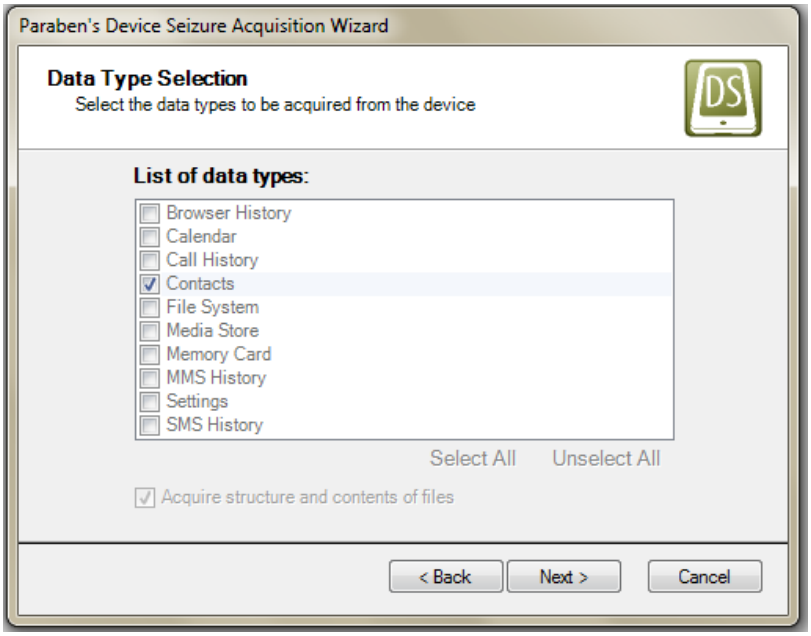
10. Seleccionamos Android (logical) y clic sobre el botón Next
11. Ingresar al teléfono celular y activar cada uno de los opciones que señala la ventana siguiente:



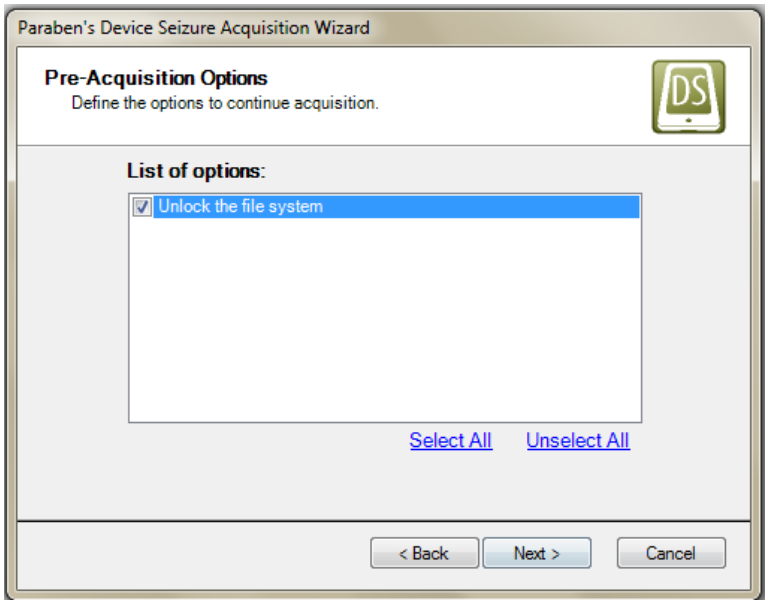
12. Clic en el botón next, se habilita el tipo de conexión para el dispositivo celular conectado



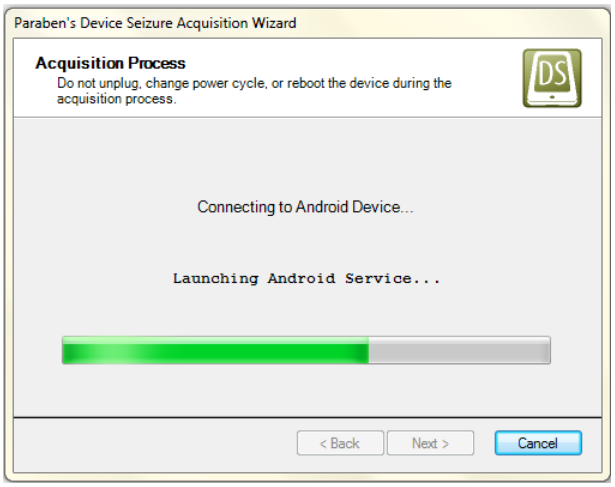
13. Seleccionar los tipos de archivos que se necesita extraer del teléfono celular, luego dar clic sobre el botón next.



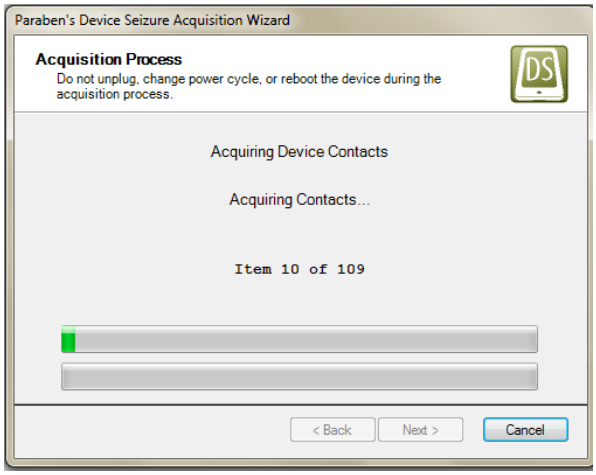
14. Activar la casilla de verificación *Desbloquear el sistema de archivos*, clic en el botón next



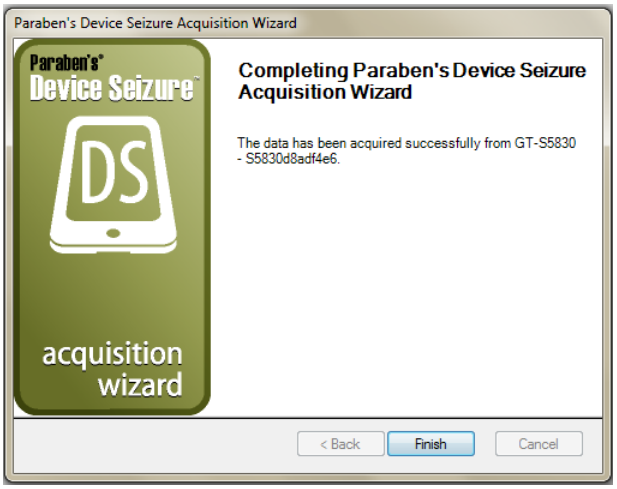
15. La herramienta procede a la extracción de la evidencia digital mediante la conexión a través del dispositivo celular

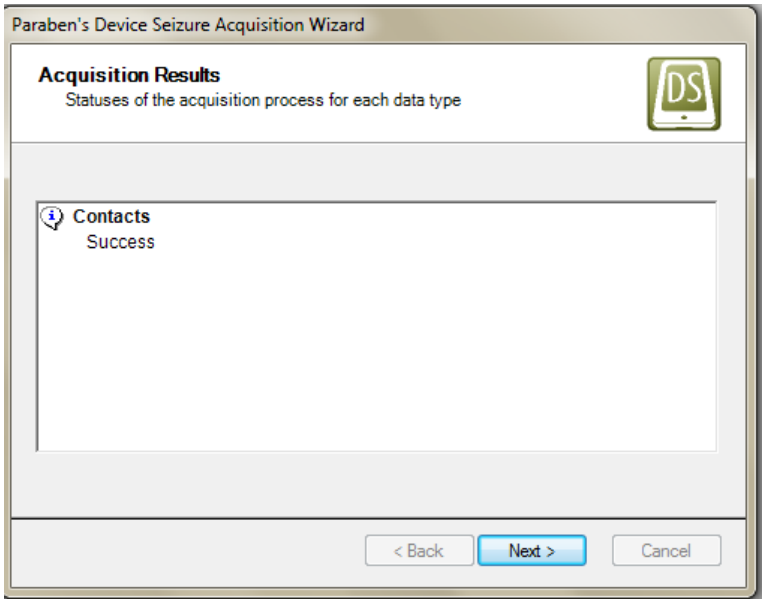


16. La herramienta procede con la extracción de la información, esperar unos minutos

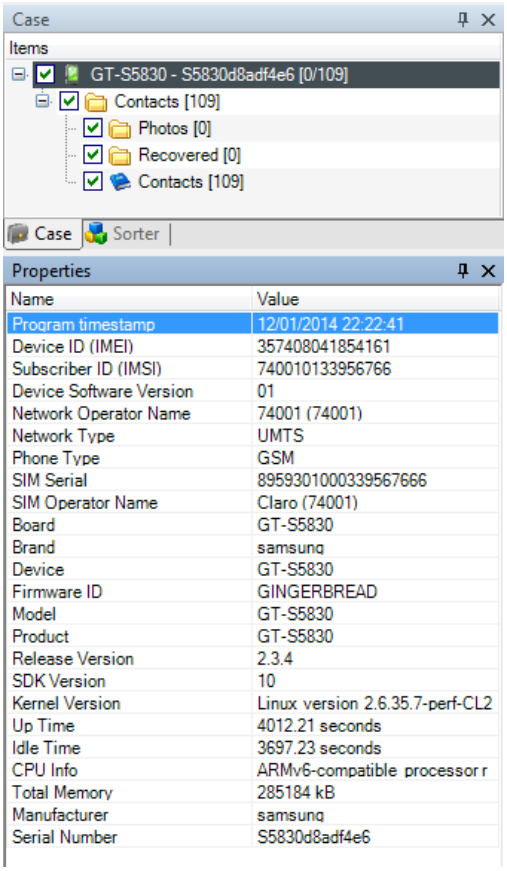


17. Si no ha ocurrido ningún tipo de error se visualizará la siguiente ventana que indica que se ha completado la extracción de evidencia digital y que se realizó con éxito el proceso.

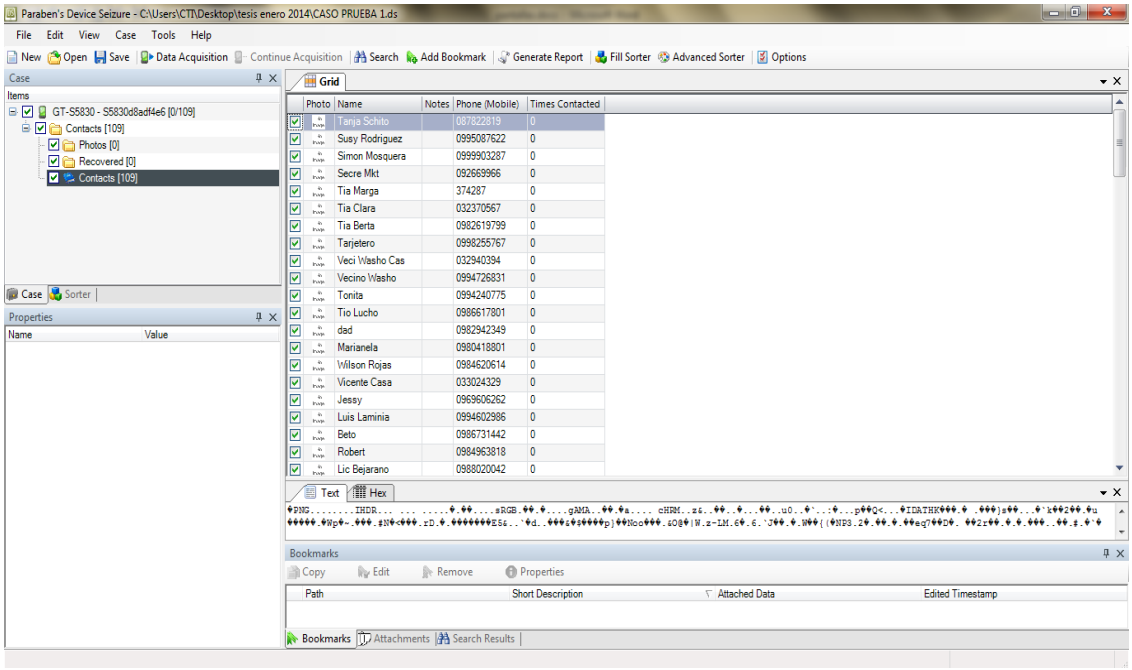


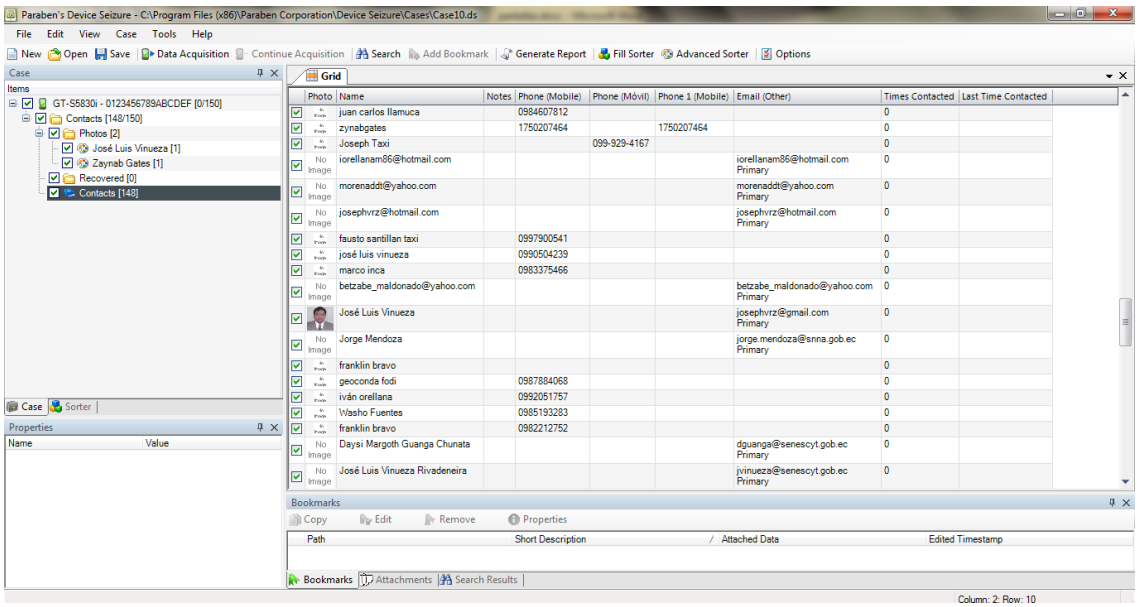


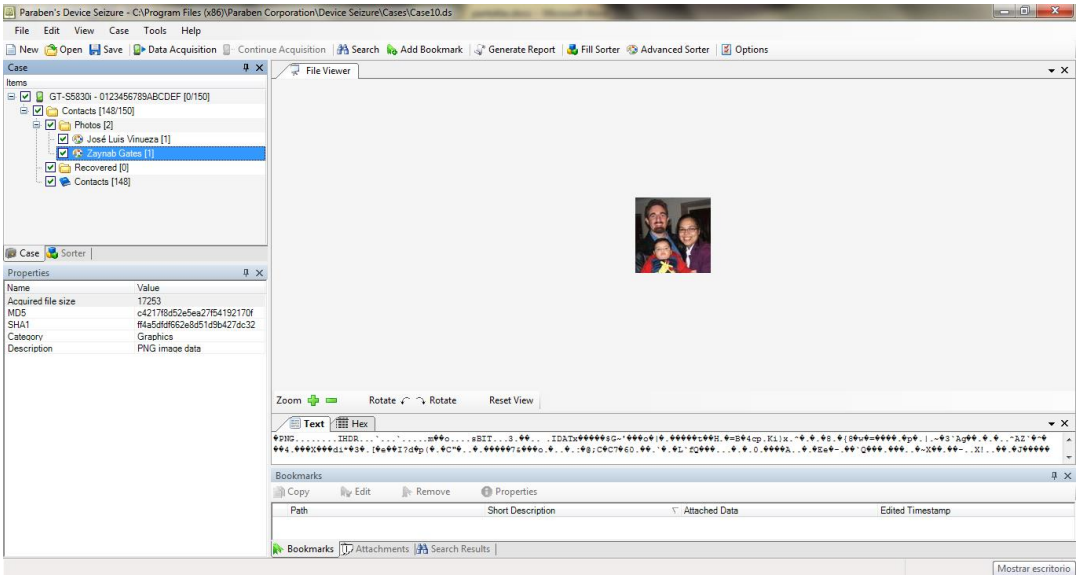
18. La información extraída del teléfono celular se presenta a continuación:

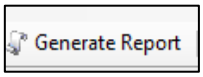


Name	Value
Program timestamp	12/01/2014 22:22:41
Device ID (IMEI)	357408041854161
Subscriber ID (IMSI)	740010133956766
Device Software Version	01
Network Operator Name	74001 (74001)
Network Type	UMTS
Phone Type	GSM
SIM Serial	8959301000339567666
SIM Operator Name	Claro (74001)
Board	GT-S5830
Brand	samsung
Device	GT-S5830
Firmware ID	GINGERBREAD
Model	GT-S5830
Product	GT-S5830
Release Version	2.3.4
SDK Version	10
Kernel Version	Linux version 2.6.35.7-perf-CL2
Up Time	4012.21 seconds
Idle Time	3697.23 seconds
CPU Info	ARMv6-compatible processor r
Total Memory	285184 kB
Manufacturer	samsung
Serial Number	S5830d8adf4e6


Paraben's Device Seizure - C:\Users\CTI\Desktop\tesis enero 2014\CASO PRUEBA 1.ds
File Edit View Case Tools Help
New Open Save Data Acquisition Continue Acquisition Search Add Bookmark Generate Report Fill Sorter Advanced Sorter Options
Case
Items
GT-S5830 - S5830d8adf4e6 [0/109]
Contacts [109]
Photos [0]
Recovered [0]
Contacts [109]
Case Sorter
Properties
Name Value
Grid
Photo Name Notes Phone (Mobile) Times Contacted
Tanja Schito 087822819 0
Susy Rodriguez 0995087622 0
Simon Mosquera 0999903287 0
Secre Mkt 092669966 0
Tia Marga 374287 0
Tia Clara 032370567 0
Tia Berta 0982619799 0
Tarjetero 0998255767 0
Veci Washo Cas 032940394 0
Vecino Washo 0994726831 0
Tonita 0994240775 0
Tio Lucho 0986617801 0
dad 0982942349 0
Marianela 0980418801 0
Wilson Rojas 0984620614 0
Vicente Casa 033024329 0
Jessy 0969606262 0
Luis Laminia 0994602986 0
Beto 0986731442 0
Robert 0984963818 0
Lic Bejarano 0988020042 0
Text Hex
Bookmarks
Copy Edit Remove Properties
Path Short Description Attached Data Edited Timestamp
Bookmarks Attachments Search Results

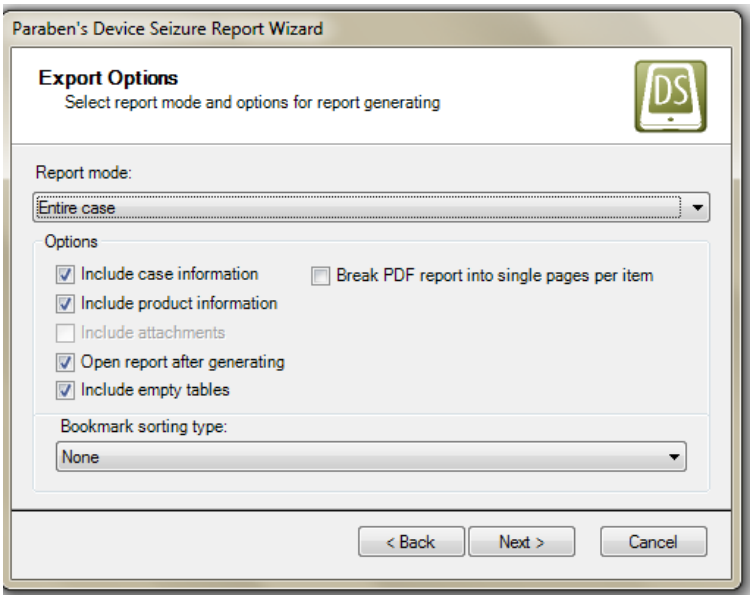

Paraben's Device Seizure - C:\Program Files (x86)\Paraben Corporation\Device Seizure\Cases\Case10.ds
File Edit View Case Tools Help
New Open Save Data Acquisition Continue Acquisition Search Add Bookmark Generate Report Fill Sorter Advanced Sorter Options
Case
Items
GT-S5830i - 0123456789ABCDEF [0/150]
Contacts [148/150]
Photos [2]
José Luis Vinueza [1]
Zaynab Gates [1]
Recovered [0]
Contacts [148]
Case Sorter
Properties
Name Value
Grid
Photo Name Notes Phone (Mobile) Phone (Móvil) Phone 1 (Mobile) Email (Other) Times Contacted Last Time Contacted
juan carlos llamuca 0984607812 0
zynabgates 1750207464 1750207464 0
Joseph Taxi 099-929-4167 0
iorellanam86@hotmail.com iorellanam86@hotmail.com Primary 0
morenaddt@yahoo.com morenaddt@yahoo.com Primary 0
josephvrz@hotmail.com josephvrz@hotmail.com Primary 0
fausto santillan taxi 0997900541 0
josé luis vinueza 0990504239 0
marco inca 0983375466 0
betzabe_maldonado@yahoo.com betzabe_maldonado@yahoo.com Primary 0
José Luis Vinueza josephvrz@gmail.com Primary 0
Jorge Mendoza jorge.mendoza@snna.gob.ec Primary 0
franklin bravo 0
geoconda fodi 0987884068 0
iván orellana 0992051757 0
Washo Fuentes 0985193283 0
franklin bravo 0982212752 0
Daysi Margoth Guanga Chunata dguanga@senescyt.gob.ec Primary 0
José Luis Vinueza Rivadeneira jvinueza@senescyt.gob.ec Primary 0
Bookmarks
Copy Edit Remove Properties
Path Short Description Attached Data Edited Timestamp
Bookmarks Attachments Search Results
Column: 2; Row: 10

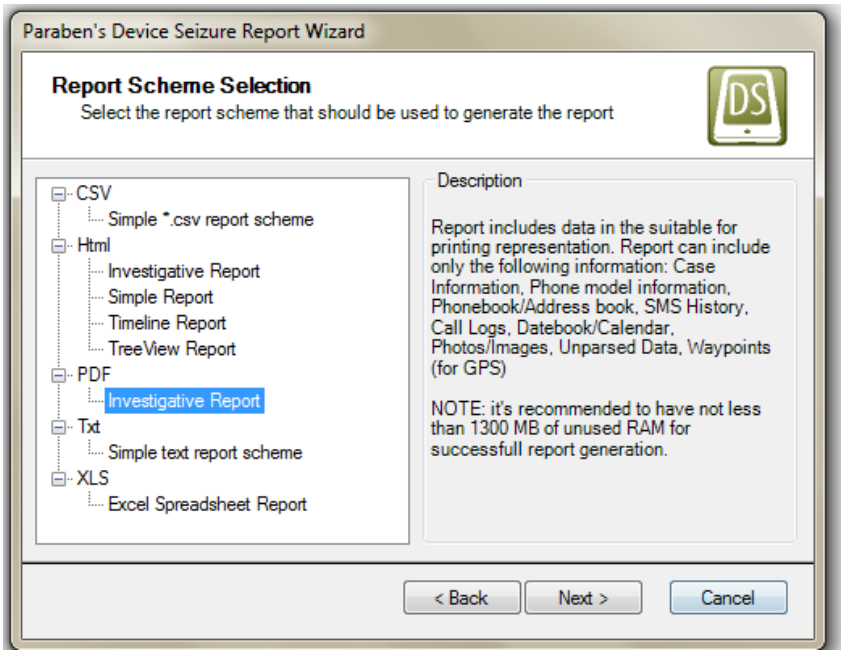


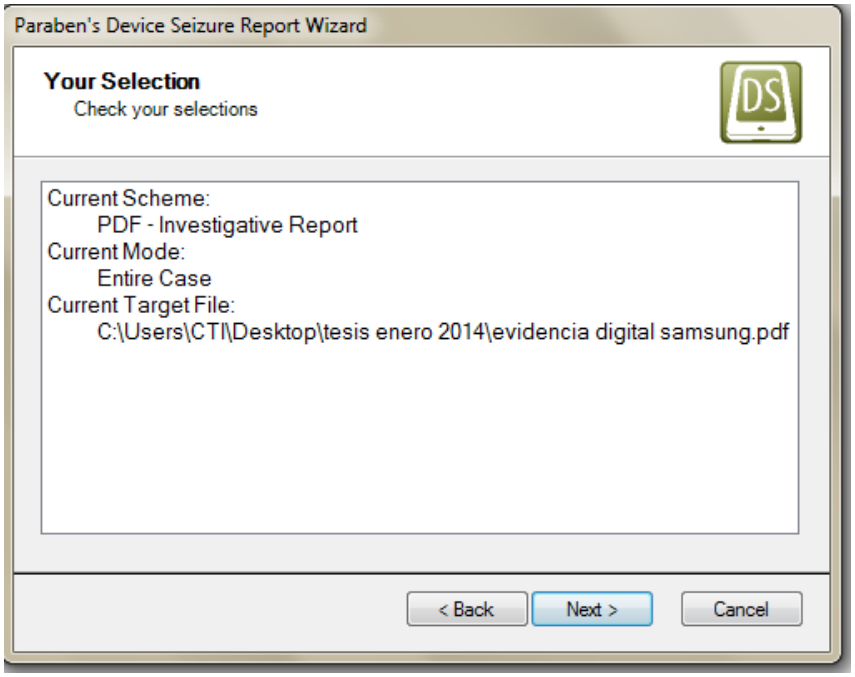
19. La herramienta es capaz de generar un informe con toda la información obtenida para lo cual accedemos a la opción 

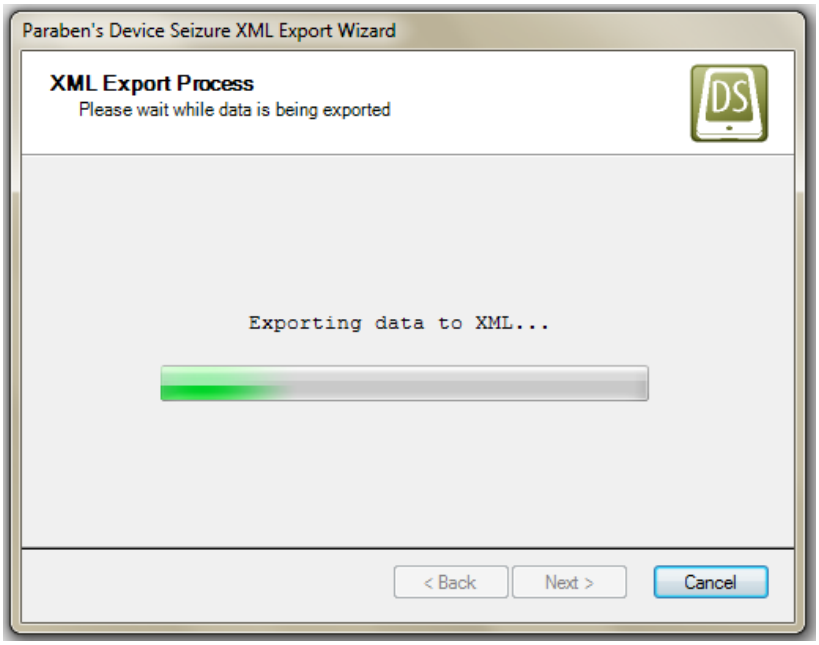
(*Generate Report)* de la barra de herramientas. La herramienta puede generar reports con extensión .pdf, .xml, xls, .txt, .html, .csv

20. También a través de la herramienta podemos exportar la información extraída como se muestra en la siguiente ventana




Paraben's Device Seizure Report Wizard
Report Scheme Selection
Select the report scheme that should be used to generate the report
CSV
Simple *.csv report scheme
Html
Investigative Report
Simple Report
Timeline Report
TreeView Report
PDF
Investigative Report
Txt
Simple text report scheme
XLS
Excel Spreadsheet Report
Description
Report includes data in the suitable for printing representation. Report can include only the following information: Case Information, Phone model information, Phonebook/Address book, SMS History, Call Logs, Datebook/Calendar, Photos/Images, Unparsed Data, Waypoints (for GPS)
NOTE: it's recommended to have not less than 1300 MB of unused RAM for successfull report generation.
< Back
Next >
Cancel

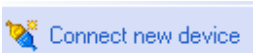

Paraben's Device Seizure Report Wizard
Your Selection
Check your selections
Current Scheme:
PDF - Investigative Report
Current Mode:
Entire Case
Current Target File:
C:\Users\CTI\Desktop\tesis enero 2014\evidencia digital samsung.pdf
< Back
Next >
Cancel


Paraben's Device Seizure XML Export Wizard
XML Export Process
Please wait while data is being exported
Exporting data to XML...
< Back
Next >
Cancel

PANTALLAS DE OBTENCIÓN DE EVIDENCIA DIGITAL CON LA HERRAMIENTA SUITE OXIGEN FORENSIC

Dispositivo celular a analizar: Sony Ericsson W810i

1) Iniciar la herramienta, clic botón Inicio / Todos los Programas / Oxygen Software / Oxygen Forensic Suite 2010 (Trial) /OxyForensic_Trial

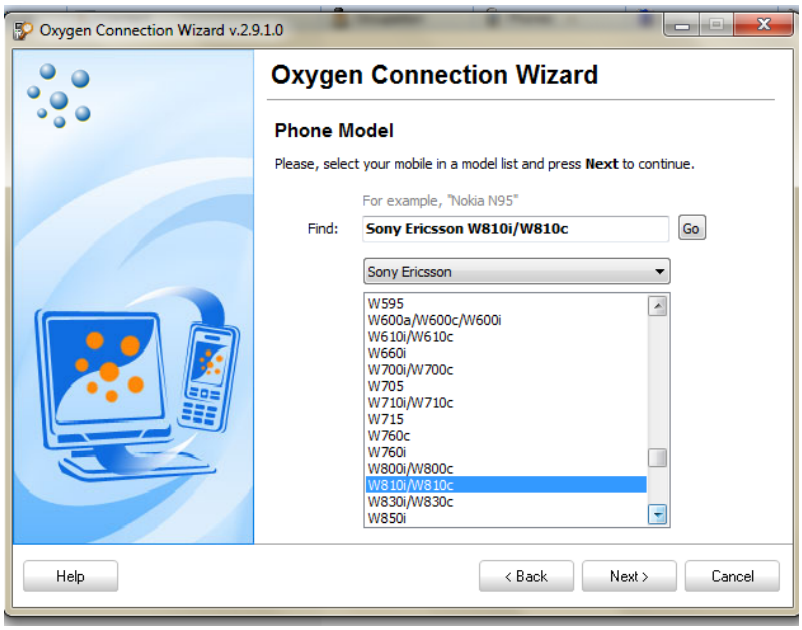
2) Clic sobre el botón 

(*Connect new device*) de la barra de herramientas, situada en la parte izquierda de la ventana se visualizará el asistente de conexión:

3)

4) Conectar el teléfono celular a través del puerto USB o encender el bluetooth del equipo celular
5) Como se va a conectar mediante bluetooth, elegimos la opción *Connect via Bluetooth*, clic en el botón *Next*

6) Seleccionamos el tipo de modelo de celular del cual vamos a extraer la evidencia digital, como se muestra en la pantalla siguiente:



7) Activamos la casilla de verificación eligiendo el tipo de conexión a utilizar, clic en el botón *Next*

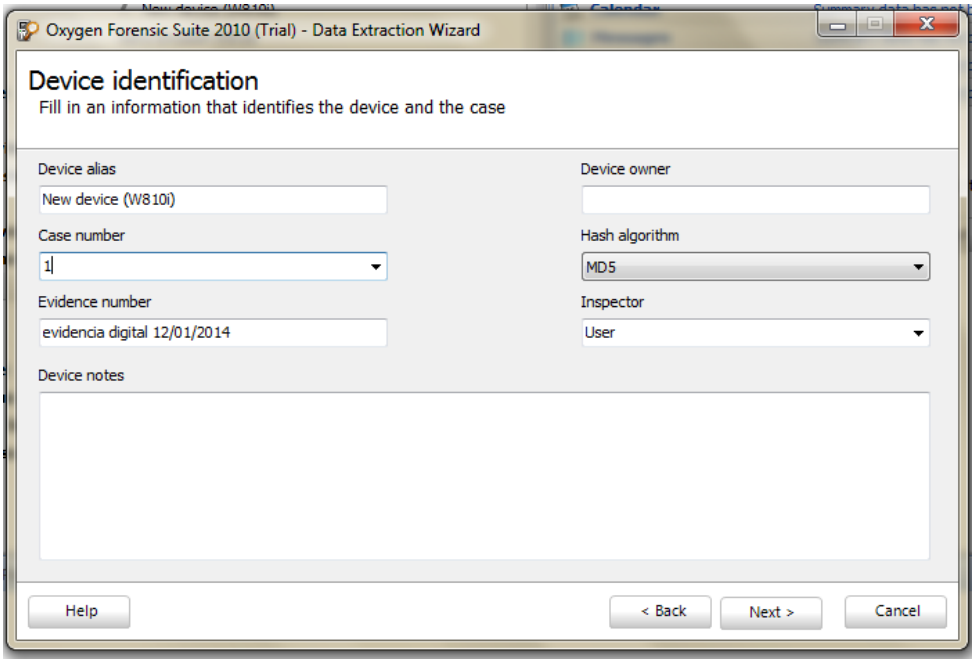
8) Clic en el botón *Search* para que la herramienta empiece a detectar al dispositivo celular conectado, seleccionamos el dispositivo a analizar en este caso el teléfono tienen nombre a través del dispositivo bluetooth el nombre es Fernando, elegimos y damos clic en el botón *Next*

9) Se visualiza la siguiente ventana, hay que esperar unos segundos a que se conecte con el dispositivo celular, una vez encontrado este dispositivo damos clic en el botón *Next*

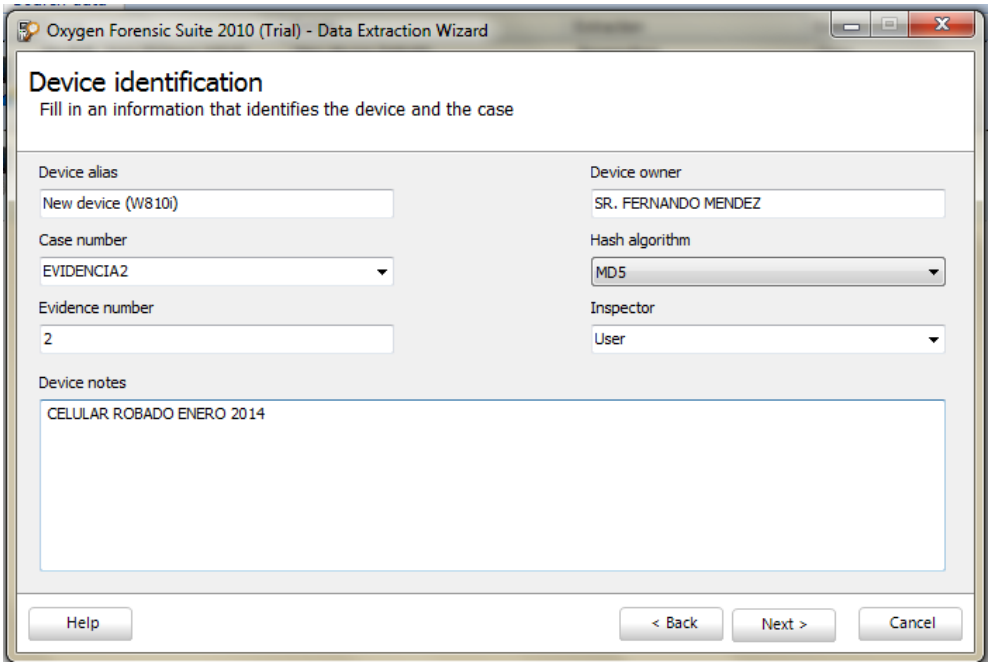
10) Clic en el botón *Next,* una vez que ha sido satisfactoriamente detectado el dispositivo celular, clic en el botón *Next*

11) La ventana siguiente presenta el IMEI del equipo celular conectado a la herramienta

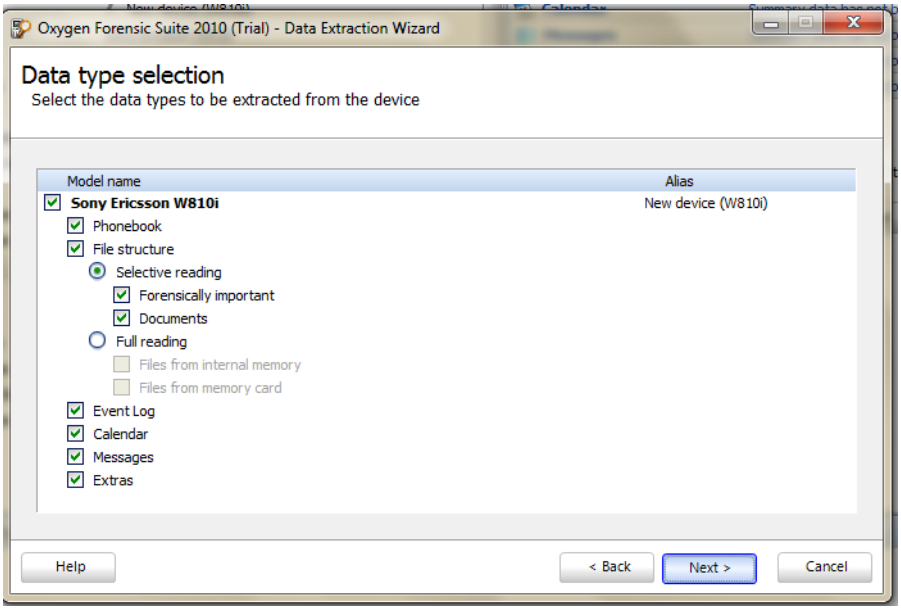
12) Llenar los siguientes campos requeridos para la extracción de la evidencia digital, una vez llenado los campos clic en el botón *Next*



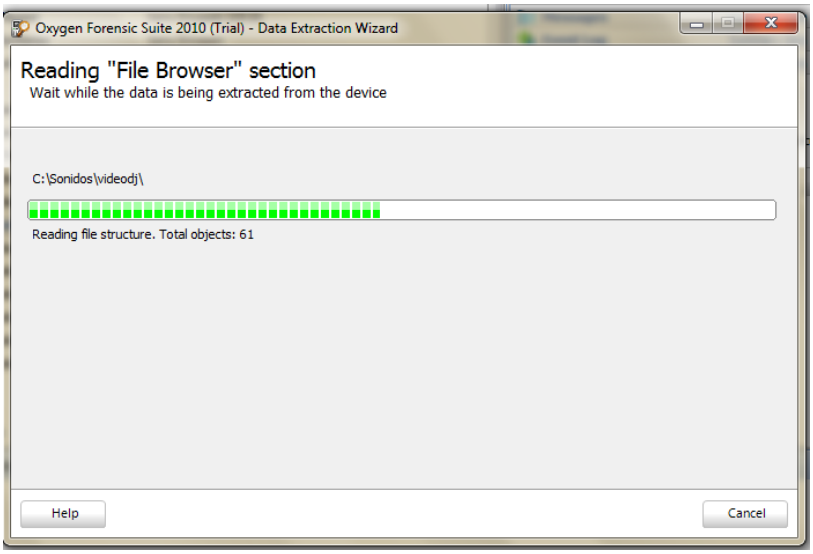
13) Llenar los para continuar conla extracción de la evidencia digital, una vez llenado los campos clic en el botón *Next*

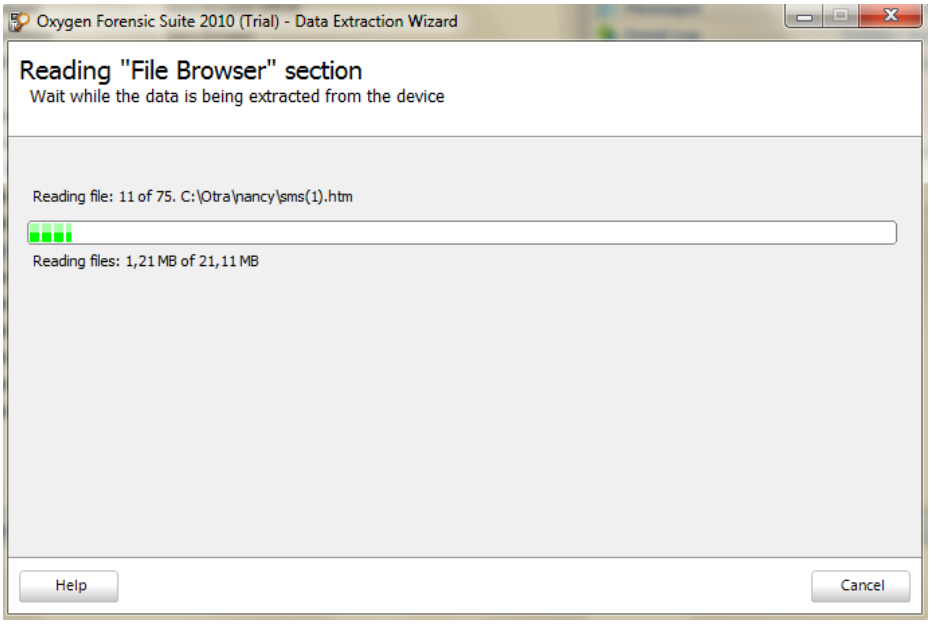


14) Seleccionar que tipo de datos se desea extraer (Agenda telefónica, mensajes, archivos de audio y video, calendario, eventos, documentos), clic en el botón *Next*

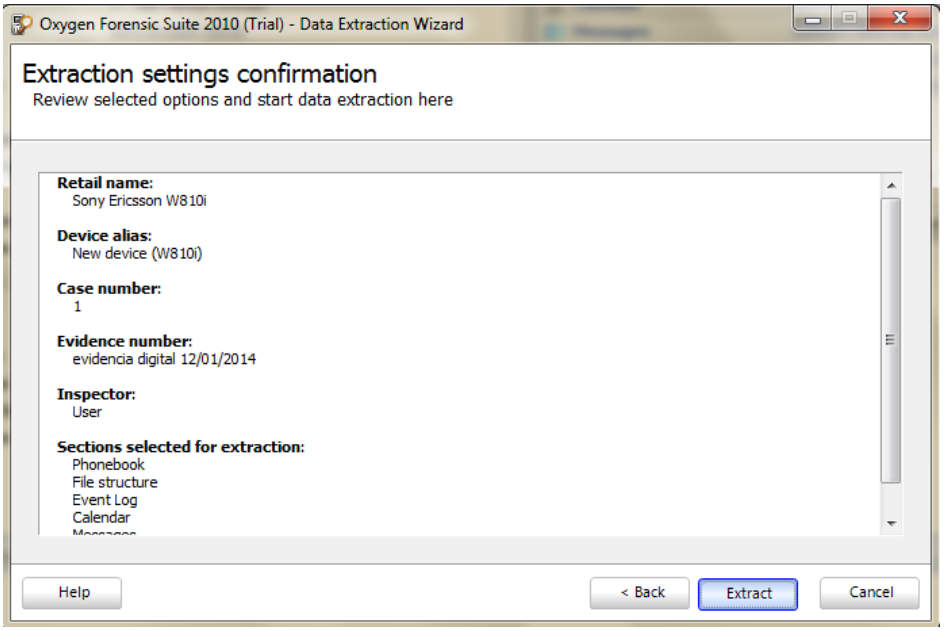


15) Esperar a que inicie a leer los archivos seleccionados del equipo celular, clic en el botón *Next*

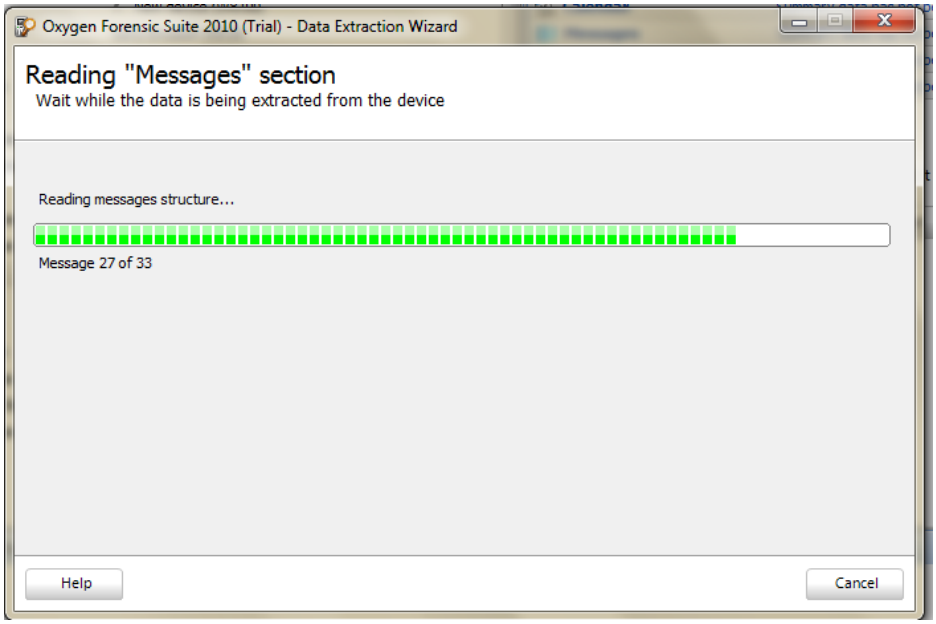




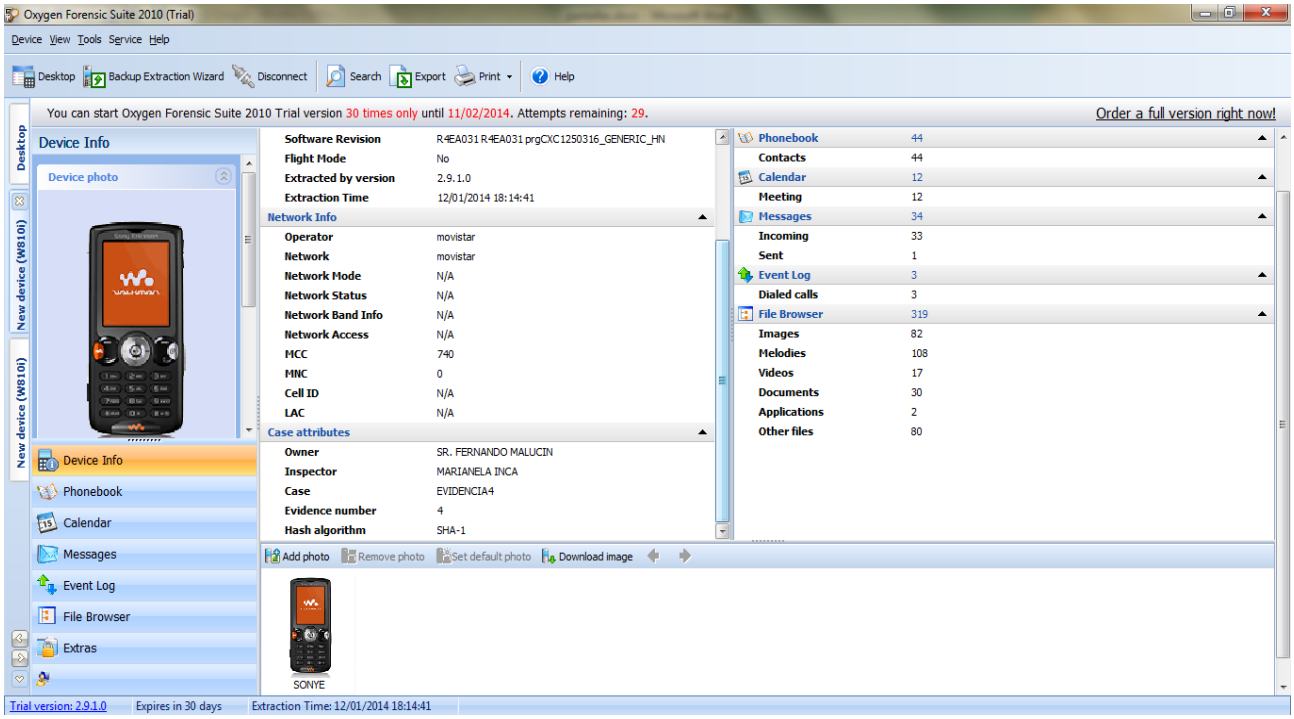
16) Confirmar la extracción de la evidencia digital, clic en el botón *Next*



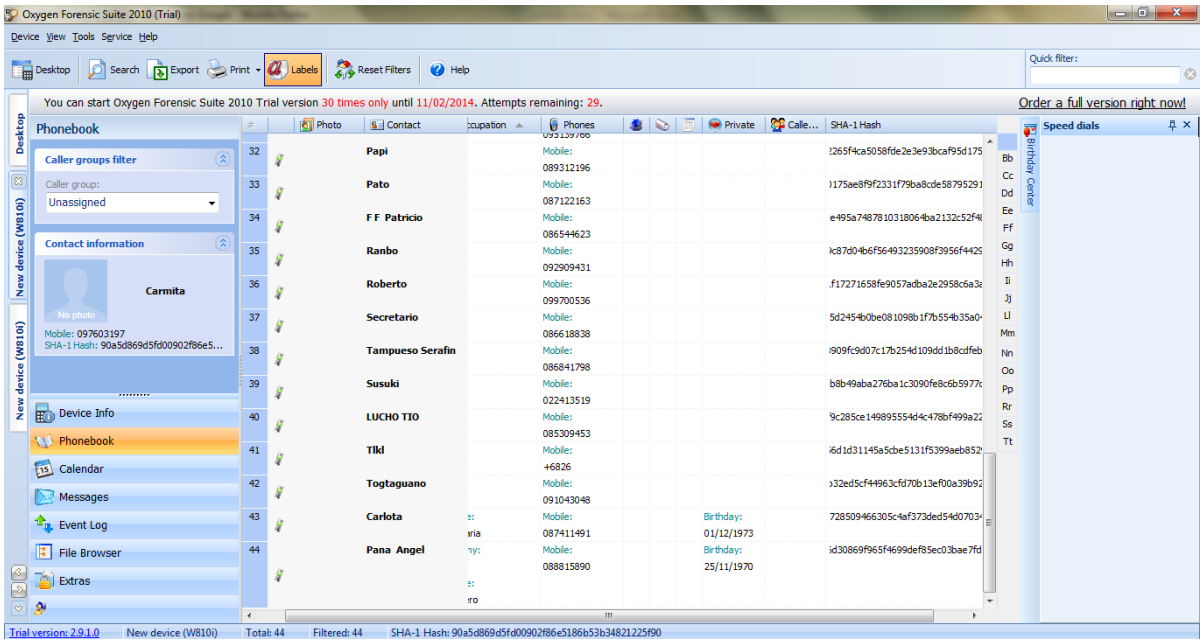
17) Esperar a que inicie con la descarga de los archivos seleccionados del equipo celular, clic en el botón *Next*



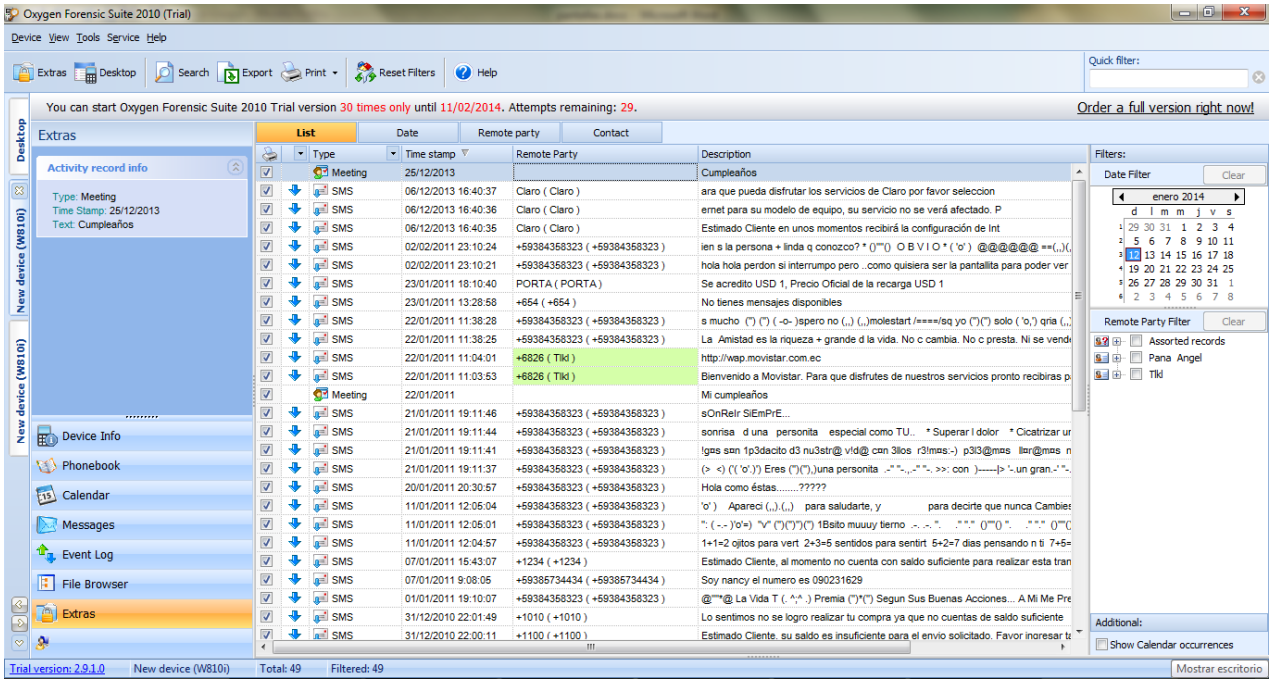
18) Una vez que se ha procedido con la descarga de los archivos del teléfono celular se mostrará la siguiente ventana que muestra información que contiene el equipo celular, y que será considerada como evidencia digital.



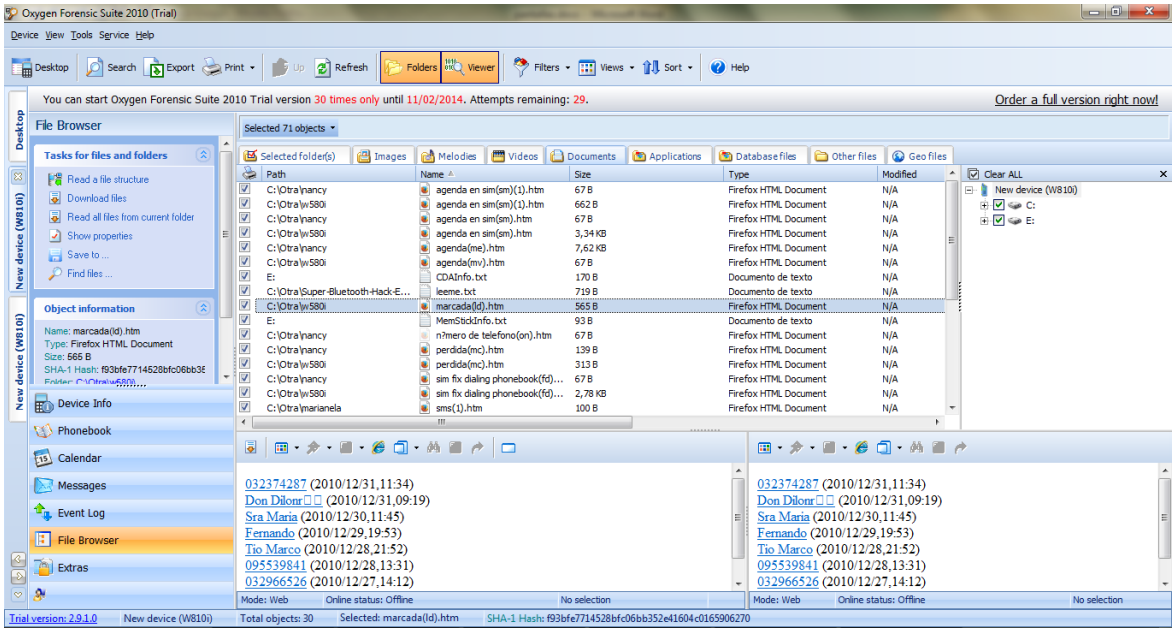
19) Clic sobre *Phonebook* para *p*resentar información de la agenda telefónica



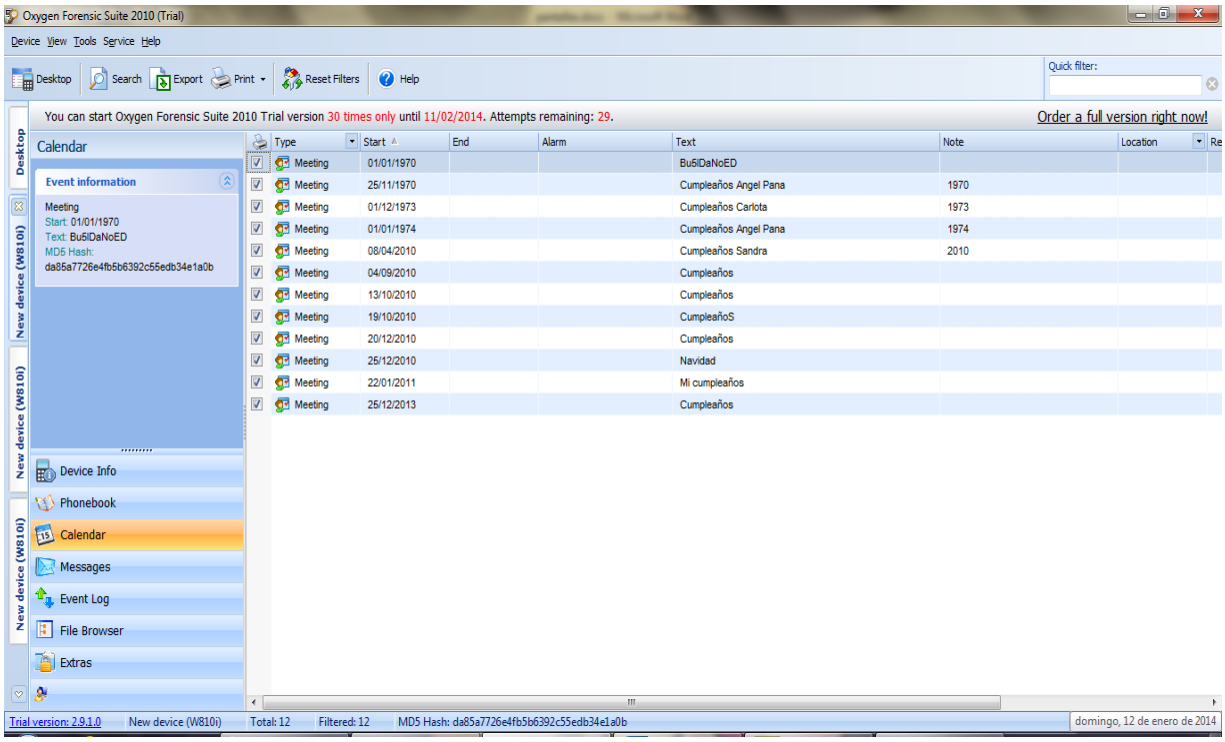
20) Clic sobre *Messages* para *p*resentar información de los mensajes contenidos en el equipo celular.



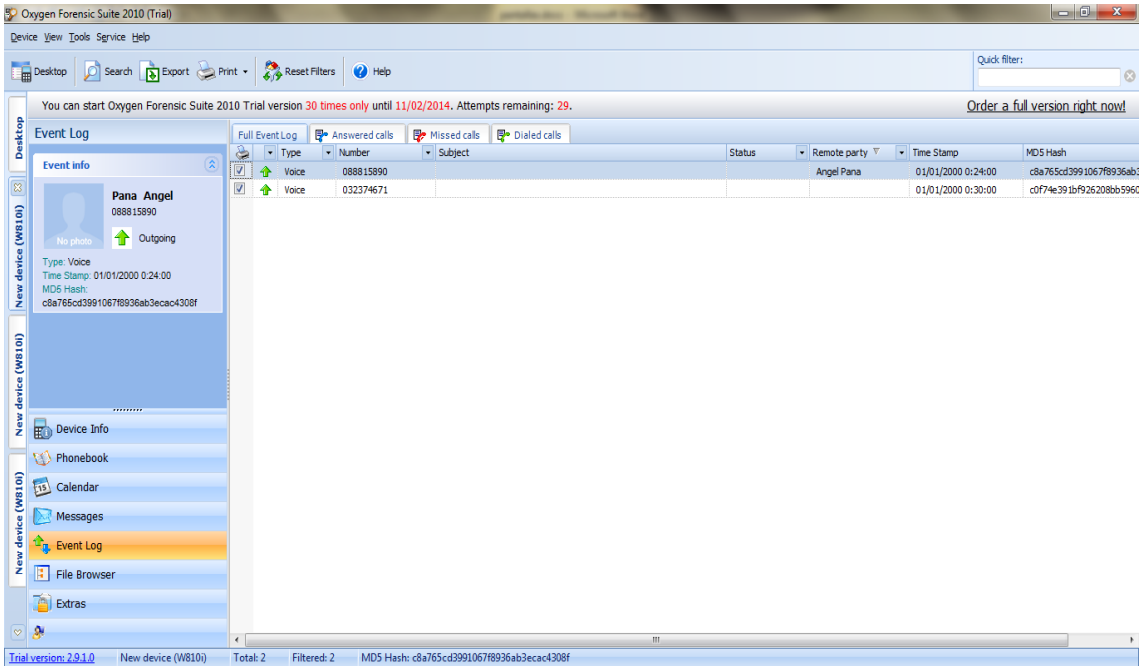
21) Clic sobre *File Browser* para *p*resentar archivos contenidos en el equipo celular.



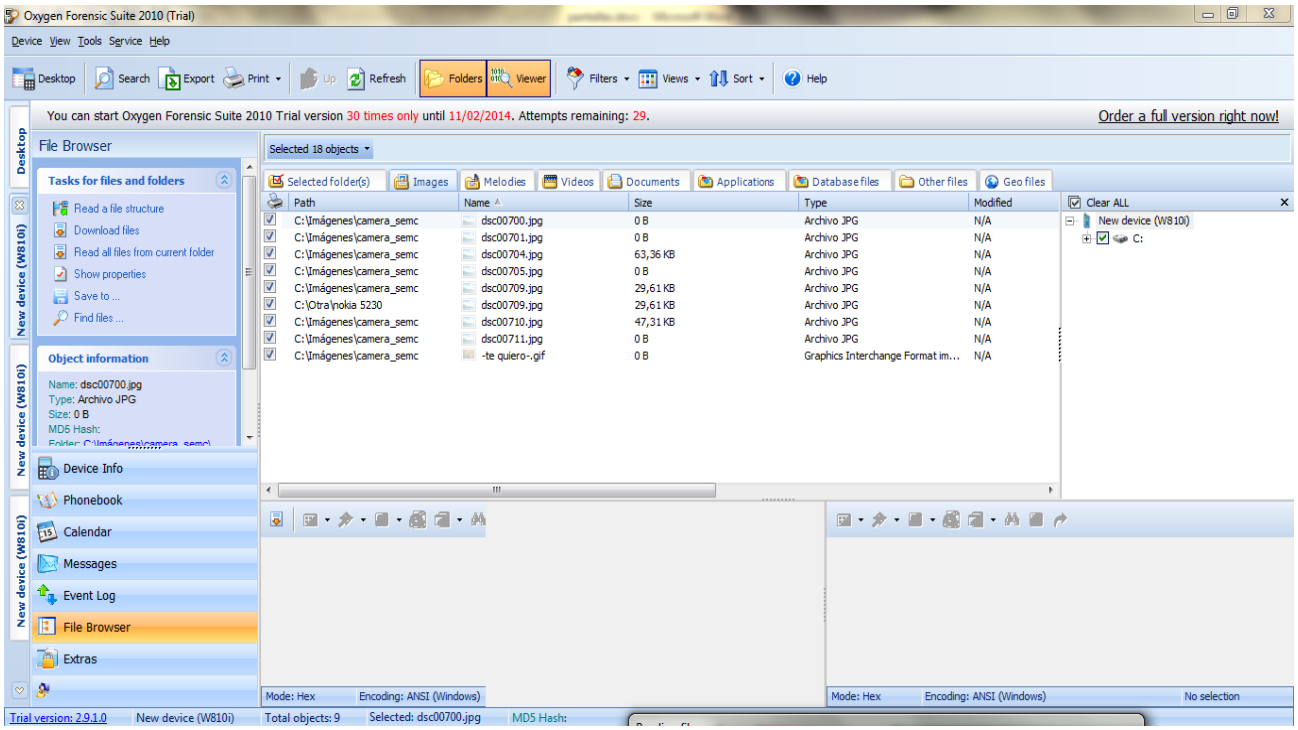
22) Clic sobre *Calendar* para *p*resentar información contenida en el calendario del equipo celular.



23) Clic sobre *Event log* para visualizar información sobre registro de eventos almacenados en el equipo celular.



24) Clic sobre *File Browser* visualiza archivos: imágenes videos, aplicaciones, otros archivos almacenados en el equipo celular.



PANTALLAS DE OBTENCIÓN DE EVIDENCIA DIGITAL CON LA HERRAMIENTA MOBILedit Forensic

Dispositivo celular a analizar: Sony Ericsson W810i

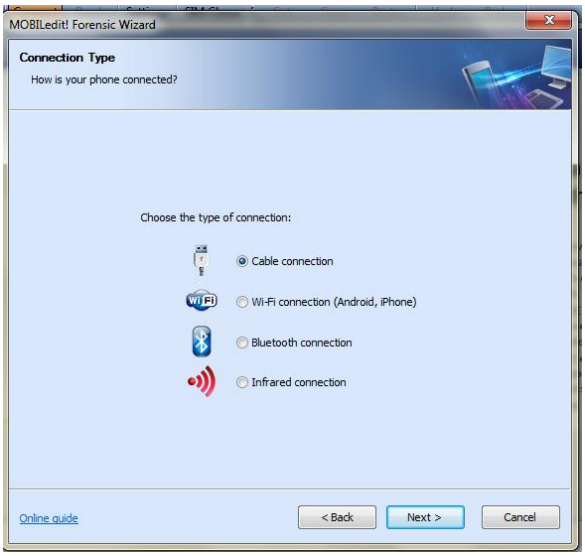
1. Iniciar la herramienta, clic botón Inicio / Todos los Programas / MOBILedit Forensic / MOBILedit Forensic

2. Clic en el botón 

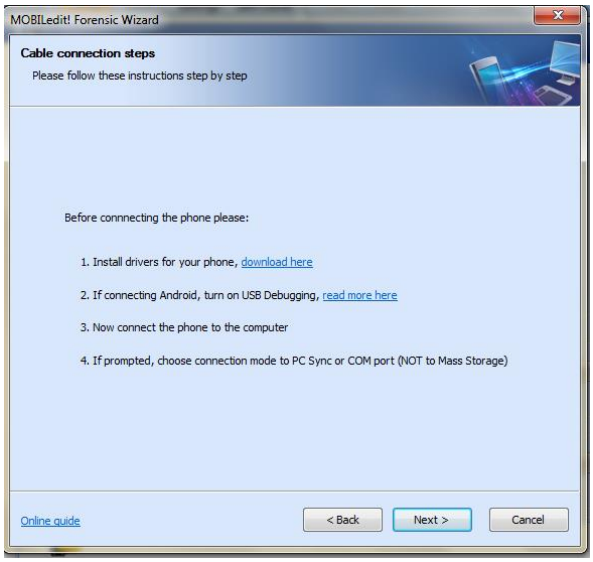
(*Connet)* de la barra de herramientas

3. Seleccionar el tipo de dispositivo a conectar, elegirla opción *Phone*

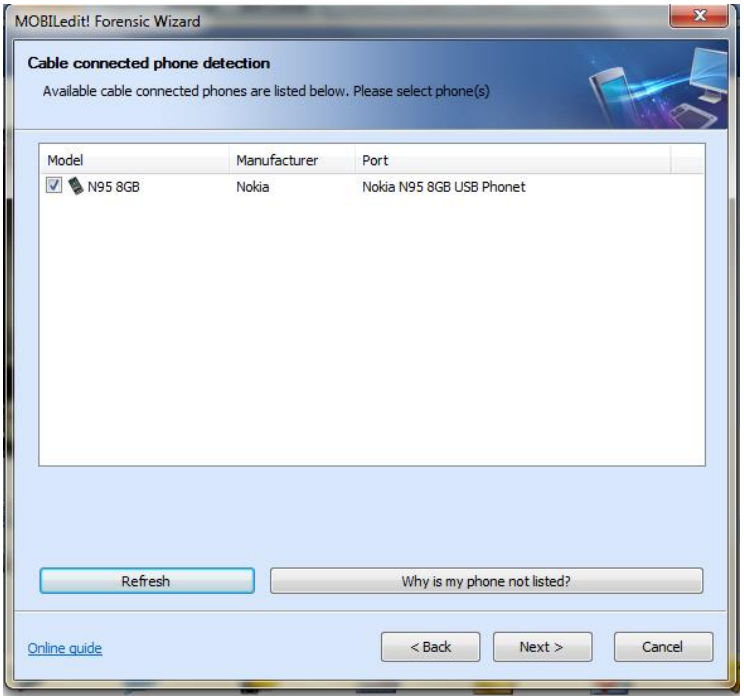
4. Seleccionar el tipo de conexión a utilizar, elegirla la opción *Cable connection*, clic en el botón *Next*



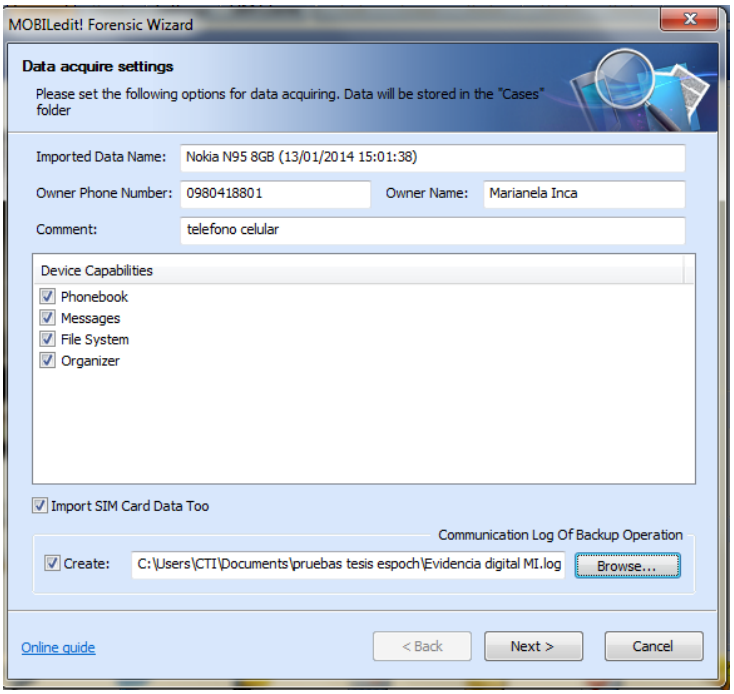
5. Para la extracción de la evidencia digital debemos asegurarnos que: el teléfono celular este encendido, que este activado el dispositivo bluetooth, y que el mismo este en modo visible, así como también este activado el bluetooth del computador, o si se va a conectar mediante cable conectar el cable del teléfono celular al puerto USB del computador (en el caso de no tener los drivers del equipo a examinar descargar dando clic en *download here*), clic en el botón *Next*



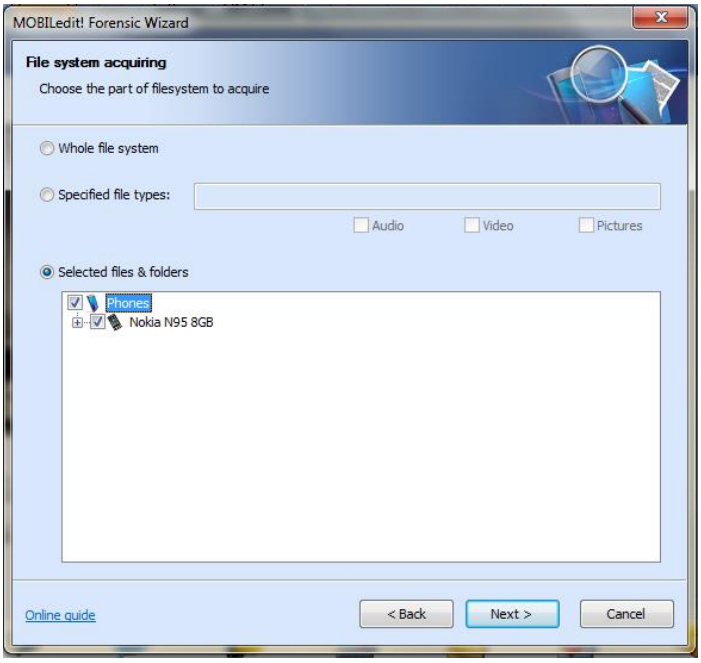
6. Clic en la opción *Refresh* para que inicie con la examinación para la extracción de información del equipo celular, una vez identificado el equipo celular, clic en el botón *Next*



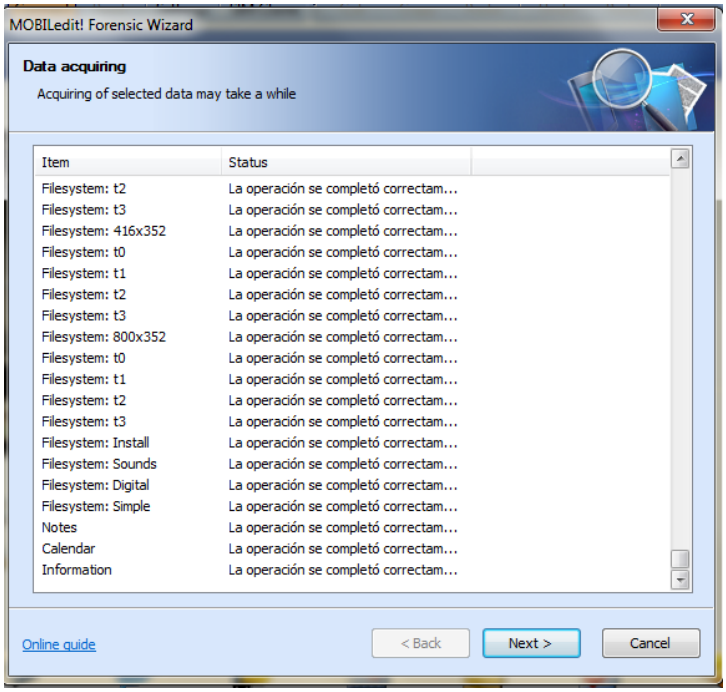
7. Proceder a llenar los campos solicitados en la siguiente ventana para la obtención de información, clic en el botón *Next*



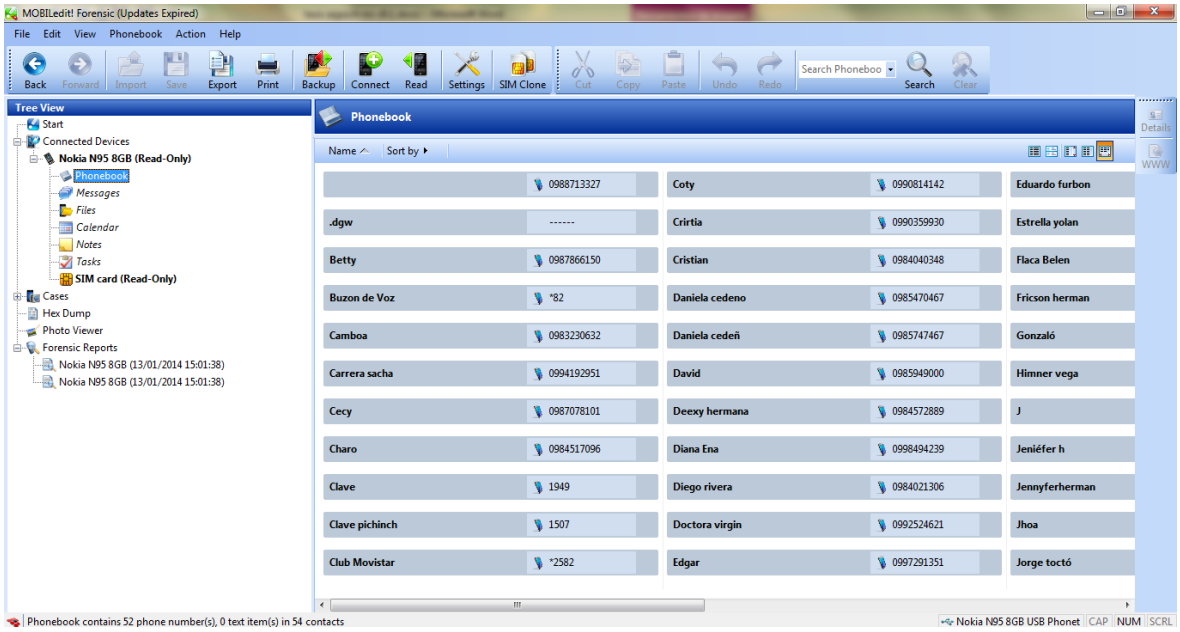
8. Seleccionar que tipo de archivos y de donde se desea extraer la información, para mi caso práctico clic en *Selected files & folders*, clic *Phones*, clic Nokia N95 8GB, clic en el botón *Next*

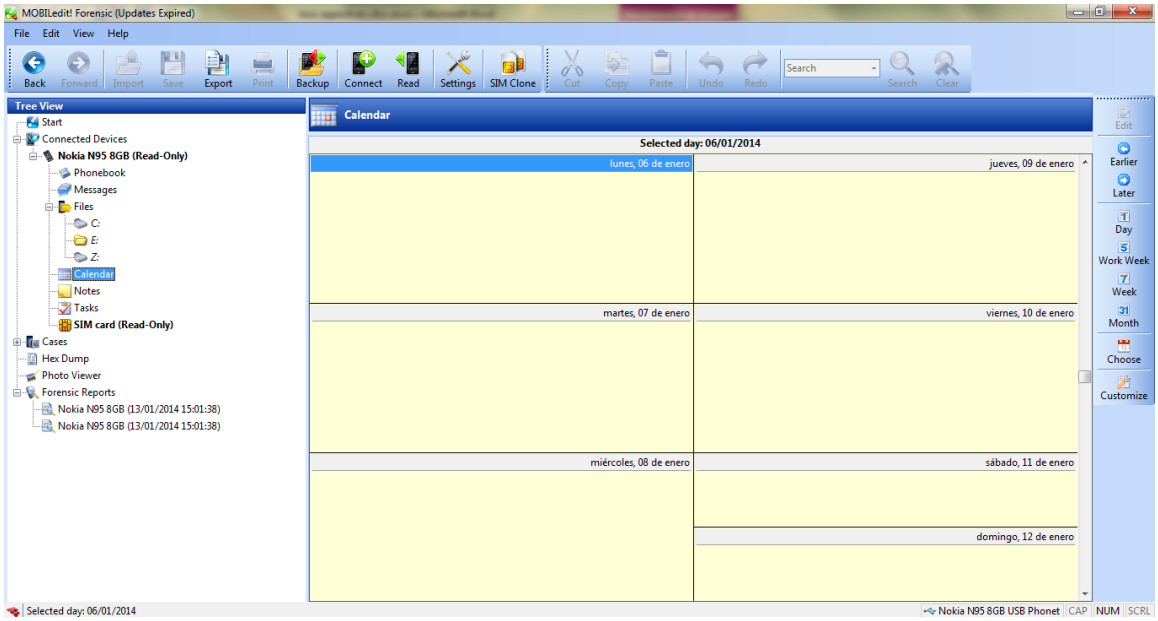


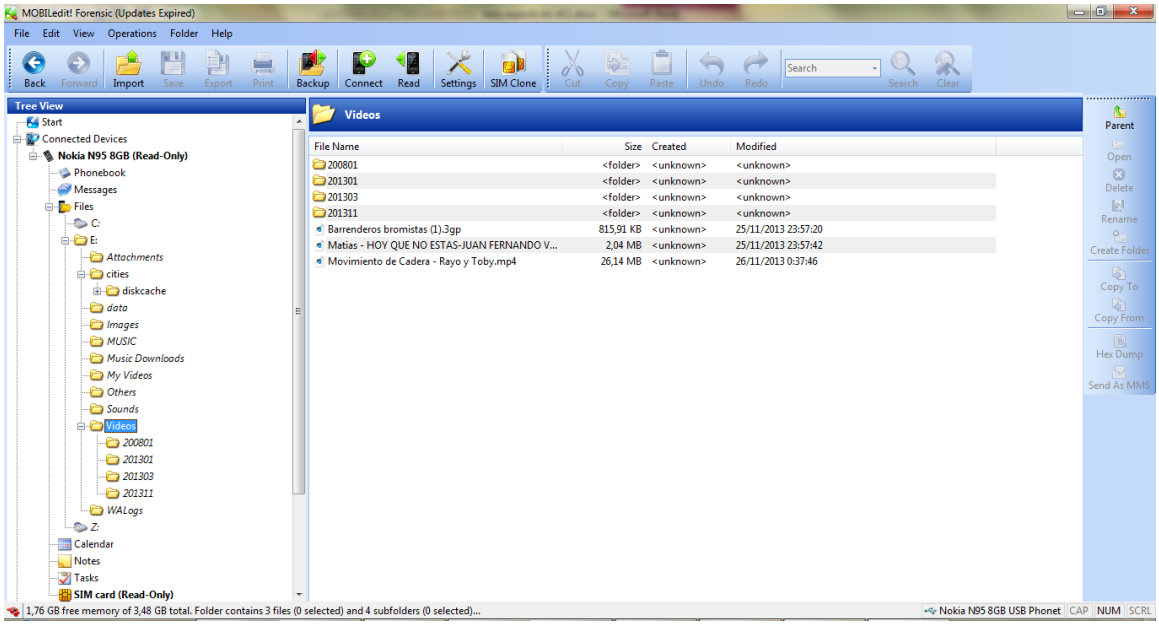
9. Esperar unos segundos a que se inicie a descargar la información considerada como evidencia del teléfono celular, clic en el botón *Next*



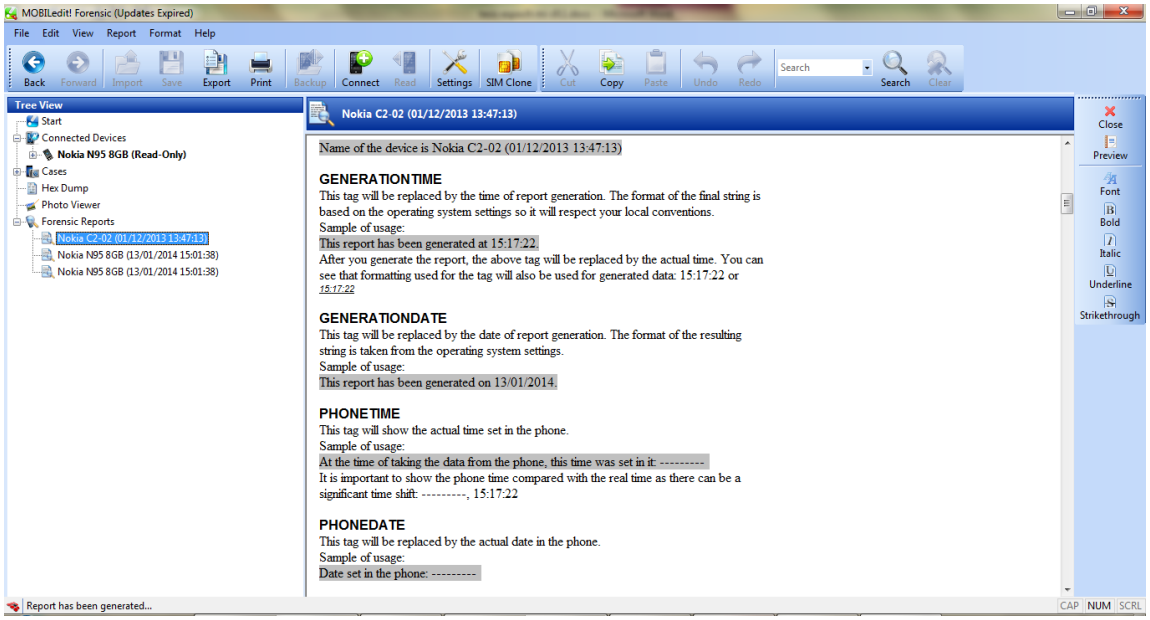
10. Una vez que se ha extraído la información se muestra las siguientes ventanas con los datos del teléfono celular y los archivos contenidos (agenda telefónica, mensajes, calendario, archivos, notas, tareas) en este:







11. La herramienta puede generar reportes con extensión: .xls, .xml, .rtf


MOBILedit! Forensic (Updates Expired)
File Edit View Report Format Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Search Clear
Tree View
Start
Connected Devices
Nokia N95 8GB (Read-Only)
Cases
Hex Dump
Photo Viewer
Forensic Reports
Nokia C2-02 (01/12/2013 13:47:13)
Nokia N95 8GB (13/01/2014 15:01:38)
Nokia N95 8GB (13/01/2014 15:01:38)
Nokia C2-02 (01/12/2013 13:47:13)
Name of the device is Nokia C2-02 (01/12/2013 13:47:13)
GENERATIONTIME
This tag will be replaced by the time of report generation. The format of the final string is based on the operating system settings so it will respect your local conventions.
Sample of usage:
This report has been generated at 15:17:22.
After you generate the report, the above tag will be replaced by the actual time. You can see that formatting used for the tag will also be used for generated data: 15:17:22 or 15:17:22
GENERATIONDATE
This tag will be replaced by the date of report generation. The format of the resulting string is taken from the operating system settings.
Sample of usage:
This report has been generated on 13/01/2014.
PHONETIME
This tag will show the actual time set in the phone.
Sample of usage:
At the time of taking the data from the phone, this time was set in it: ---------
It is important to show the phone time compared with the real time as there can be a significant time shift: ---------, 15:17:22
PHONEDATE
This tag will be replaced by the actual date in the phone.
Sample of usage:
Date set in the phone: ---------
Close
Preview
Font
Bold
Italic
Underline
Strikethrough
Report has been generated...
CAP NUM SCRL

ANEXO D

REPORTE FORENSE

Investigador Forense: Marianela Inca

Riobamba 2014

REPORTE EXAMINADOR FORENSE DESCRIPCIÓN DE DATOS

Nombre y apellido: ……
Institución a la que pertenece: ……
Cargo: ……
Fecha: ……

DATOS A RECOPILAR PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL

FASE 1

1. **Datos del ciudadano(s) al que se incautan los dispositivos y/o accesorios**

Nombre: …… ……...
Cédula de ciudadanía: …… ……...

2. **Procedencia del equipo celular:**
……
……...
……...

3. **Croquis de la escena de incautación del dispositivo celular**

4. **Descripción de los componentes electrónicos incautados**

TIPO DE DISPOSITIVO Y/O ACCESORIO	MARCA	NUMERO DE SERIE

5. **Observaciones**
……
……

REPORTE EXAMINADOR FORENSE DESCRIPCIÓN DE DATOS

FASE 2

6. **Herramientas forenses y utilitarios a utilizar**

……

……..

……..

……..

7. **Extracción de información del teléfono celular a examinar**

Se instala las herramientas forenses y utilitarios para realizar el análisis forense, se procede con la extracción de la información, para no alterar la información a ser considerada como evidencia digital se realizará una copia de seguridad.

8. **Registro de la cadena de custodia del dispositivo a examinar.**

Entidad:			**Tipo del elemento físico:**		
Fecha(DD/MM/AA)			**IMEI:**		
Ciudad:			**Numero Serial:**		
Sitio Exacto del hallazgo:			**Marca y referencia:**		
Descripción del elemento físico de prueba					
Fecha	**Hora**	**Nombre completo de quien recibe el elemento físico de prueba.**	**Propósito del traspaso de cadena de custodia.**	**Observaciones**	**Firma**

9. **Observaciones**

……

……

……

REPORTE EXAMINADOR FORENSE DESCRIPCIÓN DE DATOS

FASE 3

10. **Registro de la información recuperada para análisis**

TABLA XVI. Formulario de registro de la cadena de custodia [44]

Caso N°		**Código de evidencia:**	
Investigador:			
Examinador:			
Descripción del caso:			
RECEPCIÓN PARA EL ANÁLISIS			
Fecha:		**Hora:**	
DETALLES DEL TELÉFONO CELULAR			
Propietario:			
Condición:			
Fabricante:			
Modelo:			
Serial:			
IMEI:			
Número de teléfono:			
Operadora:			
Número de tarjeta SIM			
CARACTERÍSTICAS DEL TELÉFONO CELULAR			
Cámara: ☐ **Ringtons** ☐ **Capacidad de imágenes:** ☐ **Calendario:** ☐	**SMS:** ☐ **MMS:** ☐ **USB:** ☐ **Tarjeta externa:** ☐	**Agenda Telefónica:** ☐ **Capacidad de almacenamiento:** ☐ **Bluetooth** ☐ **Renvió de datos:** ☐ **Comandos de vos** ☐	
PARTICULARIDADES			
Teléfono Bloqueado:			
Cable:			
Fabricante de la batería:			
N° de serie de la batería:			

11. **Observaciones**

……

……

……

12. **ANEXOS**

Anexo D1. Formulario de identificación del personal

Anexo D2. Formulario de identificación y detección

Anexo D3. Formulario de identificación del dispositivo

Anexo D4. Formulario de elementos incautados

[44] LÓPEZ M., Análisis forense digital. Segunda Edición., 2007., pp. 13-20., E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

REPORTE EXAMINADOR FORENSE DESCRIPCIÓN DE DATOS

Anexo D1. Formulario de identificación del personal

TABLA XVII. Formulario identificación del personal [45]

FUNCIÓN	NOMBRE	IDENTIFICACIÓN (C.I.)
Investigador		
Examinador Forense		
Custodio de la evidencia		
Datos y firma del responsable quien llena el formulario		
_____ **Firma** **Responsable: ……..** **CI: ……**		

Anexo D2. Formulario de identificación y detección

TABLA XVIII. Formulario identificación y detección [46]

Fecha:		**Hora:**	
Ciudad:			
Dirección:		**Teléfono:**	
Observación del lugar de los hechos:			
Personas encontradas en el lugar de los hechos:			
Nombres y Apellidos		**Identificación (C.I.)**	
Entidad:			
Cargo:			
_____ **FIRMA**			

[45] LÓPEZ M., Análisis forense digital. Segunda Edición., 2007., pp. 20-30., E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[46] LÓPEZ M., Análisis forense digital. Segunda Edición., 2007., pp. 31-35., E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

REPORTE EXAMINADOR FORENSE DESCRIPCIÓN DE DATOS

Anexo D3. Formulario de identificación del dispositivo

TABLA XIX. Formulario identificación del dispositivo [47]

Caso N°		**Código de evidencia:**		
Fecha:			**Hora:**	
ESTADO DE CONEXIÓN				
Conectado:		**Desconectado:**		
Estado	**Encendido:**		**Apagado:**	
Estado de protección PIN	**Activado:**		**Desactivado:**	
Estado de protección	**Activado:**		**Desactivado:**	
INFORMACIÓN GENERAL				
Propietario:				
Dispositivo aislado:				
Accesorios del celular:				

Anexo D4. Formulario de elementos incautados

TABLA XX. Formulario elementos incautados [48]

Caso N°						
Fecha:			**Hora:**			
Tipo de dispositivo	**Marca**	**Modelo**	**Serial**	**Descripción**	**Estado**	**Propietario**
Observación:						

FIRMA

Responsable

C.I. …….

[47] LÓPEZ M., Análisis forense digital. Segunda Edición., 2007., pp. 21-28., E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[48] LÓPEZ M., Análisis forense digital. Segunda Edición., 2007., pp. 35-37., E-book: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf