PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN SISTEMAS

"ANALISIS Y APLICACIÓN DE SOFTWARE PARA LA RECUPERACIÓN FORENSE DE EVIDENCIA DIGITAL EN DISPOSITIVOS MÓVILES ANDROID"

CHRISTIAN DAVID GUERRA CASTRO

DIRECTOR: MTR. RAFAEL MELGAREJO

QUITO, 2014

INTRODUCCIÓN

A lo largo del tiempo la humanidad ha buscado sacar lo mejor de cada era y romper los paradigmas con las diferentes revoluciones como la escritura, la de la agricultura, la urbana y la industrial las cuales dieron un giro total y un avance al mundo entero.

Hoy en día, muchos expertos en el tema dicen que vivimos ya en una nueva transición de una revolución que es llamada revolución de la comunicación, la cual se puede ver día a día con el avance de los teléfonos inteligentes, cada vez computadoras más pequeñas, dispositivos prácticamente dedicados para la comunicación como tablets, ipads, etc.

En los siguientes años se estima que la venta de dispositivos móviles sea mayor que la de computadoras, ya que con la evolución y la portabilidad que tienen son una gran opción para la gente de negocios que necesita viajar más ligera de peso pero con toda su información disponible sin importar donde se encuentren.

Debido a esto se crea la necesidad de herramientas para facilitar la recuperación de información importante, perdida o borrada de los dispositivos.

Tenemos varios sistemas operativos para los dispositivos móviles como Android, IOS Windows Mobile y Symbian.

Los dispositivos Android desde su lanzamiento en el 2008 han tenido una gran acogida en el mercado internacional y han presentado un crecimiento impresionante debido a su gran variedad de equipos, marcas y precios que ha podido poner a disposición de los usuarios.

Por otro lado IOS con un solo dispositivo con varias versiones del mismo ha logrado mantener una muy buena acogida entre la gente.

Windows Mobile y Symbian han tenido varios problemas para posicionarse en el mercado actual pero aún se mantienen.

Así vamos viendo como las tecnologías de estos sistemas operativos van invadiendo el mercado con su innovación y el uso de los mismos va en aumento dependiendo su fin.

DEDICATORIA

Todo este esfuerzo va dedicado a mis padres por ser un apoyo fundamental en mi vida, a mi esposa e hijo que me alentaron para conseguir este objetivo tan anelado.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. ANDROID

1.1 Historia de Android

Wikipedia define Sistema Operativo conocido en Ingles como OS (Operating System) como el programa o conjunto de programas más importantes de un ordenador ya que interactúa directamente entre el hardware y los programas de aplicación y viceversa

El sistema operativo Android fue desarrollado inicialmente por Android Inc., en el 2003, cuyo fundador fue Andy Rubin, quien después de trabajar por varios años para empresas importantes como Apple y Microsoft[1]abrió sus oficinas ubicadas en California. Su software era exclusivo para dispositivos móviles basados en Linux. En agosto del 2005 es adquirida por Google conjunto con un grupo llamado Open Handset Alliance (OHA) que es una alianza comercial de 84 compañías que se dedica a ofrecer, desarrollar hardware y software de alto nivel a los usuarios, en donde Andy Rubin pasa a ser uno de los supervisores de desarrollo[2].

Los miembros más importantes son:

- Google
- HTC
- Dell
- Intel
- Motorola
- Qualcomm
- Texas Instruments
- Samsung
- LG
- T-Mobile

[1] Salas, Danny. La historia y los comienzos de Android, el sistema operativo de Google. Internet http://www.elandroidelibre.com/2011/08/la-historia-y-los-comienzos-de-android-el-sistema-operativo-de-google.html Acceso (18 de junio de 2013)

2 Wikipedia. Android. Internet http://es.wikipedia.org/wiki/Android#cite_note-AndroidInc-11 Acceso (18 de junio de 2013)

- Nvidia
- Wind River Systems

El logo del sistema Android (Figura 1) fue diseñado por Irina Blok, que fue parte de la campaña de lanzamiento. La idea original era crear el logotipo de código muy parecido al logo de Linux, que hiciera referencia a la originalidad y a partir de ser vista por cualquier persona podría ser reconocido sin necesidad de tener el nombre escrito[3].

Figura 1: Logo de Android

Creado por: Irina Blok.. Internet http://irinablok.dunked.com/android Acceso (18 de junio de 2013)

El anuncio de Android se dio en noviembre del 2007, mismo año de la creación de la Open Handset Alliance. Junto con esto Google liberó casi la mayoría del código de, una licencia de software libre creada por la Apache Software Foundation.

[3] Dunked. Android. Internet http://irinablok.dunked.com/android Acceso (18 de junio de 2013)

Android fue creado con la finalidad que los desarrolladores puedan hacer uso de todas las funciones del dispositivo móvil, facilitando incorporar nuevas tecnologías que van surgiendo con el paso de los días, ya que la plataforma debe continuar evolucionando a medida que la comunidad de desarrolladores trabajan juntos para construir aplicaciones móviles innovadoras.[4]

Android desde sus comienzos ha tenido varias actualizaciones lo cual a muchas personas ha molestado por la fragmentación que sufren las terminales, cada versión ha sido designada con nombres de postres, y se dictamino que desde su lanzamiento recibiría actualizaciones en 18 meses[5].

El lanzamiento del primer dispositivo móvil con Android se lo realizo en Octubre del 2008, el cual fue creado en conjunto con HTC, este fue llamado Nexus (Teléfono de Google). LG también tuvo un primer dispositivo para ser lanzado antes pero el que finalmente salió primero al mercado fue el HTC[6].

1.1.1. Historial de versiones de Android

Debido al avance de la tecnología y al crecimiento de las telecomunicaciones, Andriod ha tenido que sacar varias versiones al mercado cada una de ellas mejorando y trayendo nuevas aplicaciones para facilitar el uso del dispositivo a los usuarios y creando más ventajas a los desarrolladores para aprovechar el hardware de los dispositivos.

En el 2008 se puso al mercado la versión Android 1.0 que para muchos expertos aún no estaba lista, pero Google quería poner en el mercado su software y tratar de llegar a la mayor parte de usuarios[7].

---

[4] Open Handset Alliance. Android Internet http://www.openhandsetalliance.com/android_overview.html Acceso (18 de junio de 2013)

[5] Jamie Lendino. Google's Android Update Alliance Is Already Dead Internet http://www.pcmag.com/article2/0,2817,2397729,00.asp Acceso (18 de junio de 2013)

[6] Danny Salas. La historia y los comienzos de Android, el sistema operativo de Google. Internet http://www.elandroidelibre.com/2011/08/la-historia-y-los-comienzos-de-android-el-sistema-operativo-de-google.html Acceso (18 de junio de 2013)

[7] Txema Rodriguez. La historía de todas las versiones del SDK de Android en una infografía Internet http://www.genbetadev.com/desarrollo-aplicaciones-moviles/la-historia-de-todas-las-versiones-del-sdk-de-android-en-una-infografia Acceso (19 de junio de 2013)

Los desarrolladores de Android pusieron nombres de postres americanos en ingles ordenándolos alfabéticamente.

Cada versión además está acompañada de números en manera ascendente que indican el orden de su creación.

1.1.2. La evolución de Android, de 1.5. Cupcake a 5.0. Key Lime Pie

Figura 2: Historia de versiones de Android

Creado por Manuel Cornet:. Internet http://www.abcdesevilla.es/mobility/noticia/android/todas-las-versiones-de-android-en-un-divertido-grafico-de-su-evolucion/ Acceso (19 de junio de 2013)

Cupcake fue lanzado en abril de 2009, La actualización de Android 1.5 fue lanzada, basada en núcleo Linux. Esta versión contenia varias nuevas características y correcciones.

Tabla 1: Características Cupcake

Versión	Características
• 1.5	• Soporte para teclados virtuales de terceros con predicción de texto con diccionario. • Soporte para Widgets • Grabación y reproducción. • Sincronización de Bluetooth • Mejoras al navegador web. • Fotos a los contactos. • Agregada opción de decidir la rotación. • Subir vídeos a YouTube. • Mejor tiempo de búsqueda de los satélites

Creado por: Christian Guerra en base a Internet http://www.mundoandroides.com/los-nombres-postres-de-las-diferentes-versiones-de-android-y-sus-caracteristicas-tecnicas (19 de junio de 2013)

Donut fue lanzada el 15 de septiembre de 2009, basado en el núcleo Linux 2.6.29.

Tabla 2: Características de Donut

Versión	Características
• 1.6	• Mejoras de velocidad y aplicaciones de cámara. • Controlar el consumo de la batería. • Implementación de Quick Searh Box, caja de búsqueda en la pantalla para buscar distintas fuentes. • Organización del Android Market. • Búsqueda de texto y voz. • Habilidad de los desarrolladores de incluir su contenido en los resultados de búsqueda. • Multi lenguaje • Mejoras en Galería, cámara y videocámara. • Soporte para resoluciones de pantalla WVGA.

Creado por: Christian Guerra en base a Internet http://www.mundoandroides.com/los-nombres-postres-de-las-diferentes-versiones-de-android-y-sus-caracteristicas-tecnicas (19 de junio de 2013)

Éclair fue lanzado el 26 de octubre de 2009, tuvo dos versiones 2.0 y 2.1.

Tabla 3: Características Eclair

Versión	Características
• 2.0	• Sincronización con cuentas al dispositivo para sincronización de correo y contactos. • Soporte Bluetooth 2.1. • Cámara con flash y zoom digital. • Mejorada velocidad en el teclado virtual, con diccionario inteligente que aprende el uso de palabras. • Mejora la vista agenda del calendario. • Optimización en velocidad de hardware. • Soporte para más tamaños de pantalla y resoluciones, con mejor contraste. • Mejorado Google Maps. • Nuevo Navegador. • Contactos rápidos. • Reconocimiento de voz. • Aplicaciones dedicadas para el tiempo. • Mejoras en el uso de la batería.
• 2.0.1	• Cambios en el framework.
• 2.1	• Corrección de errores en la interfaz de programación de aplicaciones.

Creado por: Christian Guerra en base a Internet http://www.mundoandroides.com/los-nombres-postres-de-las-diferentes-versiones-de-android-y-sus-caracteristicas-tecnicas (19 de junio de 2013)

Froyo fue lanzada el 20 de mayo de 2010

Tabla 4: Características Froyo

Versión	Características
• 2.2	• Posibilidad de habilitar o deshabilitar datos sobre red móvil. • Nueva aplicación Market. • Discado por voz e intercambio de contactos por Bluetooth. • Optimizaciones en velocidad, memoria y rendimiento. • Soporte para Microsoft Exchange mejorado. • Mejoras con accesos directos • Se puede compartir el internet por red. • Soporte para contraseñas numéricas y alfanuméricas. • Puede visualizar Adobe Flash. • Actualizaciones automáticas. • Radio FM.

Creado por: Christian Guerra en base a Internet http://www.mundoandroides.com/los-nombres-postres-de-las-diferentes-versiones-de-android-y-sus-caracteristicas-tecnicas (19 de junio de 2013)

Gingerbread fue lanzado el 6 de diciembre de 2010 tuvo cerca de cinco versiones.

Tabla 5: Características Gingerbread

Versión	Características
• 2.3	• Actualizado el diseño de la interfaz de usuario. • Soporte de telefonía por internet Voz IP. • Soporte para (NFC), permitiendo intercambiar datos con el contacto con otros dispositivos. • Nuevos efectos de audio. • Mejora en gráficos. • Sensores. • Cambio de tamaño en widgets. • Administrador para descarga de archivos.

Creado por: Christian Guerra en base a Internet http://www.mundoandroides.com/los-nombres-postres-de-las-diferentes-versiones-de-android-y-sus-caracteristicas-tecnicas (19 de junio de 2013)

Honeycomb fue lanzada el 22 de febrero de 2011, siendo más estable pudo ser usado ya no solo en móviles, sino también en tablets[8].

Tabla 6: Caracteristicas Honeycomb

Versión	Características
• 3.0	• Mejoras en problemas de la cámara. • Rotación de la pantalla más fluida. • Numerosas optimizaciones y corrección de errores. • Mejoras en gráficos, bases de datos, corrección ortográfica y funcionalidades Bluetooth. • Mejoras en el calendario.

[8] Nilay Patel. Motorola Atrix 4G and Xoom tablet launching at the end of February, Droid Bionic and LTE Xoom in Q2 Internet http://www.engadget.com/2011/01/26/motorola-atrix-4g-and-xoom-tablet-launching-at-the-end-of-februa/ Acceso (19 de junio del 2013)

	• Nuevas aplicaciones de la cámara en mejora de la estabilidad en los videos y resolución QVGA. • Escritorio con gráficos 3D. • Sistema multitarea mejorado.
• 3.1	• Soporta teclados externos. • Conexión con puertos USB.
• 3.2	• Soporte para hardware. • Mejoras en la pantalla.

Creado por: Christian Guerra en base a Internet http://www.mundoandroides.com/los-nombres-postres-de-las-diferentes-versiones-de-android-y-sus-caracteristicas-tecnicas (19 de junio de 2013)

Ice Cream Sandwich, su lanzamiento oficial fue el 19 de octubre de 2011, el sistema operativo que ya en ese momento captaba en gran medida el mercado de tablets y samartphone; el dispositivo escogido para mostrarlo fue en Samsung Galaxy Nexus i 9250, teléfono desarrollado conjuntamente con Google y después liberado para el resto de dispositivos[9].

Tabla 7: Ice Cream Sandwich

Versión	Características
• 4.0.1	• Mejoras en la cámara. • Navegador Chrome como navegador del sistema. • Incluye botones suaves. • Capacidad de reconocimiento facial para desbloqueo. • Realizar capturas de pantallas. • Cambios de color de led para avisos e notificaciones.

[9]Todo Android. Todo Android Internet http://www.todoandroid.es/index.php/faq-de-android/65-versiones/805-que-es-ice-cream-sandwich-40-novedades-y-caracteristicas-de-esta-version-de-android.html Acceso (19 de julio del 2013)

	• Editor de fotos. • Ver notificaciones directamente en la pantalla de bloqueo. • Realizar fotos directamente desde la pantalla de bloqueo. • Mejoras y nuevas herramientas nativas en la grabación de videos.
• 4.0.2	• Corrección de errores en diferentes componentes.
• 4.0.3	• Se introducen ligeras mejoras en algunas APIs como el de redes sociales, calendario, revisor ortográfico, texto a voz y bases de datos entre otros.
• 4.0.4	• Presento mejoras en la definición y fluidez de la pantalla • Cambios en la cámara y video. • Reconocimiento facial.

Creado por: Christian Guerra en base a Internet http://www.xatakandroid.com/sistema-operativo/especial-ice-cream-sandwich-trucos-secretos-y-mas-detalles (19 de julio de 2013)

Jelly Bean, fue anunciado el 27 de junio de 2012 en un prendido y apagado de Google que es un congreso de desarrolladores realizado para despejar dudas y presentar nuevos productos, su lanzamiento oficial en un dispositivo fue el 13 de julio de 2012 conjunto con la Nexus 7[10].

Tabla 8: Jelly Bean

Versión	Características

[10] ABC Tecnología. ABC Tecnología Internet http://www.abc.es/tecnologia/moviles-telefonia/20130709/abci-jelly-bean-android-lider-201307091722.html Acceso (19 de julio del 2013)

• 4.1	• Mejor trabajo con el procesador, haciendo mucho más fluido y estable el uso del equipo. • Más rápido al mostrar animaciones graficas • Incorporación de Google Search. • Cuenta con un sistema de notificaciones inteligentes, que permite al usuario interactuar con varias aplicaciones. • Accesos directos, widgets se auto dimensionan y pueden ser removidos o cambiados de lugar. • Teclado inteligente mucha más fácil de usar, con varios idiomas. • Reconocimiento de voz, para hablarle al equipo para que escriba el texto. [11]
• 4.2	• Puede tomar fotos de 360 grados. • Gesture Typing (La posibilidad de escribir solo deslizando el dedo sobre el teclado). • La posibilidad de tener varios usuarios en tablets. • Conexión inalámbrica con monitores y televisiones[12].
• 4.3	• Permite autocompletar los números al momento de marcación. • Nueva interfaz de cámara. • Cuanto con un informe de notificaciones de

[11] García, Damián. Xataka Android Internet http://www.xatakandroid.com/sistema-operativo/asi-es-android-4-1-jelly-bean Acceso (19 de julio del 2013)
[12] García, Damián. Xataka Android Internet http://www.xatakandroid.com/sistema-operativo/asi-es-android-4-2-el-nuevo-sabor-de-jelly-bean Acceso (19 de julio del 2013)

	las aplicaciones. • Usuarios limitados (en las tablets que cuentan con multiusuario, se puede crear usuarios con limitaciones). • Capacidad de inhabilitar aplicaciones. • Bluetooth Smarth (para conectar fácilmente a otros dispositivos y para ahorrar batería)[13].

Creado por: Christian Guerra en base a Internet http://www.xatakandroid.com/sistema-operativo/asi-es-android-4-1-jelly-bean Acceso (19 de julio del 2013), Internet http://www.xatakandroid.com/sistema-operativo/asi-es-android-4-2-el-nuevo-sabor-de-jelly-bean Acceso (19 de julio del 2013) y http://www.xatakandroid.com/sistema-operativo/novedades-en-android-4-3-jelly-bean (30 de julio del 2013)

KitKat, la versión 4.4 de Android, fue muy mencionada en varias redes sociales ya que esta nueva versión fue lanzada en conjunto con el Nexus 5 y el Nexus 7, un teléfono inteligente desarrollado por LG[14] y una Tablet desarrollada por Asus, el nombre KitKat se lo relaciona con un producto de la multinacional Nestle[15].

Tabla 9: KitKat

Versión	Características
• 4.4	• Diseño más amigable. • Notificaciones, que ayudan al usuario a verificar funcionalidades. • Mejoras en la cámara. • Aplicaciones que aprovechan a lo máximo la pantalla. • Más funcionalidades para la tectología NFC. • Optimización del uso de la batería.

[13] Alias: Comos. Xataka Android Internet http://www.xatakandroid.com/sistema-operativo/novedades-en-android-4-3-jelly-bean (30 de julio del 2013)
[14] Helle, Lia. Geekets Internet http://www.geekets.com/2013/10/lanzamiento-nexus-5-android-kitkat/# (17 de octubre del 2013)
[15] Android http://www.android.com/kitkat/ (17 de octubre del 2013)

Creado por: Christian Guerra en base a Internet http://www.xataka.com/moviles/android-4-4-kitkat-pocas-novedades-a-simple-vista-pero-con-muchos-cambios-para-el-futuro Acceso (29 de noviembre del 2013).

1.2. Ventajas y Desventajas de Android

1.2.2. Ventajas de Android

Una de las principales ventajas que tiene Android frente a otros Sistemas Operativos móviles, es que al ser su código abierto, se tiene la facilidad de corregir errores y puede ser adaptado a diferentes equipos sin importar marca o hardware, así los usuarios pueden tener Smartphones de tres diferentes gamas que son: baja, media y alta[16]. Además en la actualidad es usado en tablets, relojes, portátiles y hasta en microondas.

Un Sistema Operativo de código abierto ofrece un sin número de aplicaciones disponibles que son cerca de 700.000, contando con un 75% gratuitas, que ha sido uno de los puntos fuertes para ganar mercado a nivel mundial y varias empresas se dediquen al desarrollo de software para Android.

Android fue uno de los pioneros en poder usar varias aplicaciones al mismo tiempo, y con una administración que era capaz de suspenderlas y cerrarlas para ahorrar recursos[17].

1.2.3. Desventajas de Andriod

Android posee varias marcas, modelos, gamas y diferentes precios, pero a pesar de lo que la mayoría hubiera pensado esto se ha vuelto en una desventaja, ya que al tener varios dispositivos, es algo complicado para los desarrolladores y los usuarios, ya que no se puede aprovechar al máximo el potencial de un dispositivo. Por este motivo al desarrollar una aplicación se debe tomar en cuenta factores como el diferente tipo de hardware y diferentes versiones de Android que existe en el mercado, para tratar de que la aplicación sea estándar y funciones en todos sus dispositivos.

[16] Master Pacheco, Fernando Sistema Operativo Android para moviles. Internet: http://www.slideshare.net/navarrocar/sistema-operativo-android-11594122 (29 de Noviembre del 2013)
[17] Sistema Android Internet: http://scoello12.wordpress.com/ventajas-y-desventajas/ (29 de Noviembre del 2013)

Hay empresas como Samsung que tienen aplicaciones propias para sus teléfonos de alta gama, los cuales no tienen problema al tener mayor procesador, memoria, ram y procesamiento gráfico, a diferencia de los de baja gama.

La desventaja para los usuarios es el desconocimiento de que es lo que necesitan o quieren de un dispositivo móvil, por esto llegan a tener dispositivos subutilizados.

Tabla 10: Diferente Gamas de Android

Gama	Características
• **Alta**	• Estos dispositivos son considerados como los más potentes y los que cada empresa fabricante se quiere posicionar como una alternativa a los mejores móviles cada año. Teniendo lo último en tecnología móvil.
• **Media**	• Los dispositivos de gama media están relacionados con calidad y precio.
• **Baja**	• Los dispositivos gama baja para personas que necesitan un dispositivo con Android, pero no invertir demasiado dinero. Pueden usar la mayoría de aplicaciones pero más se usan para de mensajería instantánea y redes sociales.

Creado por: Christian Guerra en base a Internet http://faqsandroid.com/moviles-android/ (10 de febrero del 2014).

2. INFORMÁTICA FORENSE

2.1. Historia de la Informática Forense

Inicia en Estados Unidos, su creación no data una fecha específica, pero la policía y los investigadores militares se percatan de que los criminales están utilizando nuevos medios y conocimientos para sus actos de vandalismo. Es por esto que en 1978 Florida reconoce los crímenes de sistemas informáticos en el "Computer Crimes Act", en casos de sabotaje, copyright, modificación de datos.[18]

Se puede decir que la informática forense se inició en la década de 1980, en 1984, fue creado un programa del FBI, conocido ahora como CART (CART, del inglés computer analysis and response team). Michael Anderson es considerado por muchos como el padre de la informática forense quien trabajó para el gobierno, posteriormente fundó New Technologies, Inc., que hoy en día es una de las empresas más grandes especializadas en el desarrollo de software.[19]

Posteriormente se ponen especial atención en la protección de información secreta y confidencial, que por el auge de la tecnología queda desprotegida, así empiezan a diferenciarse dos campos la seguridad de la información y la informática forense.

Miembros gubernamentales encargados de la protección de información importante, secreta y confidencial, empiezan a poner énfasis en las investigaciones forenses realizadas a las posibles brechas de seguridad y también para que en un futuro se aprenda a evitar situaciones similares.

El campo de la informática forense continúa creciendo diariamente. Cada vez más investigadores privados se especializan en el área de la informática forense, así como cada vez más compañías de software se interesan por producir programas forenses nuevos y mejores de acuerdo a las necesidades del mercado que den mejores respuestas a los delitos relacionados con la tecnología.

[18] Historia De La Informática Forense Internet: https://sites.google.com/site/sykrayolab/historia-de-la-informatica-forense

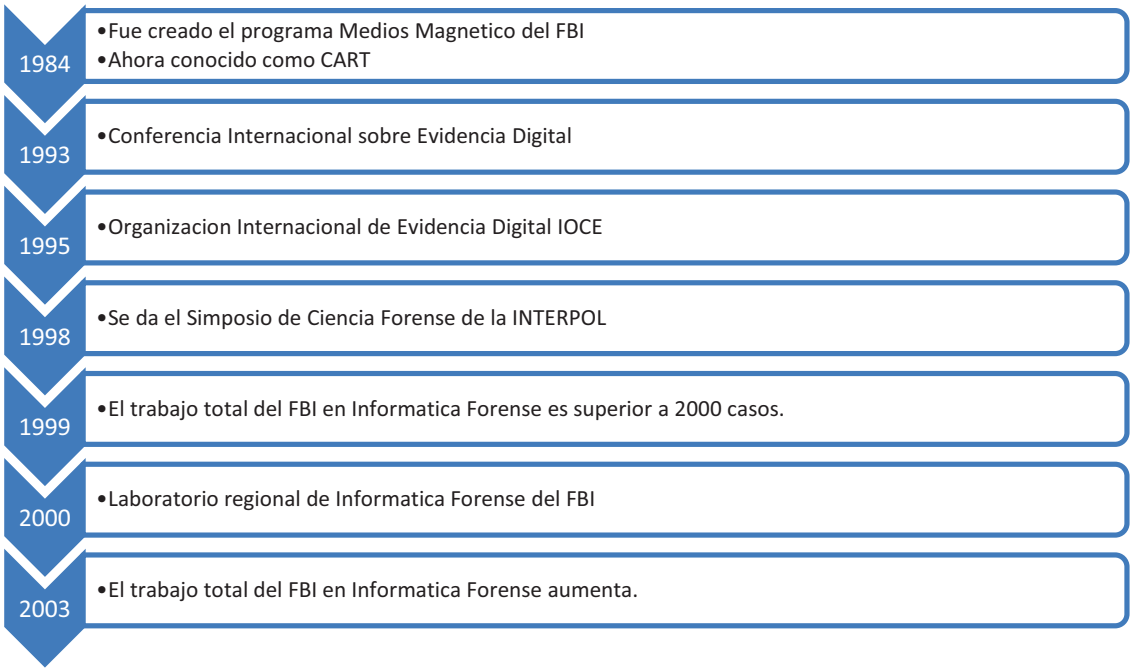
[19] Tucker Cummings La historia de la informática forense Internet: http://www.ehowenespanol.com/historia-informatica-forense-sobre_102525/ (19 de Febrero del 2014)

En los años 90 el FBI toma en consideración que las pruebas o evidencias digitales pueden ser un punto tan relevante en una investigación como el ADN, después de varias reuniones en 1995 se funda el International Organization on Computer Evidence (IOCE).

Para mazo de 1998, The High Tech Crime, un subgrupo del G8, pide al IOCE crear una serie de principios, procedimientos y métodos aplicables a las pruebas digitales a nivel mundial siendo fiables en cualquier lugar, esto tomo al IOCE dos años[20].

Cronología de la Informática Forense

Figura 3: Cronología de la Informática Forense



Creado por: Christian Guerra en base a Internet http://www.datarecovercenter.co/Servicios/Informatica-Forense/Auditoria-e-Investigacion-Forense/Historia-de-la-Informatica-Forense (10 de febrero del 2014).

[20] Rodríguez, Francisca La Informática Forense: El Rastro Digital Del Crimen Internet: http://www.derechoycambiosocial.com/revista025/informatica_forense.pdf (18 de Febrero 2014)

2.2. Análisis Forense Informático

El análisis forense de sistemas operativos consiste en la aplicación de técnicas científicas y analíticas especializadas para facilitar la recuperación y tratamiento de información después de que ocurra algún tipo de incidente.

Tiene los siguientes pasos:

- Identificar
- Preservar
- Analizar
- Presentar informe con resultados

Estas fases ayudan a la recopilación de información, autentificando y examinando datos; pero es necesario saber que datos son los que necesitan ser examinados y cuáles son las pruebas a aplicar dentro de una investigación.

El análisis forense es una disciplina que hace uso de la tecnología más avanzada, para poder preservar la integridad de los datos con procedimientos adecuados.

No solo nos ayuda a verificar e identificar ataques informáticos si no también a recuperar información oculta y borrada, por lo que necesita un conocimiento muy amplio tanto en hardware como en software y también en[21]:

- Redes
- Seguridad
- Hacking
- Cracking
- Recuperación de información[22]

[21] Auditorías de Seguridad Internet: http://www.informatica64.com/AnalisisForense.aspx Definiciones (19 de Febrero del 2014)
[22] Cómputo forense Internet: http://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Definiciones (19 de Febrero del 2014)

2.3. Fases del Análisis Forense

2.3.1. Identificar

En esta fase se usa uno de los recursos más importantes, que es el humano. Ya que se debe contar con información y técnicas para identificar de manera adecuada la evidencia digital, para esto existen guías como la Guía del United States Secret Service , o la del Australasian Centre for Policing Research entre otras.

También se debe realizar actas e identificar y clasificar correctamente la evidencia digital para tener un inventario de toda la evidencia tanto física como digital y de esta forma lograr un mejor entendimiento de lo que se tiene que realizar posteriormente.[23]

La Evidencia Digital es el conjunto de datos en formato binario, se encuentren tanto enfísicos o lógicos del sistema, los mismos pueden ser extraídos y analizados.

Tipo de Evidencia Digital

Constante: información que siempre esta guardada en el dispositivo y se conserva siempre.

Volátil: es cuando se considera una memoria temporal como archivos temporales o memoria RAM.[24]

Lógica: cualquier dato almacenado en un medio, esta información puede se puede ser clasificada en tres categorías:

- **Registros generados por computador**
  Estos son llamados registros de eventos o conocidos como logs, pueden ser utilizados como prueba tras demostrar un adecuado funcionamiento. Estos registros son inalterables por una persona.[25]

[23]Gómez, Leopoldo Sebastián M. El tratamiento de la Evidencia Digital Internet http://sebastiangomez.sytes.net/papers/ETED.pdf (19 de Febrero del 2014)
[24] Fases De La Informática Forense Internet: http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf (19 de Febrero del 2014)
[25] Gutiérrez , Juan David Informática Forense Internet: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf (19 de Febrero del 2014)

- **Registros no generados**

  Estos pueden ser generados por un usuario utilizando un editor de texto. En estos registros se debe demostrar la valides con los que fueron realizados.[26]

- **Registros híbridos**

  Estos registros son aquellos generados por la máquina, que guardan opciones escogidas previamente en el computador y son almacenados en forma de logs.

- **Registros de cada servidor**

  Son registros que genera el sistema y también de cada programa en ejecución.[27]

- **Registros de tráfico de red**

  Estos registros tienen la cantidad de datos enviados y recibidos para intercambiar información.

2.3.2. Preservar

En el proceso de preservación se deben tomar en cuenta algunos puntos básicos como son: la tecnología de punta, evitar la contaminación de la evidencia, la cadena de custodia y resguardar la información que contenga evidencia.[28]

Los pasos a seguir para preservar la evidencia son:

- Realizar copias del dispositivo de almacenamiento en donde se encuentra la información a ser analizada.
- Identificar cada una de las copias con fecha hora de creación de la copia y nombre.
- Preservar las copias, usando bloqueadores de escritura, evitando cambios en la temperatura, o evitando el contacto con campos electromagnéticos ya que la información puede ser contaminada o alterada e invalidar el proceso.[29]

[26] Zuccardi ,Giovanni Informática Forense Internet: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf (19 de Febrero del 2014)
[27] Fases De La Informática Forense Internet: http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf (19 de Febrero del 2014)
[28] Wikipedia Computo Forense Internet: http://es.wikipedia.org/wiki/C%C3%B3mputo_forense (1 de Marzo del 2014)
[29] Fases De La Informática Forense Internet: http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf (1 de Marzo del 2014)

- Documentar los métodos utilizados para la preservación de la información detalladamente.

El objetivo de la preservación de información es conservar a integridad los datos desde su fuente hasta el análisis con el fin que pueda ser utilizada como una prueba legal.[30]

2.3.3. Analizar

El análisis de la evidencia digital tiene como objetivo extraer información relevante para la investigación, en el cual se busca realizar una línea de tiempo que traza un antes y un después de un delito cometido. Para esto se aplicaran técnicas científicas y analíticas a las copias del dispositivo de almacenamiento que obtuvimos en el proceso de preservación.

Este proceso concluye al determinar los involucrados en el delito, el objetivo de su cometido, las circunstancias en las que se llevó a cabo el hecho, y las consecuencias.

Durante el proceso se pueden emplear herramientas propias del sistema operativo en el que se esté trabajando, lo importante es seguir los pasos recomendados:

- Entorno de trabajo: este debe ser adecuado ya sea que contenga ambientes similares o que las investigaciones sean realizadas en el ambiente original, con el fin de realizar diferentes tipos de pruebas.
- Reconstrucción de la secuencia temporal del ataque: determinar los archivos anteriores y posteriores al delito.
- Determinación de cómo se realizó el ataque: para esto realizaremos una cadena de acontecimientos para determinar el ataque, el objetivo y la vía de entrada.
- Identificación del autor o autores del incidente: tras identificar el objetivo del delito el siguiente paso es determinar los autores.
- Documentación: la cual debe ser llevada de la mejor manera ya que al final será la que sirva como evidencia.[31]

[30] Almeida Romo , Omar Metodología de Análisis Forense Internet: http://repositorio.utn.edu.ec/bitstream/123456789/539/21/04%20ISC%20157%20RESUMEN%20TECNICO%20ESPA%C3%91OL.pdf (1 de Marzo del 2014)

Para realizar el análisis se debe contar con la siguiente información:

- Sistema Operativo
- Conexión a Internet
- Configuración
- Actualizaciones del software
- Seguridades del Dispositivo
- Tipo de Almacenamiento
- Personas con acceso al equipo
- En qué red se encuentra conectado
- Si se tiene acceso remoto

2.3.4. Presentar datos

En la parte final de toda investigación forense informática se presentan los resultados obtenidos a través de cada una de las fases, con toda la documentación detallada de la metodología técnica utilizada, software y hardware. Se recomienda tener dos informes uno técnico y otro ejecutivo, los cuales deberán justificar el trabajo realizado para obtener la información así como el desarrollo, conclusiones y recomendaciones. Estos informes ayudaran a validar la credibilidad del análisis en cada uno de sus pasos.

[31]López Delgado, Miguel Análisis Forense Digital Internet: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf (1 de Marzo del 2014)

2.4. Aplicación de análisis forense en el Ecuador

Según la Superintendencia de Telecomunicaciones hay 16.9 millones de usuarios de telefonía móvil en el país, 3.7 millones poseían acceso a Internet hasta septiembre del 2013 y alrededor de 6.6 millones se conectan por sus medio, es decir sin utilización de datos.

De esto decimos que de alrededor de 14 millones de ecuatorianos 10.3 millones utilizan internet en su dispositivo móvil.

Encabezan la lista Pichincha con 2.3 millones de usuarios y Guayas con 1.7 millones, seguidos de Azuay, Tungurahua, Chimborazo, Loja y Los Ríos. La mayoría de usuarios están entre 18 y 25 años de edad y su principal uso va enfocado a las redes sociales y correo electrónico.

Los smartphones con un valor promedio en el mercado de $400 dólares, conquistan a los usuarios de telefonía móvil, quienes pagan el paquete de conexión a internet alrededor de $20 dólares mensuales. Las operadoras se dividen el mercado siendo Claro quien tiene mayor cantidad de dispositivos con acceso a internet con 2.2 millones de usuarios, seguido de Movistar con 1.3 millones.

Se estima que el delito informático es una forma nueva de delincuencia en el país que comenzó alrededor de 1999. Por lo que se analizó que la ley debe ser involucrada ya que tenía falencias en este ámbito que han ido mejorando poco a poco gracias a la exigencia de los usuarios, quienes han incrementado el uso de Smartphones en el país. Según el INEC se estima que el 8.4% de los ecuatorianos es decir 522.640 utilizan dispositivos inteligentes. A pesar de que el Congreso Nacional aprobó el texto definitivo de la Ley de Comercio Electrónico, Mensaje de Datos y Firmas electrónicas, siguen existiendo vacíos que deben ser corregidos. Por ejemplo quienes son los encargados de realizar las investigaciones de un delito informático son el Fiscal y la Policía Judicial, pero queda la duda de si ellos tienen los conocimientos técnicos suficientes para poder llevar a cabo este tipo de investigaciones.

En el año 2002 se aprobó la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, también se reformó el código penal con referencia a los delitos informáticos.

La Constitución Política del Ecuador y la reforma señalan que el Ministerio Público se hará cargo del conocimiento de las causas, y dirigirá la investigación[32].

Ecuador creo la Unidad de Delitos Informáticos del Ministerio Publico llamada UDIMP, la cual estaba estructurada de la siguiente forma:

Figura 4: Estructura de la Unidad Delitos Informáticos del Ministerio Publico

Creado por: Christian Guerra en base a Internet: http://repositorio.utn.edu.ec/bitstream/123456789/539/9/04%20ISC%20157%20CAPITULO%20IV.pdf (1 de Marzo del 2014)

[32]Lilia Quituisaca Samaniego Informática Forense Internet: http://www.academia.edu/1883410/Informatica_Forense (1 de Marzo del 2014)

Coordinación Nacional:

Conformada por un Coordinador Nacional, los Agentes Fiscales y personal de apoyo de la Unidad con conocimientos en Delitos Informáticos, es la encargada de la coordinación entre el Ministerio Público y la Policía Judicial así como dar las políticas y directrices generales de la investigación de los Delitos Informáticos a nivel nacional. Tiene cuatro secciones:

1. **Sección de Inteligencia:** su objetivo es recoger la información y datos de los delitos informáticos a través de miembros de la Policía Judicial con conocimientos de informática e inteligencia policial.
2. **Sección Operativa:** realiza las investigaciones de los delitos informáticos, y tiene varios grupos de investigación de acuerdo al delito cometido:
    - Fraudes informáticos y telecomunicaciones, este grupo está a cargo de la investigación de los fraudes informáticos en todas sus modalidades incluyendo las tarjetas magnéticas
    - Pornografía Infantil, grupo encajado de perseguir e investigar a los pedófilos que utilizan la Internet para desarrollar relaciones personales con menores de edad.
    - Seguridad Lógica y Terrorismo Informático o Ciberterrorismo, este grupo está encargado de investigar a quieres amenazan la seguridad lógica de los Sistemas Informáticos y seguridad interna y externa de posibles ataques de terrorismo informático.
    -
3. **Sección Técnica y Forense:** está encargada de realizar el análisis de las evidencias encontradas en la escena del delito. Tiene el apoyo del dos grupos:
    - Grupo de Apoyo Técnico, especializado en recolectar las evidencias
    - Grupo de Análisis Forense, especializado en el análisis de hardware y software.[33]

[33] Informática Forense, Inserción Jurídica Internet: http://repositorio.utn.edu.ec/bitstream/123456789/539/9/04%20ISC%20157%20CAPITULO%20IV.pdf (1 de Marzo del 2014)

2.4.1. Leyes Internacionales de la Informática Forense

Los países más destacados en el tratamiento de delitos informáticos tanto con leyes, personal especializado y equipamiento son:

- España
- Estados Unidos
- Bolivia
- Argentina
- Chile
- Brasil
- Colombia
- Francia
- Holanda
- Gran Bretaña
- Venezuela

En Latinoamérica algunos de estos países cuentan con regulaciones que tipifica los delitos informáticos, en otros países se ha procedido a la reforma penal para castigar los delitos informáticos.

Tabla 7: Leyes en Latinoamérica

	Ley de Comercio Electrónico, Mensajes de Datos	Ley de Uso de correo Electrónico	Ley de Habeas Data	Ley de Transparencia y Acceso a la Informática	Ley de Pornografía Infantil	Ley de Delitos Informáticos	Ley de propiedad Intelectual
Argentina	X		X			X	X
Bolivia				En Proceso			
Brasil	X		X				
Chile	X		X		X		X
Colombia	X		X	X		X	
Costa Rica						X	
Ecuador	X		X	X			X
Guatemala	X						
México				X		En Proceso	
Panamá	X						
Paraguay				X			
Perú		X		X	X	X	
República Dominicana	X						
Uruguay		En Proceso					
Venezuela	X					X	

Creado por: Christian Guerra en base a Estadísticas de la Organización de Estados Americanos (OEA) Internet: Estadísticas de la Organización de Estados Americanos (OEA) (1 de Marzo del 2014)

3. SOFTWARE FORENSE EN MÓVILES ANDROID

3.1. Software para la recuperación forense en móviles Android.

En la actualidad los teléfonos inteligentes son más parecidos a los ordenadores, debido al gran avance tecnológico, siguiendo las tendencias y las necesidades de los usuarios.

Ahora tienen grandes ventajas como:

- Memoria RAM más amplia.
- Memoria interna cada vez de mayor capacidad.
- Internet móvil.
- GPS.
- Cámara.
- Wifi.

Todas estas facilidades también se han convertido en desventajas al momento de realizar:

- Fraudes electrónicos.
- Comunicaciones para realizar delitos.
- Pornografía

Con todo esto se ha vuelto una necesidad el uso de software de investigación para poder actuar de manera correcta y acertada en la obtención de información que es de vital importancia dentro de un proceso judicial.

3.1.2. Análisis forense de dispositivos móviles

Es considerada como parte de la práctica forense digital, que es la recuperación de datos relacionados con evidencia. Al hablar de dispositivos móviles, con la gran evolución y necesidades de los usuarios hoy en día no solo se está hablando de celulares sino también de PDA, GPS y Tablet PC.

El análisis forense de los dispositivos móviles, se va llevando a cabo alrededor de 14 años, su necesidad se dio que fue necesario por el uso de teléfonos inteligentes y las técnicas que existían no satisfacían por completo las necesidades[34].

Los teléfonos inteligentes dieron un gran salto, ya que ya no se podía solo guardar información personal como contactos, fotos, calendario y SMS. También pueden navegar por internet, videos, correos electrónicos, GPS, acceso a documentos almacenados tanto en la memoria interna y en la nube.

Pese al gran avance en el análisis forense de los dispositivos móviles, aún hay cosas como determinar exactamente el lugar de donde se realizó una llamada utilizando la información de la cobertura, el gran avance tecnológico de los dispositivos, como cambio de versiones de sistemas operativos, diferentes periféricos, conectores, cambios de cables, capacidad de almacenamiento en el dispositivo y en la nube. Esto obliga a usar diferentes tipos de procesos, estar pendientes de los cambios tanto en software y hardware ya que prácticamente se ha considerado que se está tratando con computadores.

Por estos motivos siempre se recomienda a los investigadores a utilizar software calificado y apropiado conjunto con procesos y estándares para que toda la investigación pueda tener éxito y poder ser utilizada frente a un tribunal como evidencia, conservando la credibilidad de la información y el trabajo.

[34] Casey, Eoghan. Digital Evidence and Computer Crime, Second Edition. (1 de Marzo del 2014)

3.2. Software para la recuperación forense en móviles

Hoy en día en el mercado se tiene una gran variedad de software tanto pagado como libre, disponible para diferentes sistemas operativos como Linux y Windows.

Al momento de elegir el software es muy importante tener en cuenta de que requerimos y los procedimientos internacionales para que la evidencia pueda servir al final del trabajo.[35]

El software más reconocido en varios sitios web y libros son:

- **Oxygen Forensic**

  Es considerado una de las más populares por ser una de las más completas en recuperación forense es desarrollado por Oxygen Sofware fundada en el año 2000 es especializada en el desarrollo de software para exámenes forenses avanzados para dispositivos móviles inteligentes. Actualmente venden ciertos productos en español con varias versiones que difieren de las necesidades de cada empresa.

  Consta de varias versiones de software:

  Oxygen Forensics Suite Pro, es una de las más completas ya que puede extraer la información necesaria para la investigación forense, analizando información de fotografías, historiales de conexión, análisis de caché de navegadores.

  Oxygen Forensics Suite Pro Analyst, tiene como principal objetivo procesos de recuperacion de contraseñas

  Oxygen Forensis Suite Pro, esta versión puede realizar un rooting, es decir realizar todas las extracciones como un usuario administrador la cual permite analizar más afondo la información.[36]

[35] Sánchez Cordero, Pedro, Forensics Power Internet: conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html (15 de Marzo del 2014)
Artículo I. [36] Oxygen Forensics. Internet http://www.informatica64.com/OxygenForensics.aspx (1 de Abril del 2014)

Especificaciones

- Conexión por cable, bluetooth e infrarrojo.
- Asistente de Extracción de Datos e información
- Compatible con Symbian, Windows Mobile, Apple IOS, Android, Blackberry y Bada.
- Acceso al calendario, tareas y notas.
- Información de llamadas entrantes, salientes y perdidas,
- Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.
- Acceso a los archivos del dispositivo móvil y memoria flash.
- Geo localización.
- Integridad de los datos de verificación.

- **MOBILedit Forensic**

  Es capaz de realizar extracciones simultáneas de múltiples dispositivos, exportaciones de datos a XML, HTML, PDF, MS Wordand MS Excel. Consta de actualizaciones automáticas para mantener su instalación hasta a la fecha.

  Puede realizar copia de seguridad mejorada del sistema de archivos y la exportación Modo multimedia (MTP) de detección y resolución de la conexión, exportación de los datos de la Tarjeta SIM ampliado, es compatible con varios sistemas operativos móviles.

  La compañía que desarrolla el software fue fundada en 1996 con la primera herramienta de investigación forense llamada Simedit comercialmente conocida como MOBILedit. La compañía ha sido líder en la industria, teniendo clientes como departamentos de seguridad del Gobierno de diverso países.

  El software recoge todos los datos posibles desde el teléfono móvil y genera un amplio informe en un PC que se puede almacenar o imprimir.[37]

[37] MOBILedit! Forensic Features. Internet: http://www.mobiledit.com/company (1 de Abril del 2014)

Especificaciones

- Conexión por cable y bluetooth
- Asistente de Extracción de Datos e información
- Compatible con Symbian, Windows Mobile, Apple IOS, Android, Blackberry, Media Tek MeeGO y Bada.
- Acceso al calendario, tareas y notas.
- Información de llamadas entrantes, salientes y perdidas,
- Log de envío y recepción de mensajes SMS, MMS, messajes de correo electrónico.
- Acceso a los archivos del dispositivo movil y memoria flash.
- Geo localización.
- Integridad de los datos de verificación.

- **Device Seizure**

  Es considerado un sistema para la extracción y análisis. Device Seizure desde el comienzo fue desarrollado con la intención de ser usado en el campo forense y ser fiable. Tiene funciones de análisis, adquisiciones lógicas y físicas, analizadores de datos avanzados, visores de archivos, integración de Google Earth, una base de datos back-end para facilitar el uso de datos contenidos en los teléfonos inteligentes.

  Es desarrollado por Paraben Corporation, es una compañía de investigación tecnológica, Paraben fundada en 1999 en Estados Unidos tuvo una gran acogida con el lanzamiento de PDA Incautación en el 2002.

  Paraben ofrece también tiene entrenamiento en lugares de los Estados Unidos, el Reino Unido, Europa, y Australia. Con varios años de experiencia en informática forense, considerado una de las experimentadas ya que desde su creación siempre mantuvo la misma línea en el software[38].

[38] Paraben Corporation. Internet: https://www.paraben.com (1 de Abril del 2014)

Especificaciones

- Conexión por cable y bluetooth
- Compatible con Symbian, Windows Mobile, Apple IOS, Android y Blackberry
- Extracción de claves del usuario.
- Información de llamadas entrantes, salientes y perdidas,
- Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.
- Geo localización.

- **XRY**

Es un software diseñado para funcionar en Windows que le permite realizar una extracción forense de datos, en dispositivos móviles inteligentes, unidades de navegación GPS, módem 3G, reproductores de música portátiles, tablets e IPads. [39]
XRY ha sido diseñado y desarrollado con una interfaz de usuario muy fácil de usar y cuenta con un gran soporte técnico.
Desarrollado por Micro Systemation, es una compañía en tecnología forense, con presencia en Europa y Estados. La compañía se dedica a las comunicaciones móviles desde 1984[40].

Especificaciones

- Conexión por cable.
- Compatible con Symbian, Windows Mobile, Apple IOS, Android y Blackberry.
- Extracción de claves del usuario.
- Información de llamadas entrantes, salientes y perdidas,
- Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.
- Geo localización.
- Cuenta con hardware adicional para facilitar el análisis.

[39] Micro Systemation. Internet: http://www.msab.com/xry/what-is-xry (18 de Abril del 2014)
[40] Micro Systemation. Internet: http://www.msab.com/company/about-us (18 de Abril del 2014)

- **Simcon**

  Es un software que permite obtener una la imagen de todos los archivos en una tarjeta SIM GSM/3G a un el lector de tarjetas SIM forense, con lo que se requiere hardware adicional. Se puede analizar mensajes de texto y los contactos guardados[41].

  Especificaciones

  - Compatible con todos los dispositivos móviles GSM
  - Información de llamadas entrantes, salientes y perdidas,
  - Log de envío y recepción de mensajes SMS.
  - Cuenta con hardware adicional para facilitar el análisis.

- **FINALMobile Forensics**

  Es un software diseñado para la captura y análisis de datos en un dispositivo móvil y usa un asistente de base de datos para hacer más fácil el uso, que proporciona una mayor recuperación y tiene un asistente para poder exportar análisis con la descripción de los datos obtenidos[42].

  ES desarrollado por FinalData Inc., que se dedicado al desarrollando herramientas de software.

  Ha concedido marcas por toda Asia y Estados Unidos. Posee algunas de las herramientas más simples de utilizar la tecnología más avanzadas y sofisticadas para el análisis de datos procedentes de legados digitales como ordenadores y teléfonos móviles en el interés de obtener pruebas necesarias para investigaciones penales[43].

  Especificaciones

  - Compatible con todos los dispositivos móviles GSM
  - Información de llamadas entrantes, salientes y perdidas,
  - Log de envío y recepción de mensajes SMS.

[41] Simcon Forensics. Internet: http://www.simcon.no Acceso(19 de Abril del 2014)
[42] Final Data. Internet: http://finaldata.com/Forum2/?s=PRD&c=18&n=51 Acceso (19 de Abril del 2014)
[43] Final Data. Internet: http://finaldata.com/Company/?s=COM.CEO Acceso (20 de Abril del 2014)

- **AFLogical**

  Este software desarrollado por la compañía viaForensics, dedicada a promover la seguridad móvil en todo el mundo; es una herramienta que después de extraer los datos del dispositivo Android los almacena en la tarjeta SD del examinador en formato CSV con el fin de analizar fácilmente los datos.

  Consta de las siguientes versiones:

  ViaExtract, por ser un software exclusivo de Android ofrece un análisis forense más específico y profundo que cualquier otra herramienta del mercado, como resultado da un informe claro y conciso.

  AFLogical Law Enforcement, herramienta que como su nombre lo indica necesita de la aplicación de una ley activa o de un correo electrónico de gobierno, para usarla es necesario anotar el propósito del registro. Las especificaciones son las mismas que viaExtract.

  AFLogical Open Source Edition, esta es una versión gratuita que extrae todos los MMS disponibles, SMS, contactos y registros de llamadas desde su dispositivo Android[44].

  Especificaciones

  - Compatible con Android
  - Acceso al calendario, tareas y notas.
  - Información de llamadas entrantes, salientes y perdidas,
  - Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.
  - Acceso a los archivos del dispositivo móvil y memoria flash.
  - Geo localización.

[44] Via Forensics. Internet: https://viaforensics.com/resources/tools/android-forensics-tool/ Acceso (20 de Abril del 2014)

- **Osaf-toolkit**

  El Kit de herramientas de Osaf fue desarrollado como un proyecto por un grupo de estudiantes de informática de la Universidad de Cincinati, además de ser un software libre su objetivo era sistematizar los análisis de malware de Android, es decir que con el kit de herramienta de Osaf el análisis y estudios forenses sea lo más sencillo posible[45].

  Además de la herramienta crearon una comunidad la Osaf Community donde los profesionales de la seguridad, analistas, desarrolladores y los recién llegados pueden aprender, discutir y compartir metodologías unos con otros; la idea fue crear un marco unificado sobre como manipular el malware dentro de los dispositivos Android[46].

  Especificaciones

  - Compatible con Android
  - Acceso al calendario, tareas y notas.
  - Información de llamadas entrantes, salientes y perdidas,
  - Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.
  - Acceso a los archivos del dispositivo móvil y memoria flash.
  - Geo localización.

[45] Open Source Android Forensics Toolkit. Internet: http://sourceforge.net/projects/osaftoolkit/ Acceso (20 de Abril del 2014)
[46] OSAF Internet http://osaf-community.org/home.html Acceso (20 de Abril del 2014)

3.3. Comparación de software forense

Tabla 8 Cuadro comparativo de Software forense

SOFTWARE	CAPTURA DE DATOS	ANALISIS DE MENSAJES	ANALISIS DE CONTACTOS	ANALISIS DE LOG DE EVENTOS	ANALISIS DE BACK	ANALISIS DE DATOS BORRADOS	INFORMACION DE GEOLOCALIZACION	GENERACION DE INFORMES	HARTWARE ADICIONAL
Oxygen Forensic	✓	✓	✓	✓	✓	✓	✓	✓	
MOBILedit! Forensic	✓	✓	✓	✓	✓	✓	✓	✓	
Device Seizure	✓	✓	✓		✓	✓	✓	✓	
XRY	✓	✓		✓	✓		✓		✓
SIMCON		✓		✓					✓
FINALMobile Firensics		✓		✓					
AFLogical	✓	✓		✓			✓		
OSAF-toolkit	✓	✓		✓			✓		

Creado por: Christian Guerra en base a la Investigación realizada en el Capítulo 5

4. SOFTWARE PARA PRUEBAS

4.1. Software para las pruebas

Después de investigar varias herramientas, se ha concluido que algunas simplemente son un medio para copiar la información de la memoria interna o externa, o extraen información de la tarjeta SIM.

Se debe tener en cuenta que no solo existe información de contactos mensajes y llamadas, tenemos muchas más funcionalidades que son independientes de la tarjeta SIM, por esto es importante realizar un análisis más afondo para obtener datos más exactos.

Para las pruebas se va a utilizarlas tres herramientas de software mas completas según el análisis realizado que son:

- Oxygen Forensic
- MOBILedit Forensic
- Device Seizure

4.1.1. Oxygen Forensic

Oxygen Forensic es una herramienta de análisis que puede extraer información desde cualquier dispositivo móvil.

Esta aplicación no solo se limita a la extracción de:

- Mensajes SMS
- Mensajes SMS
- Correo electrónico
- Mensajes MMS
- Geo posiciones
- Fotos de la cámara
- Eventos de calendario
- Caché web para navegadores móviles estándar
- Modificaciones de contactos y eventos de calendario

Tiene un asistente de extracción de datos que descarga toda la información del dispositivo disponible. Se puede complementar este proceso con una función para la generación automática de informes forenses y filtrar la información para obtener un mayor detalle.

Oxygen Forensic Suite se destaca por extraer lo siguiente[47]:

- Información general del dispositivo.
- Datos de la tarjeta SIM.
- Lista completa de contactos con toda la información personal
- Registro de llamadas
- Información de SMS

[47] Sofpedia. Internet: http://www.softpedia.es/programa-Oxygen-Forensic-Suite-153966.html Acceso (20 de Abril del 2014)

Versiones

- Oxygen Forensic Suite cuenta con dos versiones Analyst y una Standard. Para poder utilizar cualquier versión hay que enviar un pedido al fabricante, y una respuesta de cinco días hábiles.

Tabla 9 Comparación de Versiones

Detalles	Oxygen Forensic® Suite 2014 Analyst	Oxygen Forensic® Suite 2014 Standard
	Pagada	Gratuita
General		
Conexión por cable (original)	X	X
Conexión por bluetooth	X	X
Conexión por inflarojo	X	X
Conexión con el dispoXtivo	X	X
Asistente de Extracción de Datos	X	X
Dispositivo de extracción de información técnica	X	X
Dispositivos y plataformas compatibles		
Dispositivos compatibles	Más 8200 Dispositivos Compatibles	Mas 8200 Dispositivos Compatibles
Actualizaciones semanales regulares de apoyo a nuevos dispositivos	X	X
Symbian OS (datos básicos)	X	X
Symbian OS (ampliado de datos)	X	X
Windows Mobile (datos básicos)	X	X
Windows Mobile (datos extendida)	X	X
Blackberry	X	X
apple iOS	X	X
OS Android	X	X
Bada OS	X	X
Dispositivos Chinos	X	
Dispositivos exclusivos (Vertu, Mobiado, etc)	X	X
Otros dispositivos (Nokia, Motorola, Samsung, Sony Ericsson,	X	X

etc)		
Directorio telefónico		
Contactos	X	X
Etiquetas de campo personalizado para los contactos	X	X
Contactos con fotos	X	X
Marcación rápida	X	X
Grupos de llamantes	X	X
Organizador		
Calendario	X	X
Tareas	X	X
Notas	X	X
Entrada hora de la última modificación	X	X
Eventos		
Información Las llamadas entrantes, salientes y perdidas	X	X
GPRS, EDGE, CSD, HSCSD, Wi-Fi	X	X
Log enviado y recibido mensajes SMS, MMS, mensajes de correo electrónico	X	X
Mensajería		
SMS en carpetas estándar	X	X
MMS y mensajes de correo electrónico en carpetas estándar	X	X
Mensajes SMS en carpetas personalizadas	X	X
MMS y mensajes de correo electrónico en carpetas personalizadas	X	X
Sistema de archivos y multimedia		
Sistema de archivos en la memoria del teléfono y tarjeta de memoria flash	X	X
Fotos, videos y grabaciones de voz	X	X
Built-in visor hexadecimal	X	X
Visor de texto incorporado (Sin formato)	X	X
Visor de texto incorporado (Unicode, UTF-8, UTF-16, más de 50 juegos de caracteres nacionales)	X	X

Built-in visor de imágenes	X	X
Incorporado en el visor de multimedia	X	X
Incorporado en el visor de contenido web	X	X
Extras		
Posicionamiento evento Geo (Lifeblog)	X	
Posicionamiento evento Geo (EXIF / XMP)	X	
Cronología	X	
Estadísticas de Comunicación	X	
agregados Contactos	X	
La evidencia clave	X	
iPhone lector de copia de seguridad protegido por contraseña	X	
Analizador de Skype	X	
Conexiones Web y Servicios de Localización	X	
Lector de copia de seguridad DMG	X	
Lector de copia de seguridad IPD Blackberry	X	
Lector de copia de seguridad IPD Blackberry protegida con contraseña	X	
Aplicaciones	X	
diccionarios	X	
Servicios de Google	X	
Google Mail, Google Maps, Google Calendar, Google Talk, Google +		
Yahoo! Services	X	
Yahoo! Messenger, Yahoo! Correo		
Redes Sociales	X	
Twitter, Twinkle, Foursquare, Facebook, etc		
Mensajeros	X	
Skype, Facebook Messenger, Yahoo! Messenger, Touch, Kik Messenger, HeyTell, TEXTIE, etc		
Navegadores Web analizador	X	
Navegador web por defecto,		

Firefox, Dolphin, Skyfire, Nintesky, UCBrowser, Atomic, etc		
productividad	X	
Dropbox, Evernote, Remember The Milk, etc		
instrumentos		
Plist Visor	X	
Visor de bases de datos SQLite	X	
Datos eliminados de las bases de datos SQLite	X	
Backup Viewer IPD	X	
Nokia PM Visor	X	
Búsqueda		
Filtrado de datos Contexto	X	X
Búsqueda de texto (incluyendo Unicode)	X	X
Búsqueda de texto a través de todos los contenidos del dispositivo	X	X
Buscar texto en varios dispoXtivos	X	
Búsqueda de actividad de contactos en múltiples dispoXtivos	X	
Export & Informes		
Las plantillas de informes	X	X
Formato de exportación	Microsoft Excel (XLS) PDF	Microsoft Excel (XLS) PDF
Vista previa e impreXón de informes	X	X
otro		
Integridad de los datos de verificación	MD5, SHA-1, SHA-2, CRC, HAVAL, GOST R34.11-94	MD5, SHA-1, SHA-2, CRC, HAVAL, GOST R34.11-94
soporte Unicode	X	X

Creado por: Christian Guerra en base a Oxygen Forensic Internet: http://www.oxygen-forensic.com/en/compare/

4.1.2. MOBILedit Forensic

La aplicación tiene la capacidad de mostrar todos los datos del dispositivo móvil y también de generar copias, dejando intacta la información dentro del dispositivo

MOBILedit! Forensic puede mostrar una información detallada como:

- Información del dispositivo.
- Detalles sobre IMEI.
- Versiones de software.
- Versiones hardware.
- Plataforma.

Proporciona informes con seguridades para no ser adulterados fácilmente y poder ser usado dentro de un tribunal de justicia.

Puede mostrar todos los datos posibles desde el dispositivo y genera un amplio informe en una PC con la capacidad de almacenar o imprimir[48].

En los informes que puede presentar la aplicación se detalla lo siguiente:

- Historial de llamadas.
- Lista de contactos.
- Mensajes,
- Fotos.
- Grabaciones de voz.
- Vídeo.
- Archivos.
- Calendario.
- Tareas.
- Notas.
- La agenda del teléfono.

Sus características principales son:

- Analizar fotos vía una conexión por Bluetooth, infrarrojo o cable
- Actualizaciones en línea
- Incluye un generador de informes basado en plantillas personales
- Los informes se generan en cualquier idioma

[48] Sofpedia. Internet: http://www.softpedia.es/programa-MOBILedit-Forensic-71469.html Acceso (20 de Abril del 2014)

Versiones

MOBILedit cuenta con diferentes tipos de software para el área forense que son MOBILedit Forensic y Forensic Express.

Tabla 10 Comparación de Versiones

Detalles	MOBILedit Forensic	MOBILedit Forensic Express
General		
Conexión por cable	X	X
Conexión por bluetooth	X	X
Conexión por inflarojo	X	X
Nombre del teléfono, fabricante y modelo	X	X
IMEI	X	X
Intensidad de la señal, estado de la batería	X	
Revisión operador de red actual, tipo de conexión, hardware y software	X	
Restante espacio de almacenamiento	X	
Resolución de la pantalla del teléfono	X	
Plataforma Teléfono / OS	X	X
Copia IMEI	X	X
Symbian OS	X	X
Windows Mobile	X	X
Blackberry	X	X
Apple iOS	X	X
Android	X	X
Bada	X	X
MediaTek	X	X
Bada	X	X
MeeGo	X	X

Directorio telefónico		
Contactos	X	X
Etiquetas de campo personalizado para los contactos	X	
Contactos con fotos	X	
Marcación rápida	X	
Grupos de llamantes	X	
Organizador		
Calendario	X	
Tareas	X	
Notas	X	
Entrada hora de la última modificación	X	
Eventos		
Información Las llamadas entrantes, salientes y perdidas	X	
GPRS, EDGE, CSD, HSCSD, Wi-Fi	X	
Log enviado y recibido mensajes SMS, MMS, mensajes de correo electrónico	X	X
Mensajería		X
SMS en carpetas estándar	X	X
MMS y mensajes de correo electrónico en carpetas estándar	X	X
Mensajes SMS en carpetas personalizadas	X	
MMS y mensajes de correo electrónico en carpetas personalizadas	X	
Sistema de archivos y multimedia		
Sistema de archivos en la memoria del teléfono y tarjeta de	X	

memoria flash		
Fotos, videos y grabaciones de voz	X	
Cronología	X	
Estadísticas de Comunicación	X	
Contactos agregados	X	
Aplicaciones	X	X
Formato de exportación	Microsoft Excel (XLS), PDF, XML	X
Vista previa e impreXón de informes	X	X

Creado por: Christian Guerra en base a Mobileedit Internet: http://www.mobiledit.com/downloads.htm?show=8

4.1.3. Device Seizure

Device Seizure es una herramienta que ha ido progresando de la mano con la evolución de la informática forense, ya que cuenta con la experiencia de tecnologías como Paraben's PDA Seizure & Paraben's Cell Seizure que fueron utilizadas para Palm, los usuarios tienen ahora acceso a una herramienta poderosa de investigación forense para dispositivo[49].

Sus principales características son:

- Recuperación de datos eliminados tanto, lógicos y físicos.
- Presentación de informes avanzada.
- Ordena los archivos adquiridos en categorías.
- Búsqueda avanzada (expresiones booleanas, Unicode y expresiones regulare)
- Admite clonación de tarjetas SIM
- Opciones avanzadas de comunicación

Versiones

Device Seizure 6.66 tiene una sola versión la cual es pagada, en su sitio web existen herramientas como Email Examiner, Chat Examiner, SIM Card Seizurre. Estas son realizan un trabajo más explícito y no solo en dispositivos móviles sino también en ordenadores.

[49] Sofpedia. Internet: http://www.softpedia.es/programa-Device-Seizure-47141.html Acceso (20 de Abril del 2014)

4.2. Diseño de las pruebas para software

Se van a realizar los siguientes procedimientos:

- Instalación
- Aplicación de software
- Análisis de resultados obtenidos

4.2.1. Instalación

Se va realizar una documentación desde la instalación que será realizada una computadora portátil Toshiba Satellite P745-S4102 que cumple con los requerimientos para el software.

Tabla 11 Caracteristicas Toshiba Satellite

Características
Intel Core i3
Windows 7 64 bits
6GB RAM

Creado por: Christian Guerra en base a Toshiba Internet:

http://www.toshiba.com/us/computers/laptops/satellite/P740/P745-S4102

EL software que se usara son las versiones que facilitan los fabricantes para pruebas, ya que todos son de licencia pagada.

Versiones de software para las pruebas

- Oxygen Forensic® Suite 2014 Standar, es la versión que el fabricante facilito después de un contacto vía email, explicando sobre la investigación.
- MOBILedit Forensic cuenta con versiones de pruebas para desarrolladores con número de ejecuciones por un tiempo de 30 días.
- Device Seizure 6.66 cuenta con versión de prueba con un tiempo de 30 días, luego de esto su se requiere se deberá comprar una licencia.

4.2.2. Aplicación de software

Para las pruebas se va a utilizar un solo dispositivo móvil con las tres herramientas, para facilitar el análisis y la comparación de los datos obtenidos por cada herramienta.

Dispositivo móvil Samsung S4 i9506.

Tabla 12: Características Samsung S4 i9506

GENERAL	2G Network	GSM
	3G Network	HSDPA
	SIM	Micro
	Anunciado	2012
MEDIDAS	Dimensiones	133.9 x 68.7 x 9.1
	Peso	139 g
	Tamaño	4.7 PULGADAS
DATOS	Velocidad	HSDPA,
	WLAN	Wi-Fi 802.11
	Bluetooth	v4.0
	NFC	Yes
	USB	Mini USB
CAMARA	Principal	16 MP

Creado por: Christian Guerra en base a GSMARENA Internet: http://www.gsmarena.com/lg_nexus_4_e960-5048.php

4.2.3. Análisis de resultados obtenidos

Este proceso se va a realizar en el siguiente capítulo empezando desde la instalación del software, a inspeccionar, limpiar y transformar datos con el objetivo de resaltar información que nos sea útil para la investigación, lo que sugiere conclusiones. Es decir que con los resultados de cada prueba van a ser documentados para poder realizar un análisis comparativo entre herramientas para poder ver cuál es alcance de cada herramienta.

5. INSTALACIÓN Y PRUEBAS DE SOFTWARE SELECIONADO

5.1. Oxygen Forensics

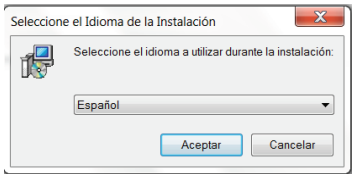
5.1.1. Instalación

Para la instalación de Oxygen Forensinc Suite 2014, solo se necesita el software proporcionado por el proveedor que se lo puede obtener en la página oficial http://www.oxygen-forensic.com/en y los drivers del dispositivo móvil en el que se lo va a utilizar, no es nada complicada ya que es muy amigable y no se necesita de personal técnico para realizarla.

Para esta investigación se utilizó la versión de prueba que nos proporcionó el fabricante después de ponernos en contacto con ellos.

Al ejecutar el instalador nos proporciona varias opciones de idioma, en este caso se ha seleccionado el idioma Español

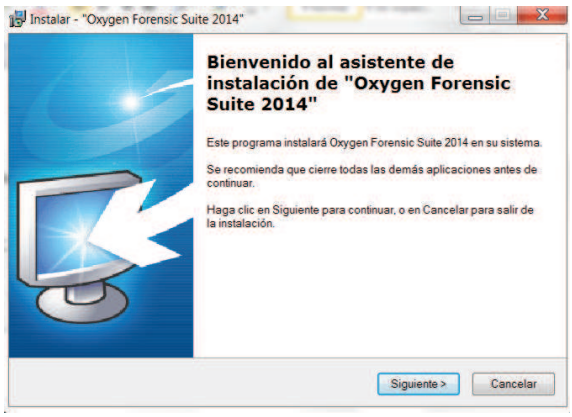
Figura 5: Inicio de instalación (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

El asistente de instalación nos da la bienvenida y nos indica que se va a iniciar la instalación

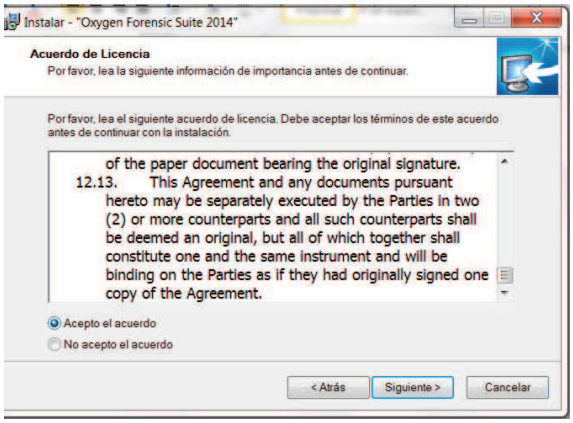
Figura 6: Inicio de asistente de instalación (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se presenta un acuerdo con la licencia, que presenta términos de uso del software, en el cual se va a proceder aceptar.

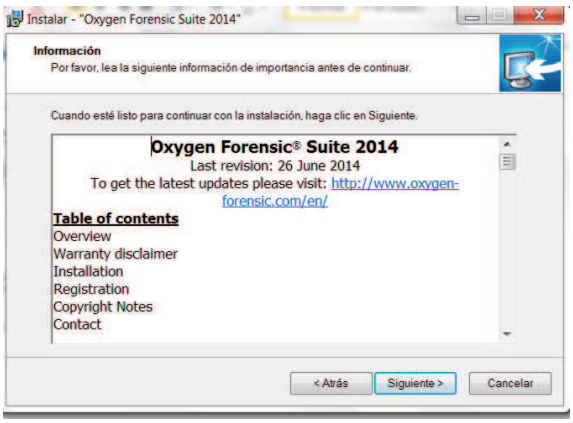
Figura 7: Acuerdo de licencia (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se verifica la información y el contenido del instalador.

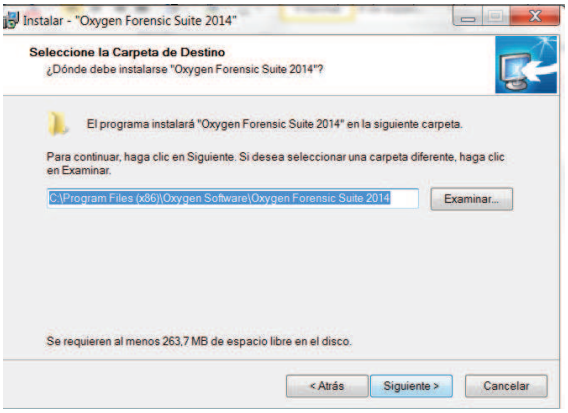
Figura 8: Información (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se selecciona el lugar donde será el destino de instalación en el disco duro.

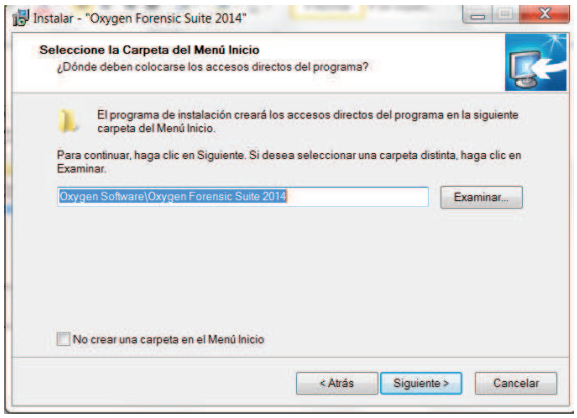
Figura 9: Selección de carpeta de destino (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se selecciona la carpeta de y el nombre como va a estar en el menú inicio.

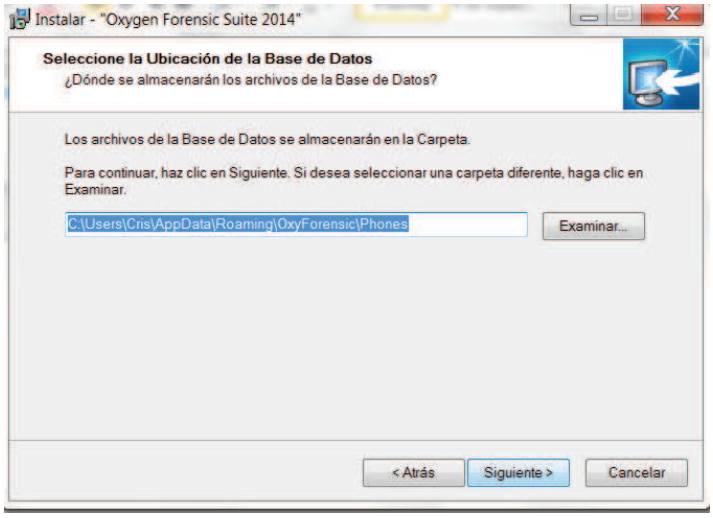
Figura 10: Selección de carpeta en el menú inicio (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se selecciona el lugar donde se va a crear una base de datos, con la información que el software va obtener de los diferentes dispositivos móviles.

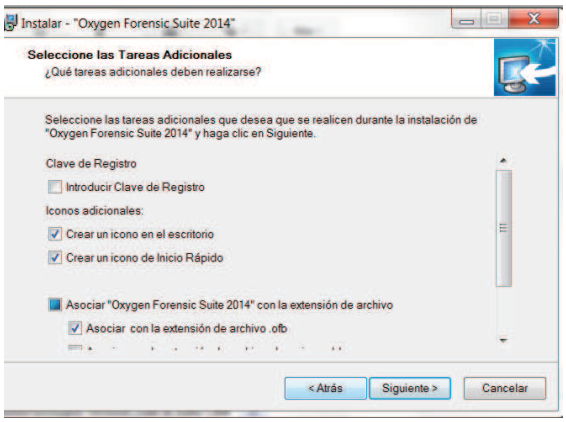
Figura 11: Selección de ubicación de la base de datos (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Si se desea se puede crear accesos directo al software

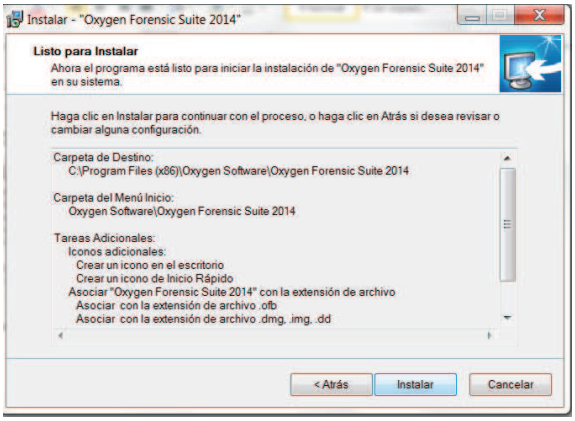
Figura 12: Creación de accesos directos (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Después de seleccionar las diferentes opciones obtenemos un resumen de lo obtenido anteriormente y procedemos con la instalación

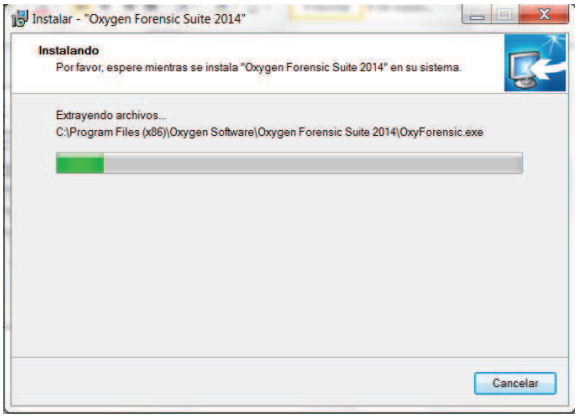
Figura 13: Resumen de opciones seleccionadas (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

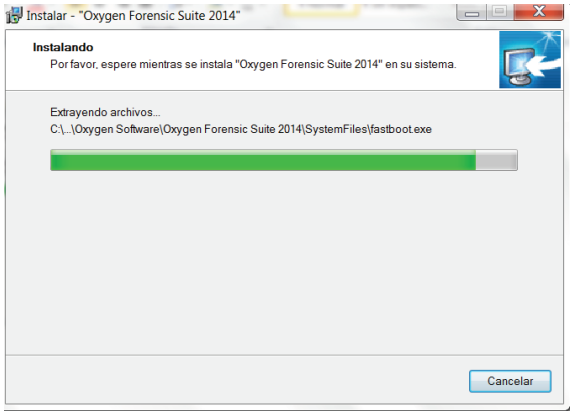
Se procede a instalar el software como lo muestra las siguientes figuras.

Figura 14: Proceso de instalación (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Figura 15: Proceso de instalación (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

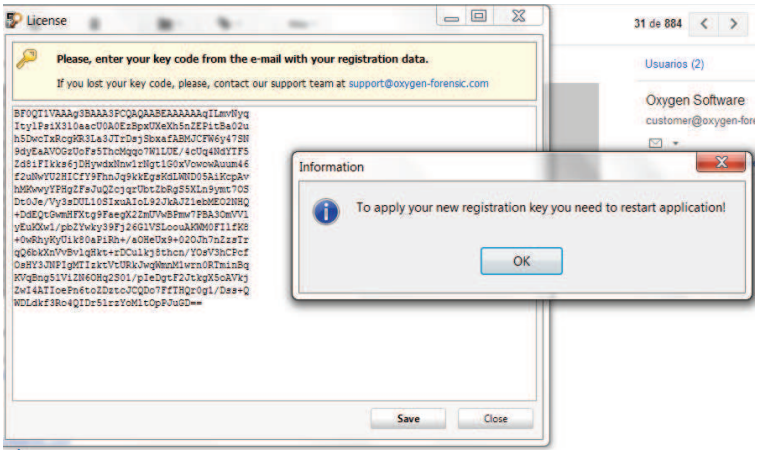
Al terminar la instalación nos permite ejecutar al finalizar.

Figura 16: Información de la instalación (Oxygen Forensic Suite 2014)

Creado por: Christian Guerra

Al abrir el Oxygen Forensic Suite 2014, se tiene que ingresar el código de la licencia, el cual nos fue proporcionado por el fabricante.

Figura 17: Ingreso de licencia (Oxygen Forensic Suite 2014)



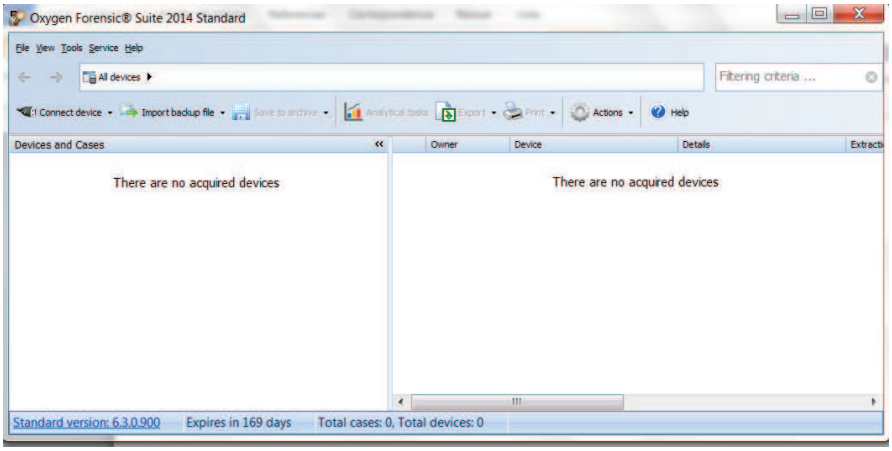
Creado por: Christian Guerra

Al validar la licencia inmediatamente se ejevuta el el software.

Figura 18: Inicio (Oxygen Forensic Suite 2014)

Creado por: Christian Guerra

Figura 19: Pantalla de inicio (Oxygen Forensic Suite 2014)



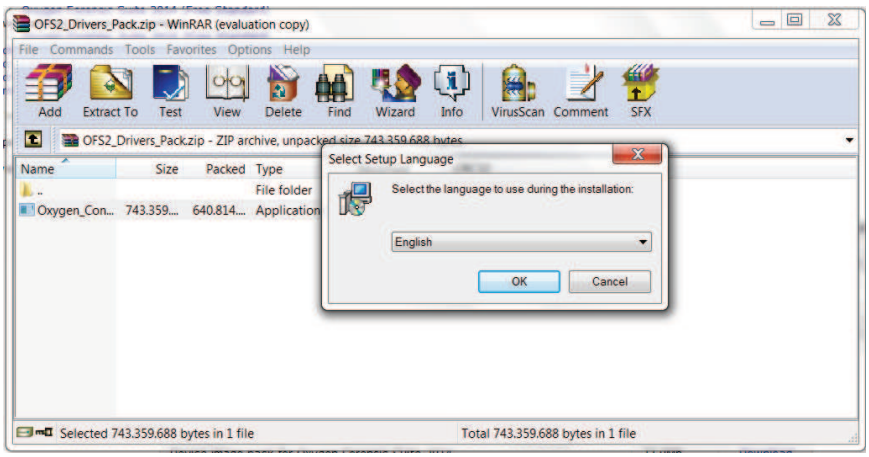
Creado por: Christian Guerra

Para el correcto funcionamiento del software se requiere instalar los drivers de los dispositivos móviles, estos drivers también. El cual fue proporcionado también por el fabricante.

Oxígen Forensic Suite de 2014 se distribuye en dos sistemas de licencias del programa, la una es un certificado de Internet con la unión de hardware y una licencia con dongle USB.

Se ejecuta el instalador el cual nos da la opción de escoger un idioma, el cual va a ser utilizado durante la instalación.

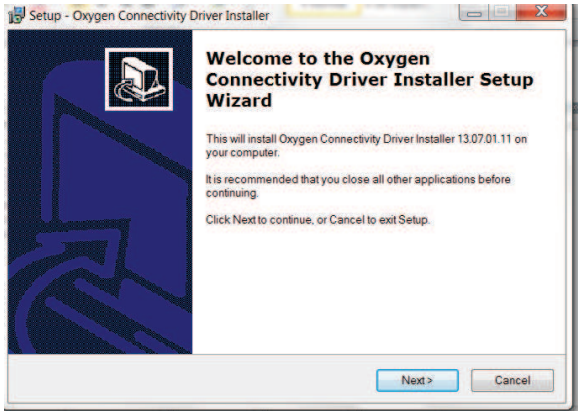
Figura 20: Instalación de Drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

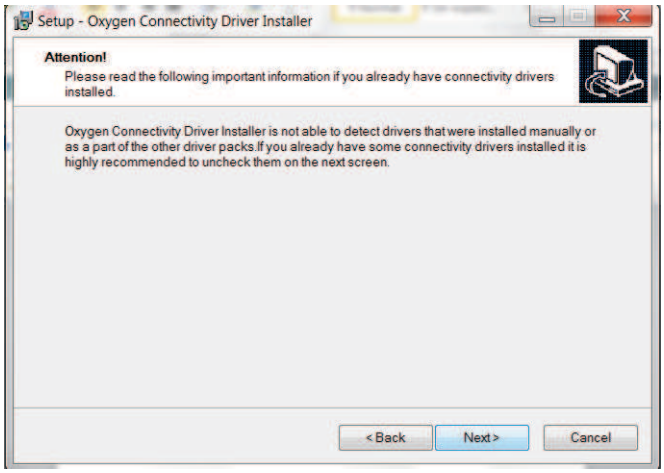
El instalador nos da la bienvenida con un resumen de la versión y recomendaciones.

Figura 21: Asistente de Instalación de Drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

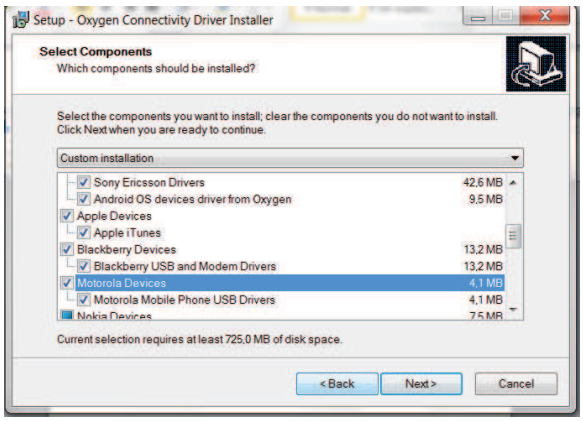
Figura 22: Advertencia de instalación de Drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se puede seleccionar uno o varios drivers para facilitar la coneccion de Oxygen Forensic.

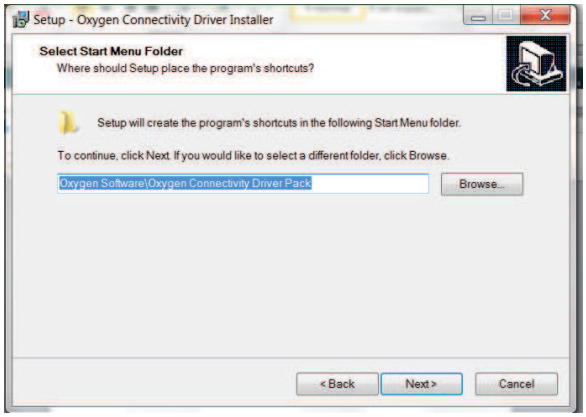
Figura 23: Selección de Drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se escoge el lugar donde se va instalar y a ubicar los accesos directos en la carpeta de menú.

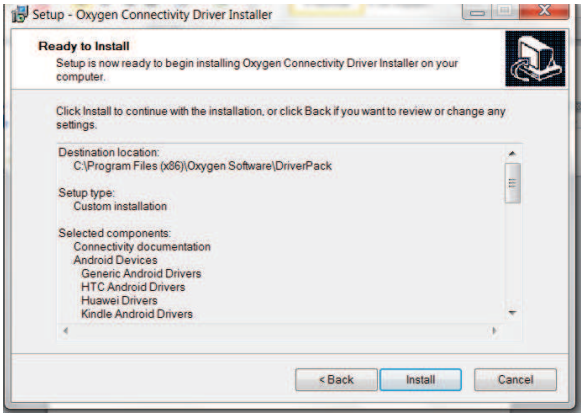
Figura 24: Selección de la carpeta menú (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Presenta un resumen de todo lo seleccionado para instalar y direcciones donde se va ubicar los accesos directos.

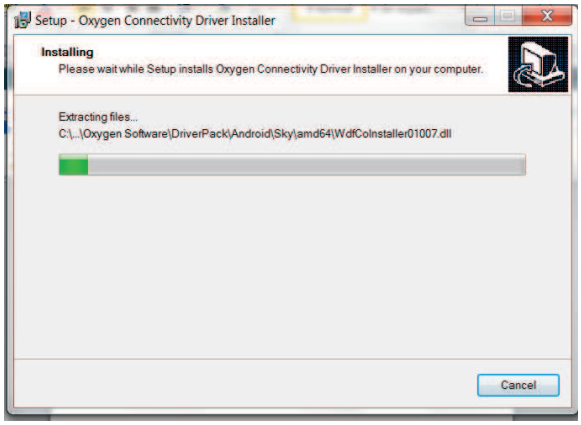
Figura 25: Resumen de instalación de drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

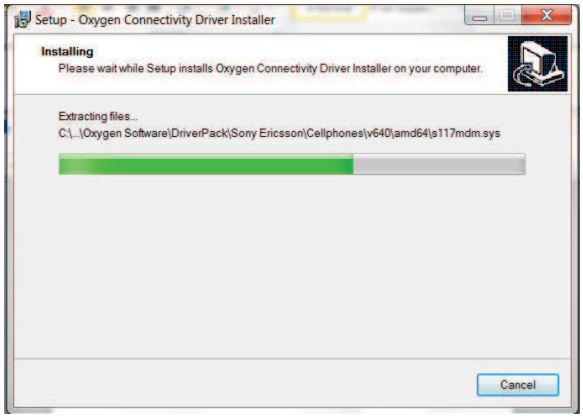
Se procede a instalar los drivers para facilitar la conexión con los diferentes dispositivos moviles.

Figura 26: Proceso de Instalación de Drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Figura 27: Proceso de Instalación de Drivers (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

5.1.2. Aplicación de software

La aplicación va hacer conectada al dispositivo móvil Samsung S4, mediante un cable USB, para probar sus funcionalidades.

Al conectar el dispositivo debe estar desbloqueado, no funciona si se encuentra bloqueado para poder reconocer al dispositivo. La primera información que nos muestra, es el modelo IMEI y la versión actual del Android.

Figura 28: Conexión por cable con el dispositivo móvil (Oxygen Forensic Suite 2014)

Creado por: Christian Guerra

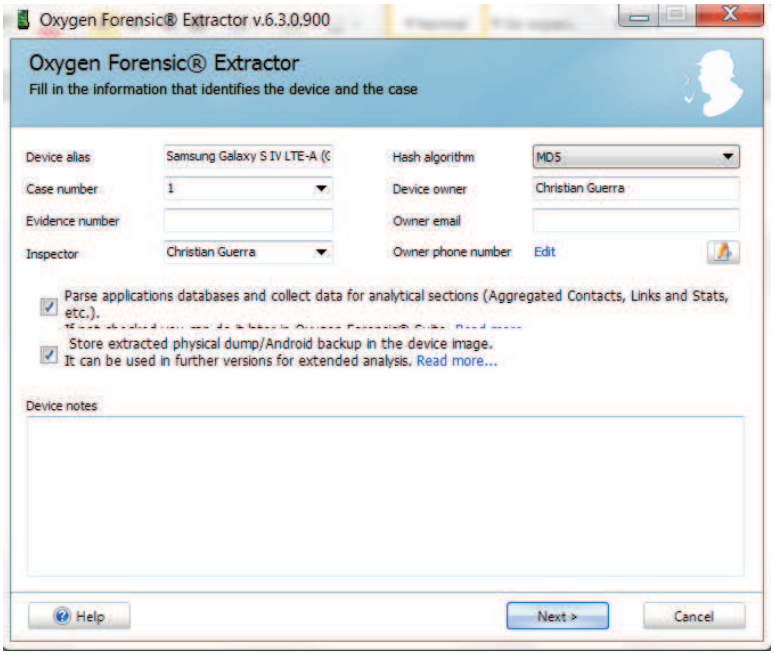
Luego de verificar la información básica del dispositivo, se nos pide ingresar la siguiente información:

- Número de caso
- Nombre del dispositivo
- Número de evidencia
- Nombre del inspector

- Nombre del propietario del dispositivo móvil
- Email
- Número telefónico del propietario del dispositivo móvil

También hay dos opciones que nos permite elegir qué información a extraer.

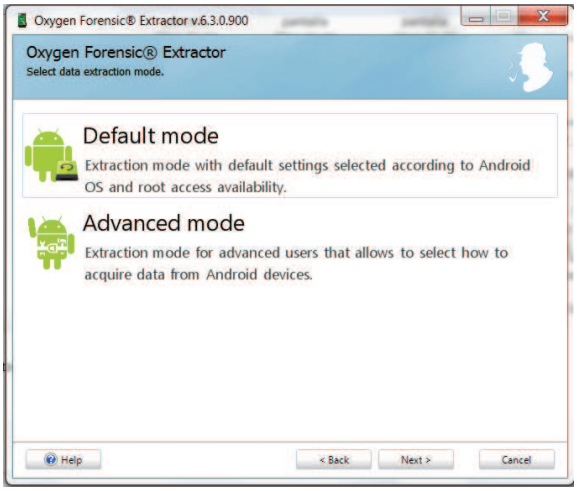
Figura 29: Identificación del dispositivo móvil (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Luego nos presenta dos tipos de extracción, la primera es una extracción definida por las opciones antes seleccionadas de acuerdo a la versión de Android y al acceso que se tenga al sistema operativo

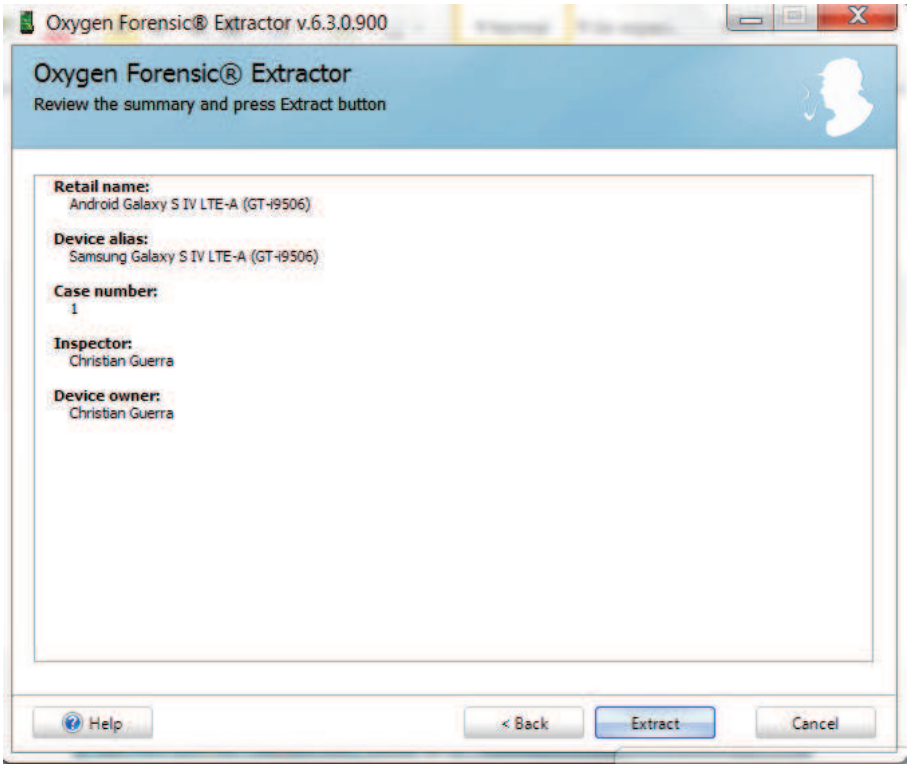
Figura 30: Selección de modo de extracción de información (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Nos presenta un resumen de la información que se proporciono anteriormente, y procedemos con la extracción.

Figura 31: Resumen de donde se va a extraer la información (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se nos presenta una ventana en la cual nos da información de cómo se ejecuta el proceso de copia de la información.

Figura 32: Proceso de copia de información (Oxygen Forensic Suite 2014)

Creado por: Christian Guerra

Al terminar la copia de seguridad, se extrae la información del dispositivo.

Figura 33: Extracción de datos del dispositivo móvil (Oxygen Forensic Suite 2014)

Creado por: Christian Guerra

AL terminar la extracción en un menú, nos muestra la información a la cual podemos acceder, en este versión que nos facilitó el proveedor existen algunas opciones que no están disponibles. La información extraída esta en diferentes clasificaciones como:

- Información del explorador del internet
- Calendario
- Contactos Agregados, esta opción no está disponible en esta versión.
- Contactos
- Agenda
- Estados, esta opción no está disponible en esta versión.
- Lista de llamadas tanto realizadas como recibidas.
- Lista de mensajes de texto realizados como recibidos.
- Diccionarios, esta opción no está disponible en esta versión.

Figura 34: Presentación de información obtenida (Oxygen Forensic Suite 2014)

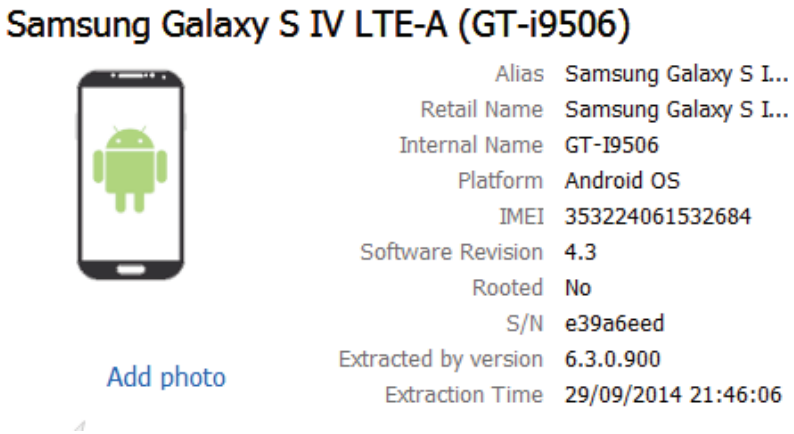
Creado por: Christian Guerra

También podemos ver información del dispositivo, en el cual nos muestra:

- Modelo
- Versión del sistema operativo

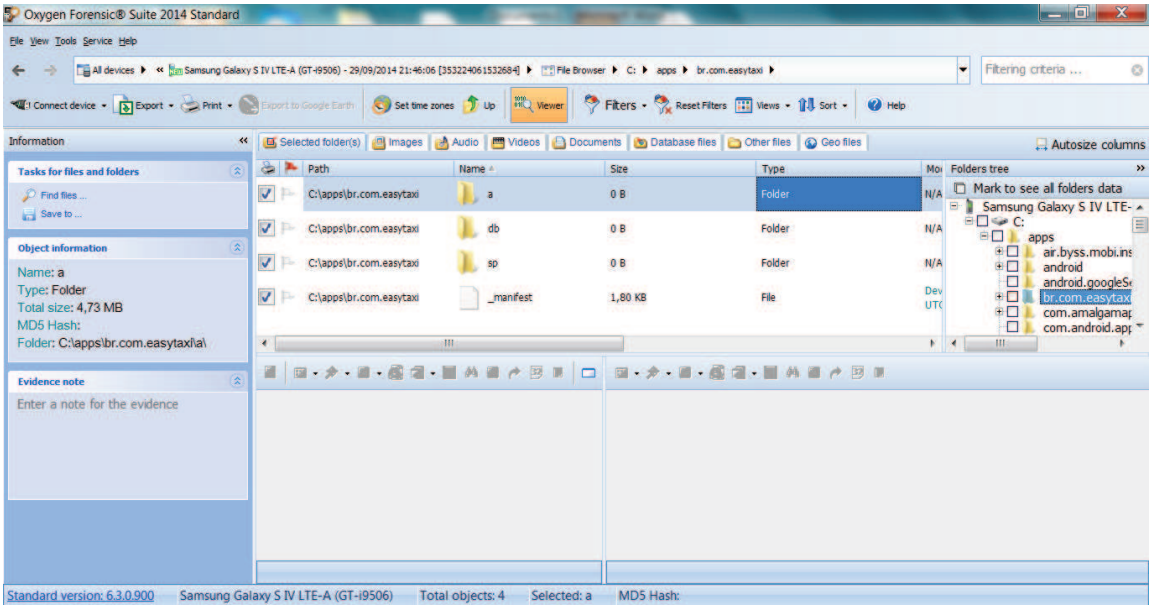
- IMEI
- MAC
- Tiempo de extracción de información

Figura 35: Información Acerca del dispositivo móvil (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

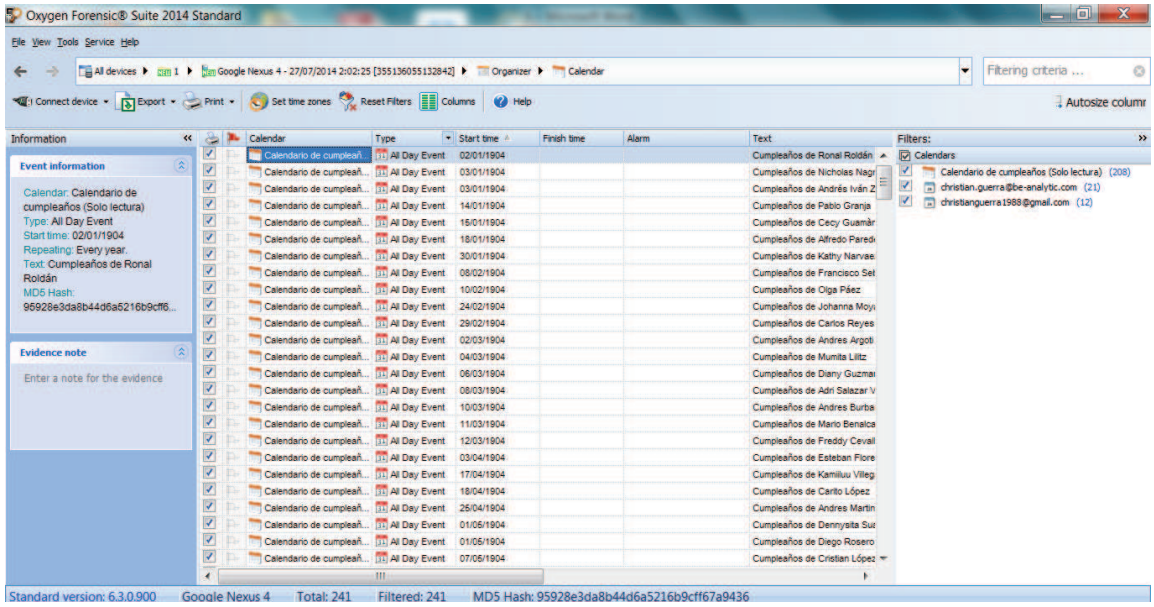
Figura 36: Información del almacenamiento del dispositivo móvil (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

En esta ventana se puede observar el calendario del dispositivo móvil, en este caso es un calendario de Gmail, que tiene asociadas dos cuentas de correo electrónico.

Figura 37: Información de calendario (Oxygen Forensic Suite 2014)

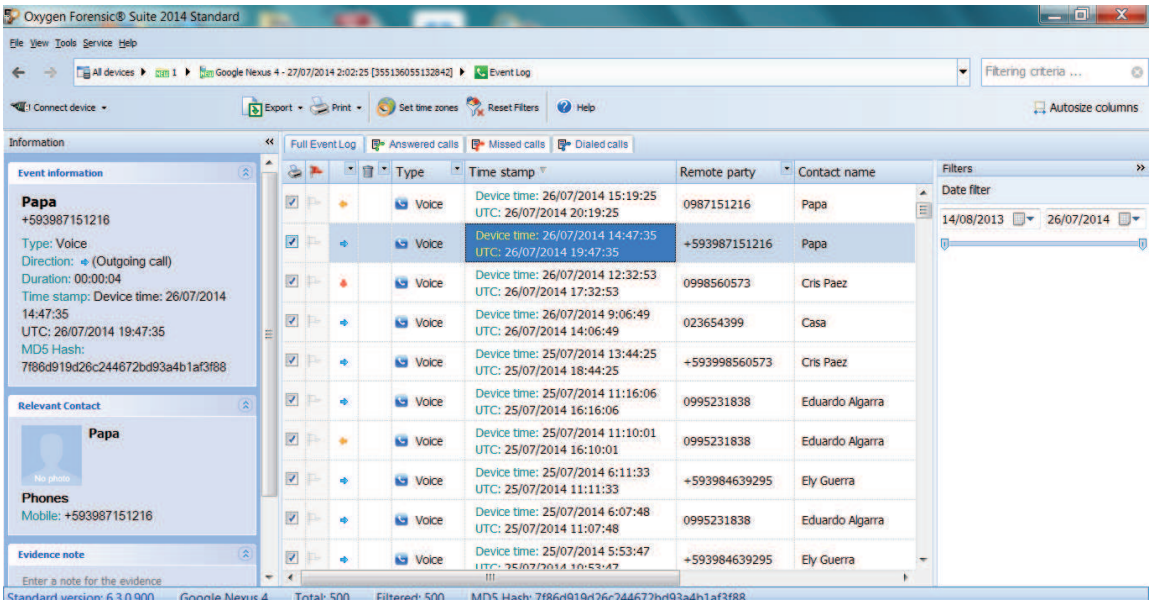


Creado por: Christian Guerra

Información de llamadas con detalles como:

- Numero de contacto
- Fecha y hora de llamada
- Tipo de llamada
- Duración de llamada

Figura 38: Información extraída de llamadas (Oxygen Forensic Suite 2014)

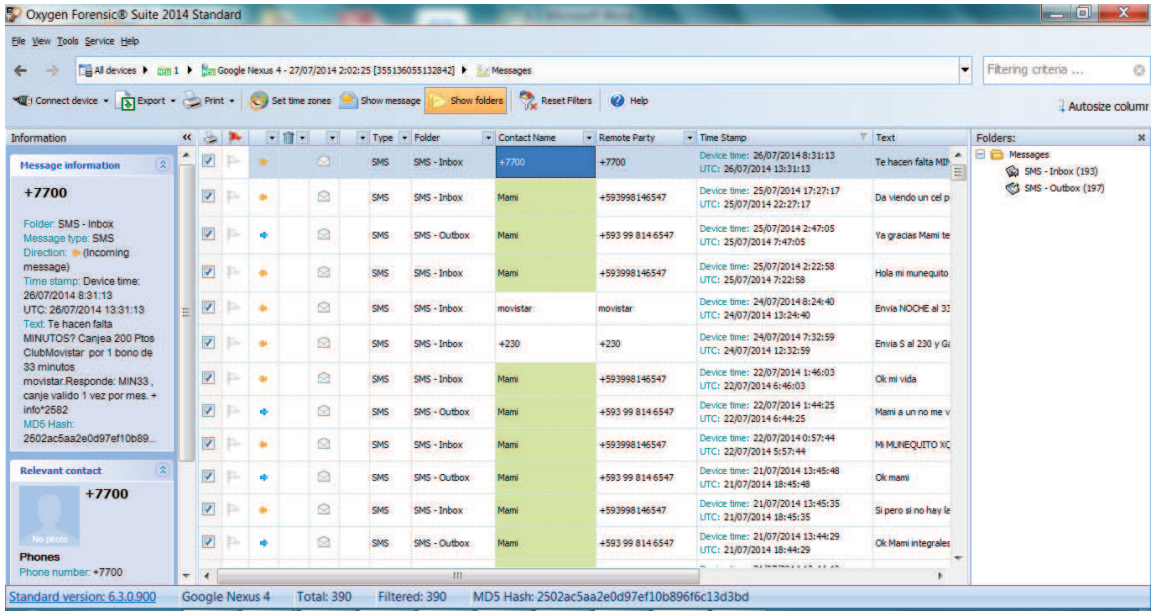


Creado por: Christian Guerra

En los mensajes de texto nos muestra los siguientes detalles:

- Si es mensaje enviado o de salida
- EL texto enviado
- Fecha y hora de creación del mensaje de texto

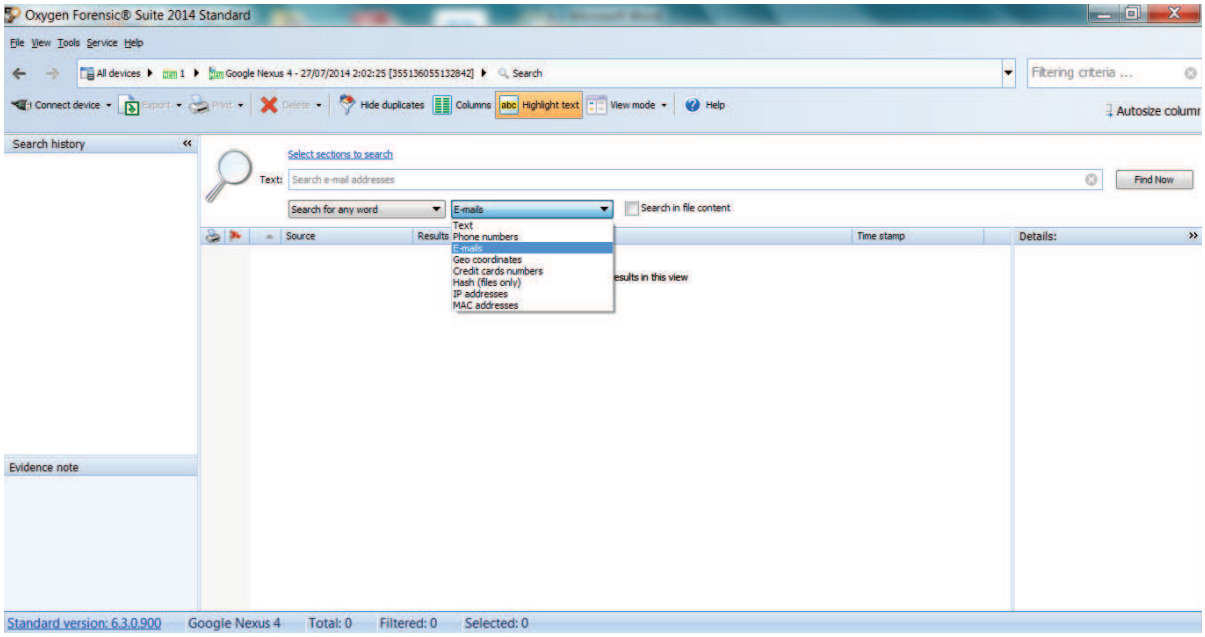
Figura 39: Información extraída de mensajes de texto (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Si se desea buscar algo en particular cuenta con un buscador muy completo, que con palabras claves se genera una búsqueda en toda la información extraída.

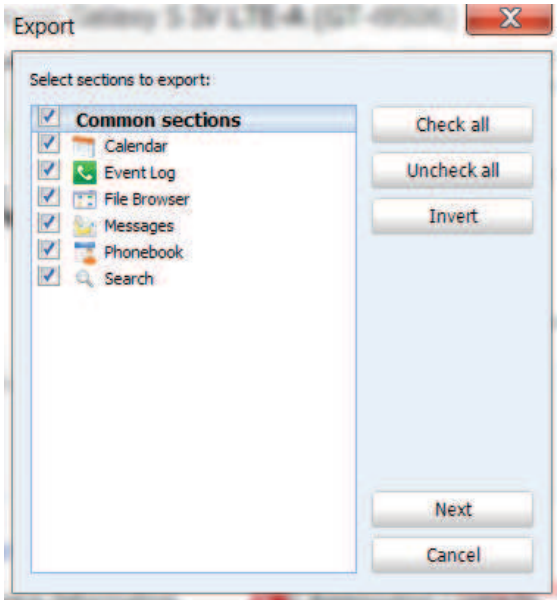
Figura 40: Buscador por tipo de información extraída (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Tiene la opción de generar un reporte con la información, para que pueda ser presentada en formato PDF.

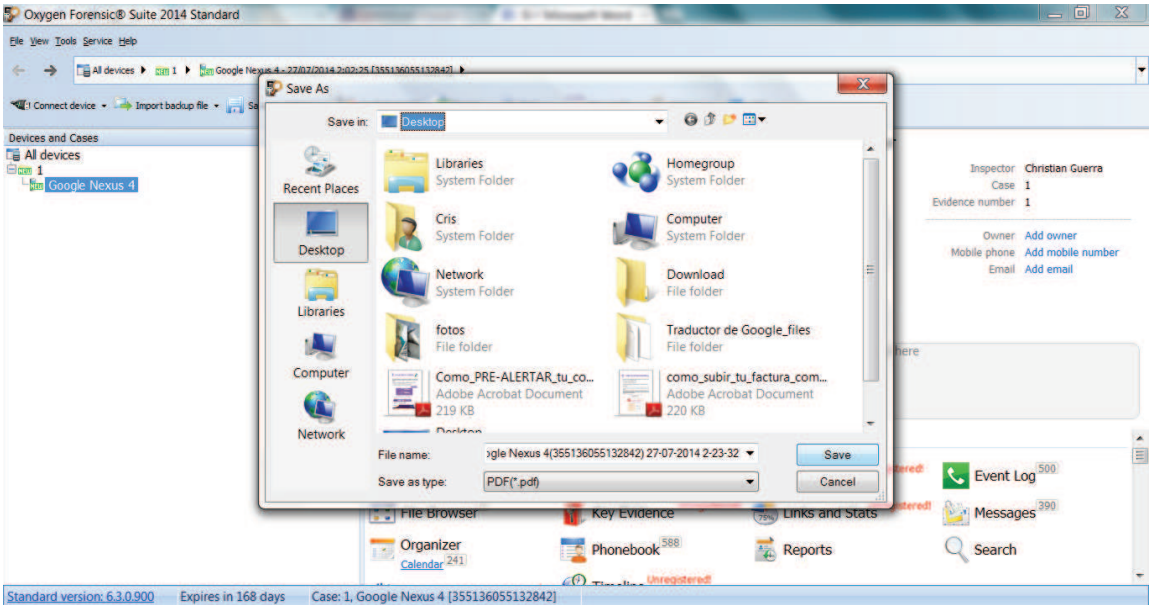
Figura 41: Selección de datos para informe (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Al elegir la opción de exportar nos pide la ubicación donde va a ser guardado el archivo con la información.

Figura 42: Guardado del informe generado (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

5.1.3. Análisis de resultados obtenidos

Oxygen Forensic suite 2014, cumple con el requerimiento fundamental en un análisis forense ya que realiza una copia bit a bit de la información, preservando la integridad de los datos en el dispositivo móvil y en la copia.

Nos presenta una amplia gama de facilidades al momento de realizar una investigación, la gran ventaja es el tener fechas exactas de la creación de llamadas, contactos, etc.

Es una herramienta muy fácil de usar e intuitiva, muy amigable con el usuario, se puede obtener un reporte que facilita la presentación de los resultados, como se puede ver a continuación los detalles del reporte.

En el reporte se nos da la información básica del dispositivo móvil.

Figura 43: Reporte del dispositivo móvil (Oxygen Forensic Suite 2014)

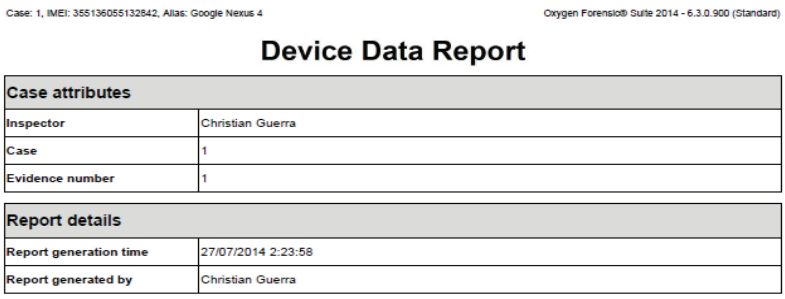
Device Data Report

Common information	
Alias	Samsung Galaxy S IV LTE-A (GT-I9506)
Retail Name	Samsung Galaxy S IV LTE-A (GT-I9506)
Manufacturer	N/A
Internal Name	GT-I9506
Platform	Android OS
IMEI	353224061532684
Software Revision	4.3
Bluetooth MAC address	?
Rooted	No
IMSI	N/A
S/N	e39a6eed
Extracted by version	6.3.0.900
Extraction Time	29/09/2014 21:46:06
Hash algorithm	MD5

Creado por: Christian Guerra

Se nos permite ver quien fue la persona que realizo el analis y fechas, que es muty importante dentro de la investigacion forense.

Figura 44: Informe de análisis (Oxygen Forensic Suite 2014)



Case: 1, IMEI: 355136055132842, Alias: Google Nexus 4 — Oxygen Forensic® Suite 2014 - 6.3.0.900 (Standard)

Device Data Report

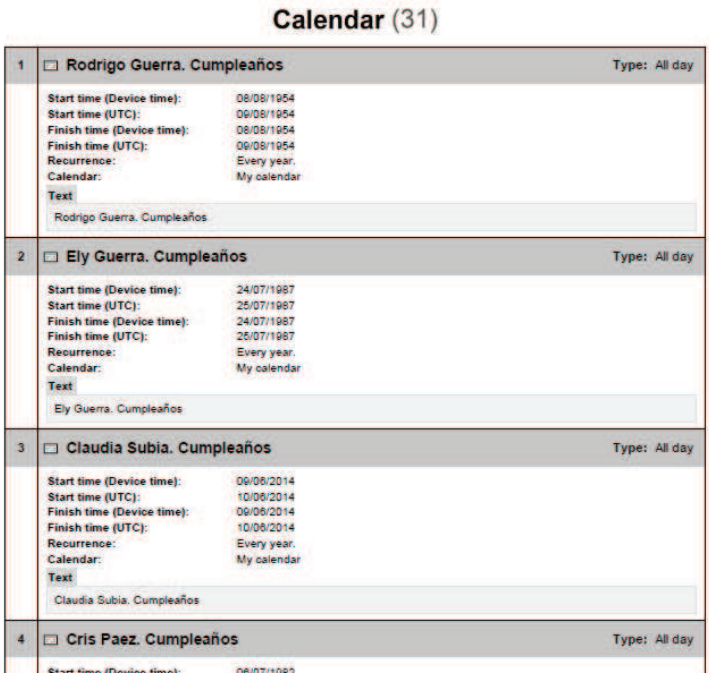
Case attributes	
Inspector	Christian Guerra
Case	1
Evidence number	1

Report details	
Report generation time	27/07/2014 2:23:58
Report generated by	Christian Guerra

Creado por: Christian Guerra

En el calendario nos dio una extraccion de 31 registros, estos pertenecen al calendario de Gmail, en este caso el dispositivo tenia registrado dos cuentas, y nos muestra con gran detalle cada una de las cosas registradas.

Figura 45: Registro de Calendario (Oxygen Forensic Suite 2014)



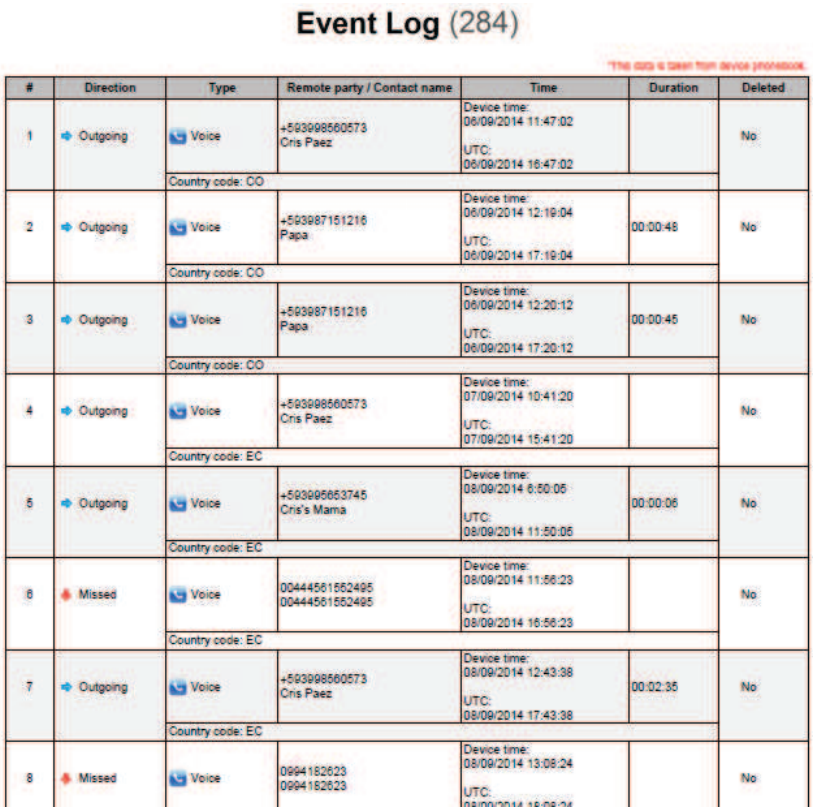
Calendar (31)

1	Rodrigo Guerra. Cumpleaños	Type: All day
	Start time (Device time):	08/08/1954
	Start time (UTC):	08/08/1954
	Finish time (Device time):	08/08/1954
	Finish time (UTC):	09/08/1954
	Recurrence:	Every year.
	Calendar:	My calendar
	Text	
	Rodrigo Guerra. Cumpleaños	
2	Ely Guerra. Cumpleaños	Type: All day
	Start time (Device time):	24/07/1987
	Start time (UTC):	25/07/1987
	Finish time (Device time):	24/07/1987
	Finish time (UTC):	25/07/1987
	Recurrence:	Every year.
	Calendar:	My calendar
	Text	
	Ely Guerra. Cumpleaños	
3	Claudia Subia. Cumpleaños	Type: All day
	Start time (Device time):	09/06/2014
	Start time (UTC):	10/06/2014
	Finish time (Device time):	09/06/2014
	Finish time (UTC):	10/06/2014
	Recurrence:	Every year.
	Calendar:	My calendar
	Text	
	Claudia Subia. Cumpleaños	
4	Cris Paez. Cumpleaños	Type: All day

Creado por: Christian Guerra

En los llamados Event Log se hace referencia a todas las llamadas tanto entrantes como salientes del dispositvo movil, con fechas exactas, de esto se obtuvo 284 registros.

Figura 46: Registro de llamadas (Oxygen Forensic Suite 2014)



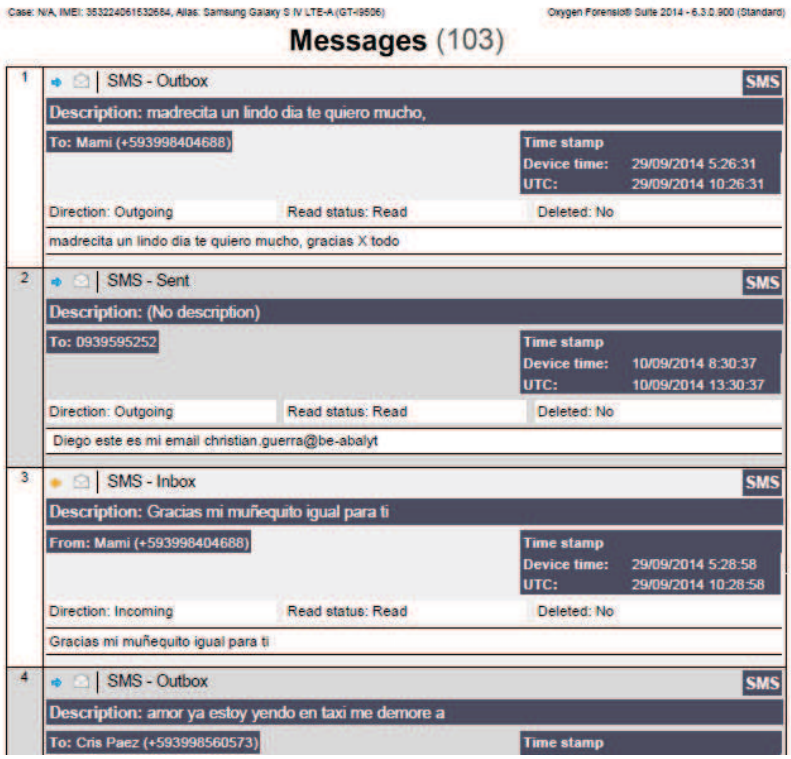
Event Log (284)

#	Direction	Type	Remote party / Contact name	Time	Duration	Deleted
1	Outgoing	Voice	+593998560573 Cris Paez	Device time: 06/09/2014 11:47:02 UTC: 06/09/2014 16:47:02		No
	Country code: CO					
2	Outgoing	Voice	+593987151216 Papa	Device time: 06/09/2014 12:19:04 UTC: 06/09/2014 17:19:04	00:00:48	No
	Country code: CO					
3	Outgoing	Voice	+593987151216 Papa	Device time: 06/09/2014 12:20:12 UTC: 06/09/2014 17:20:12	00:00:45	No
	Country code: CO					
4	Outgoing	Voice	+593998560573 Cris Paez	Device time: 07/09/2014 10:41:20 UTC: 07/09/2014 15:41:20		No
	Country code: EC					
5	Outgoing	Voice	+593995653745 Cris's Mama	Device time: 08/09/2014 6:50:06 UTC: 08/09/2014 11:50:06	00:00:06	No
	Country code: EC					
6	Missed	Voice	00444561552495 00444561552495	Device time: 08/09/2014 11:56:23 UTC: 08/09/2014 16:56:23		No
	Country code: EC					
7	Outgoing	Voice	+593998560573 Cris Paez	Device time: 08/09/2014 12:43:38 UTC: 08/09/2014 17:43:38	00:02:35	No
	Country code: EC					
8	Missed	Voice	0994182623 0994182623	Device time: 08/09/2014 13:08:24 UTC:		No

Creado por: Christian Guerra

En los mensajes de texto tanto de entrada y salida se obtuvieron 103 registros.

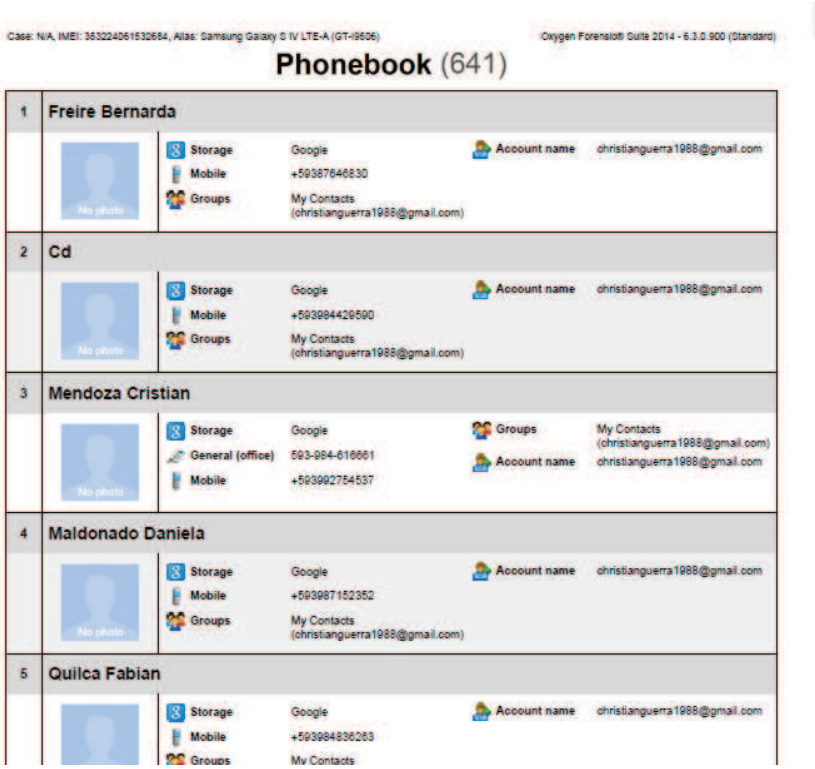
Figura 47: Registro de Mensajes de Texto (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

En la agenda de contactos se obtuvieron 641 en los cuales constan tambien contactos de los correos electronicos

Figura 48: Registros de Contactos (Oxygen Forensic Suite 2014)



Creado por: Christian Guerra

Se obtuvo tambien el grupo de contactos registrados como favoritos en el dispositvo movil que fueron un total de 5 registros.

Figura 49: Registro de Contactos Favoritos (Oxygen Forensic Suite 2014)

Case: 1, IMEI: 355136055132842, Alias: Google Nexus 4 — Oxygen Forensic® Suite 2014 - 6.3.0.900 (Standard)

Favourites (5)

Id	Full name	Number
ID 1	Mami	Alicia.Castro@presidencia.gob.ec
ID 2	Castro Janeth	+593992741677
ID 3	Paez Cris	cristina_paezc@hotmail.com
ID 4	Metroservice	02-262-0078
ID 5	Paez Cardenas Maria Cristina	cristina_paezc@hotmail.com

End of report

Signed by _____

Creado por: Christian Guerra

5.2. MOBILedit Forensic

5.2.1. Instalación

Para la instalación de MOBILedit se utilizó un instalador que se puede obtener de la pagina oficial http://www.mobiledit.com, para pruebas que contiene la herramienta y los drivers necesarios para conectarse a diferentes dispositivos móviles.

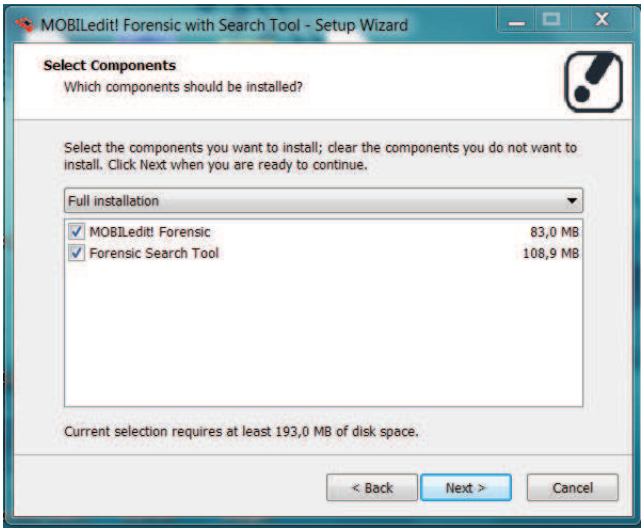
Al ejecutar lo primero que se instala es con el asistente es la herramienta, con varios componentes.

Figura 50: Inicio de Instalación (MOBILedit Forensic)

Creado por: Christian Guerra

En la instalación completa nos permite seleccionar dos componentes, el MOBILedit! Forensic y Forensic Search Tool.

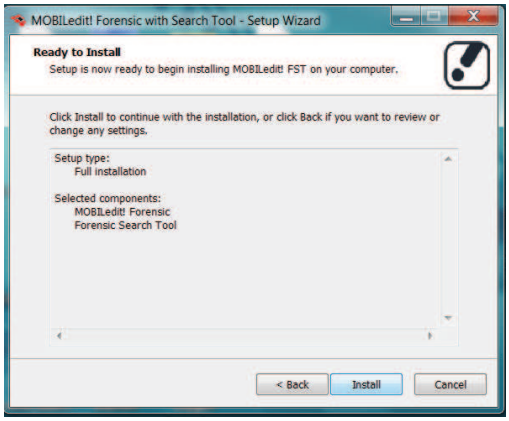
Figura 51: Selección de Componentes (MOBILedit Forensic)



Creado por: Christian Guerra

Después de seleccionar os componentes, presenta un resumen de las opciones seleccionadas anteriormente.

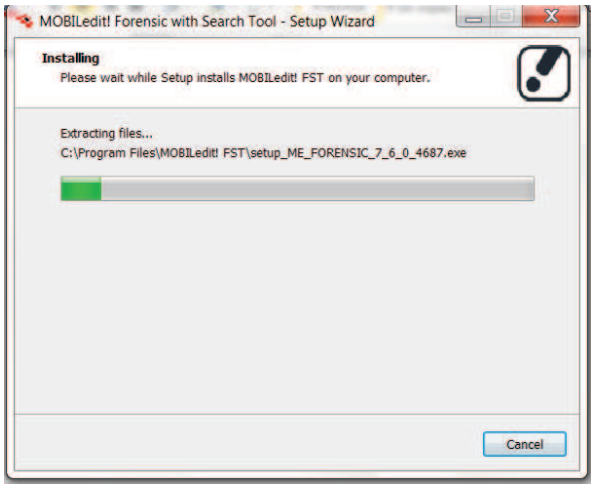
Figura 52: Informe de Componentes Seleccionados (MOBILedit Forensic)



Creado por: Christian Guerra

Se presenta una ventana con el proceso de preinstalación de los componentes.

Figura 53: Proceso de Instalación (MOBILedit Forensic)



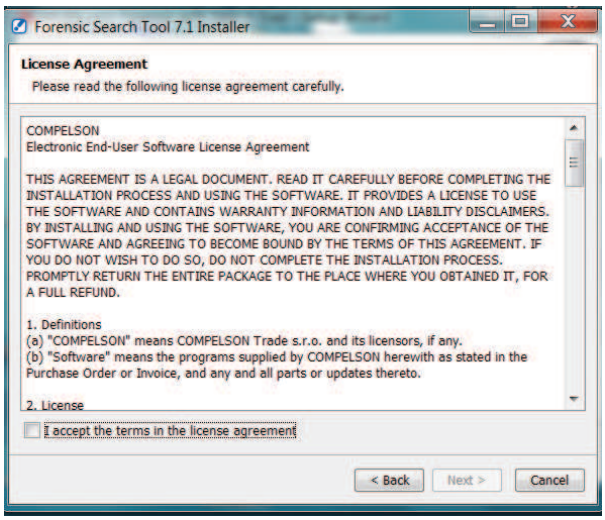
Creado por: Christian Guerra

Figura 54: Proceso de Instalación (MOBILedit Forensic)

Creado por: Christian Guerra

Presenta unos términos de licencia del uso de la herramienta.

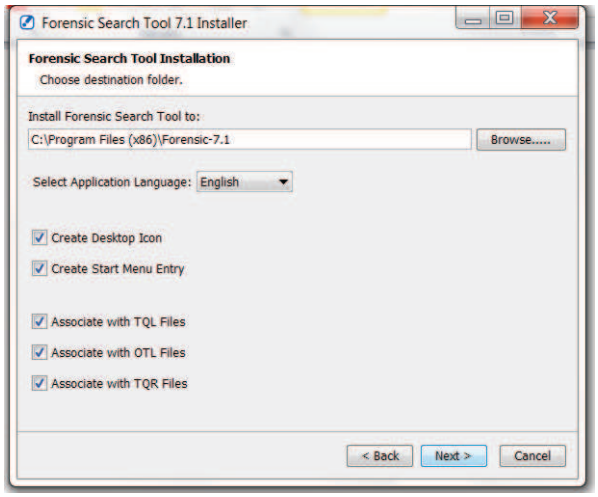
Figura 55: Términos de licencia (MOBILedit Forensic)



Creado por: Christian Guerra

Se puede elegir el lugar donde se va a instalar el componente Forensic Searc Tool, y se desea crear accesos directos, y con qué tipos de archivos se desea asociar

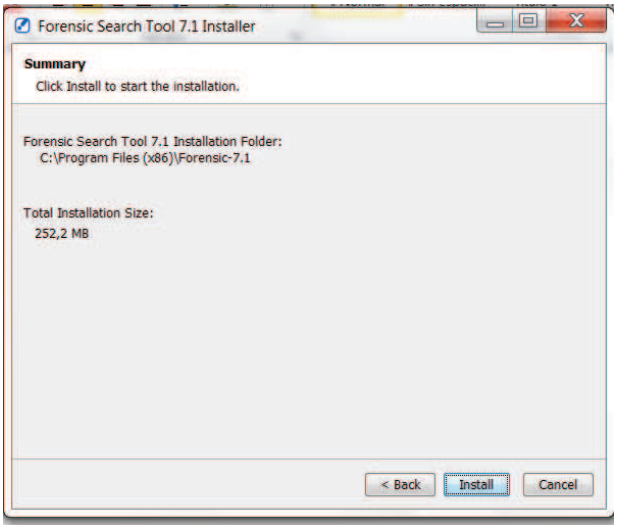
Figura 56: Lugar de Instalación (MOBILedit Forensic)



Creado por: Christian Guerra

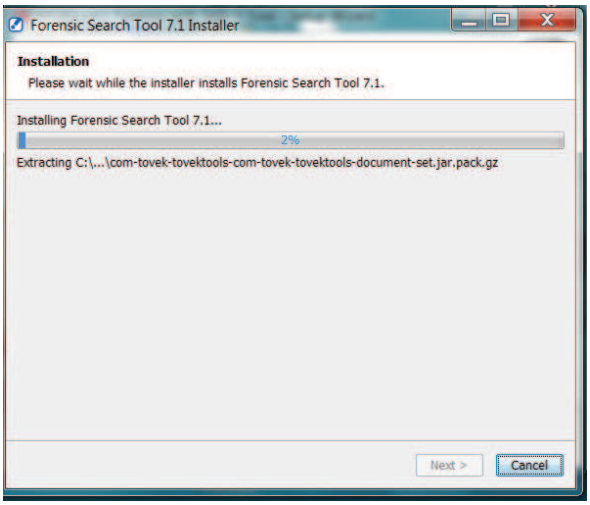
Resumen de instalación del componente Forensic Search Tool, que contiene las opciones previamente seleccionadas.

Figura 57: Resumen de Instalación (MOBILedit Forensic)



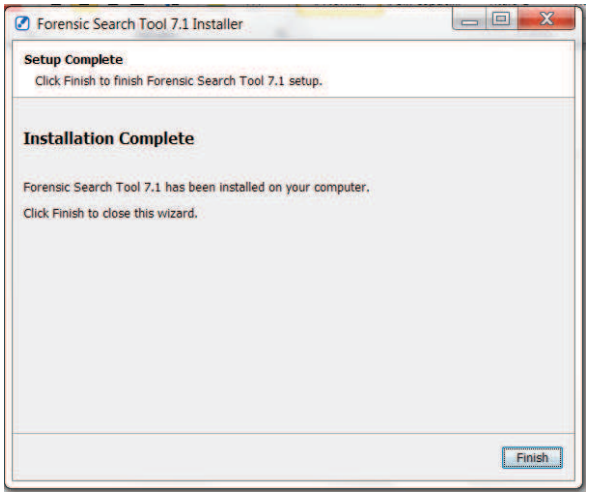
Creado por: Christian Guerra

Figura 58: Proceso de Instalación (MOBILedit Forensic)



Creado por: Christian Guerra

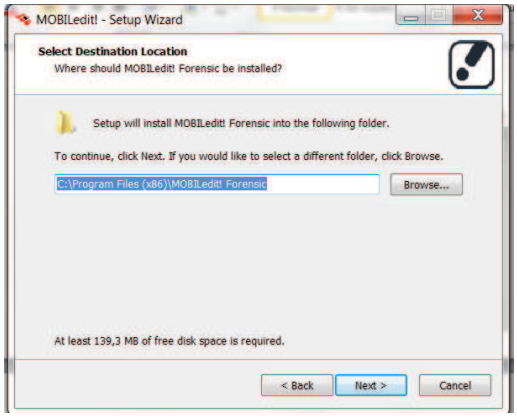
Figura 59: Final de Instalación de Componente (MOBILedit Forensic)



Creado por: Christian Guerra

Al terminar de instalar el Forensic Search Tool, continua un procedimiento similar con el MOBILedit! Forensic, con el primer paso de elegir el lugar donde se va a realizar la instalación.

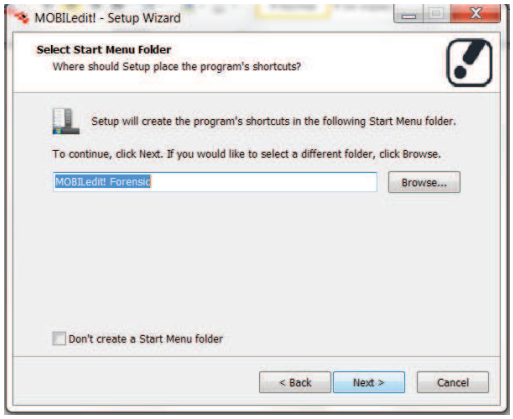
Figura 60: Lugar de Instalacion del Doftware (MOBILedit Forensic)



Creado por: Christian Guerra

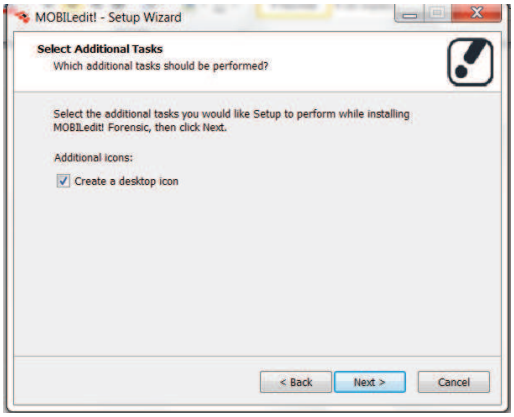
Se puede escoger si se desea ubicar en la carpeta de menú, para facilitar al usuario ejecutar la aplicación, as i como también acceso directo.

Figura 61: Lugar de Instalación en la carpeta Menú (MOBILedit Forensic)



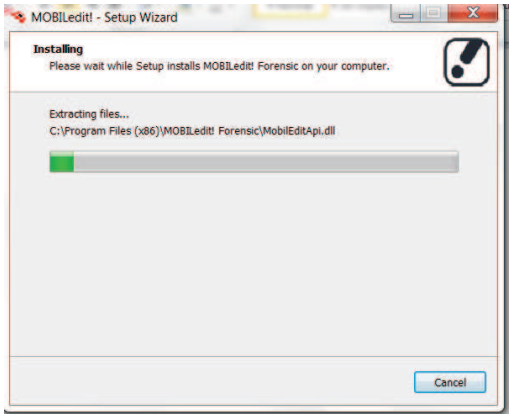
Creado por: Christian Guerra

Figura 62: Creacion de Acceso Directo (MOBILedit Forensic)



Creado por: Christian Guerra

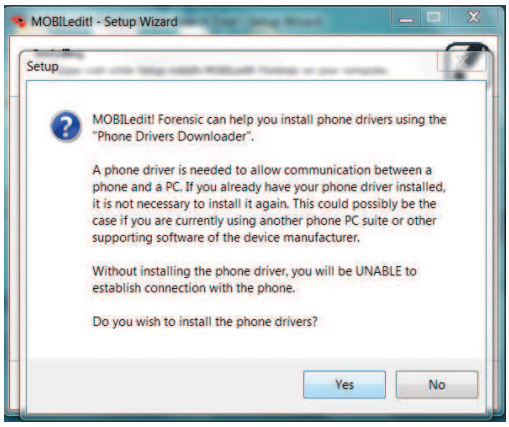
Figura 63: Proceso de Instalación (MOBILedit Forensic)



Creado por: Christian Guerra

Después de la instalación se recomienda instalar los dirvers para poder conectar a diferentes dispositivos moviles.

Figura 64: Sugerencia de Instalación de Drivers (MOBILedit Forensic)



Creado por: Christian Guerra

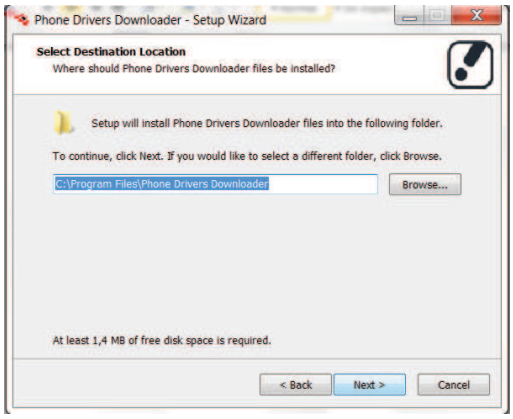
En el proceso de instalación de los drivers se lo realiza a través de un asistente de instalación.

Figura 65: Inicio de Instalación de Drivers (MOBILedit Forensic)

Creado por: Christian Guerra

Se elige el lugar de instalación de los drivers.

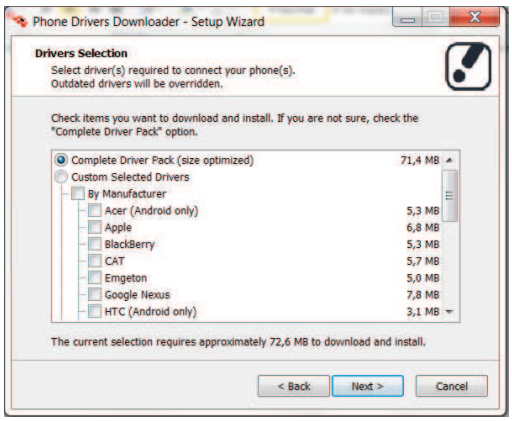
Figura 66: Lugar de Instalación de Drivers (MOBILedit Forensic)



Creado por: Christian Guerra

Podemos elegir para qué fabricante de dispositivos móviles se desea o también podemos instalar todos, en este caso se instaló todos.

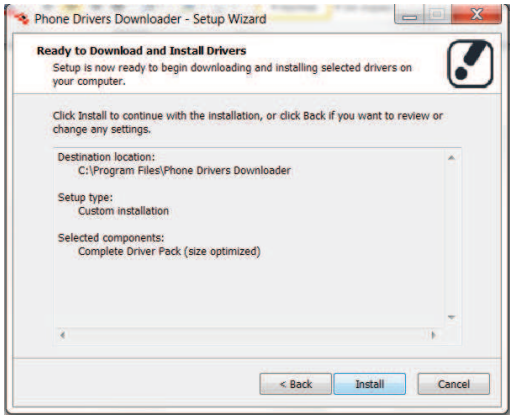
Figura 67: Opciones de Drivers (MOBILedit Forensic)



Creado por: Christian Guerra

Según la selección de los drivers nos presenta un resumen de lo antes seleccionado, antes de proceder a descargar y a instalar.

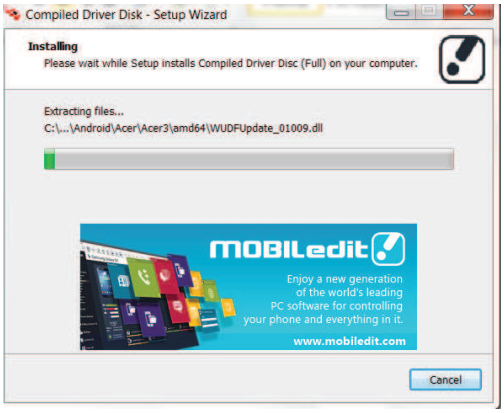
Figura 68: Referencia de Instalacion de Drivers (MOBILedit Forensic)



Creado por: Christian Guerra

En el proceso de instalación nos muestra cómo avanza la descarga y luego la instalación, lo cual dura algunos minutos.

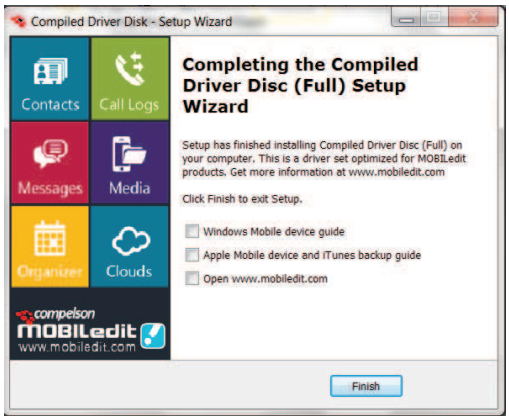
Figura 69: Proceso de Instalación (MOBILedit Forensic)



Creado por: Christian Guerra

Al finalizar nos muestra una ventana indicando más información acerca de algún dispositivo en especial

Figura 70: Finalización de Instalación (MOBILedit Forensic)

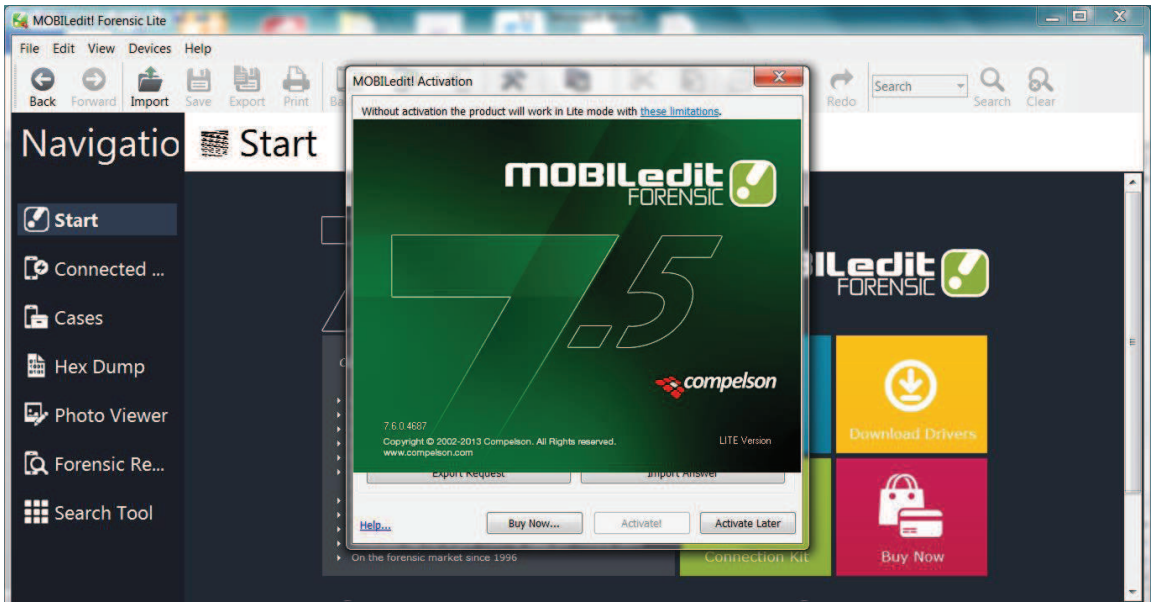


Creado por: Christian Guerra

5.2.2. Aplicación de software

Al ejecutar por primera vez MOBILedit Foresic, nos presenta una ventana muy amigable al usuario y la posibilidad de activación por un serial o una prueba. En este caso se va a utilizar la prueba.

Figura 71: Pantalla Inicial (MOBILedit Forensic)



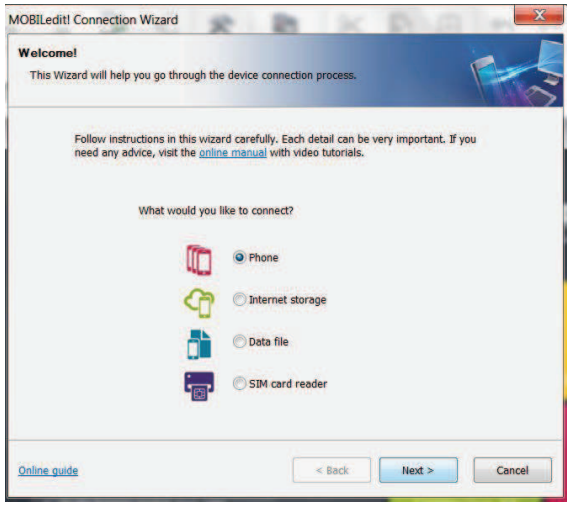
Creado por: Christian Guerra

Para conectar a un dispositivo móvil nos presenta varias opciones

- Teléfono
- Un memoria en la nube
- Un archivo
- Tarjeta de memoria

Para nuestra investigación se procedió a conectar directamente con el móvil.

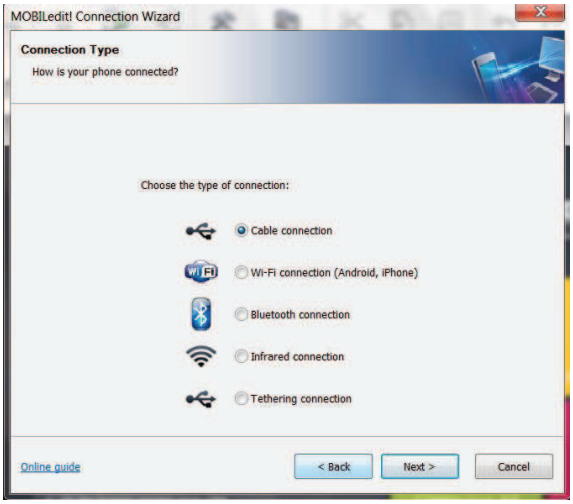
Figura 72: Conexión con Dispositivo Móvil (MOBILedit Forensic)



Creado por: Christian Guerra

Para conectase se lo puede realizar por distintos medios, inalámbricos o por cable.

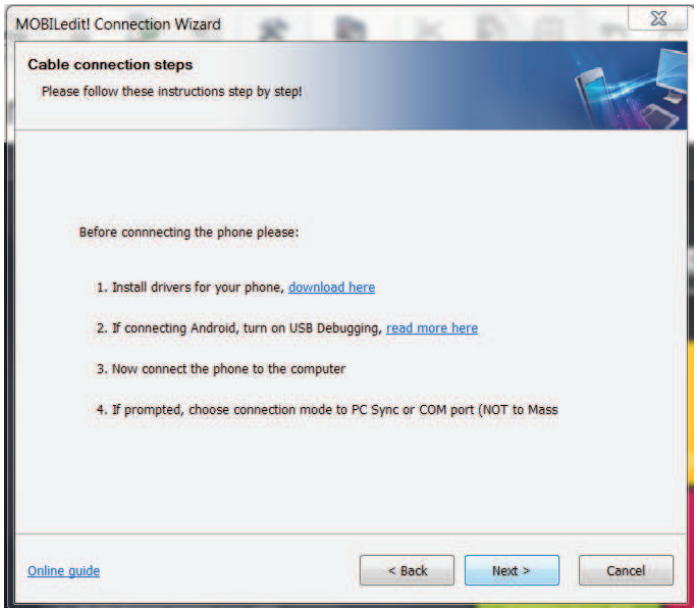
Figura 73: Tipo de Conexión (MOBILedit Forensic)



Creado por: Christian Guerra

Después de escoger el medio de conexión, nos muestra unos pasos a seguir antes de conectarse finalmente.

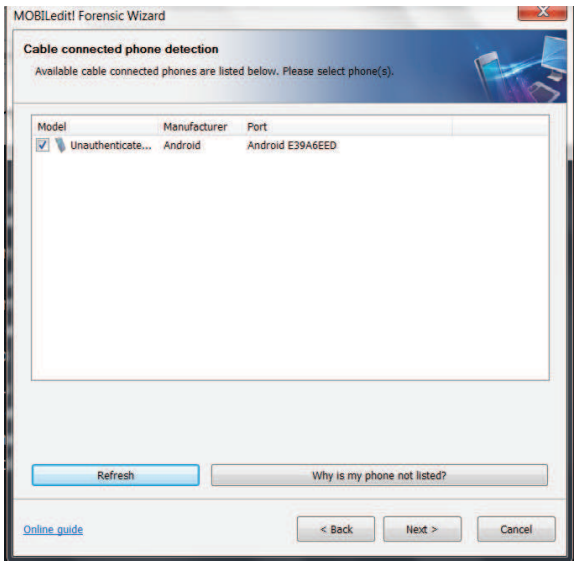
Figura 74: Instrucciones Conexión (MOBILedit Forensic)



Creado por: Christian Guerra

Al realizar la búsqueda encuentra e dispositivo móvil con ayuda del driver para poder reconocerlo.

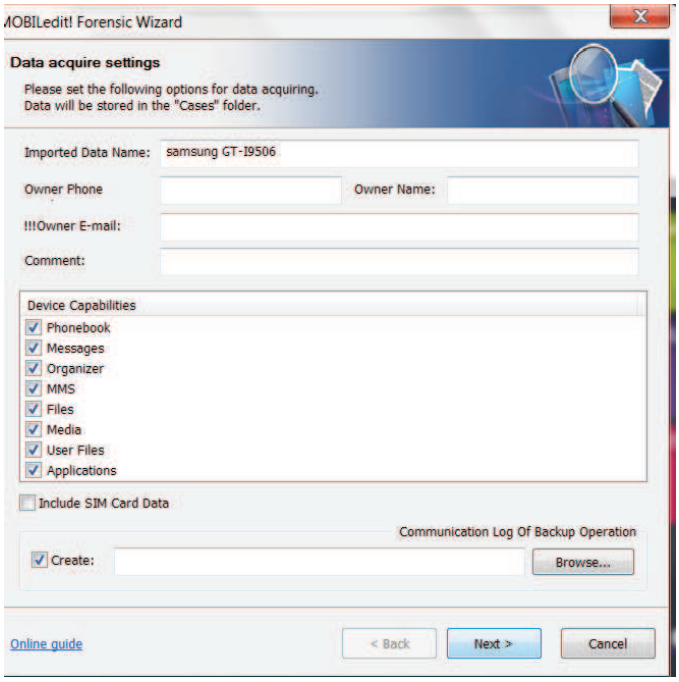
Figura 75: Búsqueda de Driver (MOBILedit Forensic)



Creado por: Christian Guerra

Nos Pide ingresar algunos datos del dispositivo, con el cual se va realizar el análisis, y también elegir la información que desea extraer.

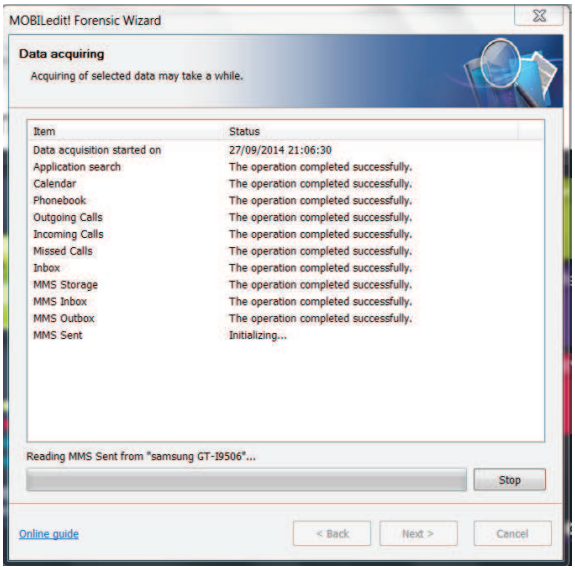
Figura 76: Detalles de la Extracción (MOBILedit Forensic)



Creado por: Christian Guerra

En el proceso de extracción muestra de manera organizada como adquiere la información de las opciones seleccionadas.

Figura 77: Proceso de Extracción (MOBILedit Forensic)



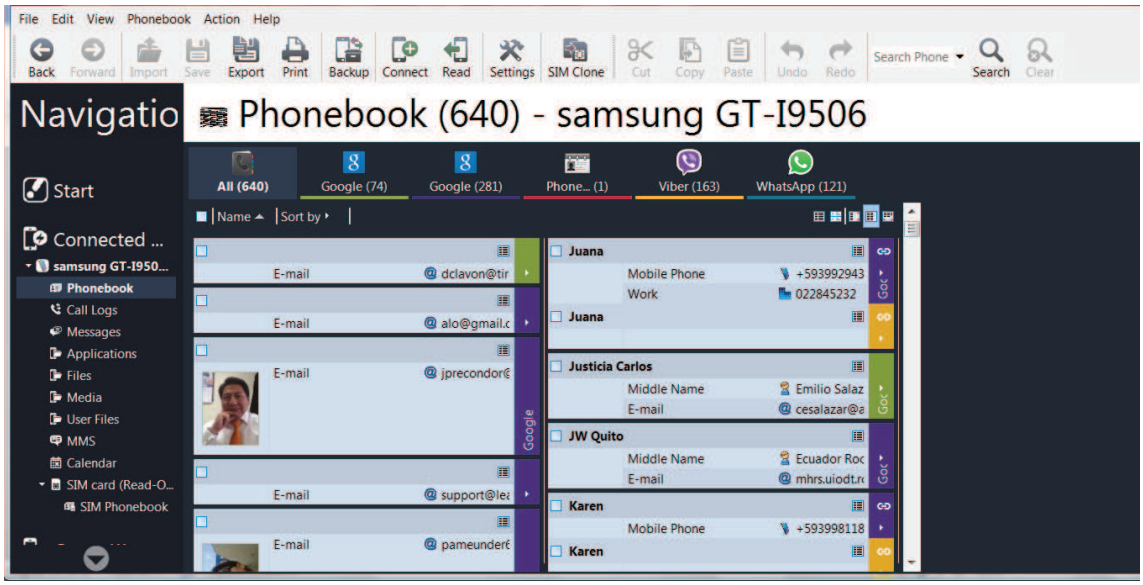
Creado por: Christian Guerra

5.2.3. Análisis de resultados obtenidos

Al terminar la extracción de la información, se pudo comprobar que realizó una copia bit a bit, como se requiere. Sin adulterar la información en el dispositivo móvil.

En el reporte se puede observar 640 contactos de la agenda, y también una clasificación, a cuentas y aplicaciones están ligadas los contactos.

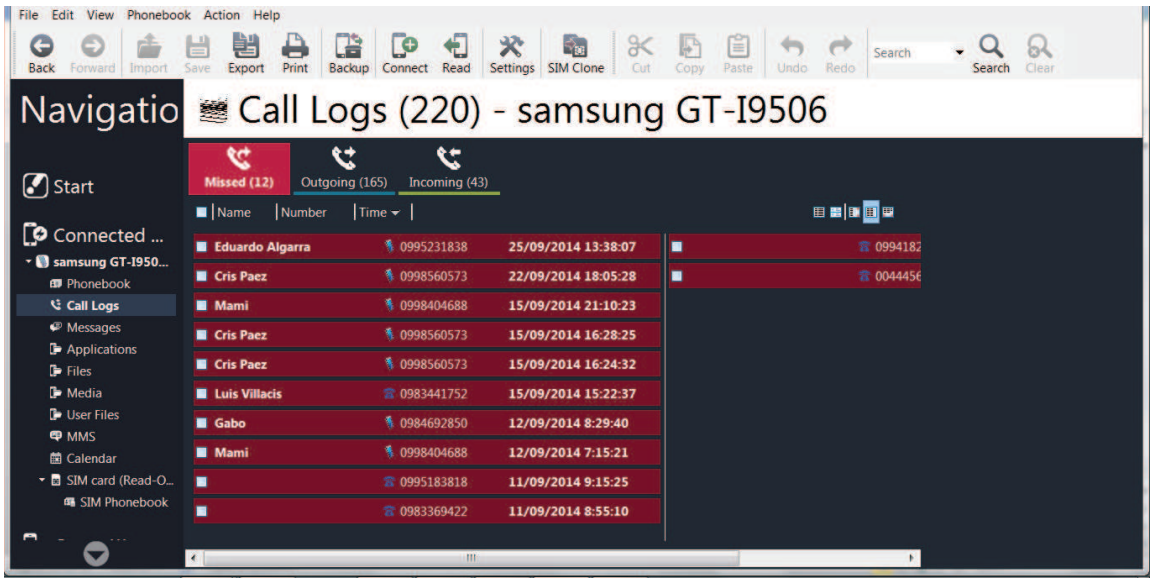
Figura 78: Registro de Contactos (MOBILedit Forensic)



Creado por: Christian Guerra

En el registro de llamadas se obtuvo 220, con un detalle de fecha y hora de cada una.

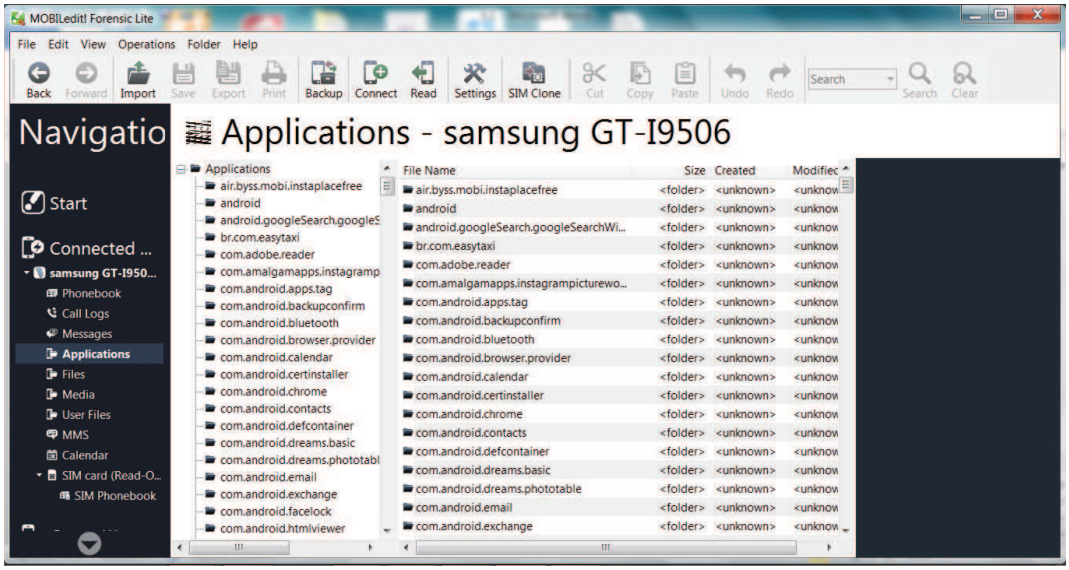
Figura 79: Registros de Llamadas (MOBILedit Forensic)



Creado por: Christian Guerra

Detalla también las aplicaciones instaladas acompañadas del directorio de ubicación en el dispositivo.

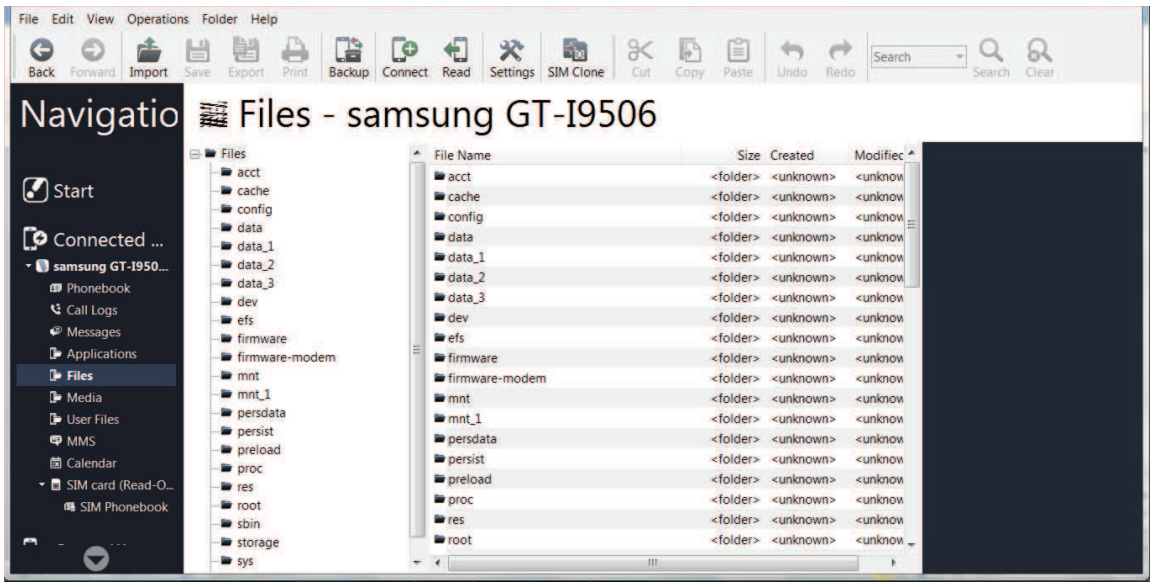
Figura 80: Regitros de Aplicaciones (MOBILedit Forensic)



Creado por: Christian Guerra

Se puede acceder también a información, guardada como archivos personales por ejemplo fotos.

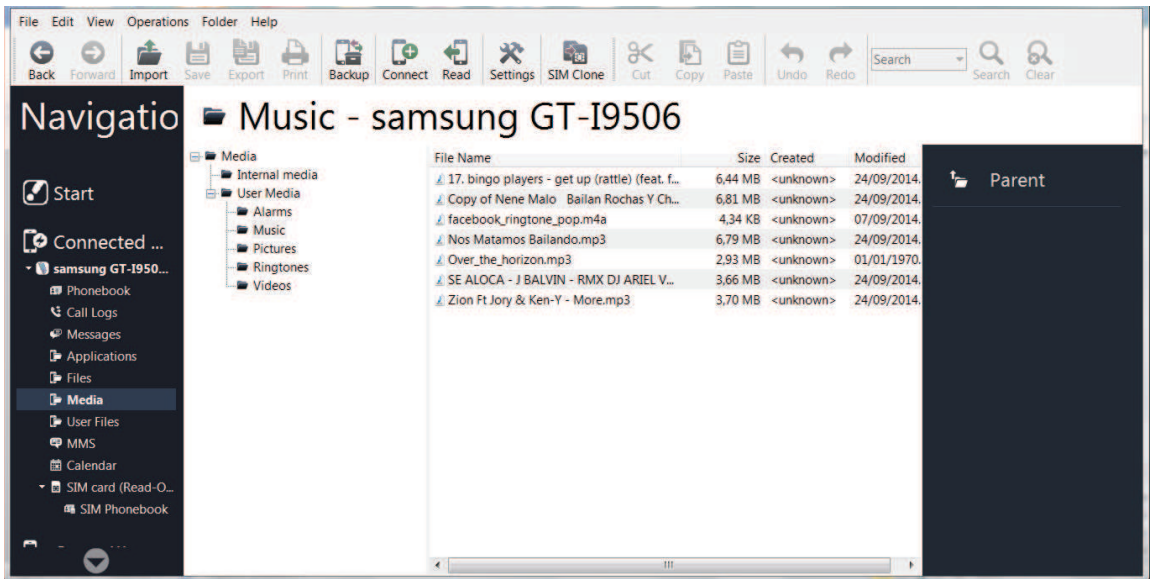
Figura 81: Registro de Archivos (MOBILedit Forensic)



Creado por: Christian Guerra

Nos muestra la música en el dispositivo, con la fecha de la última modificación.

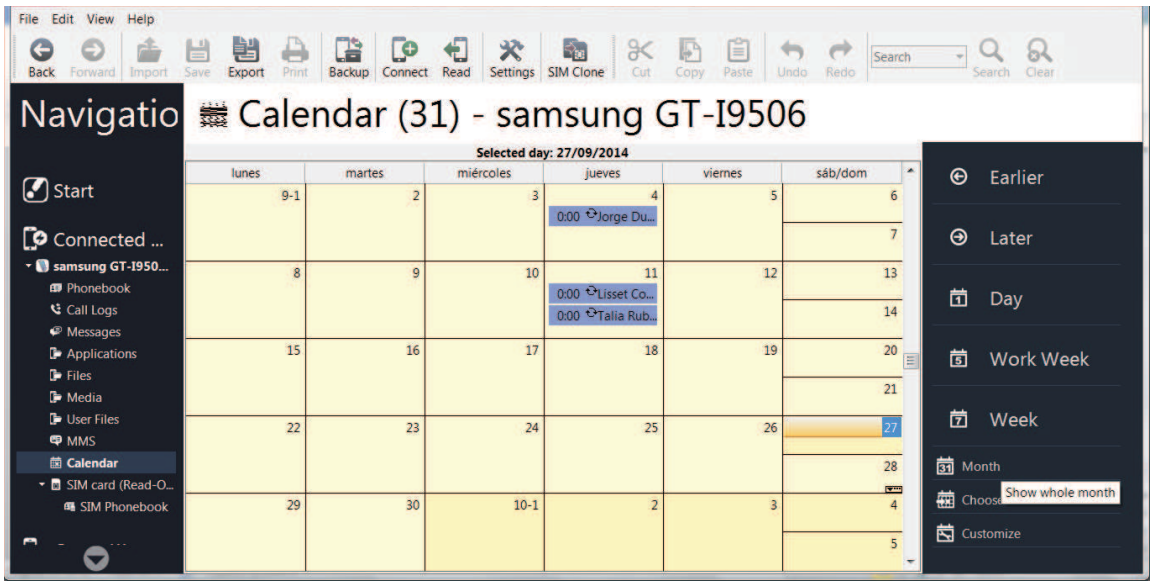
Figura 82: Registros de Musica (MOBILedit Forensic)



Creado por: Christian Guerra

En el calendario, podemos ver los eventos creados, pero no especifica si pertenecen alguna determinada cuenta.

Figura 83: Registros de Calendario (MOBILedit Forensic)



Creado por: Christian Guerra

5.3. Device Seizure

5.3.1. Instalación

Para la instalación de Device Seizure, en su página web oficial https://www.paraben.com/device-seizure.html nos permite descargar, una herramienta para realizar pruebas con la aplicación.

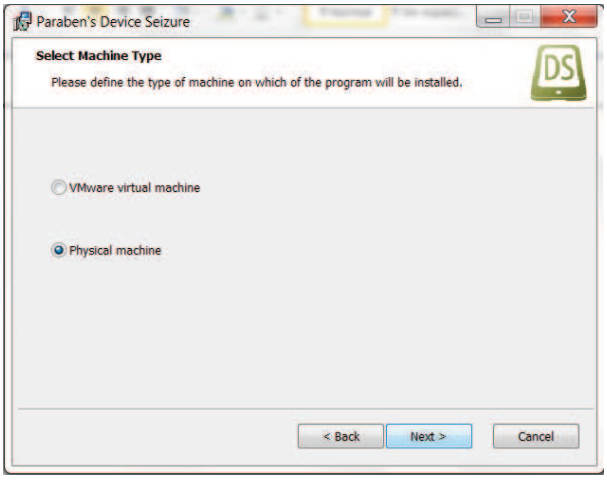
Al iniciar la instalación, se nos presenta un asistente dando la bienvenida, mostrando la versión que se va a instalar.

Figura 84: Inicio de instalación (Device Seizure)

Creado por: Christian Guerra

Para proceder la instalación, debemos especificar si se va realizar en una máquina física o en una virtual.

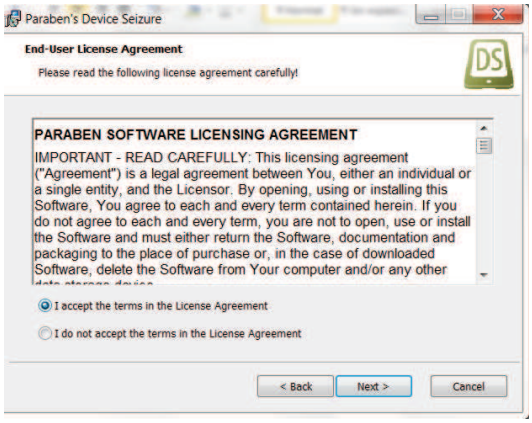
Figura 85: Tipo de Ambiente (Device Seizure)



Creado por: Christian Guerra

Se nos presenta los términos y condiciones de uso de la herramienta.

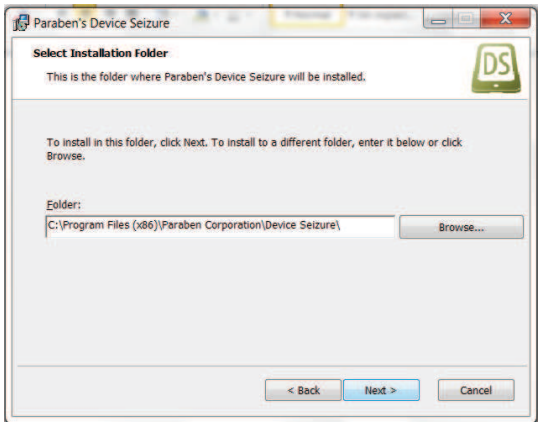
Figura 86: Licencia de Uso de Software (Device Seizure)



Creado por: Christian Guerra

Se nos pide la ubicación donde se va a realizar la instalación de la herramienta.

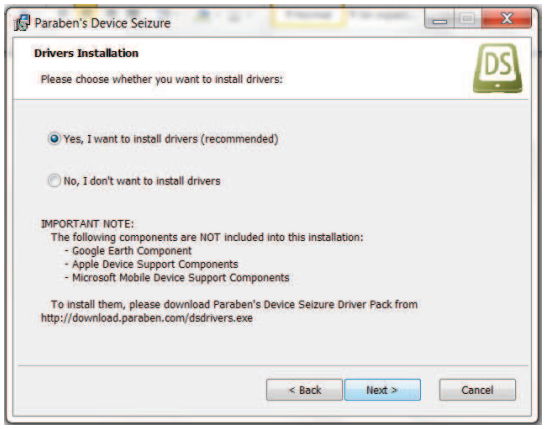
Figura 87: Lugar de Instalación (Device Seizure)



Creado por: Christian Guerra

Pregunta si se desea instalar los drivers que van a facilitar la conexión con los dispositivos móviles. En este caso se escogió que si se instale, además es la opción recomendada por el fabricante

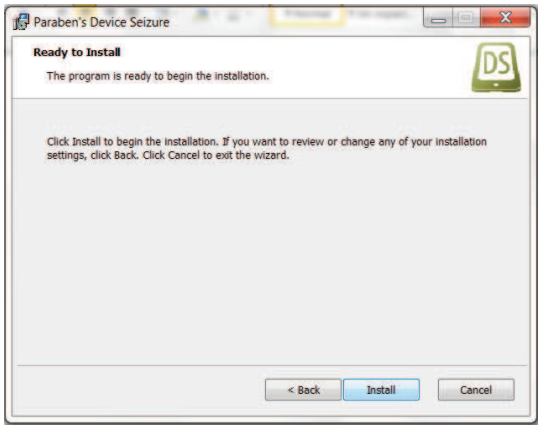
Figura 88: Instalación de Drivers (Device Seizure)



Creado por: Christian Guerra

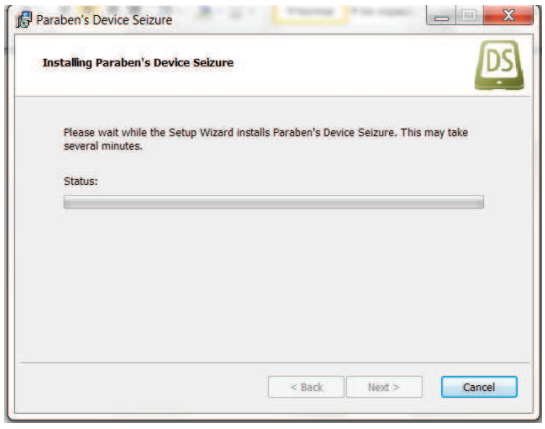
Se procede a la instalación de los drivers, que en este caso contiene el instalador de la herramienta.

Figura 89: Inicio de Instalación de Drivers (Device Seizure)



Creado por: Christian Guerra

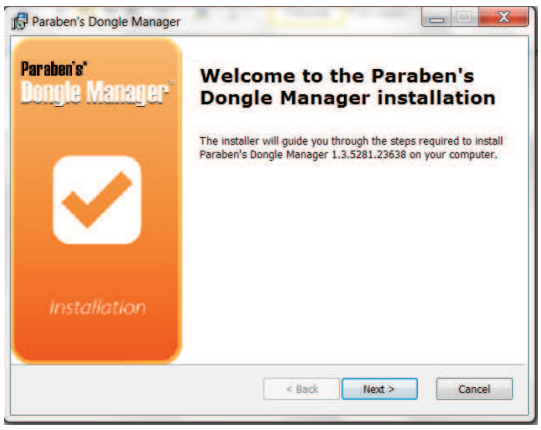
Figura 90: Proceso de Instalación (Device Seizure)



Creado por: Christian Guerra

Al terminar la instalación de los drivers, se comienza la instalación de cada componente, que es necesario para la utilización de la herramienta.

Figura 91: Inicio de Instalación del Administrador (Device Seizure)



Creado por: Christian Guerra

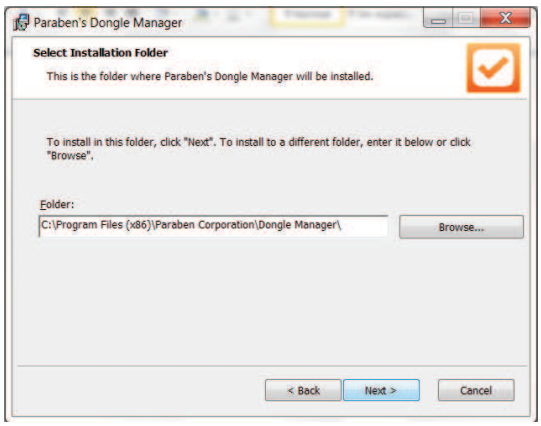
Se nos presenta los términos y condiciones del uso.

Figura 92: Términos y Condiciones de Uso (Device Seizure)

Creado por: Christian Guerra

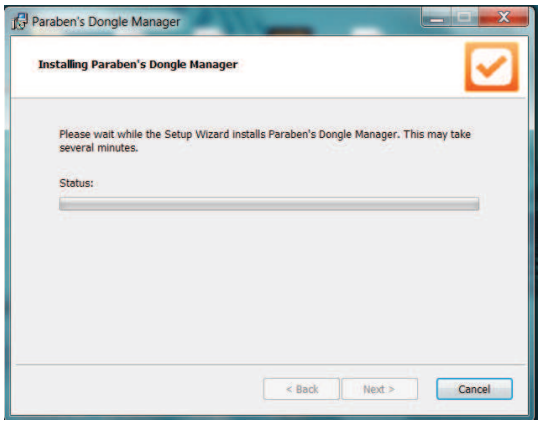
Se tiene que proporcionar la ubicación donde se va a instalar la herramienta.

Figura 93: Lugar de Instalación del Administrador (Device Seizure)



Creado por: Christian Guerra

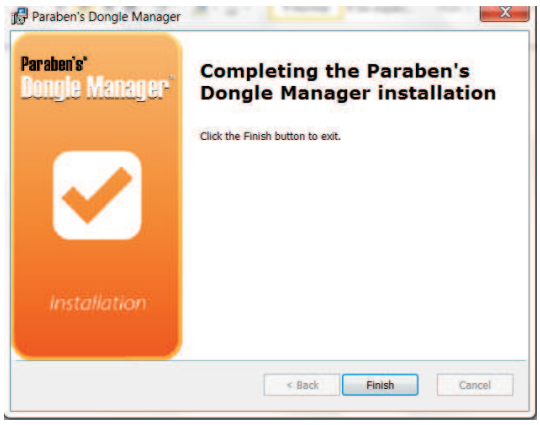
Figura 94: Proceso de Instalación (Device Seizure)



Creado por: Christian Guerra

Al terminar el proceso de instalación se nos presenta una ventana, indicando que se ha terminado y con esto podemos empezar a ser uso de la herramienta.

Figura 95: Instalación Completa del Administrador (Device Seizure)

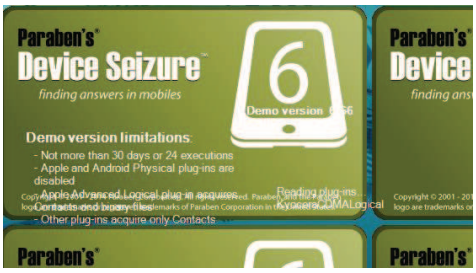


Creado por: Christian Guerra

5.3.2. Aplicación de software

Al iniciar la herramienta, nos especifica que como es de prueba , podemos usarla por 30 días o 24 ejecuciones.

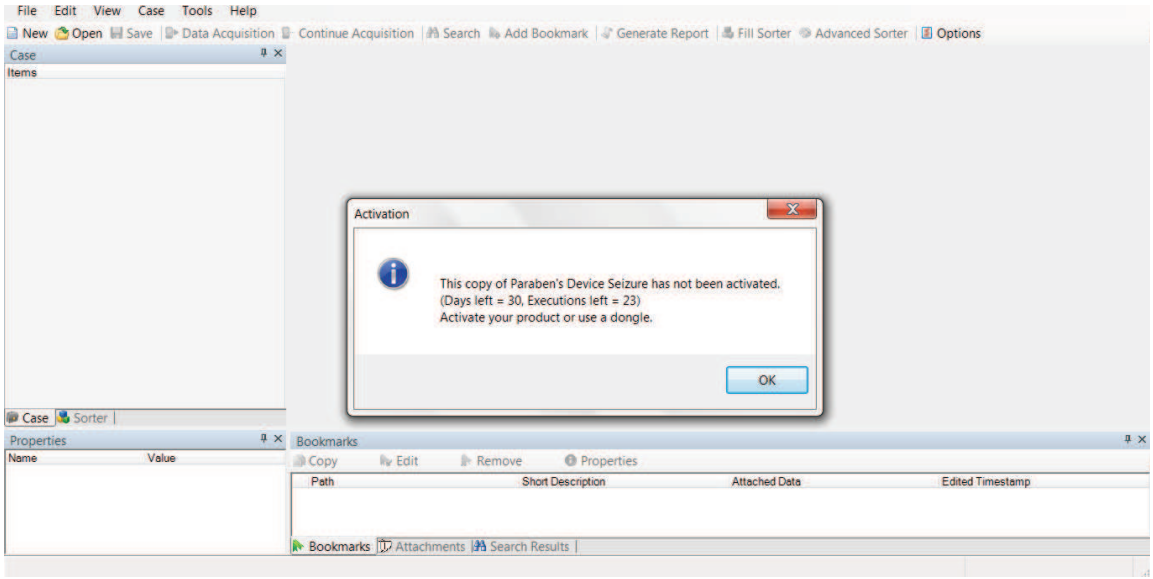
Figura 96: Inicio de Aplicación (Device Seizure)



Creado por: Christian Guerra

En el menú principal, aparece una ventana con la información del número de días y ejecuciones que nos quedan para usar la herramienta.

Figura 97: Pantalla Principal (Device Seizure)



Creado por: Christian Guerra

Al iniciar podemos abrir un caso guardad, crear uno nuevo o adquirir la información, que es lo que se va a seleccionar a continuación.

Figura 98: Inicio de Extracción (Device Seizure)

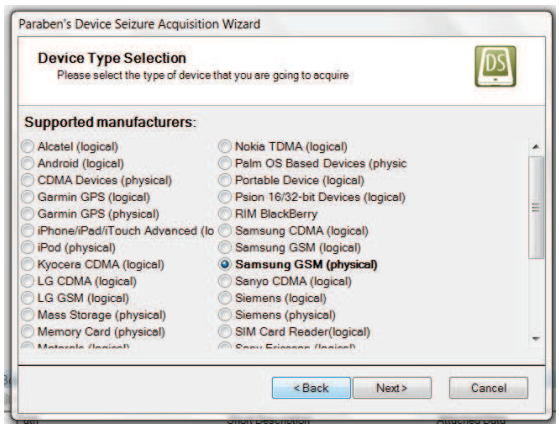
Creado por: Christian Guerra

Pese a ver instalado los drivers que contenía el instalador, se tuvo varios problemas y se probó con las siguientes opciones:

- Samsung GSM (Logical)
- Samsung GSM (Physical)
- Android (Logical)

Siendo la última opción escogida la valida, para reconocer al dispositivo móvil.

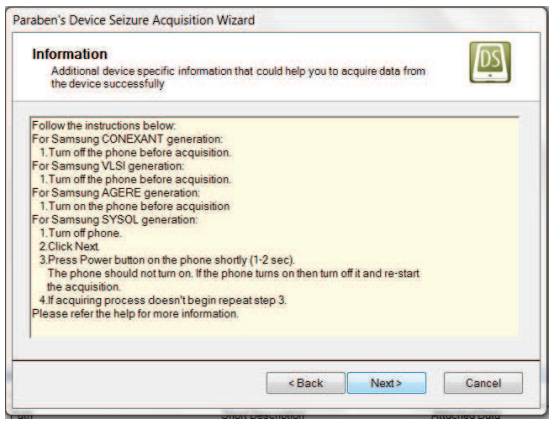
Figura 99: Selección de Tipo de Dispositivo (Device Seizure)



Creado por: Christian Guerra

Nos muestra pasos a seguir para continuar con la conexión, y luego realizar la extracción.

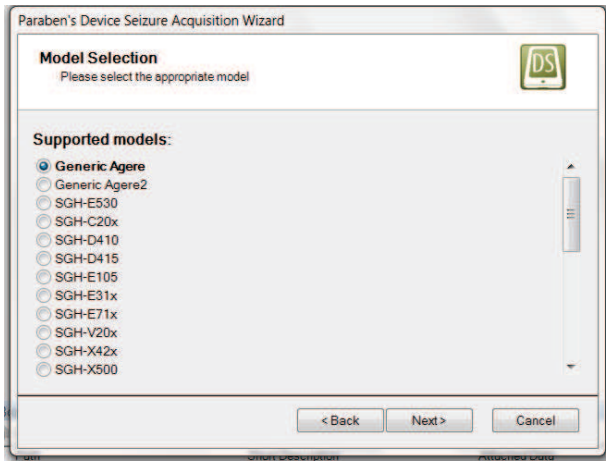
Figura 100: Información de Proceso de Extracción (Device Seizure)



Creado por: Christian Guerra

Después pide elegir el modelo del dispositivo, al no encontrar el modelo, se seleccionó la opción Generic Agere.

Figura 101: Selección de Modelo (Device Seizure)



Creado por: Christian Guerra

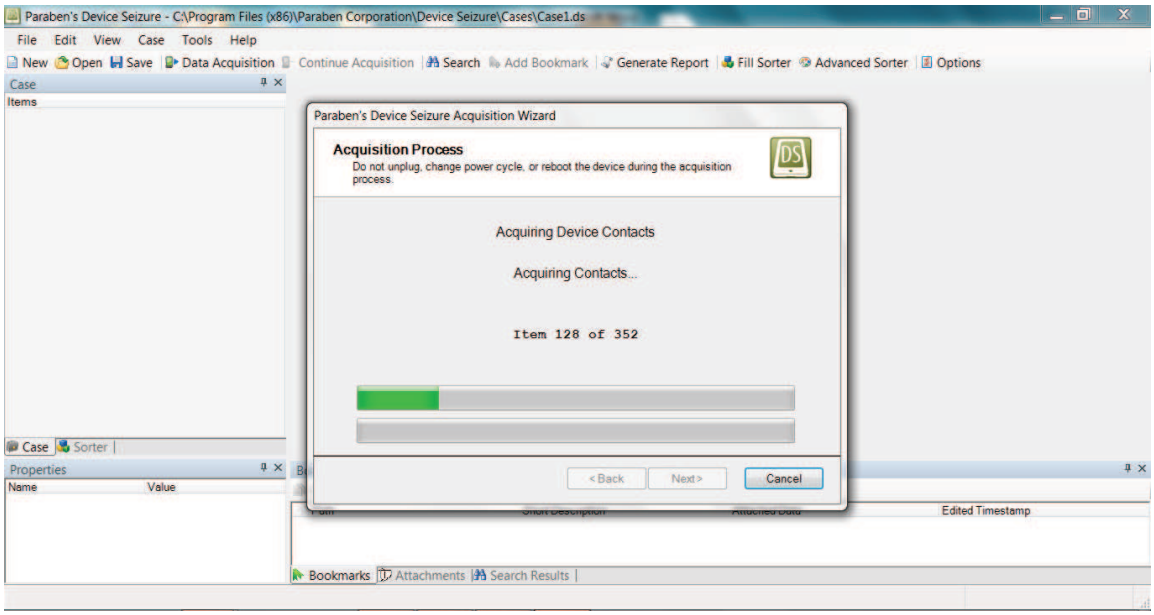
Se procede a seleccionar el dispositivo que esté conectado al computador.

Figura 102: Selección de Conexión (Device Seizure)

Creado por: Christian Guerra

Se realiza el proceso de extracción de información muy rápido y sin ningún inconveniente.

Figura 103: Proceso de Extracción de Información (Device Seizure)

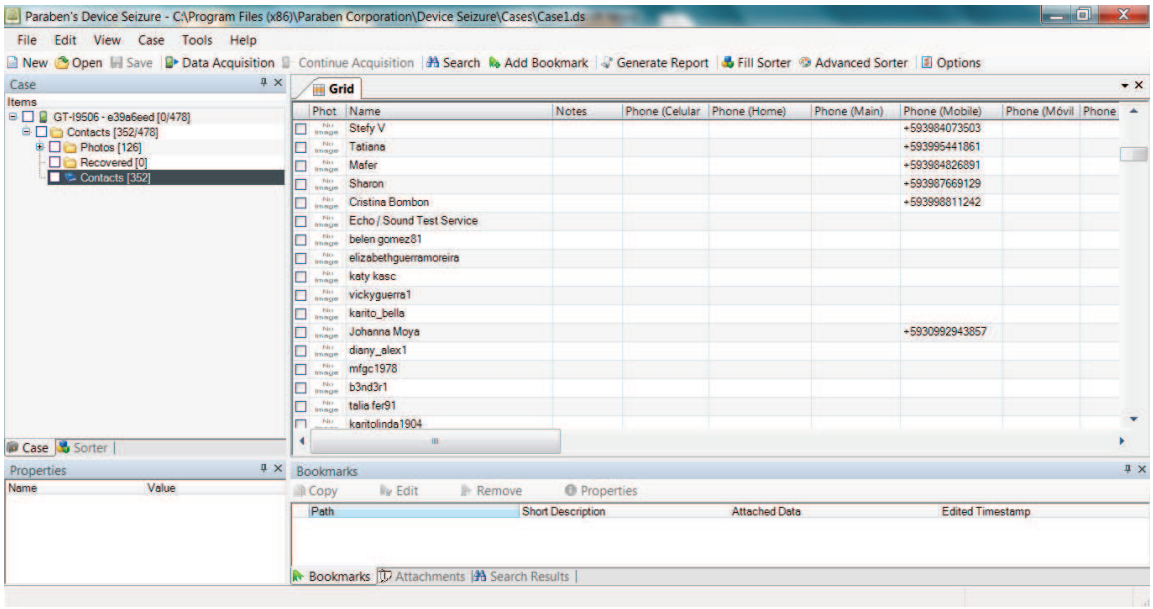


Creado por: Christian Guerra

5.3.3. Análisis de resultados obtenidos

Cuando termina la extracción de datos, y observar la información nos podemos dar cuenta que lo único que se pudo obtener fueron 126 fotos, y 352 contactos.

Figura 104: Registros de Contactos (Device Seizure)



Creado por: Christian Guerra

5.4. Comparación de datos obtenidos

Para realizar la comparación, su utilizo número de registros obtenidos en la clasificación de:

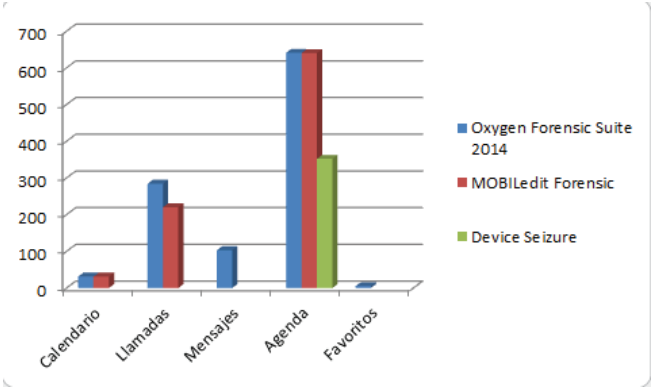
- Agenda
- Calendario
- Favoritos
- Llamadas
- Mensajes

En la **Figura 105** nos podemos dar cuenta que Oxygen Forensic Suite y MOBILedit Forenseic, son los que más información pudieron extraer del dispositivo móvil, por lo tanto son los que tienen resultados similares.

En la diferencia de registros de llamadas entre Oxygen Forensic Suite y MOBILedit es porque no se realizó el mismo día las pruebas y los datos en el dispositivo móvil cambiaron.

Por otro lado Device Seizure solo pudo obtener datos de la agenda y no todos como las otras herramientas, se deduce que al usar solo una licencia de prueba no pudimos utilizar todas sus funcionalidades.

Figura 105: Comparación de Resultados Obtenidos.



Creado por: Christian Guerra

Tabla 13: Resultados Obtenidos

	Oxygen Forensic Suite 2014	MOBILedit Forensic	Device Seizure
Calendario	31	31	
Llamadas	284	220	
Mensajes	103		
Agenda	641	640	352
Favoritos	5		

Creado por: Christian Guerra

La información que se obtuvo fue comparada con la del dispositivo móvil, las más acertadas fueron las de Oxygen Forensic Suite y MOBILedit. Cabe recalcar que las tres herramientas se usaron licencias de prueba para investigación.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Al dar como terminada la instigación de análisis forense en dispositivos móviles con Android se ha llegado a las siguientes conclusiones:

1. Se investigó minuciosamente al elegir los programas de software para las pruebas, porque existen una gran cantidad que se oferta en el mercado, y para utilizar los más reconocidos en el campo forense.
2. Para cumplir con el objetivo del presente proyecto de disertación de grado, se solicitó los instaladores al proveedor porque todo el software es licenciado, en el caso de Oxygen Forensic Suite 2014.
3. Después de analizar el procedimiento y software para la recuperación forense de evidencia digital en dispositivos móviles Android y aplicar tres de los programas de software loa más importante en equipos, se concluye que es un trabajo minucioso que se debe tener claro que información se va utilizar.
4. Al definir las pruebas a realizar, se tuvo que tener muy en cuenta el potencial de cada herramienta, porque cada una tiene características diferentes para facilitar la investigación, como la creación de reportes finales, entre otras.
5. El uso de los diferentes software forense, no fue tan complicado desde su instalación hasta el uso, ya que cuentan con manuales, asistentes de instalación y asistentes de uso. También son muy amigables para el usuario.
6. Oxygen Forensic es más eficiente, por su facilidad de uso, la información que obtiene es confiable y completa.

6.2. Recomendaciones

El presente trabajo de investigación nos lleva a las siguientes recordaciones:

1. Para evaluar una herramienta para la recuperación de evidencia digital forense en dispositivos móviles, es necesario utilizar nuevas tecnologías que ofrecen características técnicas adecuadas y seguras.
2. Se recomienda utilizar el software del proveedor oficial, para facilitar cualquier duda directamente con los desarrolladores, como ejemplo en nuestro caso se tuvo inconveniente al conectar con el dispositivo móvil a Oxygen Forensic Suite 2014, pero al escribir al proveedor nos dio indicaciones de cómo hacerlo.
3. Para utilizar el software es necesario validar la compatibilidad del dispositivo móvil, para utilizar al máximo las diferentes herramientas.
4. Es importante leer los manuales de los fabricantes tanto de instalación y de uso para no tener problemas al utilizar los componentes del software.
5. Contar con los drivers indicados para no tener problemas de conectividad.

BIBLIOGRAFÍA

ABC Tecnología. ABC Tecnología Internet http://www.abc.es/tecnologia/moviles-telefonia/20130709/abci-jelly-bean-android-lider-201307091722.html Acceso (19 de julio del 2013)

Alias: Comos. Xataka Android Internet http://www.xatakandroid.com/sistema-operativo/novedades-en-android-4-3-jelly-bean (30 de julio del 2013)

Almeida, Romo. Omar Metodología de Análisis Forense Internet: http://repositorio.utn.edu.ec/bitstream/123456789/539/21/04%20ISC%20157%20RESUMEN%20TECNICO%20ESPA%C3%91OL.pdf (1 de Marzo del 2014)

Android http://www.android.com/kitkat/ (17 de octubre del 2013)

Auditorías de Seguridad Internet: http://www.informatica64.com/AnalisisForense.aspx Definiciones (19 de Febrero del 2014)

Casey, Eoghan. Digital Evidence and Computer Crime, Second Edition. (1 de Marzo del 2014)

Cómputo forense Internet: http://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Definiciones (19 de Febrero del 2014)

Dunked. Android. Internet http://irinablok.dunked.com/android Acceso (18 de junio de 2013)

Fases De La Informática Forense Internet: http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf (1 de Marzo del 2014)

Fases De La Informática Forense Internet: http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf (1 de Marzo del 2014)

Fases De La Informática Forense Internet: http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf (19 de Febrero del 2014)

Final Data. Internet: http://finaldata.com/Company/?s=COM.CEO Acceso (20 de Abril del 2014)

Final Data. Internet: http://finaldata.com/Forum2/?s=PRD&c=18&n=51 Acceso (19 de Abril del 2014)

Francisca Rodríguez, LA INFORMÁTICA FORENSE: EL RASTRO DIGITAL DEL CRIMEN Internet: http://www.derechoycambiosocial.com/revista025/informatica_forense.pdf (18 de Febrero 2014)

García, Damián. Xataka Android Internet http://www.xatakandroid.com/sistema-operativo/asi-es-android-4-1-jelly-bean Acceso (19 de julio del 2013)

García, Damián. Xataka Android Internet http://www.xatakandroid.com/sistema-operativo/asi-es-android-4-2-el-nuevo-sabor-de-jelly-bean Acceso (19 de julio del 2013)

Gómez, Leopoldo Sebastián M. El tratamiento de la Evidencia Digital Internet: http://sebastiangomez.sytes.net/papers/ETED.pdf (19 de Febrero del 2014)

Gutiérrez , Juan David Informática Forense Internet: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf (19 de Febrero del 2014)

Helle, Lia. Geekets Internet http://www.geekets.com/2013/10/lanzamiento-nexus-5-android-kitkat/# (17 de octubre del 2013)

Historia De La Informatica Forense Internet: https://sites.google.com/site/sykrayolab/historia-de-la-informatica-forenseSistema Android Internet: http://scoello12.wordpress.com/ventajas-y-desventajas/ (29 de Noviembre del 2013)

Informática Forense, Inserción Jurídica Internet: http://repositorio.utn.edu.ec/bitstream/123456789/539/9/04%20ISC%20157%20CAPITULO%20IV.pdf (1 de Marzo del 2014)

Lendino ,Jamie. Google's Android Update Alliance Is Already Dead Internet http://www.pcmag.com/article2/0,2817,2397729,00.asp Acceso (18 de junio de 2013)

López Delgado, Miguel. Análisis Forense Digital Internet: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf (1 de Marzo del 2014)

Master Pacheco, Fernando Sistema Operativo Android para moviles. Internet: http://www.slideshare.net/navarrocar/sistema-operativo-android-11594122 (29 de Noviembre del 2013)

Micro Systemation. Internet: http://www.msab.com/company/about-us (18 de Abril del 2014)

Micro Systemation. Internet: http://www.msab.com/xry/what-is-xry (18 de Abril del 2014)

MOBILedit! Forensic Features. Internet: http://www.mobiledit.com/company (1 de Abril del 2014)

Open Handset Alliance. Android Internet http://www.openhandsetalliance.com/android_overview.html Acceso (18 de junio de 2013)

Open Source Android Forensics Toolkit. Internet: http://sourceforge.net/projects/osaftoolkit/ Acceso (20 de Abril del 2014)

OSAF Internet http://osaf-community.org/home.html Acceso (20 de Abril del 2014)

Oxygen Forensics. Internet http://www.informatica64.com/OxygenForensics.aspx (1 de Abril del 2014)

Paraben Corporation. Internet: https://www.paraben.com (1 de Abril del 2014)

Salas Danny. La historia y los comienzos de Android, el sistema operativo de Google. Internet http://www.elandroidelibre.com/2011/08/la-historia-y-los-comienzos-de-android-el-sistema-operativo-de-google.html Acceso (18 de junio de 2013)

Salas, Danny. La historia y los comienzos de Android, el sistema operativo de Google. Internet http://www.elandroidelibre.com/2011/08/la-historia-y-los-comienzos-de-android-el-sistema-operativo-de-google.html Acceso (18 de junio de 2013)

Sánchez Cordero, Pedro. Forensics Power Internet: conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html (15 de Marzo del 2014)

Simcon Forensics. Internet: http://www.simcon.no Acceso(19 de Abril del 2014)

Sofpedia Internet: http://www.softpedia.es/programa-Oxygen-Forensic-Suite-153966.html Acceso (20 de Abril del 2014)

Sofpedia. Internet: http://www.softpedia.es/programa-Device-Seizure-47141.html Acceso (20 de Abril del 2014)

Todo Android Internet http://www.todoandroid.es/index.php/faq-de-android/65-versiones/805-que-es-ice-cream-sandwich-40-novedades-y-caracteristicas-de-esta-version-de-android.html Acceso (19 de julio del 2013)

Tucker, Cummings. La historia de la informática forense Internet: http://www.ehowenespanol.com/historia-informatica-forense-sobre_102525/ (19 de Febrero del 2014)

Txema Rodriguez. La historía de todas las versiones del SDK de Android en una infografía Internet http://www.genbetadev.com/desarrollo-aplicaciones-moviles/la-historia-de-todas-las-versiones-del-sdk-de-android-en-una-infografia Acceso (19 de junio de 2013)

Via Forensics. Internet: https://viaforensics.com/resources/tools/android-forensics-tool/ Acceso (20 de Abril del 2014)

Wikipedia Computo Forense Internet: http://es.wikipedia.org/wiki/C%C3%B3mputo_forense (1 de Marzo del 2014)

Wikipedia. Android. Internet http://es.wikipedia.org/wiki/Android#cite_note-AndroidInc-11 Acceso (18 de junio de 2013)

Zuccardi, Giovanni. Informática Forense Internet: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf (19 de Febrero del 2014)