UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

SOFTWARE PARA LA RECOLECCIÓN DE INFORMACIÓN EN LA INVESTIGACIÓN FORENSE EN SMARTPHONES.

Proyecto de Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN: Seguridad Computacional

AUTOR: Guerra González Erika Afrodita

TUTOR: Ing. David Omar Guevara Aulestia Mg.

Ambato – Ecuador

Octubre-2017

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: SOFTWARE PARA LA RECOLECCIÓN DE INFORMACIÓN EN LA INVESTIGACIÓN FORENSE EN SMARTPHONES, de la señorita Erika Afrodita Guerra González, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato octubre, 2017

EL TUTOR

Ing. David Guevara

AUTORÍA

El presente Proyecto de Investigación titulado: SOFTWARE PARA LA RECOLECCIÓN DE INFORMACIÓN EN LA INVESTIGACIÓN FORENSE EN SMARTPHONES, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato octubre, 2017

Erika Afrodita Guerra González

CC: 1804458444

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato octubre, 2017

Erika Afrodita Guerra González

CC: 1804458444

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Franklin Mayorga y el Ing. Rubén Nogales, revisó y aprobó el Informe Final del Proyecto de Investigación titulado SOFTWARE PARA LA RECOLECCIÓN DE INFORMACIÓN EN LA INVESTIGACIÓN FORENSE EN SMARTPHONES, presentado por la señorita Erika Afrodita Guerra González de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Mg. Elsa Pilar Urrutia Urrutia

PRESIDENTA DEL TRIBUNAL

Ing. Mg. Franklin Mayorga

DOCENTE CALIFICADOR

Ing. Mg. Rubén Nogales, Mg

DOCENTE CALIFICADOR

DEDICATORIA:

A Afrodita mi madre, que me llena de orgullo, no va a haber manera de devolverte todo el esfuerzo, dedicación y el amor, no sé dónde me encontraría de no ser por tu ayuda, tu compañía y tu amor.

A mi hija Katherine, por tu afecto y cariño, eres la razón de mi felicidad, de mi esfuerzo y de mis ganas de buscar siempre lo mejor para ti; te agradezco porque a tu corta edad me enseñas a encontrar el lado dulce de las cosas. Eres mi motivación más grande.

A mi esposo Gabriel, porque tu ayuda fue fundamental y por estar conmigo en los momentos difíciles motivándome y ayudándome, por creer en mi capacidad y brindarme tu comprensión, cariño y amor.

Te lo agradezco muchísimo, mi vida.

Erika Guerra González

AGRADECIMIENTO:

Agradezco a mi tutor el Ing. David Guevara por tener toda la paciencia del mundo, por ayudarme y guiarme en este proyecto.

A mi madre por hacer todo lo posible para brindarme la mejor educación, por haberme enseñado que con esfuerzo y constancia todo es posible.

A mi hija por hacer que vea la vida cada día de una forma diferente y hacer que me esfuerce por ella todos los días.

A mi esposo por su apoyo incondicional en especial en los malos momentos, por su ayuda y su esfuerzo para hacer esto posible.

A mi familia por estar siempre pendientes de mí y de pasos.

A ti loquillo ángel por ser el hermano y la mano amiga que estuvo conmigo en mi peor momento brindándome tu hombro, tus consejos y tus oídos.

Erika Guerra González

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

EL PROBLEMA

1.1 TEMA DE INVESTIGACIÓN

Software para la recolección de información en la Investigación Forense en Smartphones en la ciudad de Ambato.

1.2 PLANTEAMIENTO DEL PROBLEMA

Actualmente los dispositivos móviles son parte de la vida cotidiana de las personas, en especial aquellos dispositivos llamados *Smartphones,* que permiten a los usuarios conectarse a Internet, acceder a redes sociales y manejar documentos; en Ecuador según el Instituto Nacional de Estadísticas y Censos (INEC) [1] en el año 2015 dice que, 3084886 ecuatorianos declararon tener al menos un Smartphone, en comparación con el año 2011 cuando la cifra de ecuatorianos que tenían un Smartphone era de 522640; lo cual indica que la tendencia en comercialización de estos dispositivos es seguir creciendo eso se puede evidenciar en el número de líneas móviles activas que en el año 2016 fue de 14,5 millones frente a 16,4 millones de habitantes país según [2].

Los smartphones no solamente son usados para tareas comunes como recibir y enviar mensaje y llamadas, sino que también brindan las mismas funcionalidades que pueden brindar los ordenadores. Esta razón hace que los smartphones en la actualidad se conviertan en una potente fuente de evidencia digital en una investigación forense. Y por lo tanto también existe la necesidad de acceder a la posible evidencia que pueda contener el Smartphone para ser presentada en un formato admisible [3] [4].

Esencialmente, la investigación forense se lleva a cabo con la ayuda de herramientas. Sin embargo, teniendo en cuenta los diferentes tipos de smartphones y el hecho de que existen numerosos sistemas operativos móviles y fabricantes de hardware, es poco probable que se encuentre una herramienta forense única que pueda adquirir todos los datos requeridos desde todos los smartphones, por lo tanto existe la necesidad de saber qué herramienta forense es la más adecuada para un Smartphone o sistema operativo específico, para adquirir los datos necesarios o un conjunto de datos, ya sea que los datos sean manipulados y modificados por el Sistema Operativo, importados y editados por el usuario [3].

Según el autor [5] las herramientas deben producir resultados válidos basadas en lo que realmente se necesita en términos de datos que son admisibles en un tribunal. La mayoría de los investigadores enfrentan un gran desafío al seleccionar la herramienta adecuada, capaz de producir una evidencia pericialmente sólida. Debido a la falta de estándares, cada proveedor de las herramientas define el término "soporte" de manera diferente. Esto crea enormes y desafiantes dificultades en los investigadores. La mayor parte de los proveedores de herramientas forenses afirman que son compatibles con el mayor número de teléfonos, lo que se ha convertido en el foco central en lugar de la calidad del software.

Estas herramientas forenses móviles son importantes para las agencias de investigación en la resolución de investigaciones criminales. Sin embargo, si los resultados producidos por estas herramientas son incorrectos o la herramienta no funciona bien para las evidencias electrónicas en este caso el Smartphone, entonces los resultados podrían considerarse inadmisibles en el tribunal de justicia, haciendo de gran importancia y ayuda una prueba del software utilizado en la investigación móvil forense.

1.3 DELIMITACIÓN

Área Académica: Hardware y Redes.

Línea de Investigación: Tecnologías de la Información.

Sublínea de Investigación: Seguridad Computacional.

Delimitación Espacial: Cuidad de Ambato.

Delimitación Temporal: La presente investigación se desarrollará en los 6 meses posteriores a la aprobación del H. Consejo Académico de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4 JUSTIFICACIÓN

La Investigación Forense contribuye a mejorar la investigación y la recuperación de la información que se almacenan en un dispositivo electrónico considerado evidencia dentro de un proceso judicial, en este caso los Smartphones, pero se necesitan de herramientas para poder extraer información que servirá de evidencia dentro del caso [5].

El software forense es capaz de formar una interfaz con el investigador con el cual puedan conectarse con el dispositivo a examinar. Para que los datos extraídos del Smartphone sean admisibles en un tribunal de justicia, un experto forense debe poder demostrar que la evidencia obtenida es sólida, lo que significa que no han sido manipulados durante todo el proceso de investigación [6].

Además, sería prioritario que exista un estudio serio, preciso y actualizado de las principales alternativas de software para realizar un análisis forense que permita identificar qué, quién, cuándo y qué medios se utilizaron en un delito [7].

Por este motivo se debe evaluar el software que puede ser utilizado en una investigación forense para la recolección de evidencia desde un punto de vista técnico, que servirá de ayuda y guia para poder utilizar el software que mejor maneje la evidencia digital (información) y la evidencia electrónica (Smartphone, ordenadores y demás dispositivos electrónicos) dentro de un proceso de investigación en el cual se encuentre involucrado un Smartphone [3].

1.5 OBJETIVOS

1.5.1 Objetivo General

- Analizar el software para la recolección de información en la investigación forense para smartphones en la ciudad de Ambato.

1.5.2 Objetivos Específicos

- Analizar información relacionada con la Investigación Forense en Smartphones en archivos y bases de datos en la fiscalía de la ciudad de Ambato.

- Estudiar la funcionalidad, aplicabilidad y eficacia del software para la Investigación Forense basándose en un estudio del software: Oxygen Forensics, Device Seizure y MOBILedit.

- Elaborar un cuadro comparativo sobre la funcionalidad, aplicabilidad y eficacia, basado en el estudio del software: Oxygen Forensics, Device Seizure y MOBILedit.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

Una vez analizada la importancia de la evaluación de software para análisis forense en Smartphones se observó que se han desarrollado proyectos similares a nivel nacional e internacional, es así que revisando los archivos en el portal de repositorios digitales COBUEC, Consorcio de Bibliotecas Universitarias del Ecuador, Google Académico, y bases de datos científicas como Modern Education and Computer Science, se ha determinado que existen trabajos con variables afines a este tema, los mismos que se describen a continuación:

Yu Lung Li realizó un seminario de graduación acerca del software forense utilizado en dispositivos Android. Sus conclusiones sobre el trabajo realizado fueron que la velocidad de extracción de datos depende de la cantidad de datos que tiene el Smartphone, además de que algunas de las aplicaciones analizadas permiten generar un reporte acerca de los datos extraídos y que con el manual se facilita la instalación de aplicaciones de análisis forense del dispositivo móvil. El software que se utilizó para el estudio fue: Bitpim, Seizure Paraben, Oxygen y MOBILedit, mientras que el análisis se realizó en el dispositivo Android Samsung T959 [8].

Así mismo se presenta como tema de disertación de grado el documento de Christian G. en una de las conclusiones más importantes se detalla que al definir las pruebas que se realizan, se tuvo que tomar en cuenta el potencial de cada herramienta, porque cada una tiene características diferentes para facilitar la investigación, como la creación de reportes finales. El software que se utilizó para la investigación fue: Oxygen, Mobiledit y Device Seizure mientras que el análisis se lo realzó en el dispositivo: Android Samsung S4 i9506 [7].

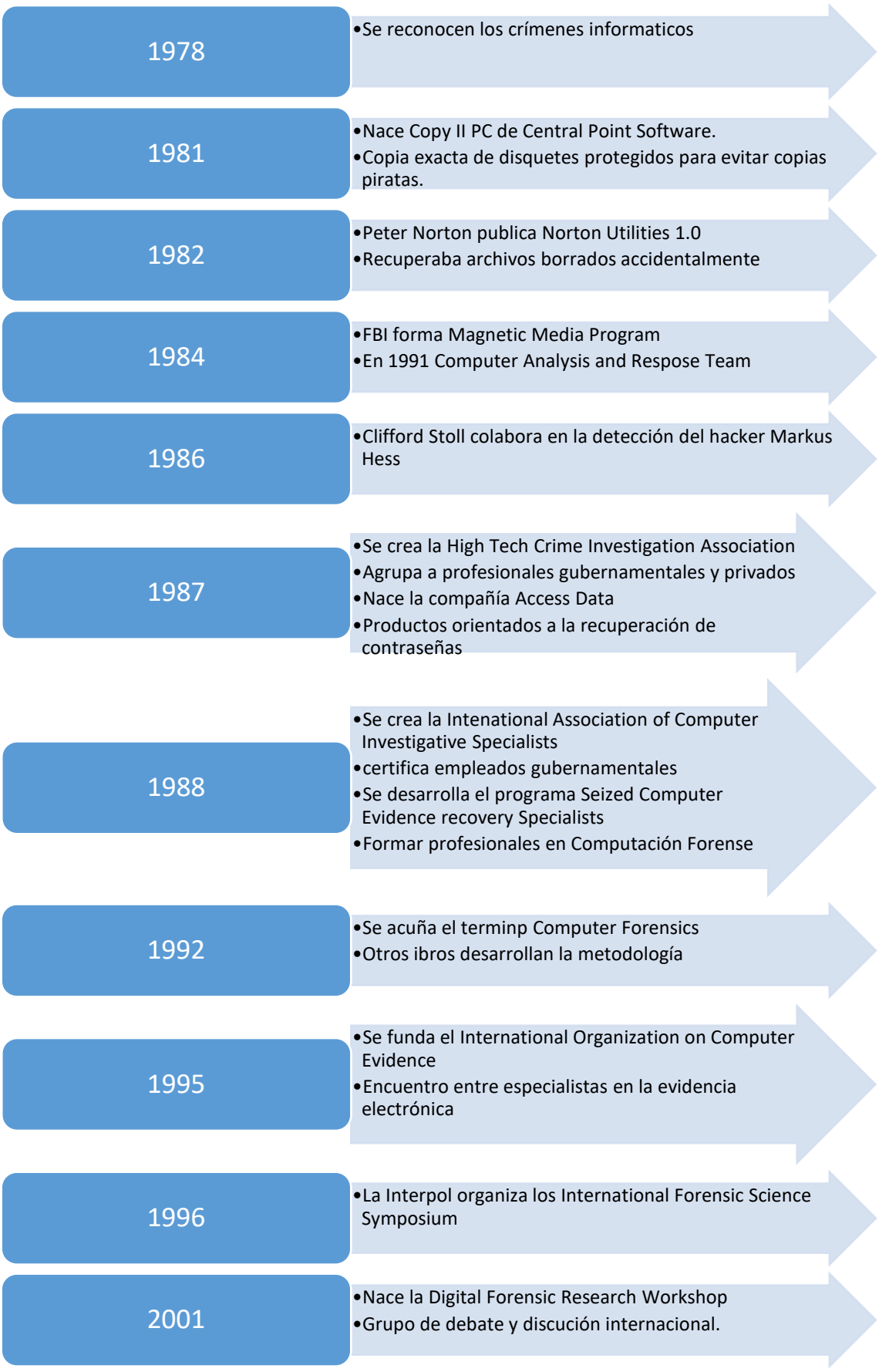
Según Maxwell A., Shahzad S. and Oliver P. en su investigación concluyen que Las capacidades crecientes de los dispositivos móviles, así como los cambios en curso en los paradigmas de comunicación e informática, además del uso generalizado y muchos beneficios en las actividades profesionales y privadas para sus usuarios, también han abierto muchas oportunidades para sus abusos en acciones y acciones no deseadas, incluido el uso de técnicas anti-forenses para evitar la detección mientras se investiga. Por otra parte, la sofisticación de los usuarios y las aplicaciones disponibles hace que sea mucho más fácil explotar diversas técnicas anti- forenses para obstaculizar posibles investigaciones digitales. Para hacer frente a estos desafíos, se requirió extender el plan de prueba del teléfono inteligente con énfasis para contrarrestar cualquier intento potencial anti-forense. El novedoso marco de pruebas, basado en los criterios existentes, puede evaluar una aplicación mientras se encarga también del uso de técnicas potencialmente forenses. El software utilizado para la investigación fue MoDeFo Software, el cual es un software licenciado y los dispositivos probados fueron: Xperia X1 y Nokia 5800 [9].

Según Oluwafemi O. y Sefiyat O. en su investigación *Comparative Evaluation of Mobile Forensic Tools* concluyen que el estudio tuvo como objetivo evaluar el rendimiento de algunas herramientas forenses para adquirir datos, con énfasis en datos eliminados, desde teléfonos Android. Los resultados de nuestro estudio muestran que dos de las cuatro herramientas, Access Data FTK Imager y EnCase, funcionaron mejor que MOBILedit y Oxygen Forensic Suite. La capacidad de algunas de estas herramientas para adquirir datos borrados demuestra un progreso significativo en el desarrollo de procedimientos forenses eficaces y de calidad. El software que se utilizó en la investigación fue el siguente: MOBILedit, Access Data FTK Imager, Oxygen, EnCase y los dispositivos utilizados fueron: Samsung Galaxy GT-S5300 y HTC Desire 300 [3].

2.2 FUNDAMENTACIÓN TEÓRICA

2.2.1 Informática Forense

Historia de la Informática Forense


1978
•Se reconocen los crímenes informaticos
1981
•Nace Copy II PC de Central Point Software.
•Copia exacta de disquetes protegidos para evitar copias piratas.
1982
•Peter Norton publica Norton Utilities 1.0
•Recuperaba archivos borrados accidentalmente
1984
•FBI forma Magnetic Media Program
•En 1991 Computer Analysis and Respose Team
1986
•Clifford Stoll colabora en la detección del hacker Markus Hess
1987
•Se crea la High Tech Crime Investigation Association
•Agrupa a profesionales gubernamentales y privados
•Nace la compañía Access Data
•Productos orientados a la recuperación de contraseñas
1988
•Se crea la Intenational Association of Computer Investigative Specialists
•certifica empleados gubernamentales
•Se desarrolla el programa Seized Computer Evidence recovery Specialists
•Formar profesionales en Computación Forense
1992
•Se acuña el terminp Computer Forensics
•Otros ibros desarrollan la metodología
1995
•Se funda el International Organization on Computer Evidence
•Encuentro entre especialistas en la evidencia electrónica
1996
•La Interpol organiza los International Forensic Science Symposium
2001
•Nace la Digital Forensic Research Workshop
•Grupo de debate y discución internacional.

[9].

Análisis de la Informática Forense

El análisis forense es un área perteneciente al ámbito de la seguridad informática surgida a raíz del incremento de los diferentes incidentes de seguridad. En el análisis forense se realiza un análisis posterior de los incidentes de seguridad, mediante el cual se trata de reconstruir como se ha penetrado o vulnerado en el sistema. Por tanto, cuando se está realizando un análisis forense se intenta responder a las siguientes preguntas:

- ¿Quién ha realizado el ataque?
- ¿Cómo se realizó?
- ¿Qué vulnerabilidades se han explotado?
- ¿Qué hizo el intruso una vez que accedió al sistema?

El área de la ciencia forense es la que más ha evolucionado dentro de la seguridad, ya que los incidentes de seguridad han incrementado en los últimos años. Además, los ataques son diferentes y por tanto hay que actualizar las técnicas de análisis en cada momento [10].

Fases de la Investigación Forense

Fase de Identificación

La fase de identificación se refiere a la recopilación de información necesaria para trabajar sobre la fuente de datos presentada por el administrador de los servidores:
¿Qué información se necesita?
¿Cómo aprovechar la información presentada?
¿En qué orden ubico la información?
¿Acciones necesarias a seguir para el análisis forense?

- **Etapa 1:** Levantamiento de información inicial para el Análisis Forense

  La solicitud forense es un documento donde el administrador del dispositivo electrónico afectado notifica de la ejecución de un incidente y para ello solicita al equipo de seguridad la revisión del mismo, donde incluye toda la información necesaria para dar inicio al proceso de análisis.

  - La información incluida en el documento debe ser la siguiente:
  - Descripción del delito informático
  - Información general
  - Información sobre el dispositivo electrónico afectado

- **Etapa 2:** Asegurar la escena

  Para asegurar que tanto los procesos como las herramientas a utilizar sean las más idóneas se debe contar con un personal idóneo a quien se le pueda asignar la conducción del proceso forense, para ello el equipo de seguridad debe estar capacitado y entender a fondo la metodología.

- **Etapa 3:** Identificar las evidencias

  El siguiente paso y muy importante es la identificación de la evidencia presentada en nuestra escena del "crimen", la misma que estará sujeta a todos los procesos necesarios para la presentación de resultados finales, la evidencia se clasifica según:
    - Tipo de dispositivo
    - Modo de almacenamiento

Fase de Validación y preservación

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las "huellas del crimen", se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso:

- **Etapa 1:** Copias de la evidencia.

  Como primer paso se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "Copia A", "Copia B" para distinguirlas claramente del original.

- **Etapa 2**: Cadena de custodia

  Otro aspecto muy importante es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento.

Fase de Análisis

El Análisis Forense cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron. En el proceso d análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

- **Etapa 1:** Preparación para el análisis

  Se puede utilizar software como VMware5, que permitirá crear una plataforma de trabajo con varias máquinas virtuales. También se puede

utilizar una versión LIVE de sistemas operativos como Caine6, que permitirá interactuar con las imágenes de disco montadas, pero sin modificarlas. Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

- **Etapa 2:** Reconstrucción del ataque

  Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

  ● Crear una línea temporal o timeline de sucesos.

  ● Ordenar los archivos por sus fechas, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, fechas muy distintas a las de los ficheros más antiguos.

- **Etapa 3:** Determinación del ataque

  Una vez obtenida la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha.

  Estos datos, al igual que en el caso anterior, se deberán obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios.

- **Etapa 4:** Identificación del atacante

  Si ya se logró averiguar cómo entraron en el sistema, es hora de saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

  Pero si se decide perseguir a los atacantes, se deberá:

  ● Primero intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha.

● Al tener una IP sospechosa, comprobarla en el registro Ripe Ncc (www.ripe.net) o la Icann a quién pertenece. Pero, no sacar conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de spoofing.

● Utilizar técnicas de hacking ético, para identificar al atacante, por si el atacante dejó en el equipo afectado una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas.

- **Etapa 5:** Perfil del atacante

  Otro aspecto muy importante es el perfil de los atacantes y sin entrar en muchos detalles se podrá encontrar los siguientes tipos:

  ● **Hackers:** Son los más populares y se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataques suelen tener motivaciones de tipo ideológico (pacifistas, ecologistas, antiglobalización, anti Microsoft entre otros.)

  ● **SciptKiddies:** Son una nueva especie de delincuentes informáticos. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y ver que pasa.

  ● **Profesionales:** Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Suelen realizar los ataques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo.

- **Etapa 6:** Evaluación del impacto causado al sistema
  Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:
    - Ataques pasivos: En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.
    - Ataques activos: En los que se altera y en ocasiones seriamente tanto la información como la capacidad de operación del sistema.

Fase de Documentación y Presentación de las pruebas

Es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finaliza el proceso de análisis forense, esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente.

- **Etapa 1**: Utilización de formularios de registro del incidente

  El empleo de formularios puede ayudarle bastante en este propósito, estos deberán ser rellenados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que debería preparar serán:

  - Documento de custodia de la evidencia
  - Formulario de identificación de equipos y componentes

  Formulario de incidencias tipificadas

  - Formulario de publicación del incidente
  - Formulario de recogida de evidencias
  - Formulario de discos duros.

- **Etapa 2**: Informe Técnico

  Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense.

- **Etapa 3:** Informe Ejecutivo

  Este informe consiste en un resumen del análisis efectuado, pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración e incluso algunos directivos [11].

2.2.2 Evidencia Digital

La Evidencia Digital es conceptualmente lo mismo que otra evidencia – es información aprovechada en un intento de colocar a personas y eventos dentro del tiempo y el espacio para establecer la causalidad de incidentes criminales.

Sin embargo, la evidencia digital tiene un gran alcance, puede ser más sensitiva personalmente, móvil, y requerir diferente tratamiento y herramientas comparada con la evidencia física [5].

La Evidencia Digital es “información y datos de valor en una investigación que son almacenados, recibidos y transmitidos en un dispositivo electrónico” (National Institute of Justice, 2008) [13].

Dicha evidencia ha existido por décadas en formas limitadas, como ordenadores centrales y sistemas telefónicos, la importancia del procesamiento de evidencia digital se ha incrementado con la rápida proliferación de dispositivos electrónicos personales. El siglo XXI ha sido particularmente definido por los avances en reproductores de música portables, teléfonos celulares y dispositivos de computación. La Suprema Corte de Estados Unidos recientemente notifico que

los teléfonos celulares no son simplemente dispositivos de comunicación sino microordenadores que pueden servir como ordenadores; el elemento que caracteriza la moderna tecnología resulta en tres centrales características para entender como la evidencia digital difiere de las tradicionales evidencias y registros físicos: (1) La Evidencia Digital tiene un gran alcance, (2) Distribuye físicamente y personalmente la información sensible, y (3) aprovecha las cuestiones interrelacionadas de la justicia penal que va más allá del típico papel de la policía en la recopilación de pruebas [12].

2.2.3 Recolección de Evidencia Digital

Llevar un orden de recopilación de información, si la recolección de datos se realiza correctamente y de una manera ordenada, es mucho más útil en la detención del atacante y, como tal, tiene una posibilidad mucho mayor de ser admisible en un proceso judicial. El orden de recopilación debe llevarse a cabo siguiendo los siguientes pasos básicos según [15]:

- Buscar la evidencia.
- Determinar la relevancia de los datos.
- Determinar la volatilidad de la información.
- Eliminar la interferencia exterior.
- Recoger la evidencia.
- Documentar todas las acciones realizadas.

Orientaciones para Recolección de Evidencias
El procedimiento para la recolección de evidencia varía de país a país, sin embargo, existen unas guías básicas que pueden ayudar a cualquier investigador forense.
El aspecto más importante a la hora de recolectar evidencia, es la preservación de la integridad de ésta; en el caso particular de la información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha labor sea particularmente difícil [13].

Cantidad de Información recolectada.
La primera gran decisión que se debe tomar a la hora de recolectar evidencias, es la cantidad. Un investigador podría estar tentado a llevarse todo el equipo computacional que encuentre en la escena, con el fin de no arriesgarse a dejar piezas de información potencialmente importantes. Sin embargo, esta alternativa tiene sus inconvenientes, ya que el investigador podría terminar siendo demandado por dañar o alterar el sistema informático, desde este punto de vista, quizás lo indicado sería incautar sólo lo mínimo necesario para efectuar una investigación [13].

Cuidados al Hardware.
El hardware es uno de los elementos que se debe tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser usado como instrumento, como objetivo del crimen, o como producto del crimen. Generalmente, es necesario recolectar elementos de almacenamiento cd, dvd, cintas magnéticas, diskettes, memorias flash que puedan contener evidencia. En este punto se debe tomar otra decisión crítica: ¿los equipos involucrados en una investigación deben ser apagados o deben permanecer prendidos?, muchas agencias de investigación

recomiendan apagar los equipos en todas las situaciones y algunos expertos insisten en que es la mejor alternativa debido a la posibilidad de que la evidencia sea destruida mientras el ordenador permanece encendido [12].

Volatilidad de la evidencia

Con el fin de resolver un delito informático o violación a los sistemas con eficacia, es necesario examinar el sistema más como un detective que como un usuario de ordenador, en este sentido se debe examinar cada elemento con cuidado ya que pueden presentar información que nunca se pueda recuperar si se ha hecho alguna manipulación sobre los elementos.

La evidencia desaparece con el tiempo, ya sea como resultado de la actividad normal del sistema o como resultado de los actos de los usuarios.

Cada paso podrá destruir la información, por lo que todas las medidas que tome deben ser bien aplicadas la primera vez o se puede perder mucha información valiosa.

Es importante que no se busque información en áreas que normalmente no tienen razón alguna para ser accedida (como archivos personales) a menos que se haya notificado al usuario (por ejemplo, a través de un banner de inicio de sesión) que toda la información almacenada en el equipo es objeto de embargo o si se tiene razones suficientes para creer que un incidente de seguridad está ocurriendo o ha ocurrido.

En general, la evidencia informática debe ser:

- Admisible
- Auténtica
- Completa
- Confiable
- Creíble y comprensible

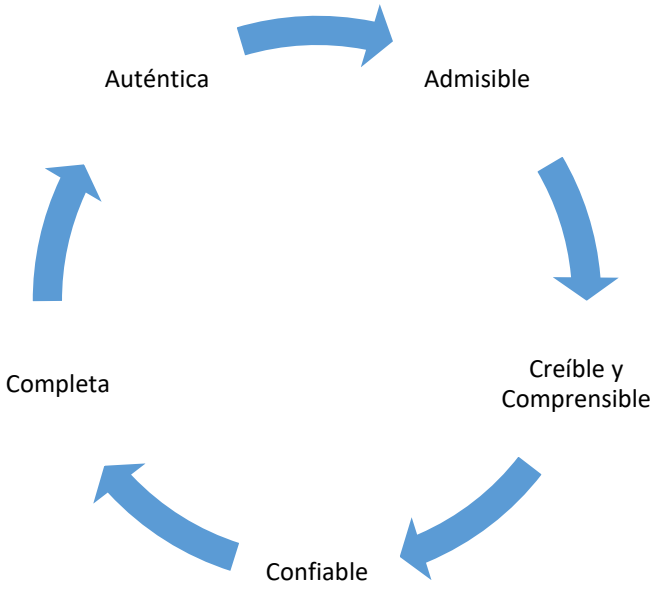


Figura 2. 1 Características de la evidencia

La evidencia volátil es evidencia la que rápidamente puede desaparecer o es sólo de carácter temporal, este tipo de pruebas tiene que ser recogida antes de que la máquina sea desconectada de la red y sea apagada, recuerde tomar las siguientes precauciones según [16]:

- No apague el sistema hasta que haya completado todos los procedimientos de recolección de pruebas para pruebas volátiles. Muchas pruebas se pueden perder cuando un sistema está apagado y el atacante puede haber alterado la puesta en marcha, apagado y servicios para destruir la evidencia.
- No confiar en los programas activos en el sistema.
- Ejecutar los programas de obtención de pruebas (software forense) en los medios de comunicación debidamente protegidos.
- No ejecute programas que modifican el tiempo de acceso de todos los archivos en el sistema.

Análisis de la Evidencia Recolectada

Recolección

La recolección de evidencia informática es un aspecto frágil de la informática forense porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- Se debe proteger los equipos del daño.
- Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).
- Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

Análisis

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque y qué daños causaron. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

Preparación para el análisis

Antes de comenzar el análisis de las evidencias se deberá:

- Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.
- Trabajar con las imágenes de disco que se recopiló como evidencias o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.
- Si dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.
- Instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En este mismo ordenador y sobre un segundo disco duro, instalar las imágenes manteniendo

la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado.

- En otro equipo instalar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y ficheros en sus discos duros., la idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme se vayan surgiendo hipótesis sobre el ataque.

Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos según [13]:

- Crear una línea temporal o timeline de sucesos.
- Ordenar los archivos por sus fechas.
- Comenzar a examinar con más detalle los ficheros logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una correlación temporal entre eventos.
- Examinar los fragmentos del archivo donde se detectan y registran los accesos FTP.

2.2.4 Aplicación de la Informática Forense en Ecuador

La investigación científica de una escena del crimen es un proceso formal, donde el llamado investigador hace referencia a la participación de diferentes personas, que documentan y adquieren evidencias, usando su conocimiento, técnicas, herramientas y generando indicios suficientes para ayudar a resolver el caso. Es por tanto necesario dejar en claro cuál es la participación que tienen estas personas dentro de una escena del crimen o del hecho.

a) Personal de Primera Respuesta
b) Examinadores de Evidencia Digital
c) Investigadores del Delito
d) Peritos

En conclusión, el personal involucrado debe tener precaución al tratar con la intimidad y privacidad de los sospechosos; también hay que tener presente que todas las personas que intervienen podrán tener un grado de responsabilidad durante la realización de su trabajo.

Para dar validez a la evidencia digital la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas estipula en su Art.1,

> Regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

En base a esta ley se puede interpretar a la información digital como mensajes de datos, ya que los define como:

> Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que

> puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes; documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

A la vez, esta información digital o mensajes de datos, constituyen evidencia digital cuando tal información tiene un valor probatorio, y por lo tanto son de interés para el proceso judicial.

De igual manera esta ley tipifica los siguientes principios generales relativos a los mensajes de datos: Art. 2, Reconocimiento Jurídico de los Mensajes de Datos,

> Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Art. 4, Propiedad Intelectual,

> Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Por esta razón en la Ley de Propiedad intelectual Art. 26, se escribe,

> También constituyen violación de los derechos establecidos en este libro cualquiera de los siguientes actos: a) Remover o alterar, sin la autorización correspondiente, información electrónica sobre el régimen de derechos.

En este punto, cabe mencionar que, para no incurrir en una violación a la ley, se debe contar con las autorizaciones judiciales respectivas. Para utilizar mensajes de datos como evidencia en un proceso judicial, se debe considerar lo expuesto en el Art. 52 de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas. Art.52 Medios de Prueba

> Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Se puede observar en este artículo que la ley tiene un enfoque hacia el Comercio Electrónico, mas no hacia evidencias digitales; por lo tanto, se recomienda que no solo se observe lo dispuesto en el Código de Procedimiento Civil, que trata de los deberes y derechos de los ciudadanos, sino también que se revise el Código de Procedimiento Penal, que es el encargado de tratar actos delictivos. De esta manera se podría afirmar que la evidencia digital es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella; es cualquier mensaje de datos almacenado y transmitido por medios electrónicos que tengan relación con el cometimiento de una acto que comprometa a los presuntos responsables y que guie a los investigadores en el descubrimiento de posibles infractores [4].

2.2.5 Análisis Forense de smartphones

El análisis forense de smartphones es parte de la práctica forense digital que ayuda a recuperar datos relacionados como evidencia. Con la evolución y necesidades de los usuarios este análisis forense se ha extendido a Tablet y GPS. La necesidad de esta práctica surgió del avance y uso de los teléfonos inteligentes, así como de sus tareas las cuales van desde el almacenamiento de información en memoria

interna como en la nube y también el acceso a Internet, lo que provocó que las técnicas que existían no satisfagan por completo las necesidades [16].

2.2.6 Comparación de software forense

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.

Tabla 2. 1 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	✓	✓		✓			✓		

Elaborado por: *Erika Guerra*

Oxygen Forensic, MOBILedit y Device Seizure son el software más reconocido en varios artículos de sitios web y libros ya que son los que más funcionalidades presentan al investigador, el software para la recolección de evidencia en su gran mayoría es de licenciado, pero los proveedores del software escogido disponen de versiones para evaluación de software.

Oxygen Forensic
Es considerado una de las más populares por ser una de las más completas en recuperación forense es desarrollado por Oxygen Software fundada en el año 2000 es especializada en el desarrollo de software para exámenes forenses avanzados para dispositivos móviles inteligentes.

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 diversos 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.

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 backend 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 [7].

2.3 PROPUESTA DE SOLUCIÓN

El presente trabajo propone beneficiar a los investigadores de la fiscalía, pudiendo ser escalable para otras entidades de seguridad, con un estudio de software para la recolección de evidencia en smartphones, que determine cual software es el que mejor maneja la evidencia digital.

CAPÍTULO III

METODOLOGÍA

3.1 MODALIDAD DE LA INVESTIGACIÓN

La presente investigación se enmarcará dentro de una investigación aplicada porque se realizará una investigación de todas las causas y factores del problema en el área de Investigación Forense de dispositivos móviles Android de la ciudad de Ambato donde se pretenderá solucionar los problemas con el uso de software.

3.1.1 Investigación documental – bibliográfica

Se considera esta modalidad ya que se recurre a diferentes fuentes obtenidas de libros, artículos científicos, tesis desarrolladas en Universidades para profundizar enfoques con respecto al tema de la investigación.

3.1.2 Investigación Aplicada

Por la utilización de los conocimientos adquiridos a lo largo de la carrera universitaria.

3.2 POBLACIÓN Y MUESTRA

La presente investigación por su característica no requiere población ni muestra.

3.3 RECOLECCIÓN DE LA INFORMACIÓN

La información requerida será recogida de fuentes seguras del internet, artículos de interés y publicaciones especializadas en el área, utilizando una lectura científica.

3.4 PROCESAMIENTO Y ANÁLISIS DE DATOS

Para el procesamiento de la información se realizará las siguientes actividades:

- Recolección de la información mediante la investigación en documentos electrónicos referentes al tema.
- Revisión de la información recogida.
- Análisis de información recolectada de documentos electrónicos.
- Lectura de artículos relacionados con la investigación presentada.
- Interpretación de los resultados mediante gráficos, cuadros para analizar e interpretar y por último redactar una síntesis de los resultados.

3.5 DESARROLLO DEL PROYECTO

A continuación, se detallan las actividades que se realizarán, para cumplir los objetivos establecidos para la presente investigación.

- Analizar información relacionada con la investigación forense en smartphones en archivos y bases de datos en la fiscalía de la ciudad de Ambato.
    - Investigación de datos estadísticos de la página del Instituto Nacional de Estadísticas y Censos.
    - Investigación y recolección de información mediante documentos electrónicos de la unidad de criminalística de la ciudad de Ambato.
    - Análisis y selección de la información recolectada.
    - Interpretación de resultados mediante cuadros y gráficos.
- Estudiar la funcionalidad, aplicabilidad y eficacia del software para la investigación forense basándose en un estudio de software: Oxygen Forensics, Device Seizure y MOBILedit.
    - Lectura de documentos electrónicos referentes a características del software: Oxygen Forensics, Device Seizure y MOBILedit.
    - Selección de características del software: Oxygen Forensics, Device Seizure y MOBILedit.
    - Descripción del ambiente de pruebas: Smartphones, Software, Ambiente de ejecución.
- Elaborar un cuadro comparativo sobre la funcionalidad, aplicabilidad y eficacia basado en el estudio del software: Oxygen Forensics, Device Seizure y MOBILedit.
    - Prueba del software: Oxygen Forensics, Device Seizure y MOBILedit, en los smartphones seleccionados.
    - Análisis de los resultados de las pruebas.
    - Tabular resultados de las pruebas.
    - Interpretación de resultados mediante gráficos y tablas.

CAPÍTULO IV

DESARROLLO

4.1. DATOS SOBRE EL USO DE DISPOSITIVOS MÓVILES EN EL ECUADOR

De la información obtenida del Instituto Nacional de Estadísticas y Censos (INEC) sobre las personas que tienen un teléfono celular, se puede observar en la Figura 4.1 que 56,3% de la población de la provincia lo tienen un teléfono celular, en comparación con el año 2015 en donde el porcentaje de personas que tenían teléfonos celulares era de 55,1%. Lo cual indica que el uso del teléfono celular va aumentando con el paso del tiempo.

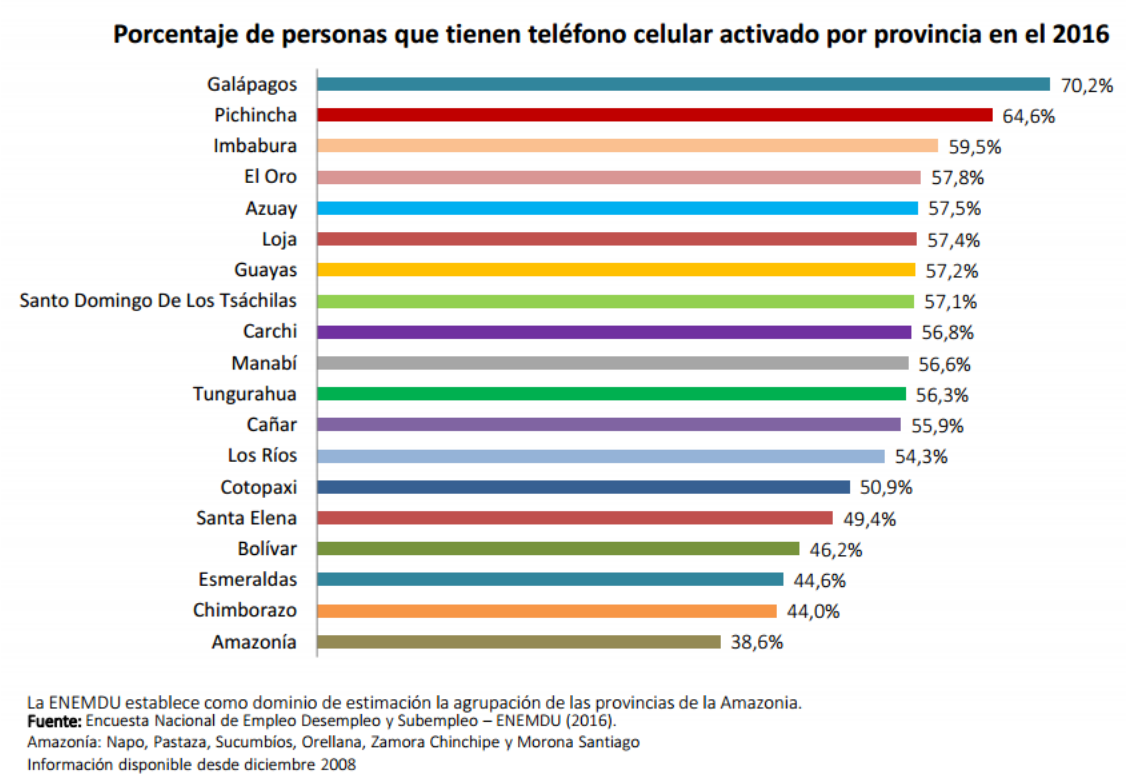
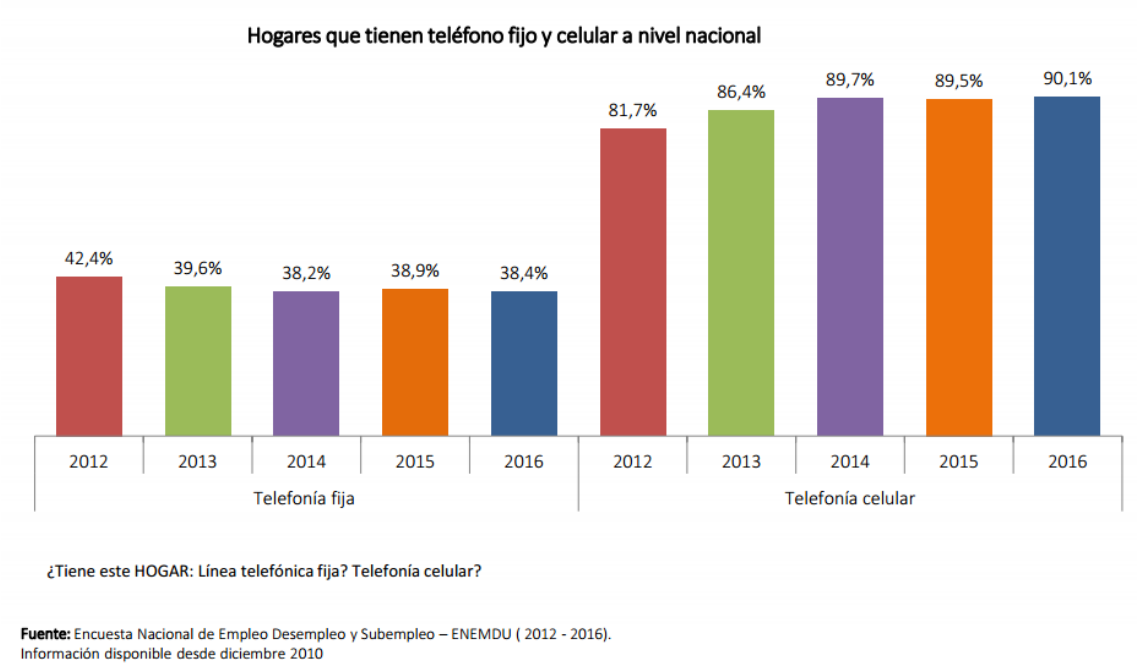


Figura 4. 1 *Porcentaje de personas que tiene un teléfono celular por provincia*

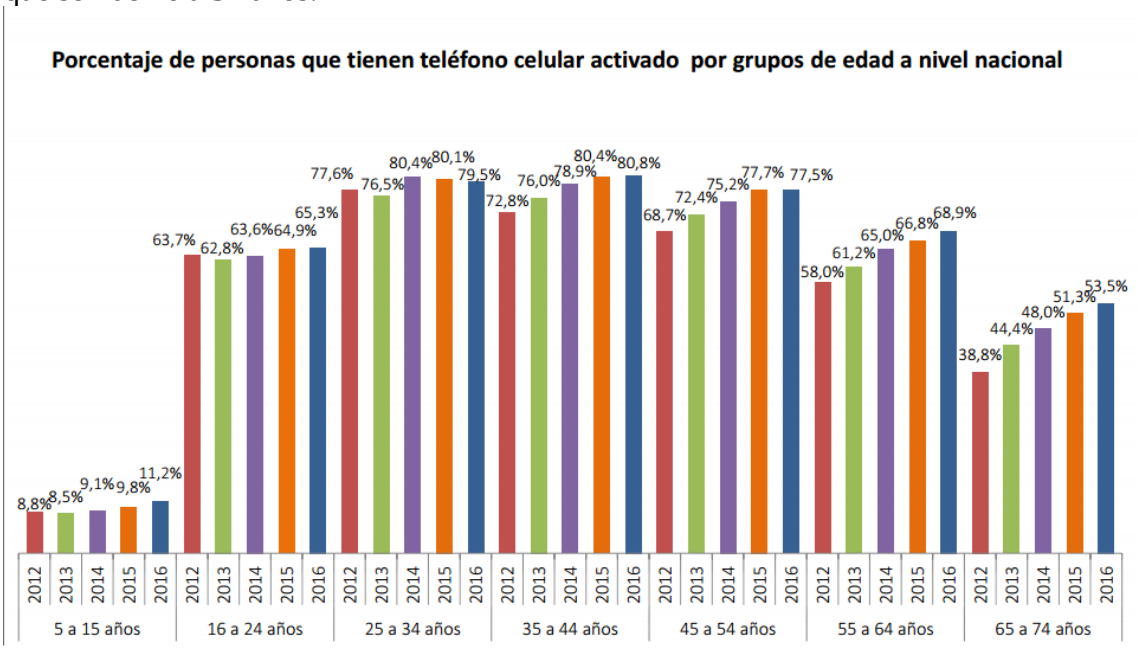
En la figura 4.2 obtenido de la página del Instituto Nacional de Estadísticas y Censos (INEC), se puede observar que hay un crecimiento de la preferencia de teléfonos celulares en los hogares**.** En el año 2015 el porcentaje de hogares en los cuales se tenían teléfonos celulares era de 89,5% y en el año 2016 es de 90,1%, lo cual demuestra la preferencia hacia los teléfonos celulares frente al teléfono fijo el cual baja en cifras cada año.



Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2012 - 2016).
Información disponible desde diciembre 2010

Figura 4. 2 *Hogares que poseen un teléfono celular*

En la figura 4.3 se puede observar que grupo de edades utilizan más los teléfonos celulares que son de 16 a 54 años.



Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2012 - 2016).
Información disponible desde diciembre 2008

Figura 4. 3 *Porcentaje de personas que tiene teléfono celular por grupos de edad*

Como se puede evidenciar en la figura 4.4 en el año 2016, del porcentaje que tiene un teléfono celular, el 52,9% tiene un Smartphone, lo cual registra un crecimiento en

comparación al año 2015 en el que se registraba un 37,7%. Estas cifras demuestran que la tendencia para adquirir Smartphones van en aumento.

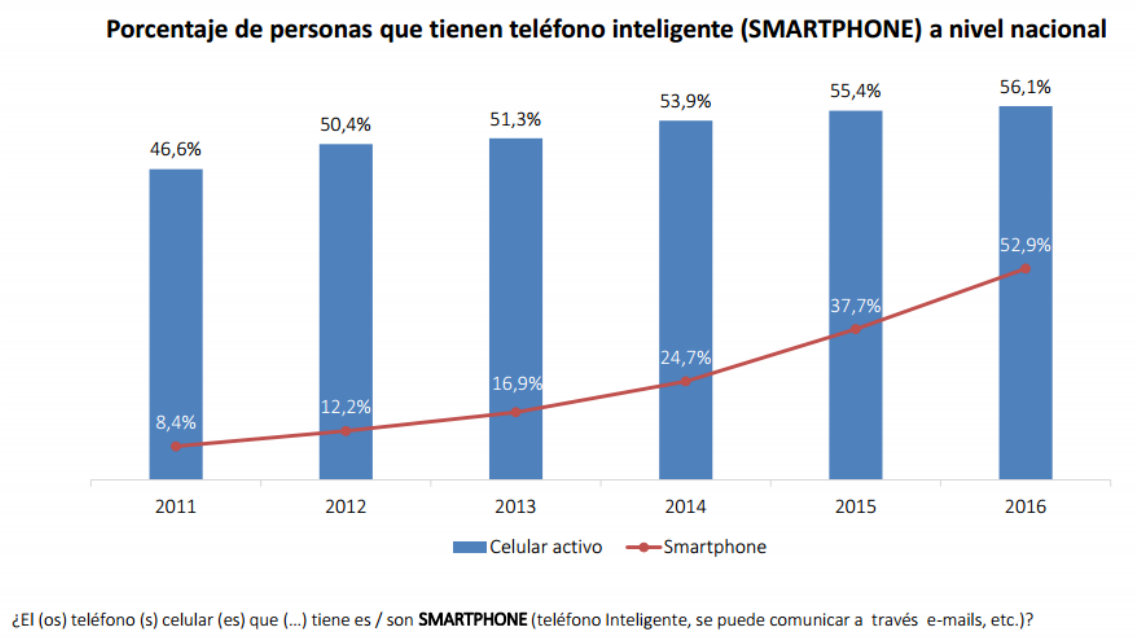


Figura 4. 4 *Porcentaje de personas que poseen un Smartphone*

En las figuras 4.1, 4.2, 4.3, 4.4 se puede observar que de la población total que existe en el Ecuador la mayoría tiene un teléfono celular y de ellos la mitad poseen un Smartphone siendo en su mayoría gente de 16 a 24 años, las cuales podrían ser víctimas de algún delito o a su vez cometer uno mediante un Smartphone.

4.2. CASOS DENUNCIADOS DE DELITO CON EVIDENCIAS EN DISPOSITIVOS MÓVILES

Según investigaciones realizadas en la página de la unidad de criminalística de la provincia de Tungurahua [17] se encontró documentación sobre casos en los que se tiene entre las evidencias teléfonos celulares los cuales podrían tener datos e información importante para una investigación.

Caso 1

Titular:	***Tres ciudadanos detenidos por presunta tenencia ilegal de droga***
Fecha	18 de abril de 2017
Lugar	Barrio La Joya

Descripción:	Entre las evidencias se encontró 14.065 gramos de marihuana lo que equivale a 28.130 dosis, la policía evitó que está cantidad sea distribuida. Se confiscó ***dos celulares***, y un vehículo. Se comentó que de las investigaciones y de los análisis de los teléfonos celulares se presume que el alcaloide iba a ser entregado a una persona que se dedica a convertirlo en tráfico de consumo interno de la provincia, al que aún no se la ha identificado.
Links:	http://www.policiaecuador.gob.ec/tres-ciudadanos-detenidos-por-presunta-tenencia-ilegal-de-droga/
	http://www.eluniverso.com/noticias/2017/04/17/nota/6141967/hallan-22-paquetes-droga-taxi-ambato

Caso 2:

Titular:	***Operativo "Libertad VI" logró el decomiso de 8.840 dosis de cocaína***
Fecha	24 de abril de 2017
Lugar	sector del Mercado Mayorista
Descripción:	se decomisó 8.840 dosis de cocaína, 40 dólares y un ***teléfono celular***. Las investigaciones continúan hasta esclarecer los hechos en base a información reservada, las evidencias se encuentran en el centro de acopio de la Unidad de Antinarcóticos. Los uniformados también decomisaron un celular con el que se conjetura ella se comunicaba con los clientes para la entrega del alcaloide.
Link:	http://www.policiaecuador.gob.ec/operativo-libertad-vi-logro-el-decomiso-de-8-840-dosis-de-cocaina/
	http://lahora.com.ec/index.php/noticias/show/1102052387/-1/Cae_la_%E2%80%98dura%E2%80%99_de_la__droga_en_Ambato.html#.WR3rdGg1-00

Figura 4. 5 *Caso Libertad VI*

Caso 3:

Titular:	***Operativos Antinarcóticos impiden comercio de 407 981,87 dosis de droga***
Fecha	23 de Septiembre de 2014
Lugar	Av. Bolivariana y calle Hipócrates
Descripción:	Dos individuos se hicieron pasar como trabajadores de una empresa de cable, y de esta forma amedrentaron a la cajera sustrayéndose dinero en efectivo. Este hecho fue comunicado a la Policía. Miembros del Grupo Operativo Motorizado, durante el operativo de control, localizaron el vehículo Chevrolet Aveo, color plomo, de placas HBB-8957, en el que se habían dado a la fuga. Cuando fueron interceptados, los ocupantes salieron en precipitada carrera, sin embargo, dos de ellos fueron interceptados y responde a los nombres: Miguel S. A. y Raúl S. A. Luego de este hecho se realizó un operativo donde fue aprehendidos, a la altura del sector La Joya, el ciudadano Kelvin P. B., quien tenía en su poder la cantidad de 2 755,90 dólares. En esta acción se decomisaron las siguientes evidencias: -1 punzón de metal -1 alicate -1 cinta de embalaje -1 cámara fotográfica ***-2 celulares*** -10 prendas de vestir y documentos personales.
Link:	http://www.policiaecuador.gob.ec/operativos-antinarcoticos-impiden-comercio-de-407-98187-dosis-de-droga-2/

Caso 4:

Titular:	***Desarticulada presunta banda que intentaba asaltar un local***
Fecha	4 de Junio de 2014
Lugar	calles Bolívar entre Mariano Eguez y Darquea
Descripción:	En Tungurahua, la Policía Nacional desarticula una peligrosa banda presuntamente vinculada con el intento de asalto y robo a un local comercial. Las indagaciones permitieron realizar una inspección en un domicilio deshabitado y contiguo al local comercial donde fueron capturados también los ciudadanos: M. A. Rubén Dario (23 detenciones por diferentes causas), F. M. Heriberto Neptalí (4 detenciones por diferentes causas) y G. CH. Mauricio Roberto (6 detenciones por diferentes causas), quienes se habían encontrado realizando un oramen en la pared que da al local comercial; aquí los efectivos encontraron: una prensa hidráulica con 6 accesorios y su estuche, 2 linternas, 1 mascarilla, 1 barra de acero, 1 pata de cabra, 1 maleta con varios costales en su interior, 1 espátula, 1 destornillador grande, 1 alicate, 1 hoja de sierra, 2 pasamontañas, 1 par de guantes de lana, 1 punta de acero, 1 pasamontañas verde, 1 spray y ***2 celulares***.
Link:	http://www.policiaecuador.gob.ec/desarticulada-presunta-banda-que-intentaba-asaltar-un-local/

Según los casos 1,2,3 y 4 se observa que dentro de la provincia de Tungurahua existen delitos en los cuales como parte de toda la evidencia recolectada se encontró teléfonos celulares los cuales pueden contener información importante y determinante para la sentencia de estos delitos.

4.3. ASPECTOS PARA EL ANÁLISIS DEL SOFTWARE

El software para la recolección de evidencia debe cumplir con características que son importantes para la evidencia dentro de un caso judicial, estos son:

- Información Básica del Smartphone (Nombre del fabricante, IMEI, operador, modelo, tiempo del teléfono, presencia de tarjeta SIM, entre otros).
- Datos Almacenados en el Smartphone (registro de llamadas, mensajes, archivos multimedia, archivos de usuario, datos de aplicaciones).
- Tiempo de extracción
- Creación de reportes
- Soporte para Smartphones de distintas marcas y modelos.

4.4. ANÁLISIS DEL SOFTWARE

Existen una gran variedad de software (tabla 2.1) que permite recuperar evidencia digital. El uso de este software sofisticado se hace necesario por las siguientes razones según [14]:

1. La gran cantidad de datos que pueden estar almacenados en un ordenador.

2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
4. Limitaciones de tiempo para analizar toda la información.
5. Facilidad para borrar archivos de ordenadores.
6. Mecanismos de encriptación, o de contraseñas.

El software forense está destinado a facilitar el trabajo de los examinadores, lo que les permite realizar su trabajo de manera oportuna y estructurada mejorando así la calidad de los resultados. Las herramientas de software forense que se van a utilizar en su mayoría pueden dar soporte a una amplia gama de dispositivos y manejan las situaciones de investigación más comunes con requisitos de nivel de habilidad modestos. Estas herramientas normalmente realizan adquisiciones lógicas, utilizando protocolos comunes para sincronización, depuración y comunicaciones, así como las situaciones más complicadas, como la recuperación de datos eliminados, las cuales a menudo requieren herramientas y conocimientos altamente especializados basados en hardware, que gracias al software seleccionado permite al usuario realizar estas tareas de forma simple [15].

Existen discrepancias entre los forenses de dispositivos móviles y los forenses informáticos clásicos debido a varios factores, entre los que se incluyen los siguientes, que limitan la forma en que funcionan estas herramientas según [16]:

• La orientación hacia la movilidad (por ejemplo, tamaño compacto y alimentación por batería, que requiere interfaces, medios y hardware especializados)

• El sistema de archivos que reside en la memoria volátil frente a la memoria no volátil en ciertos sistemas.

• Comportamiento de hibernación, suspendiendo procesos cuando está apagado o inactivo.

• La diversa variedad de sistemas operativos embebidos utilizados

• Ciclos cortos de productos para nuevos dispositivos portátiles

4.4.1 Oxygen Forensic

Figura 4. 6 *Oxygen Forensic Software*

Es un software destinado para la investigación forense en extracción y análisis de datos de teléfonos celulares, teléfonos inteligentes y tabletas. Soporta alrededor de 8400 modelos y está orientado a smartphones con particular énfasis en el análisis de los datos recuperados.
Existen varios tipos de licencias para el uso de este software: licencia en línea, dispositivo USB, y una versión empresarial; en el cual un dispositivo USB es instalado en un servidor y permite que varios ordenadores usen el software al mismo tiempo [17].

Características según [17]:

- Soporte para: Android, BlackBerry, Windows Phone, Symbian y otros 12 dispositivos.
- Extracción de datos lógica (mediante Bluetooth) y física (mediante cable USB)
- Varios dispositivos conectados al mismo tiempo
- Interfaz fácil de usar
- Gráfico Social que revela todas las conexiones sociales entre dispositivos
- Analiza datos de más de 350 aplicaciones
- Recupera datos borrados de las bases de datos de SQLite
- Recuperación de contraseñas para acceder a servicios (redes sociales, bandejas de correo, etc.)
- Búsqueda exhaustiva para revelar números de teléfono, números de tarjetas de créditos
- Recuperación de contraseñas para archivos y backup encriptados
- Importación y análisis de datos desde cuentas de Google, Apple (Cloud Forensics)
- Omite el código de bloqueo para obtener información de dispositivos IOS.

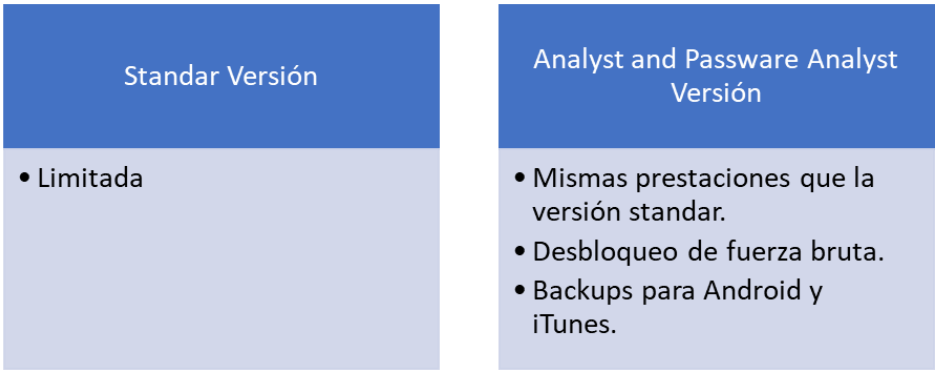


Figura 4. 7 *Versiones del Software Oxygen Forensics*

4.4.2 Device Seizure

Figura 4. 8 *Paraben Device Seizure*

Device Seizure es una herramienta de adquisición y análisis para examinar teléfonos celulares, PDA's y dispositivos GPS. Incluye software y hardware. Device Seizure puede extraer datos desde el 100% de los dispositivos móviles actuales. Usa un plugin de arquitectura de sistema expandible para tipos específicos de dispositivos y datos [18].

Características según [19] y [20]:

- Moderna interfaz
- Acceso a la nube: descarga datos directamente de las cuentas del sospechoso.
- Rechazo de contraseña: extrae contraseñas de usuario de más de 2500 dispositivos incluido iPhone (extracción física), Android (contraseñas de pantalla).
- Herramienta de soporte para IP-box y fuerza bruta.
- Detección de Malware: Analiza los permisos para aplicaciones sospechosas.
- Comparación de Casos: Permite comparar dos adquisiciones del mismo dispositivo.
- Análisis y clonación de SIM: recuperación de datos borrados de la tarjeta SIM.
- Extracciones físicas y lógicas.
- Flexibilidad: puede correr en cualquier plataforma.
- Auto-detección: Solo basta con conectar el dispositivo y la extracción comienza sin necesidad de adquirir controladores.
- Soporte para BlackBerry: traducción de respaldo de BlackBerry 10, lista de aplicaciones, traducción de datos de aplicación.
- Soporte para memoria SD: Soporta adquisición y análisis de formatos FAT y NTFS.
- Importación de registro de torre celular: Importa hoja de cálculo para ayudarle a detectar las ubicaciones en Google Maps.
- Reportes Comprensivos: Reporte Investigativo HTML, Reporte de texto simple, Reporte Simple RTF, Reporte de Texto CSV, Reporte de Resumen de Evidencia HTML, Reporte de Resultados de Escaneo de Malware, Reporte de Cronograma de Evidencia de Dispositivos Móviles, Reporte de Evidencia de Dispositivo Móvil en PDF, Reporte de Revisión de Datos de Dispositivos Móviles.

- Incorporación de un traductor de SQLite: Permite una revisión de una variedad de datos de aplicaciones con facilidad.
- JTAG Análisis de Volcado: Analiza volcados de memoria, soporte para FAT 12, FAT 16, FAT 32, EXT 4(Dispositivos Android).
- OCR: Tiene una gran variedad de paquetes para soporte de lenguajes.

PACKAGE	INTERNET LICENSE	DIRECT MACHINE LICENSE	DONGLE LICENSE (Additional Fee)
E3:UNIVERSAL	✓	✓	✓
E3:P2C	✓	✓	✓
E3:DS	✓	✓	✓
E3:EMX	✓	✓	✓
E3:NEMX	✓	✓	✓
E3:INTERNET/CHAT	✓	✓	✓
E3:VIEWER	✓	✓	

Figura 4. 9 *Versiones y licencias de Device Seizure*

4.4.3 MOBILedit Forensic

Figura 4. 10 *MOBILedit*

MOBILedit es un software que permite a los examinadores ver, buscar o recuperar toda la información de un dispositivo móvil, también permite recuperar datos borrados evitando la clave de acceso, PIN y la copia encriptada del teléfono [21].

Características según [18]:

- Extracción completa de datos de teléfonos y SIM: Historial, libreta de contactos, mensajes de texto, mensajes multimedia, archivos, calendario, notas, recordatorios.
  Información del teléfono: IMEI, sistema operativo, firmware.
  Detalles SIM: ICCID e información de localización de área.
- Soporte para la mayoría de teléfonos: Soporte para cerca de mil teléfonos y sistemas operativos como: Android, iPhone, BlackBerry, Symbian, Windows Mobile, Windows Phone, Bada, Meego, Teléfonos chinos y teléfonos CDMA.
- Evita la clave de acceso en iOS usando el método de bloqueo de archivos: Soporta la importación del bloqueo de archivos que se puede encontrar en el dispositivo sospechoso. El software es capaz de instruir en cómo obtener los archivos. Permite recuperar todos los datos desde el teléfono incluso si está bloqueado con código de acceso.
- Evita el código PIN con una herramienta de clonación de SIM: Puede clonar, crear y formatear tarjetas SIM con ICCID para dejarlo listo para su nuevo uso. Se puede conectar múltiples lectores de tarjetas SIM al mismo tiempo.

- Examina los datos del teléfono sin necesidad de tener el teléfono: Adquiere los datos del teléfono porque iTunes por defecto crea un respaldo automático de cualquier iPhone conectado. MOBILedit provee la completa extracción de datos.
- Extracción de datos de iOS incluso si el teléfono tiene encriptación para respaldos: Permite acceder a los respaldos sin necesidad de la clave de encriptación.
- Obtiene una lista de contactos de Skype, Google, Facebook sin contraseña: Entrega un reporte completo de toda la gente conectada con el sospechoso.
- Investigación de teléfonos Android vía Wi-Fi.
- El Analizador de SIM recupera toda la información posible de tarjetas SIM.
- Permite navegar, aunque la procedencia de la conexión del teléfono sin molestia: Búsqueda sencilla de cualquier teléfono en la base de datos online.
- Vista organizada de archivos multimedia: Muestra toda la información multimedia dividida en categorías (fotos, videos, grabaciones, etc.).
- Software Controlador de detección y reparación de sistemas que provee un asistente adicional con corrección: Contiene un software especial de bajo nivel que permite la detección que repara e instala el software controlador correcto remplazando el incorrecto.

MOBILedit Forensics Express

Figura 4. 11 *MOBILedit Forensic Express*

Es una aplicación de 64 bits que extrae y analiza datos de teléfonos presentándolos en un reporte utilizando extracción lógica como física. Tiene un gran soporte que incluye a la mayoría de teléfonos, mostrando informes ajustados a las necesidades y con una interfaz muy fácil de usar. Con evasión de contraseña y PIN se puede obtener acceso al bloqueo

ADB o respaldo de iTunes con aceleración de GNU y operaciones en multihilo para una mayor velocidad. Se puede integrar con "Camera Ballistics" el cual ayuda a analizar el origen de una fotografía [18].

Se puede extraer datos en pocos pasos incluyendo datos borrados, historial de llamada, contactos, mensajes de texto, mensajes multimedia, archivos, recordatorios, notas, contraseñas de cuentas y contraseñas de Wi-fi, recordatorios y datos de aplicaciones [22].

Características según [22]:

- Extracción y Análisis Físico: Permite extraer imágenes físicas y exactos clones binarios, además permite abrir imágenes creadas en el proceso de obtención de datos, contiene herramientas para recuperar archivos borrados.
- Recuperación de Datos Borrados: Contiene algoritmos especiales que permite buscar en lo profundo de bases de datos y datos que todavía residan en la cache del teléfono.
- Permite romper contraseñas con aceleración de GPU: Las contraseñas pueden ser descifrada por un intérprete de diccionario de ataques. Utiliza una aceleración de GPU y operaciones de multihilo para una máxima velocidad. Es capaz de penetrar la protección de iOS y acceder a los datos usando el método de bloqueo.
- Analizador científico de imágenes "Camera Ballistics": Cuando se combina con "Camera Ballistics" se puede identificar las imágenes tomadas por el teléfono analizado usando un sensor de huella dactilar. Toda la información recolectada se presentará en un informe PDF bien diseñado para ser presentado como evidencia.
- Integración con otras herramientas: Importa y analiza datos desde Cellebrite UFED y Oxygen. Extrae datos de teléfonos en formato de datos abiertos para obtener los archivos directamente como están en el teléfono lo cual permite utilizar otras herramientas para seguir analizando y obtener más pruebas.
- Analizador de mensajes y cronología: Recolecta información de los mensajes borrados y no borrados mostrándola en orden cronológico. Incluye información de quien envió el mensaje, que programa se usó y archivos adjuntos.
- Filtra resultados para encontrar datos más rápido: Permite buscar entre los datos extraídos con una simple palabra lo que minimiza el tamaño del reporte. [22]

Comparación de características del software según los fabricantes

En las tablas 4.1 y 4.2 se detallan las características que cada software permite obtener según las especificaciones de sus respectivos fabricantes, así como funciones que permiten ejecutar; el software que más funcionalidades tiene es MOBILedit seguido de Device Seizure:

Tabla 4. 1 *Características del Software*

	Datos									
Software	Información de dispositivo	Contactos	Llamadas	Datos de Calendario	Mensajes de texto	Datos Multimedia	Coordenadas	Contraseñas de cuentas de usuario	Datos borrados	Datos de aplicaciones
Oxygen Forensics	X	X	x	X	x	x	X	X	x	X
MOBILedit	X	X	x	X	x	x	X	X	x	X
Device Seizure	X	X	x	X	x	x	X	X	x	X

Elaborado por: *Erika Guerra (2017)*

Tabla 4. 2 *Características del Software II*

	Datos								
Software	Datos de SIM	Datos de tarjetas de memoria	Cloud Data	RAM/ROM	Correos Electrónicos	Búsqueda de Cache	Integración con otras aplicaciones	Bases de datos PDA	Bases de Datos SQLite
Oxygen Fprensics	x		x		X				X
MOBILedit	x	X		x		X	X	X	X
Device Seizure	x	X	X		X				X

Elaborado por: *Erika Guerra (2017)*

La tabla 4.3 detalla las formas de extracción que las aplicaciones pueden utilizar para la obtención datos para evidencia en la cual se puede observar que el software "Oxygen Forensics" y "MOBILedit" permite obtener evidencia con diferentes formas de conexión.

Tabla 4. 3 *Formas de extracción*

	Cable	**Bluetooth**	**Wifi**
Oxygen Forensics	X	X	x
MOBILedit	X	X	x
Device Seizure	X		

Elaborado por: *Erika Guerra (2017)*

Después de investigar varias herramientas (tabla 2.1), se ha concluido que algunas herramientas son un medio para copiar la información de la memoria interna y 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 a fondo para obtener datos más exactos.

Para las pruebas se van a utilizar las tres herramientas descritas anteriormente ya que es el software más completo según el análisis del documento [7].

4.5. ANÁLISIS DE FUNCIONALIDAD APLICABILIDAD Y EFICACIA

4.5.1. AMBIENTE DE PRUEBAS

- **SMARTPHONES**
  Según datos de la Empresa de Manifiestos y diario El Comercio [26] el listado de marcas de teléfonos y sistemas operativos que son más usados en Ecuador son:

  Por marcas:

  - Nokia: 40% 0,58 millones
  - Samsung: 15% 0,22 millones
  - LG: 10% 0,15 millones
  - Alcatel: 10% 0,14 millones
  - RIM (Blackberry): 5% 0,08 millones
  - Huawei: 4% 0,05 millones
  - Otros: 16% 0,22 millones

  Por Sistemas Operativos:

  - Android: 62% 0,9 millones
  - Blackberry: 21% 0,30 millones
  - iOS: 10% 0,15 millones
  - Windows: 7% 0,1 millones

Tabla 4. 4 *Dispositivos para pruebas*

Marca	Modelo	OS
Sony	Xperia Z3 D6603	Android 6.0.1
Blackberry	Torch 9800	Blackberry OS 6.0
Microsoft (Nokia)	Lumia 520	Microsoft Windows Phone 8.1

Elaborado por: *Erika Guerra (2017)*

- **SOFTWARE**
  El software a utilizar para las pruebas serán los siguientes:

  - MOBILedit 8.7
  - Oxygen Forensic Suite 2014
  - Device Seizure

  Se utilizará el sistema operativo Windows 10 Pro de 64 bits ya que este cumple con las especificaciones de software necesarias para la instalación de los programas detallados anteriormente.

- **HARDWARE**
  La ejecución de las pruebas en los dispositivos mencionados en la tabla 4.4 se realizará en una Laptop Sony VAIO VPCEG30EL con las siguientes especificaciones que cumplen con las especificaciones de hardware para la instalación y funcionamiento del software para la recolección de información:

  - Memoria RAM instalada: 8 GB
  - Procesador: Intel Core i3-2350M CPU 2,30GHz
  - Disco: 305244 MB

  Para la conexión entre la ordenadora se utilizará un cable USB 2,0.

4.5.2. RESULTADOS TEST DE EVALUACIÓN POR SMARTPHONE Y APLICACIÓN

- **MOBILEDIT**
  El software MobilEdit después de la adquisición de información del dispositivo muestra varias opciones y pestañas para poder trabajar con la evidencia obtenida del dispositivo, como lo son: estado del dispositivo, información común del dispositivo, datos del dispositivo.

  Las opciones que el software despliega en pantalla dependen del dispositivo conectado, así como de la versión de su software. Como se muestra en la figura 4.11.

Figura 4. 12 *Pantalla de Exploración de MobilEdit, Dispositivo Xperia Z3*

<u>Información acerca del teléfono según figura 4.12</u>

Fabricante: Nombre de la empresa que diseño el dispositivo

Modelo: Tipo específico del dispositivo

IMEI: Código exclusivo que sirve de identificador a nivel mundial

Operador: Nombre de la empresa que provee servicios de red al usuario

Tiempo del teléfono: Muestra la fecha y hora mostrada en el dispositivo

Revisión de Hardware: Muestra el número de la versión del hardware

Revisión de Software: Muestra el número de la versión del software

Redes: Muestra las redes móviles a las que puede conectarse el dispositivo

Plataforma: Muestra el nombre del sistema operativo del dispositivo

Resolución de display

Resolución de fondo de pantalla

ICCID: Serie que identifica a la tarjeta SIM

IMSI: Serie que identifica al operador

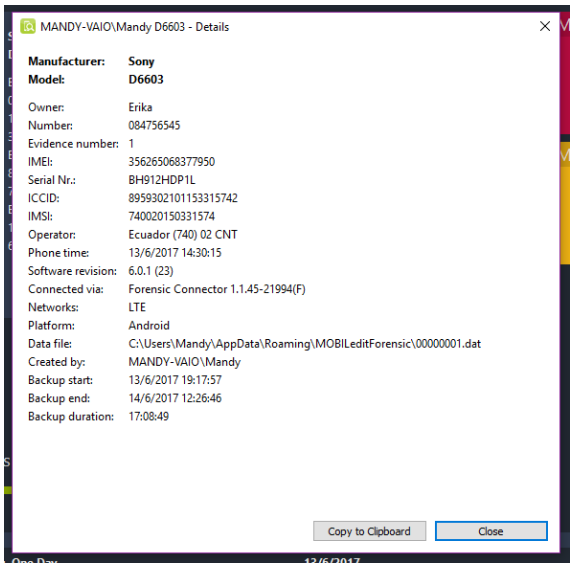


Figura 4. 13 *Información Común del Dispositivo Software MobilEdit, Dispositivo Xperia Z3*

Status del teléfono según figura 4.13

Status de Batería: Muestra el porcentaje de carga de la batería del dispositivo

Plataforma: Muestra el nombre del sistema operativo del dispositivo

Conexión: Muestra el tipo de conexión con la que se conectó el dispositivo

Figura 4. 14 Status del Dispositivo Software MobilEdit, Dispositivo Xperia Z3

Directorio Telefónico

Despliega la lista de contactos del dispositivo desde la memoria del teléfono, Google y WhatsApp como se observa en la figura 4.14 tomada de la extracción del dispositivo Sony Xperia Z3. También permite buscar contactos, filtrar, exportar, imprimir contactos y volver a cargar contactos.

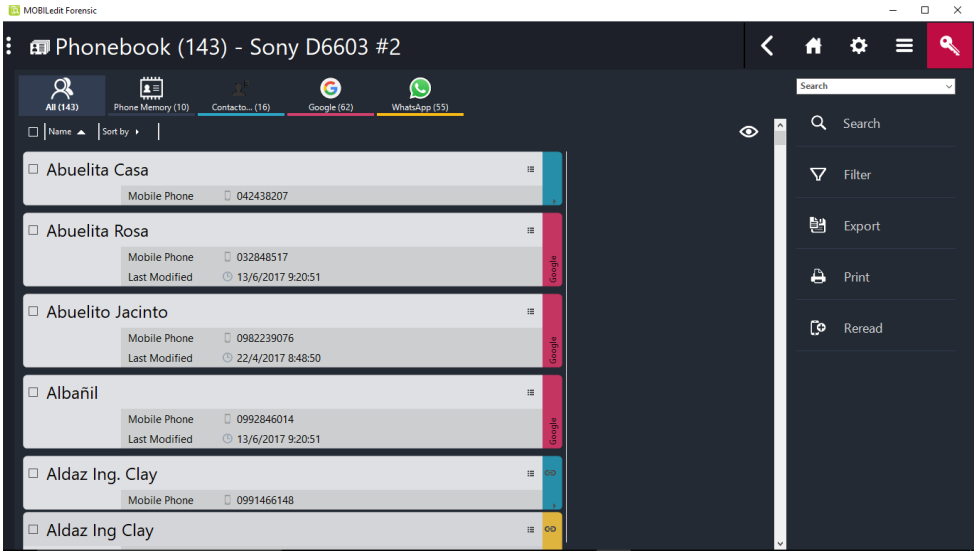


Figura 4. 15 *Directorio Telefónico Software MobilEdit, Dispositivo Xperia Z3*

Registro de Llamadas

Despliega el registro de llamadas del dispositivo permitiendo ver llamadas entrantes y salientes. También permite buscar contactos, filtrar, exportar, imprimir contactos y volver a cargar contactos tal como la muestra la figura 4.15 resultado de la prueba del dispositivo Sony Xperia Z3.

Figura 4. 16 *Registro de Llamadas Software MobilEdit, Dispositivo Xperia Z3*

Mensajes

Despliega el registro de mensajes del dispositivo como se evidencia en la figura 4.16 resultado de la prueba en el dispositivo Sony Xperia Z3, el software permitió observar los mensajes del dispositivo en distintas categorías como lo son: conversación de chat, todos, recibidos, enviados y borrador.

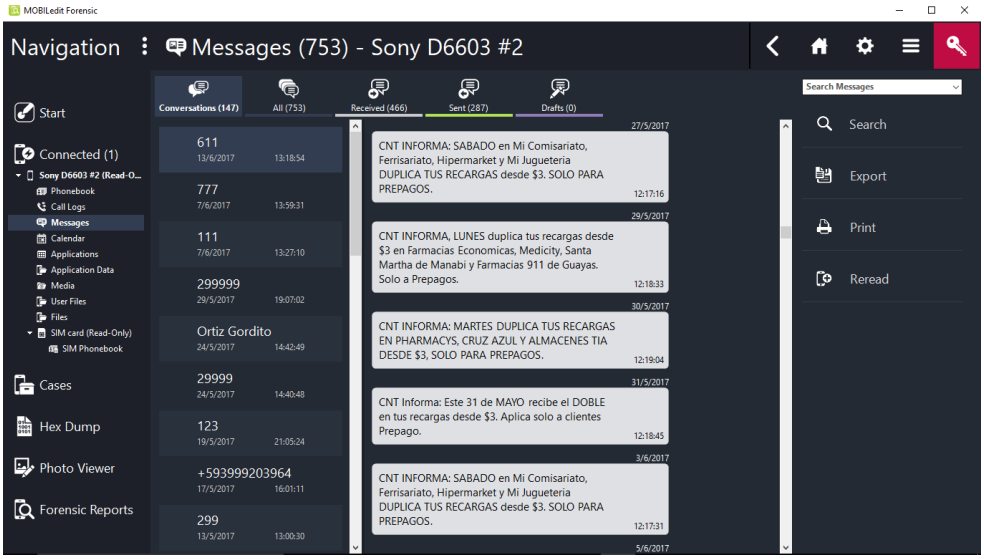


Figura 4. 17 *Mensajes Recolectados Software MobilEdit, Dispositivo Xperia Z3*

Aplicaciones

Despliega las aplicaciones instaladas en el dispositivo y permite seleccionar una aplicación y explorar su carpeta de datos. En la imagen 4.17 se observa las aplicaciones instaladas en el dispositivo Sony Xperia Z3 (Android).

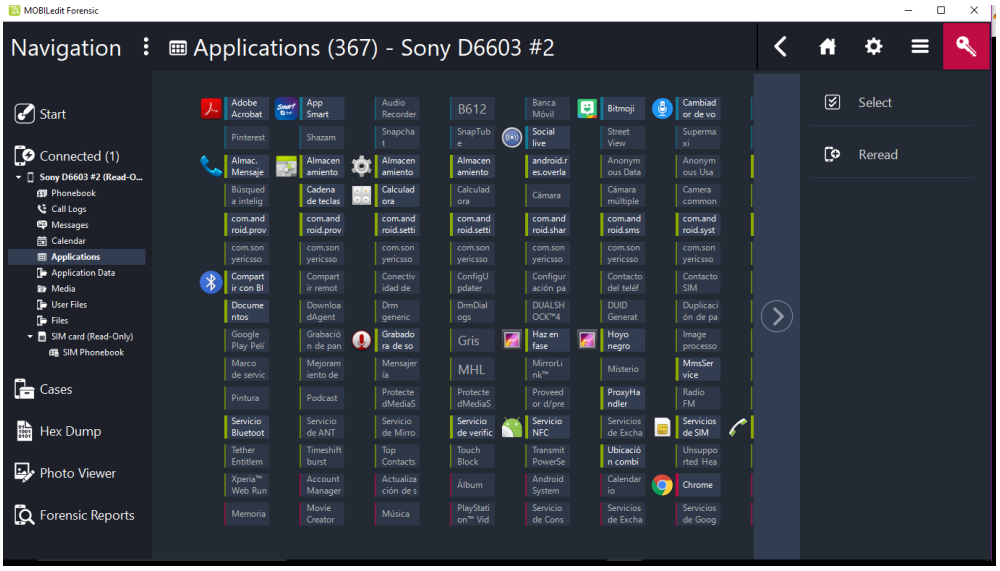


Figura 4. 18 Aplicaciones Instaladas Software MobilEdit, Dispositivo Xperia Z3

Datos de Aplicación

Permite seleccionar una carpeta y analizar los datos de aplicación del dispositivo analizado, por ejemplo, figura 4.18 resultado del análisis del dispositivo Sony Xperia Z3.

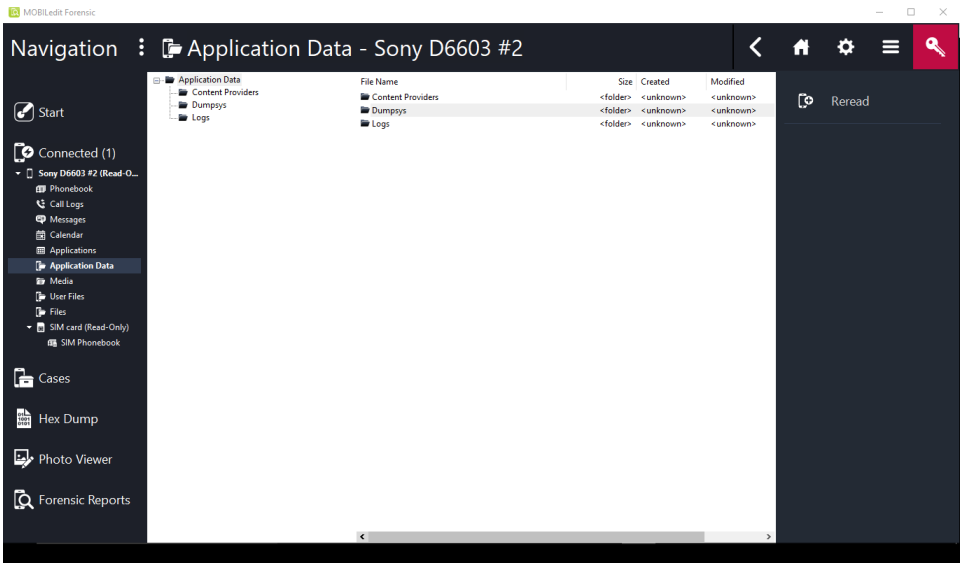


Figura 4. 19 *Datos de Aplicación Software MobilEdit, Dispositivo Xperia Z3*

Archivos de Usuario

Permite navegar por todas las carpetas que contienen datos de aplicaciones y archivos personales. En la figura 4.19 se muestran los archivos recuperados en el análisis del dispositivo Sony Xperia Z3.

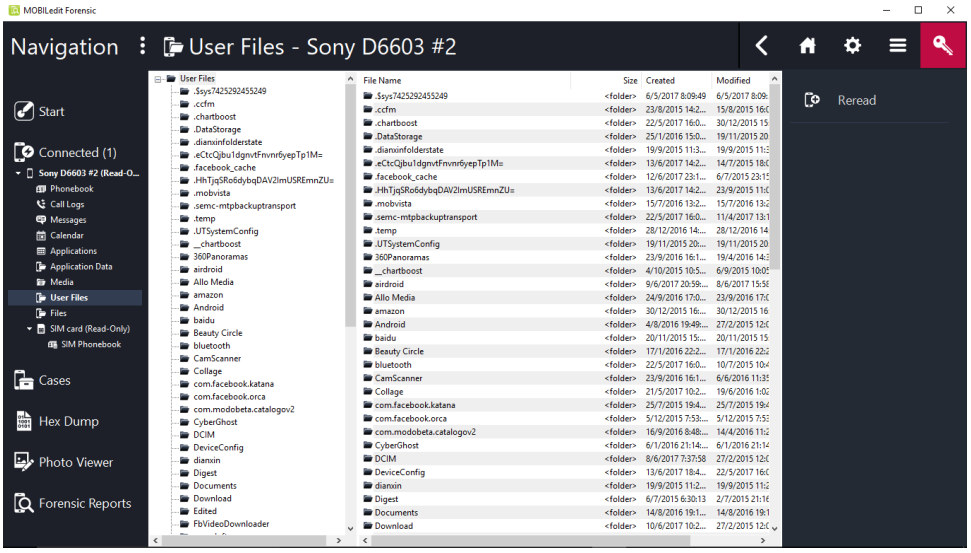


Figura 4. 20 *Archivos del Usuario Software MOBILedit, Dispositivo Xperia Z3*

Tarjeta SIM

Da una vista del directorio telefónico de la tarjeta SIM y alguna información común como: ICCID, IMSI, LAI, capacidad de contactos, capacidad de los nombres de los contactos, capacidad de mensajes como se evidencia en la figura 4.20.

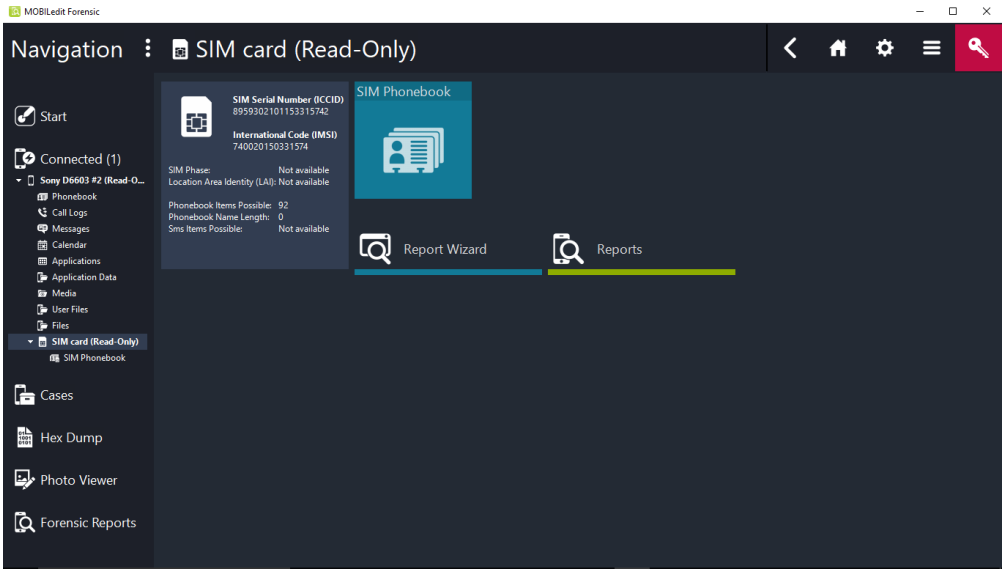


Figura 4. 21 *Información de Tarjeta SIM Software MobilEdit, Dispositivo Xperia Z3*

La figura 4.21 muestra la vista de la guía telefónica de la tarjeta SIM del dispositivo analizado en este caso es Sony Xperia Z3.

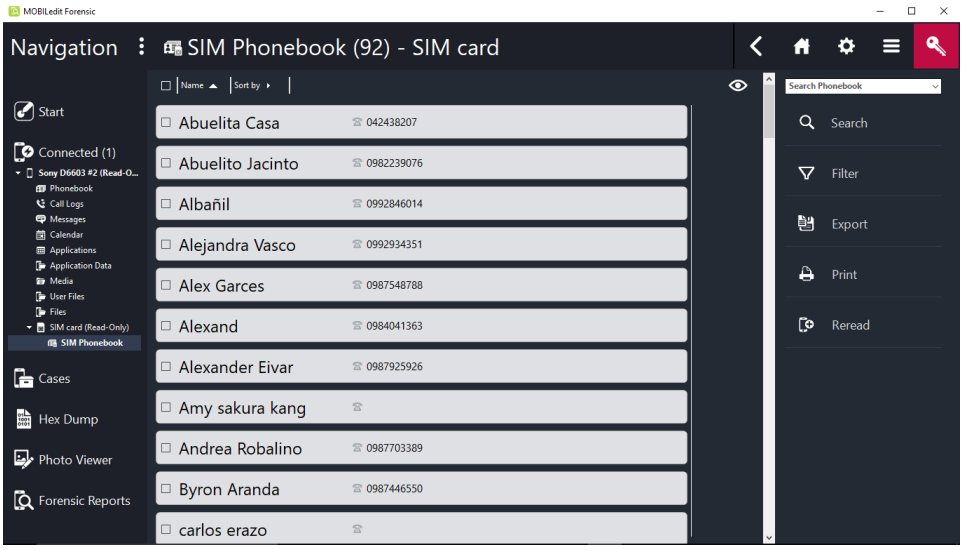


Figura 4. 22 *Libreta telefónica de tarjeta SIM Software MobilEdit, Dispositivo Xperia Z3*

Visor Hexadecimal

Permite analizar archivos de bases de datos, exportarlos, buscar y comparar como se observa en la figura 4.22.

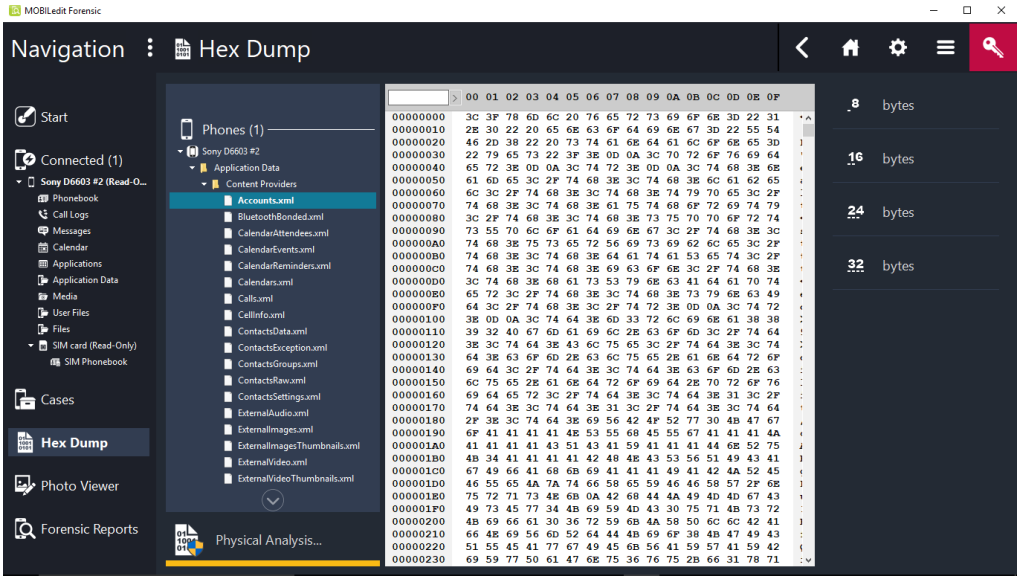


Figura 4. 23 Visor Hexadecimal Software MobilEdit, Dispositivo Xperia Z3

Reportes

En esta opción se puede exportar información seleccionada de la evidencia para poder visualizarla de una manera clara y sencilla para cualquier usuario consta de varios formatos como: XML, HTML y PDF.

La Figura 4.23 muestra la pantalla principal de la opción reportes la cual tiene diferentes opciones para la creación de reportes.

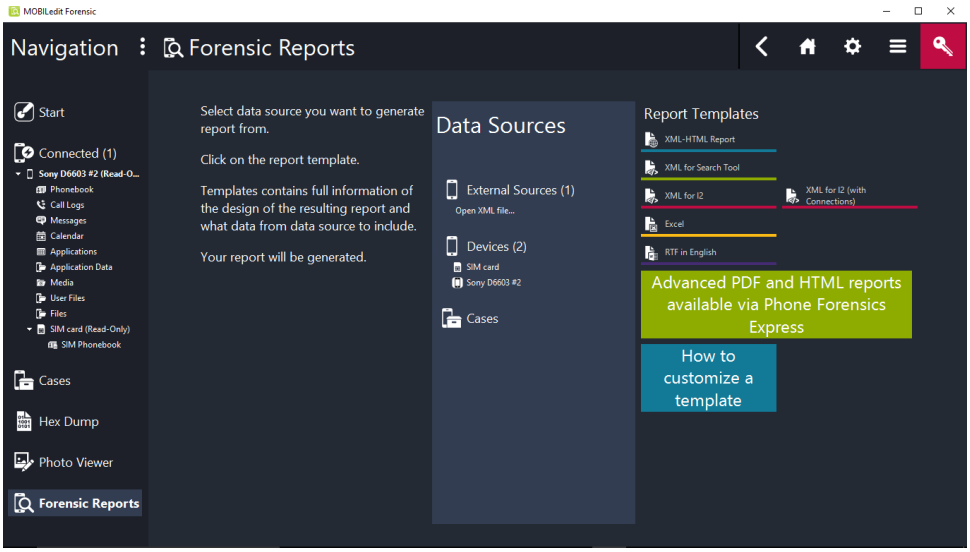


Figura 4. 24 *Pantalla Principal de Reportes Software MobilEdit, Dispositivo Xperia Z3*

- **OXYGEN FORENSIC**

  El software Oxygen Forensic después de la adquisición de información del dispositivo muestra varias opciones y funciones para poder trabajar con la evidencia obtenida del dispositivo, como observa en la figura 4.24; entre las opciones que este software brinda están: diccionario, contactos, mensajes.

  Las opciones que el software muestra en pantalla dependen del dispositivo conectado, así como de la versión de su software.

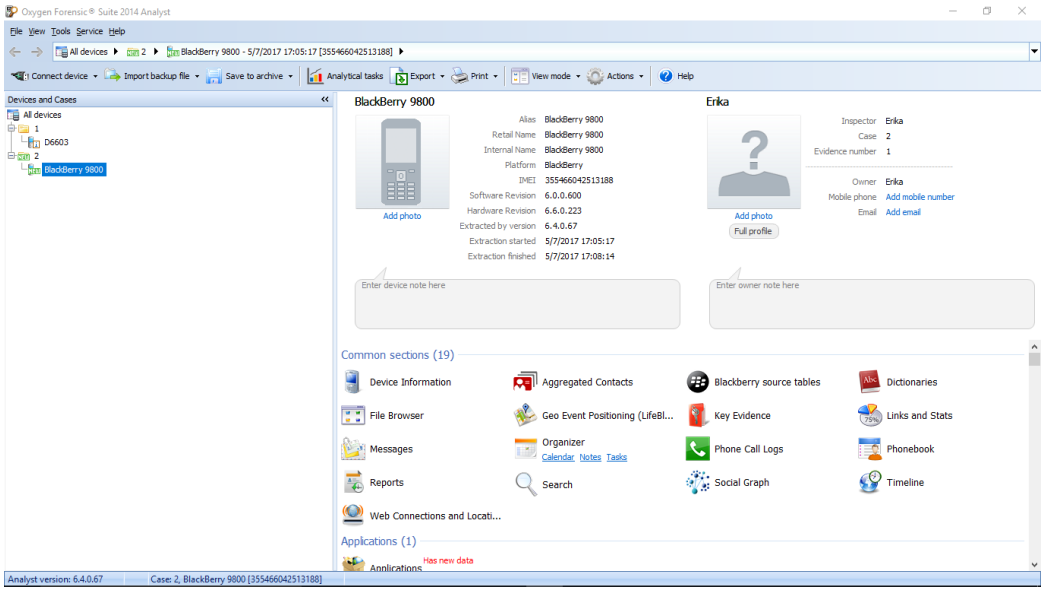


Figura 4. 25 *Información Común y Opciones de Oxygen Forensic, Dispositivo BlackBerry 9800*

Diccionario:

Permite observar las palabras que fueron ingresadas por el usuario mientras tomaba notas, mensajes. En la figura 4.25 se observa el diccionario del dispositivo BlackBerry Torch 9800.

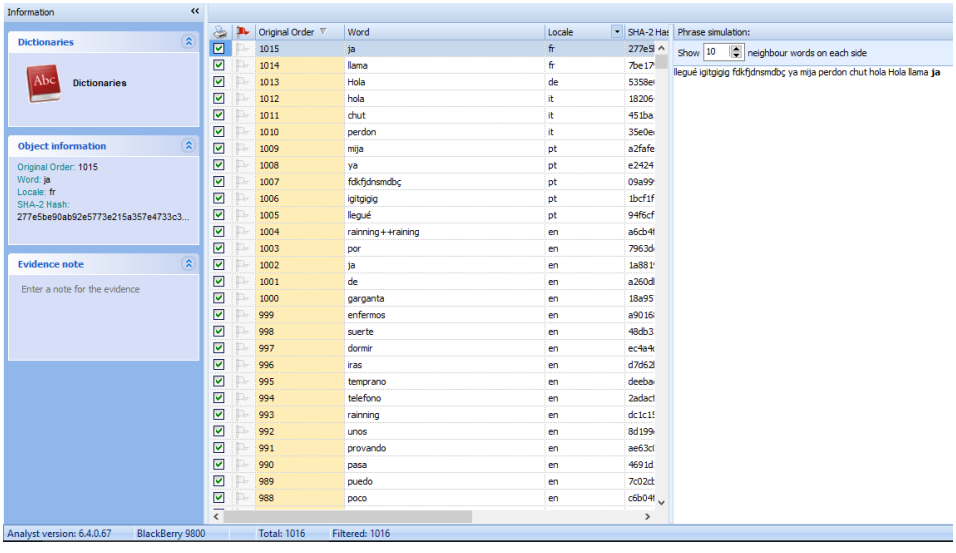


Figura 4. 26 *Diccionario del Dispositivo Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Evidencia Importante:

Esta opción permite a los investigadores visualizar la información que se vaya marcando como importante; en la figura 4.26 observa la información que fue marcada como importante del dispositivo BlackBerry Torch 9800.

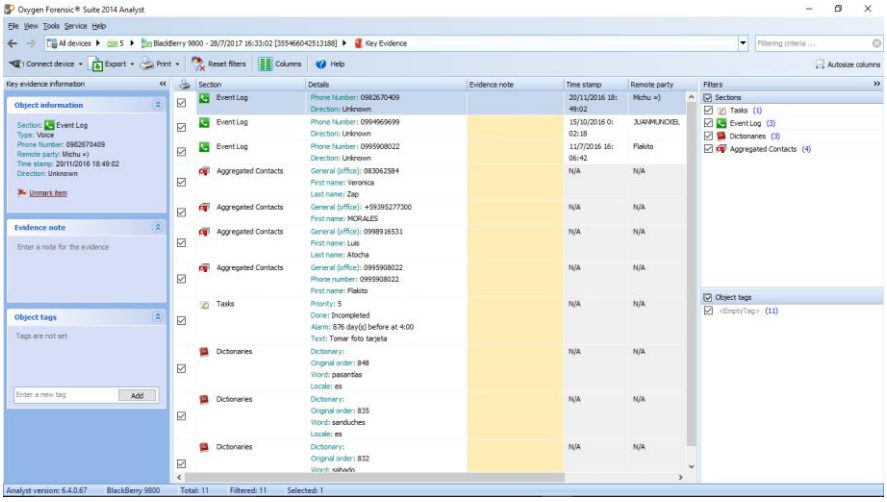


Figura 4. 27 *Información Importante Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Tareas:

En esta pestaña se muestra las tareas obtenidas del dispositivo analizado, mostrando el contenido la fecha de creación y la prioridad como se muestra en la figura 4.27.

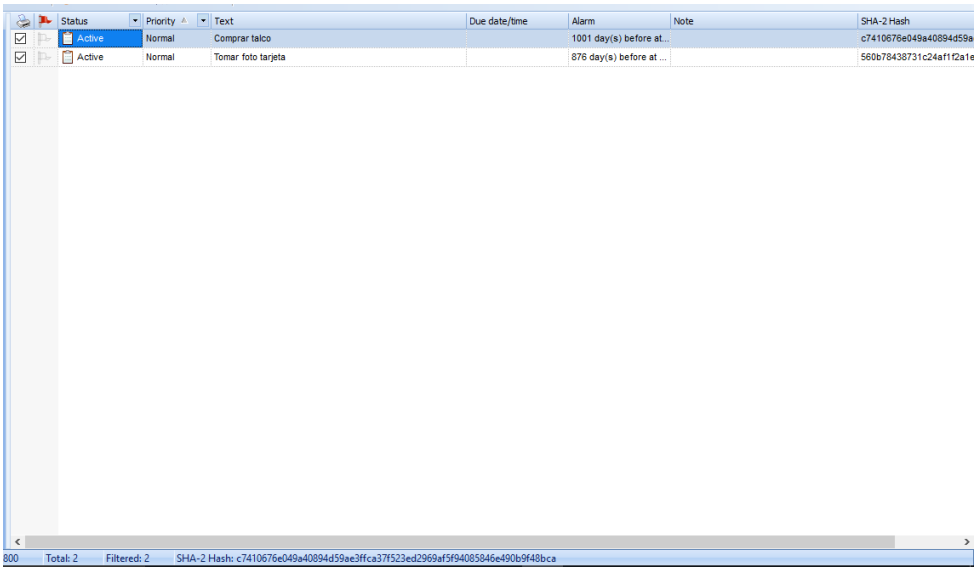


Figura 4. 28 *Tareas del dispositivo Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Registro de Eventos:

Muestra información acerca de llamadas, mensajes recibidos, enviados y borrador, y sesiones de WIFI del dispositivo analizado BlackBerry Torch 9800, ejemplo en la figura 4.28.

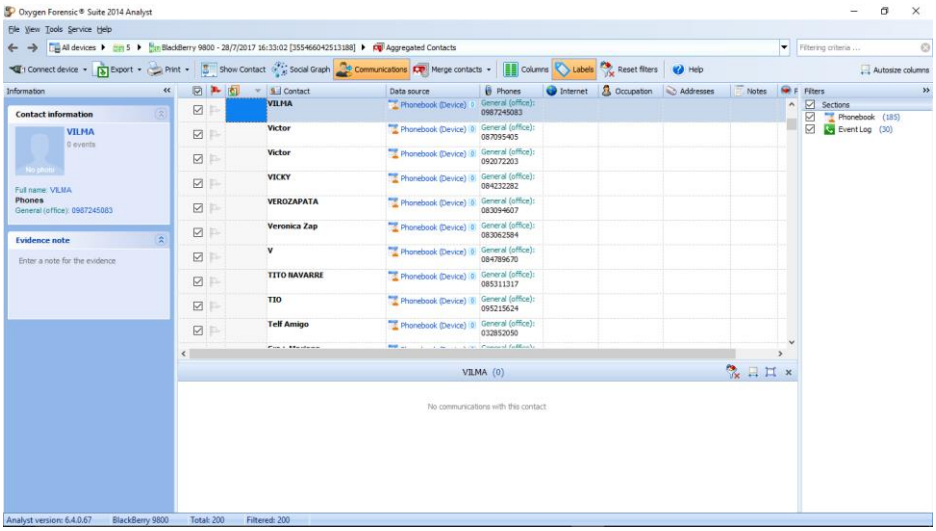


Figura 4. 29 *Registro de Eventos Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Vínculos y Status:

Provee de una conveniente vista de todas las conexiones sociales entre el dueño del dispositivo y sus contactos, como por ejemplo cuantas veces el dueño del dispositivo llamó a un determinado contacto, también muestra un gráfico con intervalos de tiempo de la interacción del dueño del equipo con sus contactos como se muestra en la figura 4.29.

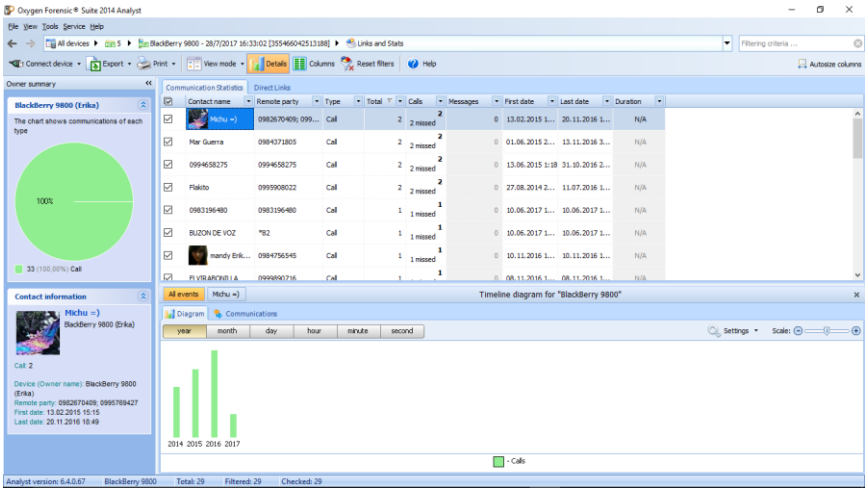


Figura 4. 30 *Vínculos y Status Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Reportes:

Permite crear archivos con información y gráficos acerca de la extracción del dispositivo como ejemplo la figura 4.30.

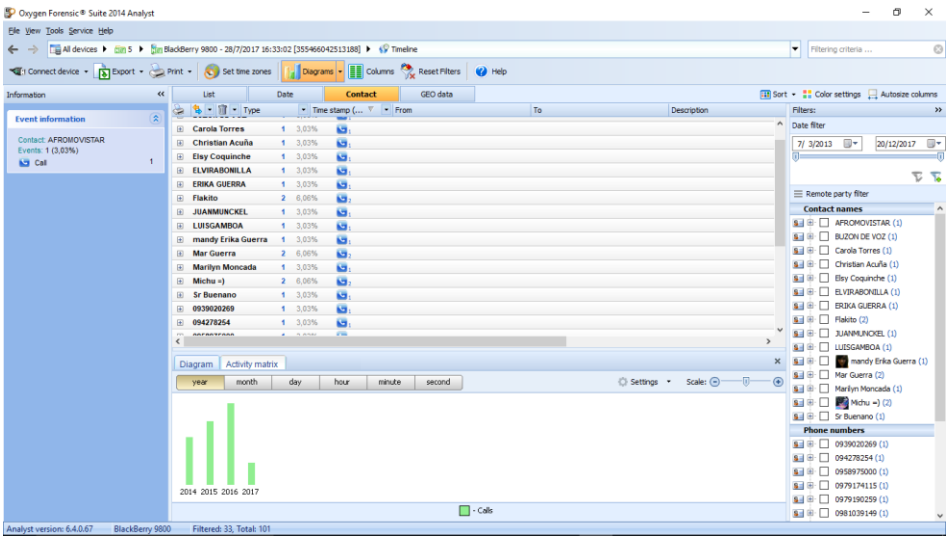


Figura 4. 31 *Reportes de Oxygen Forensic, Dispositivo BlackBerry 9800*

Línea del tiempo:

Resume todos los eventos del teléfono en un orden cronológico y muestra un gráfico de los eventos según la línea de tiempo seleccionada como se muestra en la figura 4.31.

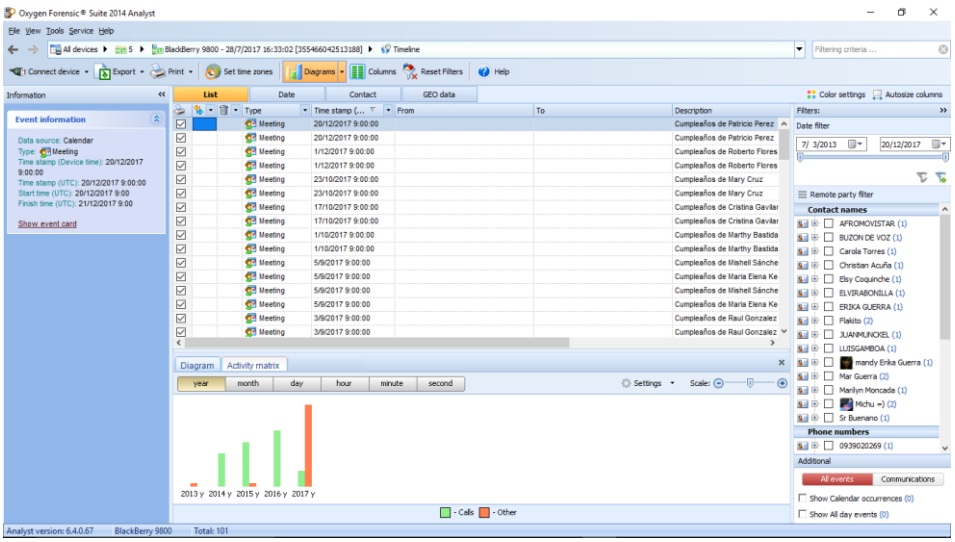


Figura 4. 32 *Línea de Tiempo Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Aplicaciones:

Despliega una lista de todas las aplicaciones que se encuentran instaladas en el dispositivo como se muestra en el gráfico 4.32.

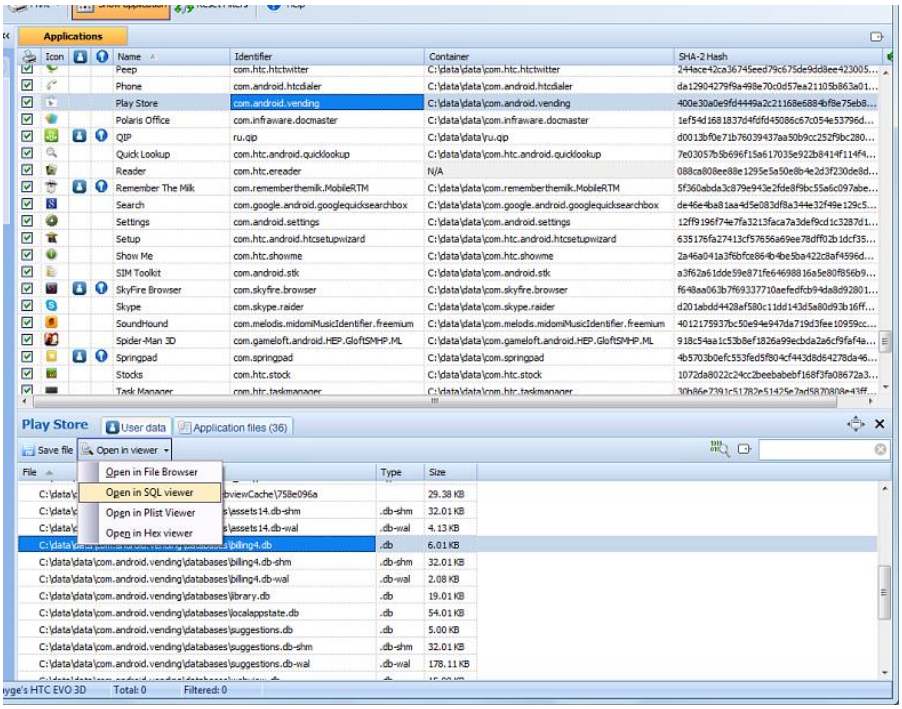


Figura 4. 33 *Aplicaciones Instaladas Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Navegador de archivos:

Presenta el sistema de archivos entero del dispositivo incluyendo fotos, videos, notas de voz y documentos.

En la figura 4.33 se muestra la opción de imágenes del navegador de archivos el cual permite obtener una visualización de las imágenes y sus propiedades como la ruta, nombre, tamaño, tipo, fecha de modificación y extensión.

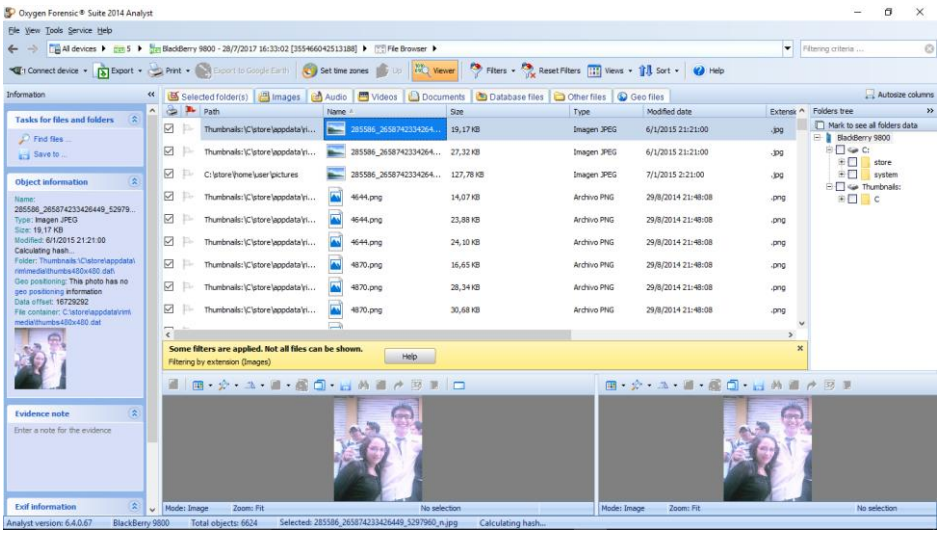


Figura 4. 34 *Visualización de Imágenes Software Oxygen Forensic, Dispositivo BlackBerry 9800*

En las figuras 4.34, 4.35, 4.36 y 4.37 se muestran las opciones de sonidos, videos y archivos de bases de datos del navegador de archivos el cual nos permite observar todos los archivos del dispositivo analizado con sus respectivas propiedades como: nombre, extensión, ruta; permitiendo al usuario escanear los archivos a profundidad.

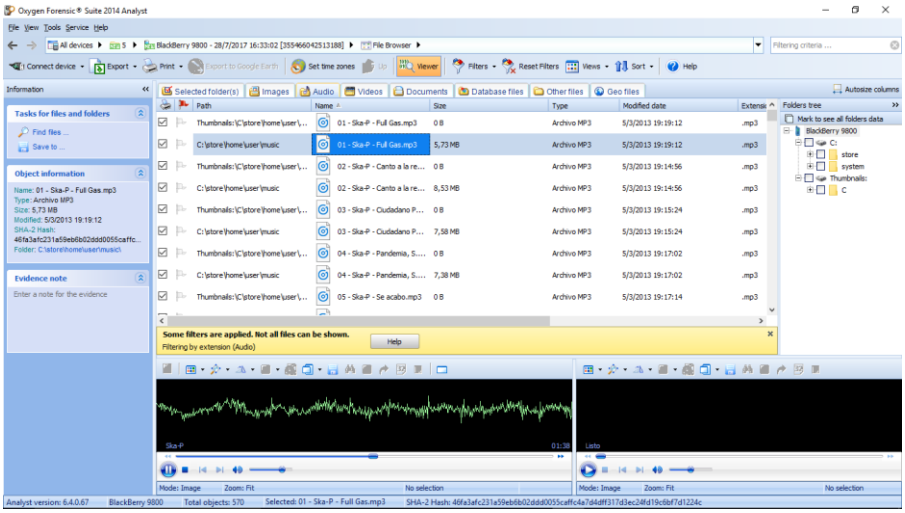


Figura 4. 35 *Visualización de Sonidos Software Oxygen Forensic, Dispositivo BlackBerry 9800*

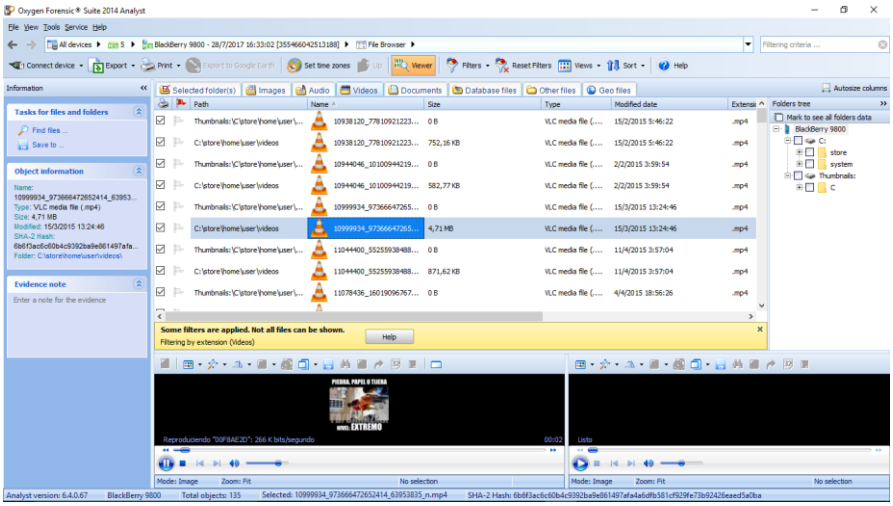


Figura 4. 36 *Visualización de Videos Software Oxygen Forensic, Dispositivo BlackBerry 9800*

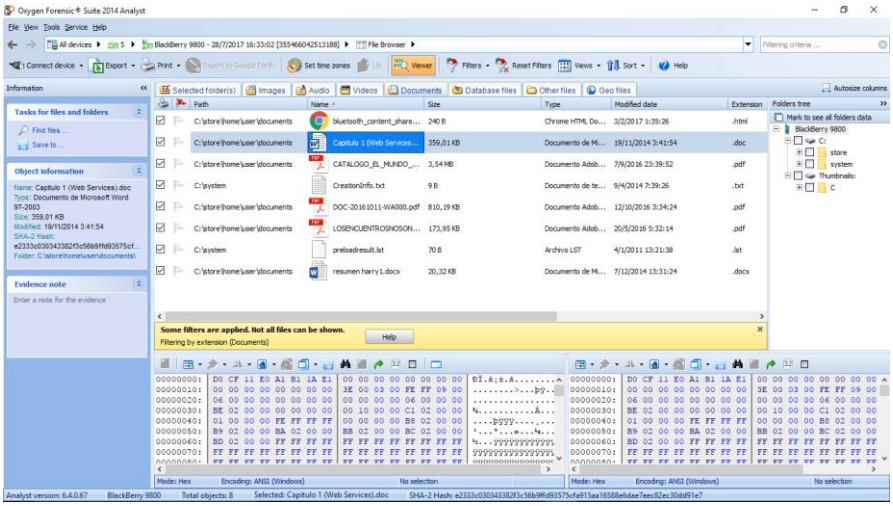


Figura 4. 37 *Visualización de archivos Software Oxygen Forensic, Dispositivo BlackBerry 9800*

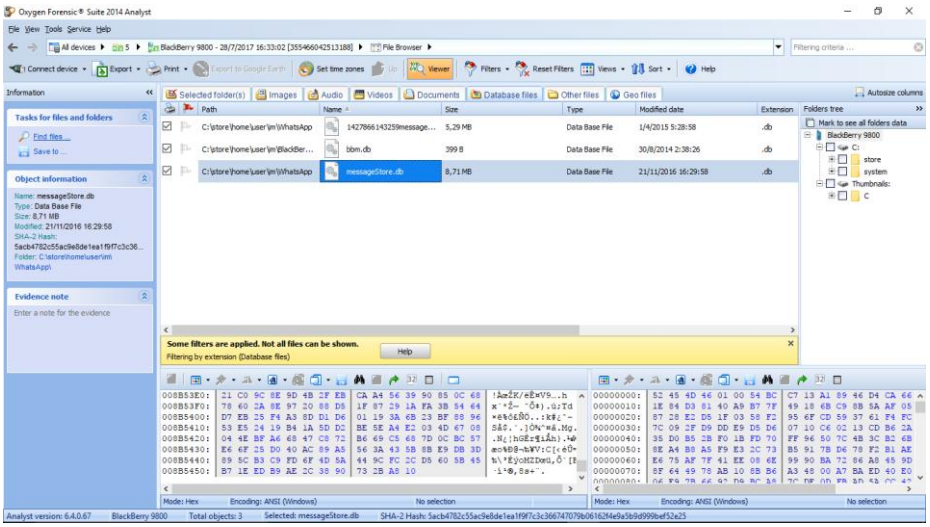


Figura 4. 38 *Visualización de Bases de Datos, Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Mensajes:

Vista de SMS, MMS, e-mail y otros mensajes con sus archivos adjuntos en la carpeta predeterminada y carpetas seleccionadas como se muestra en figura 4.38.

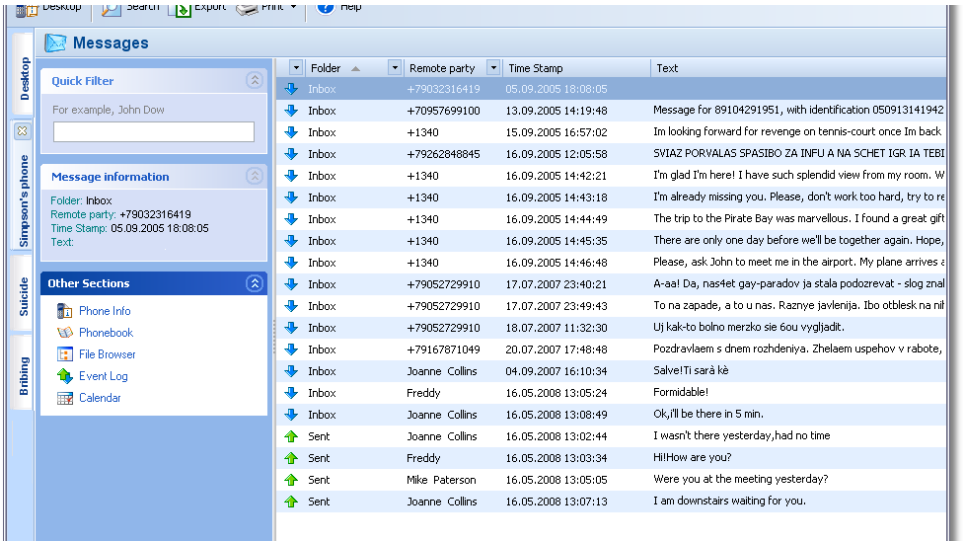


Figura 4. 39 *Visualización de Imágenes Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Búsqueda:

Permite buscar por entradas especiales analizando toda la información del dispositivo como se muestra en la figura 4.39.

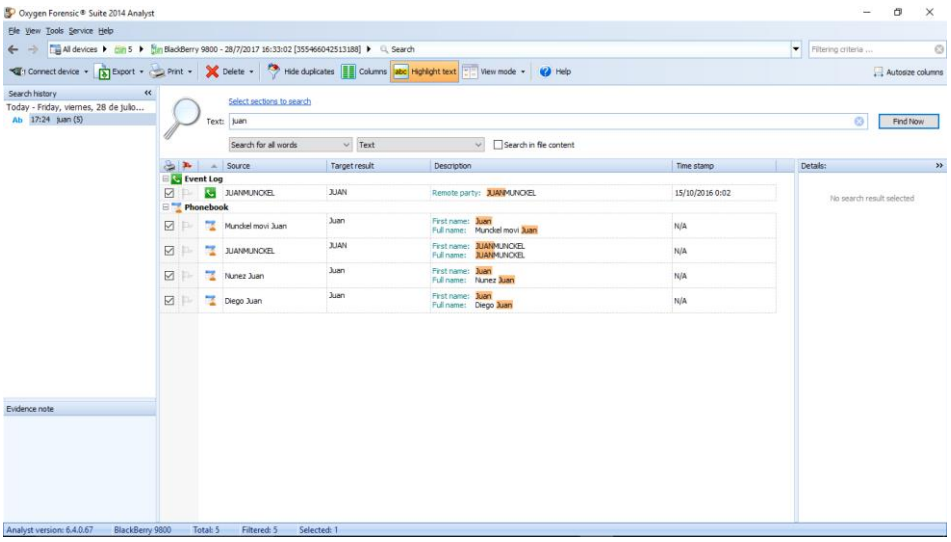


Figura 4. 40 *Búsqueda de Archivos Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Calendario:

Analiza reuniones, aniversarios, recordatorios y otros tipos de eventos como se observa en la figura 4.40.

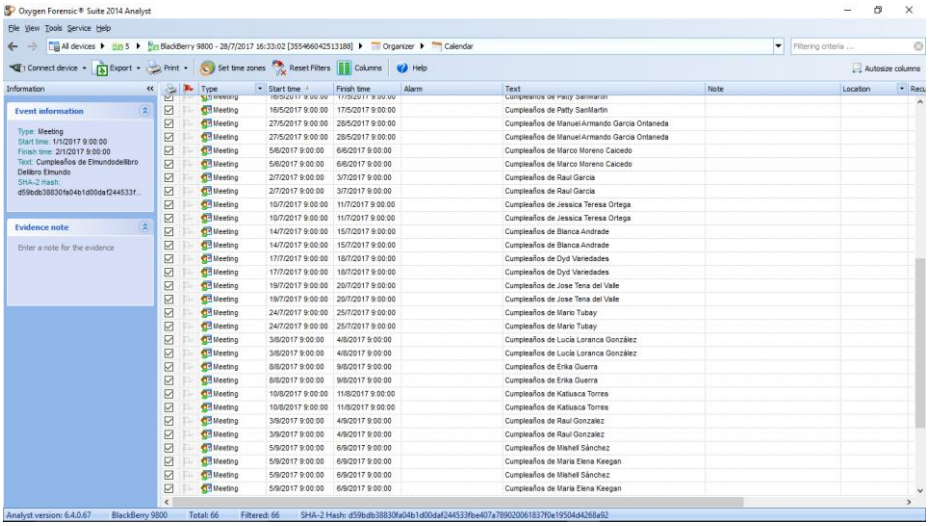


Figura 4. 41 *Calendario Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Geo posición:

Brinda la oportunidad de examinar datos y fechas de los eventos principales del dispositivo junto con la ubicación, como ejemplo la figura 4.41.

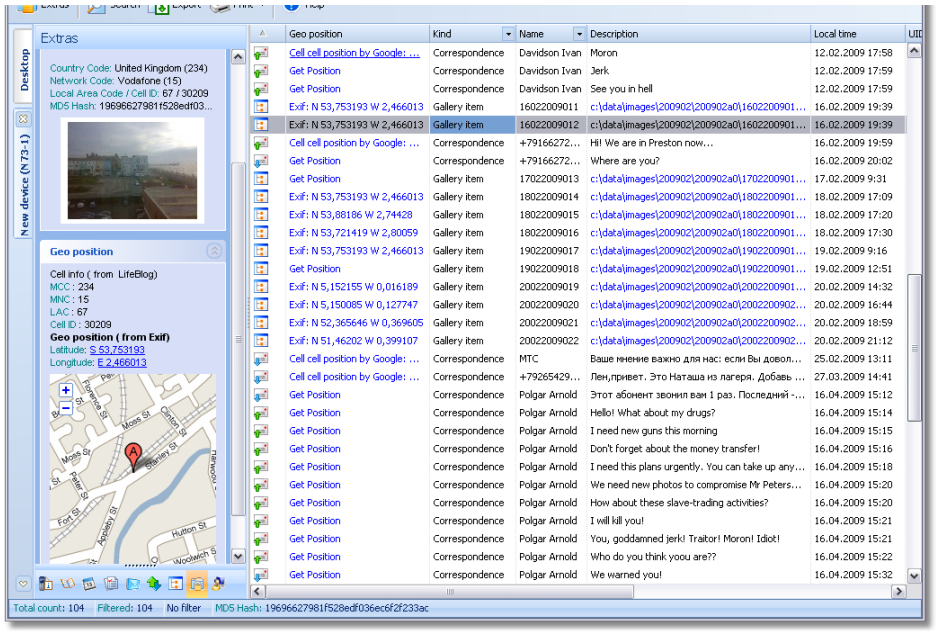


Figura 4. 42 *Posición Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Notas:

Examina notas de cualquier longitud como se observa en la figura 4.42.

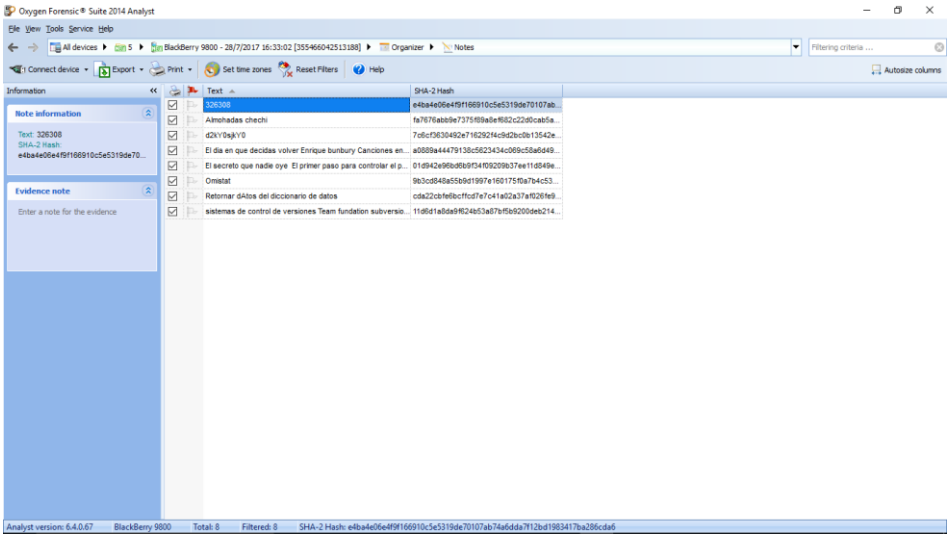


Figura 4. 43 *Notas Software Oxygen Forensic, Dispositivo BlackBerry 9800*

Grafico Social:

Ofrece una rápida carga de las comunicaciones del dueño del dispositivo y analiza las conexiones sociales con gran detalle, la figura 4.43 muestra el gráfico social del dispositivo analizado.

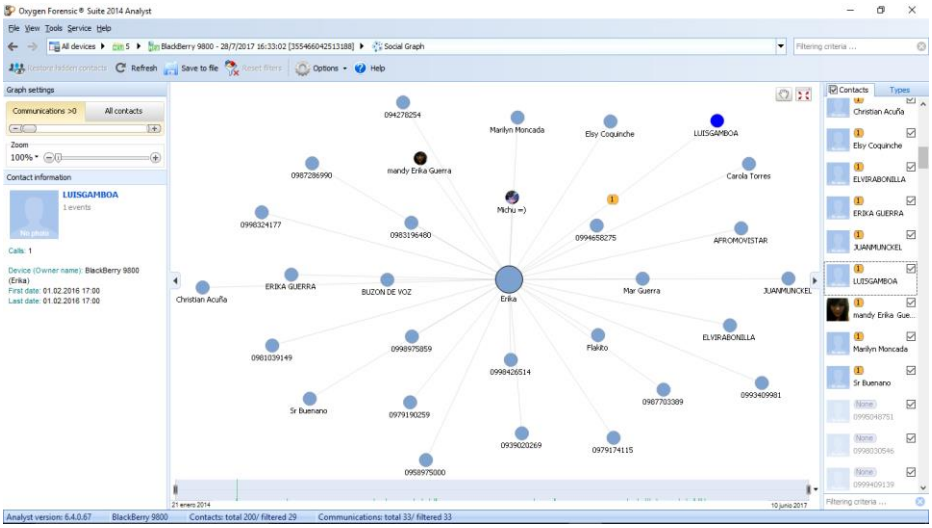


Figura 4. 44 *Gráfico Social Software Oxygen Forensic, Dispositivo BlackBerry 9800*

- **PARABEN DEVICE SEIZURE:**
  El software Paraben Device Seizure después de la adquisición de información del dispositivo muestra varias opciones y funciones para poder trabajar con la evidencia obtenida del dispositivo.

Las opciones que el software muestra en pantalla dependen del dispositivo conectado, así como de la versión de su software.

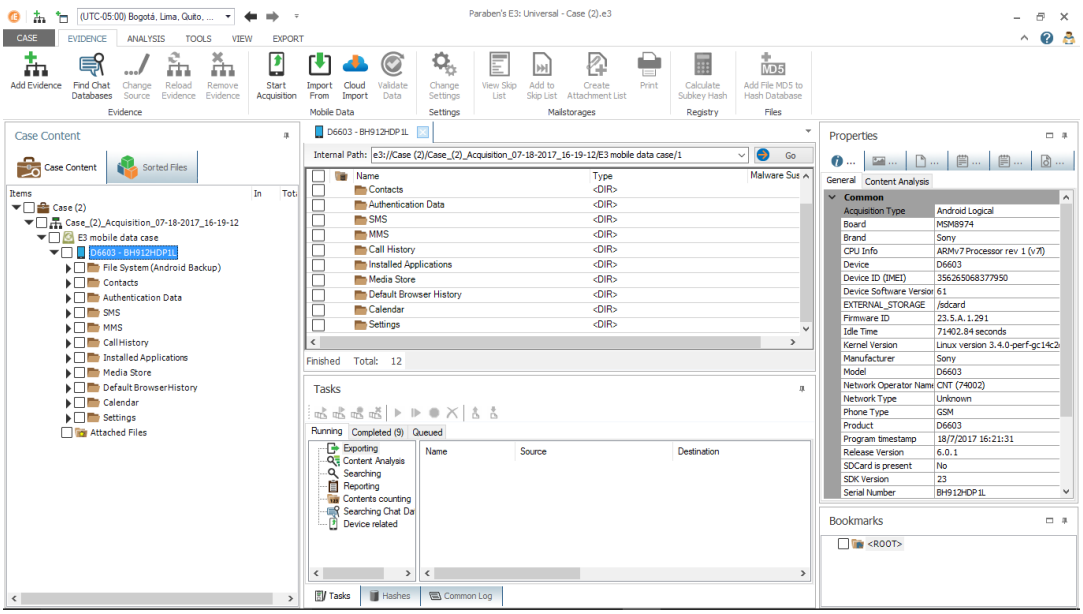


Figura 4. 45 *Pantalla con Evidencia Software Paraben, Dispositivo Xperia Z3*

Archivos de Sistema:

Muestra el contenido de las carpetas y los archivos generados por el sistema operativo, también muestra si el archivo está afectado por algún malware como se muestra en la figura 4.45.

.

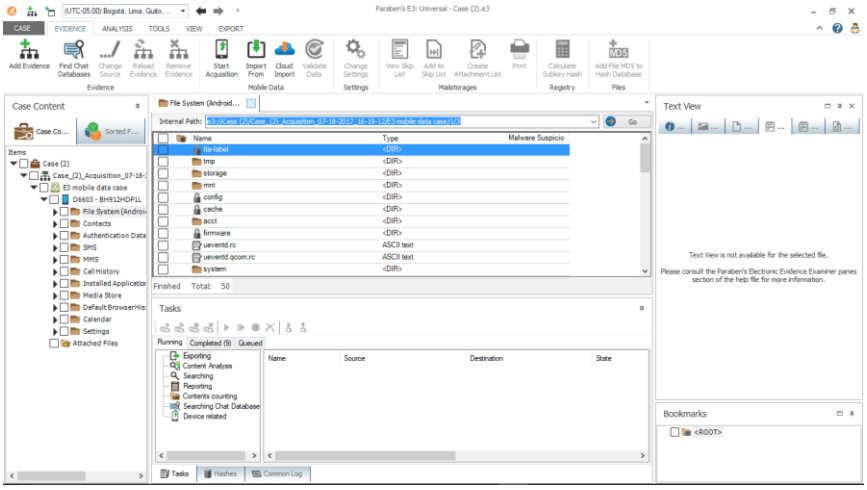


FIgura 4. 46 *Archivos del Sistema Software Paraben, Dispositivo Xperia Z3*

Contactos:

Muestra toda la información contenida en el dispositivo acerca de los contactos como sus imágenes y sus números telefónicos figura 4.46 y 4.47.

Las imágenes de los contactos son mostradas en una carpeta separada figura 4.48.

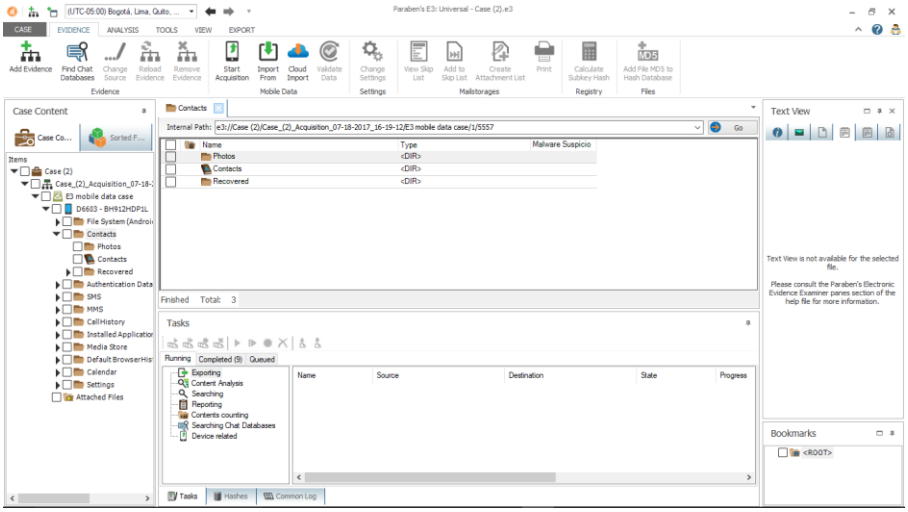


Figura 4. 47 *Pantalla Principal de Contactos Software Paraben, Dispositivo Xperia Z3*

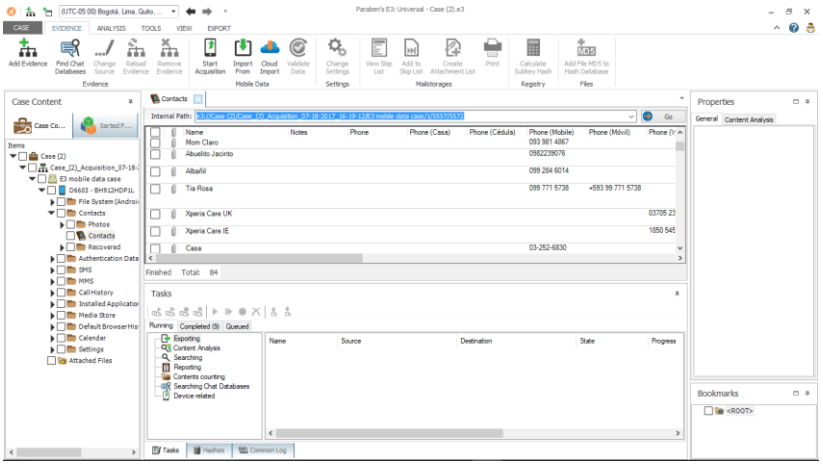


Figura 4. 48 *Contactos Software Paraben, Dispositivo Xperia Z3*

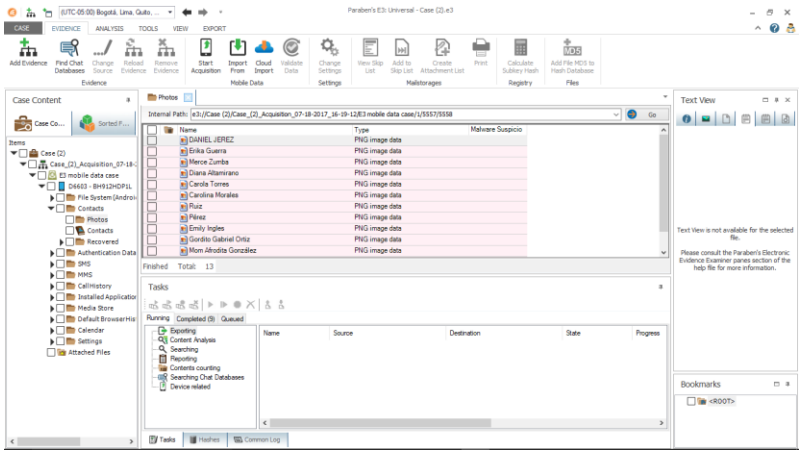


Figura 4. 49 *Imágenes de Contactos Software Paraben, Dispositivo BlackBerry 9800*

Datos de Autentificación:

Contiene la cadena de conexión con la cual la aplicación accedió al contenido del dispositivo.

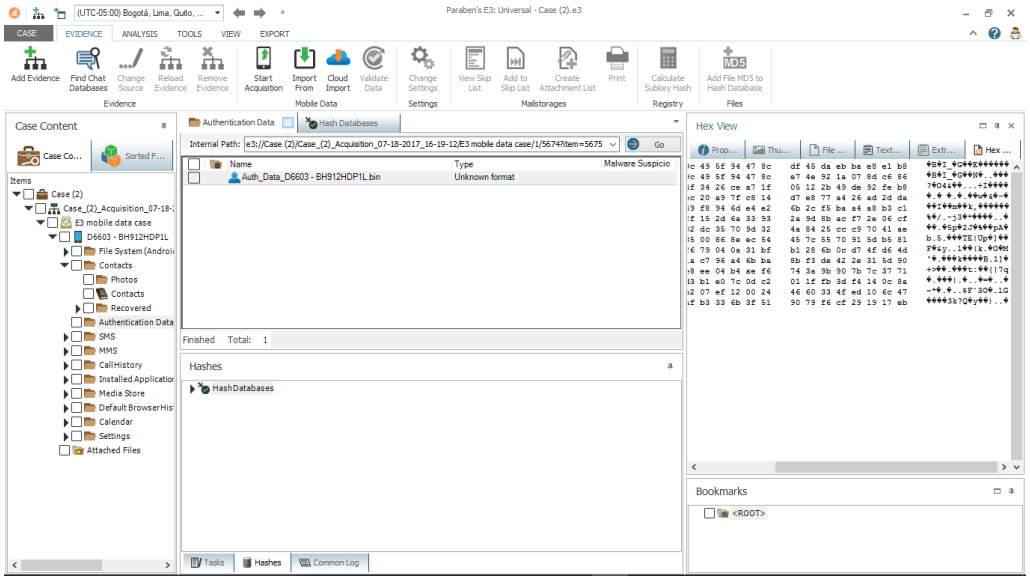


Figura 4. 50 *Datos de Autentificación Software Paraben, Dispositivo BlackBerry 9800*

Mensajes:

Muestra los mensajes de texto o multimedia que se encuentran en el dispositivo, así como el contenido, el destinatario, estado, fecha y hora, número de centro de servicio y el contenido, como se puede observar en la figura 4.50.

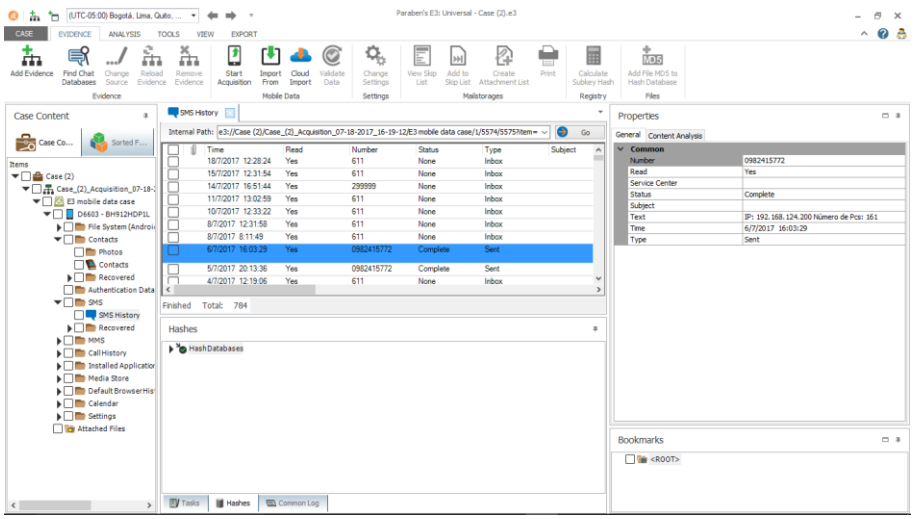


Figura 4. 51 *Mensajes Software Paraben, Dispositivo Xperia Z3*

Historial de Llamadas:

Muestra el historial de llamadas que se encuentra en el dispositivo, así como el contenido, el destinatario, estado, fecha y hora, como se observa en la figura 4.51.

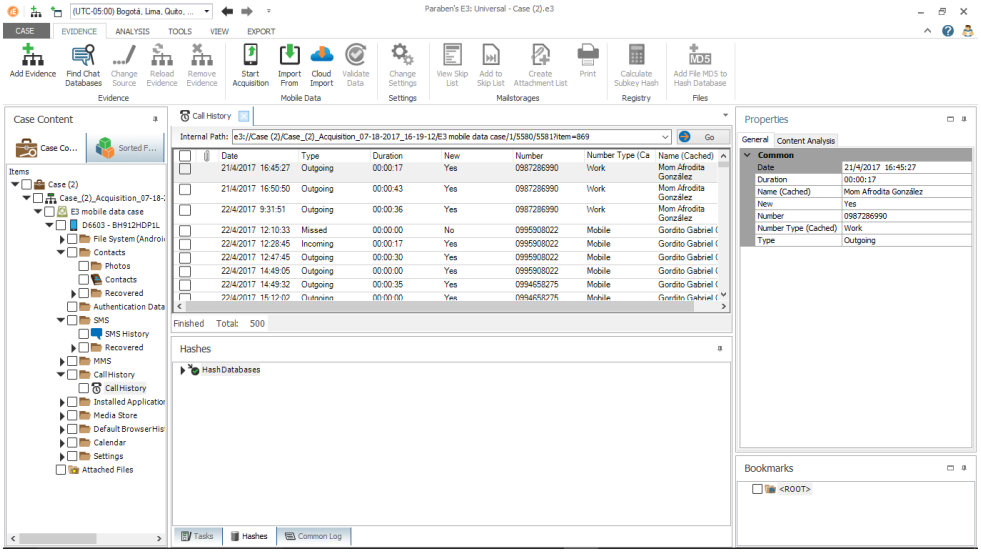


Figura 4. 52 *Historial de Llamadas Software Paraben, Dispositivo BlackBerry 9800*

Aplicaciones Instaladas:

Muestra una lista con las aplicaciones instaladas en el dispositivo analizado como se muestra en la figura 4.52.

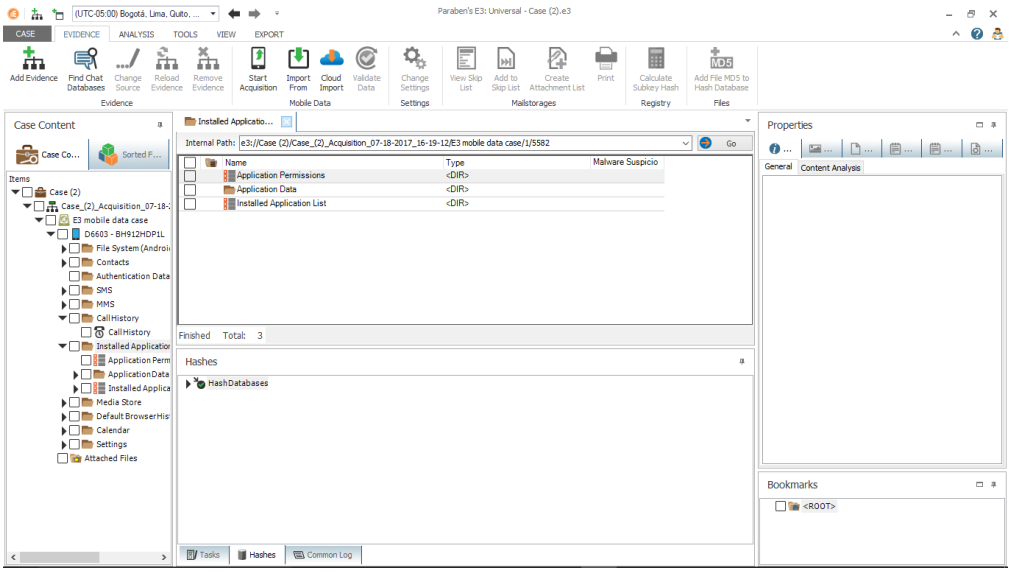


Figura 4. 53 *Aplicaciones Software Paraben, Dispositivo 9800*

Permisos de aplicación:

Muestra los permisos que tienen las aplicaciones instaladas en el dispositivo analizado como lo muestra la figura 4.53.

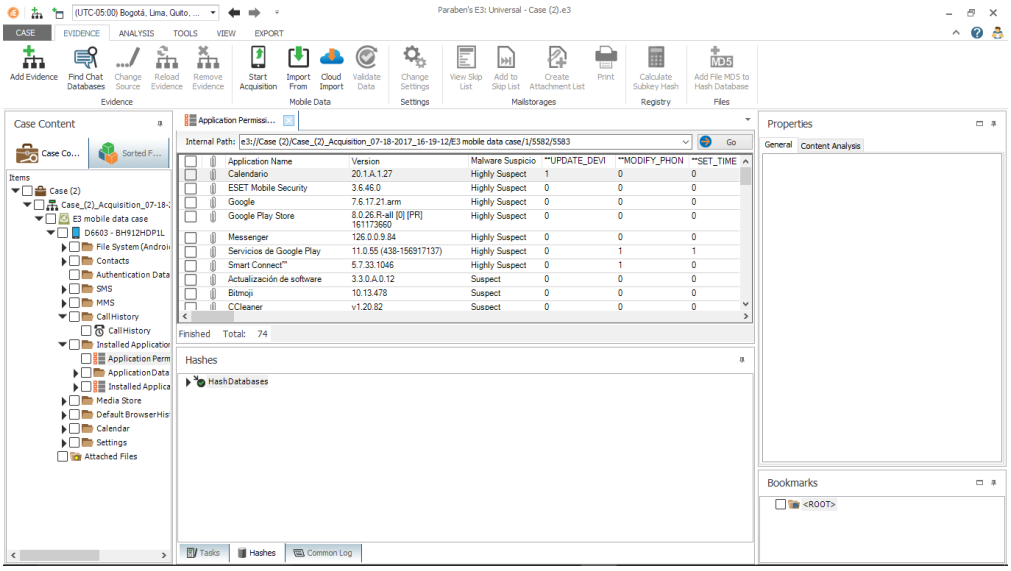


Figura 4. 54 *Permisos de las Aplicaciones Software Paraben, Dispositivo Xperia Z3*

Archivos Multimedia:

Muestra los archivos multimedia contenidos en el dispositivo analizado como lo muestra imagen 4.54.

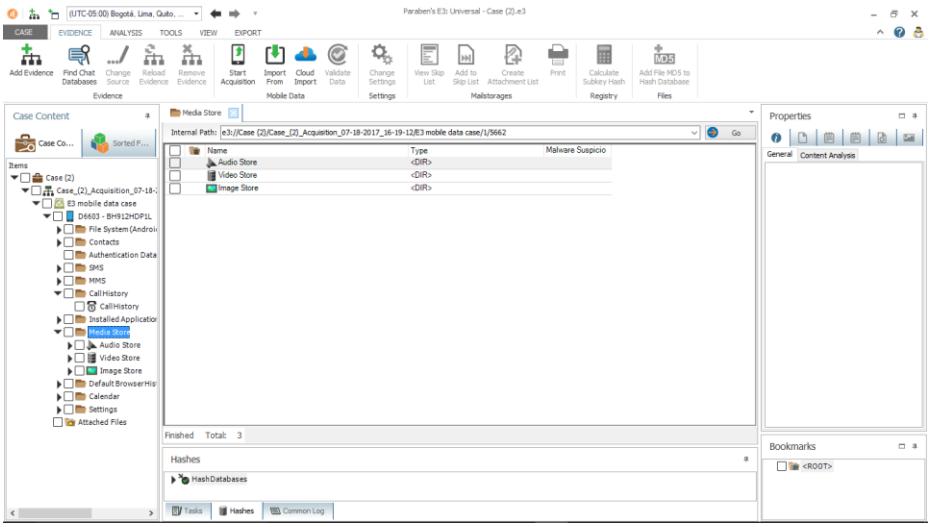


Figura 4. 55 *Archivos Multimedia Software Paraben, Dispositivo Xperia Z3*

Audio y sus opciones ejemplo figura 4.55

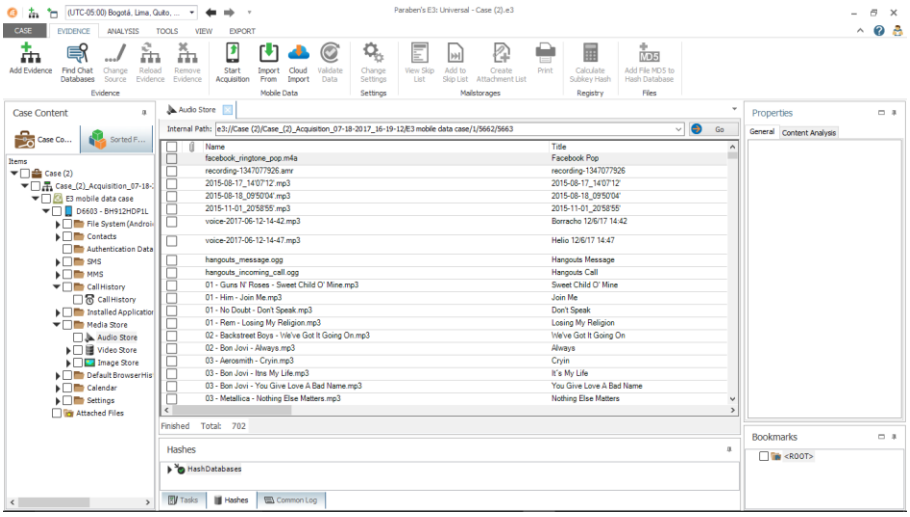


Figura 4. 56 *Audio Software Paraben, Dispositivo Xperia Z3*

Video y sus opciones ejemplo en la figura 4.56

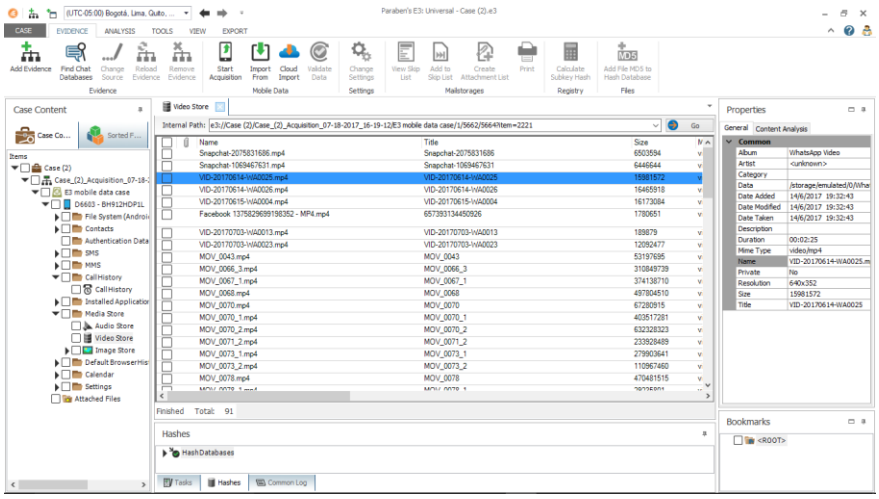


Figura 4. 57 *Video Software Paraben, Dispositivo Xperia Z3*

Imagen y sus opciones ejemplo en la figura 4.57

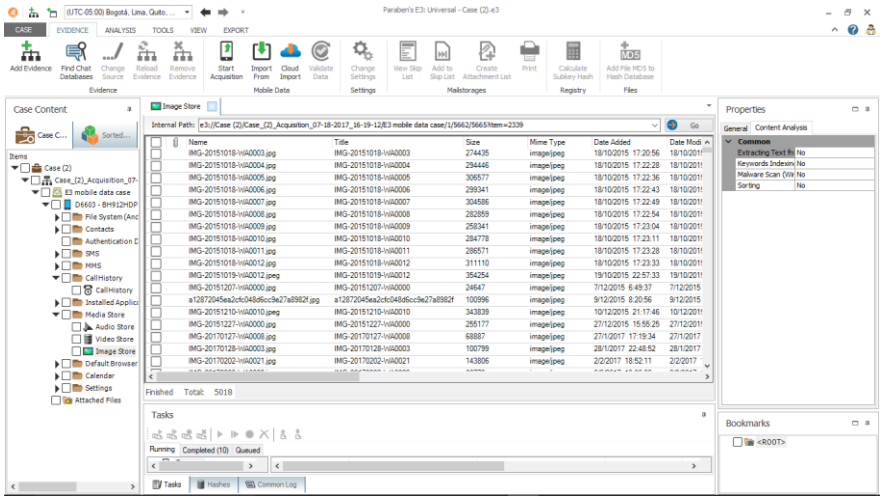


Figura 4. 58 *Imágenes Software Paraben, Dispositivo Xperia Z3*

Historial de Navegador:

Muestra el historial del navegador del dispositivo analizado ejemplo en la figura 4.58.

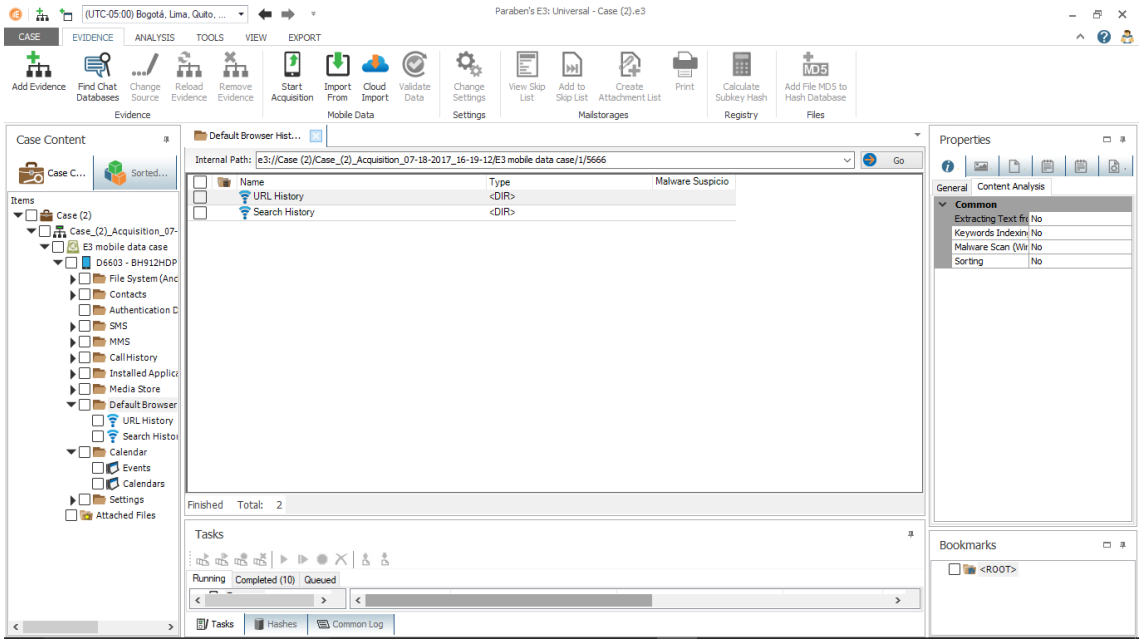


Figura 4. 59 *Historial de Navegación Software Paraben, Dispositivo Xperia Z3*

Calendario:

Muestra los eventos almacenados en el calendario del dispositivo analizado como se muestra en el dispositivo 4.59.

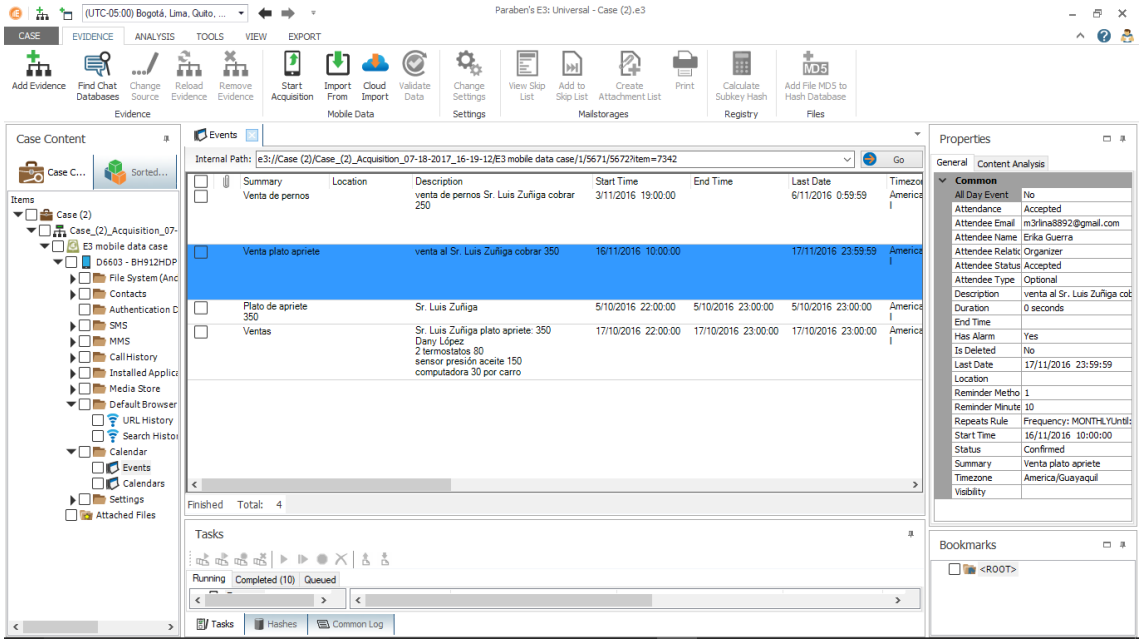


Figura 4. 60 *Calendario Software Paraben, Dispositivo Xperia Z3*

Ajustes:

Muestra en una lista los principales ajustes del dispositivo como el volumen, brillo de la pantalla, tamaño de la pantalla como se puede observar en la figura 4.60.

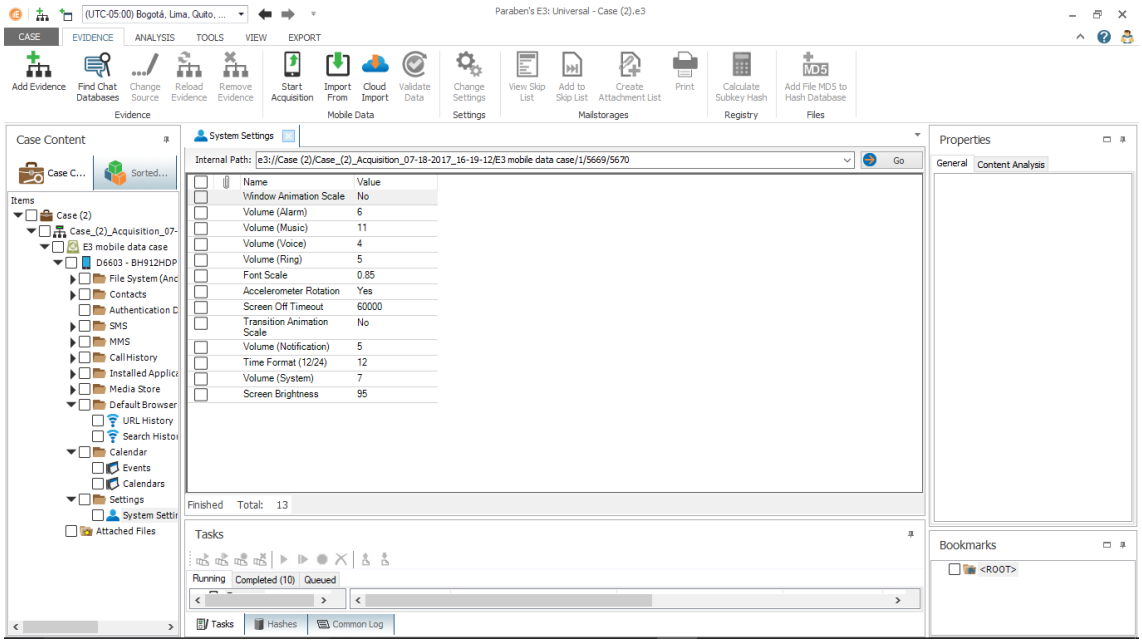


Figura 4. 61 *Ajustes Software Paraben, Dispositivo Xperia Z3*

4.5.3. TABULACIÓN DE RESULTADOS POR DISPOSITIVO.

- **Sony Xperia Z3**

Basándose en el cuadro comparativo de la tabla 4.5 se evidencia que existe información común que es importante y por lo tanto se repiten todas las aplicaciones, pero hay información recolectada que varía dependiendo del software utilizado la cual podría ser información no importante dependiendo del caso de estudio.

Tabla 4. 5 *Evaluación de Información Común Sony Xperia Z3*

Xperia Z3 (Android)			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Alias		x	
Almacenamiento Externo			x
Dirección MAC Bluetooth		x	
Fabricante	x		x
Fecha del Programa			x
ICCID	x	x	
ID de Firmware			x
Idle Name			x
IMEI	x	x	x

IMSI	x		x
Información de CPU			x
Marca			x
Memoria Total			x
Modelo	x		x
Nombre de venta		x	
Nombre del Operador de Datos			x
Nombre Interno		x	
Número de correo de voz		x	
Operador	x		x
Placa			x
Plataforma (Sistema)	x	x	
Producto			x
Redes	x		
Rooteado		x	
SD Card está presente			x
Serie de SIM			x
Serie No	x		x
SIM está presente			x
Tiempo del Teléfono	x		
Tipo de adquisión			x
Tipo de Teléfono			x
Versión de Kernel			x
Versión de SDK			x
Versión del Software	x	x	x
Vía de Conexión	x		x
Total, de Puntos en común	12	10	25

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.5 en donde se analiza la información común de los Smartphones, se tiene la figura 4.61 que el software que más información común extrae del dispositivo analizado es Paraben Device Seizure con 53% frente a MobilEdit con 26% y Oxygen Forensic con 21%.

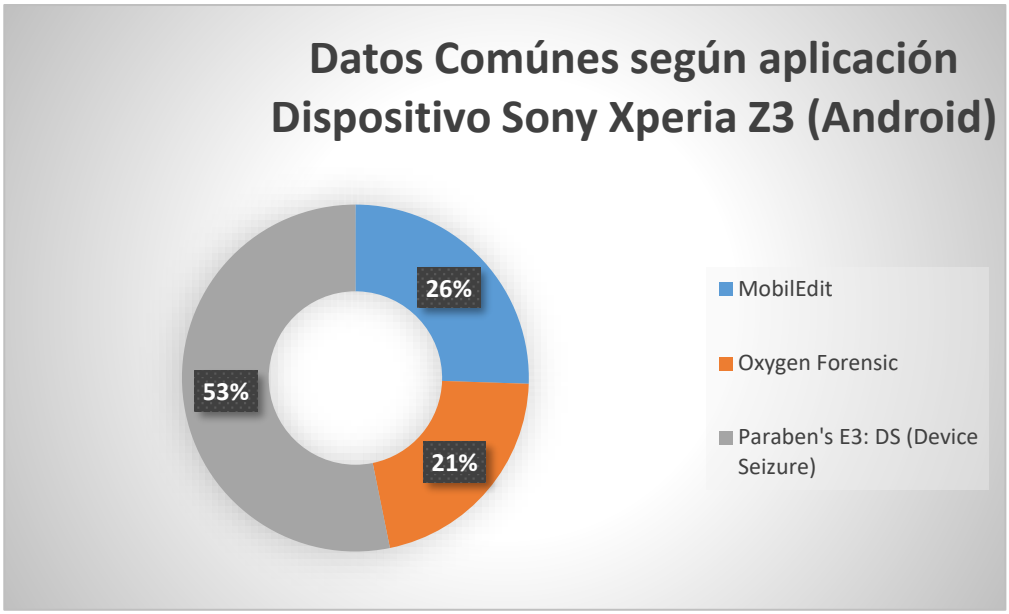


Figura 4. 62 *Datos Comunes de Aplicaciones Sony Xperia*

Basándose en el cuadro comparativo de la tabla 4.6 se evidencia que los programas extraen información en común que sería la más importante en una investigación como, por ejemplo: mensajes, registro de llamadas y contactos y por lo tanto se repiten todas las aplicaciones, pero hay información recolectada que varía dependiendo del software utilizado la cual podría ser información no importante dependiendo del caso de estudio como el diccionario y datos de autentificación.

Tabla 4. 6 *Extracción de Datos según Aplicación Dispositivo Sony Xperia Z3*

Xperia Z3 (Android)			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Estado del telefono	x		
Datos Comunes	x	x	x
Registro de llamadas	x	x	x
Mensajes	x	x	x
Directorio telefónico	x	x	x
Calendario	x	x	x
Aplicaciones	x	x	x
Datos de Aplicaciones	x		
Media	x		x
Archivos de Usuario	x		
Archivos (File System)	x	x	x

Información de SIM	x		
Notas		x	
Tareas		x	
Diccionario		x	
Evidencia Importante		x	
Vinculos y Status		x	
Reportes	x	x	x
Linea de Tiempo		x	
Busqueda		x	
GeoPosición		x	
Gráfico Social		x	
Historial de Navegador de Internet			x
Ajustes			x
Tarjeta de memoria			x
Datos de Autentificación			x
Datos Adjuntos			x
	13	17	14

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.6 en donde se analizó la extracción de la información almacenada en el Smartphone, se tiene la figura 4.62 en el que el software que más información extrae del dispositivo analizado es Oxygen Forensic con 39% frente a MobilEdit con 29% y Paraben con 32%.

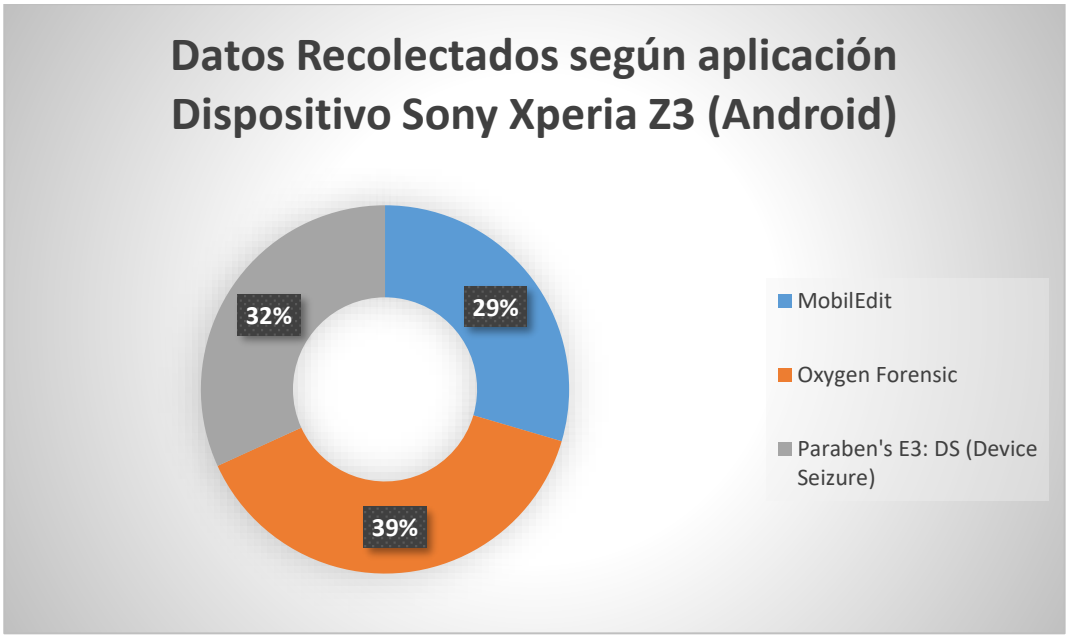


Figura 4. 63 *Información del Dispositivo Sony Xperia Z3 según la Aplicación*

Basándose en el cuadro comparativo de la tabla 4.7 se evidencia que dependiendo del software la extracción y análisis de datos puede ser menor o mayor entre si.

Tabla 4. 7 *Tiempo de Extracción de Datos en el Dispositivo Sony Xperia Z3*

Xperia Z3 (Android)			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Comienzo	16:04:14	19:17:57	16:19:12
Final	16:05:09	0:26:46	19:50:14
duración	0:00:55	5:08:49	3:31:02

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.7 tiempo de extracción de datos, se tiene la figura 4.63 en el que el software que menos se demora en extraer información del dispositivo estudiado es MobilEdit con 55 segundos seguido de Paraben con 3horas 31 minutos y 2 segundos y Oxygen Forensic con 5 horas, 8 minutos y 49 segundos.

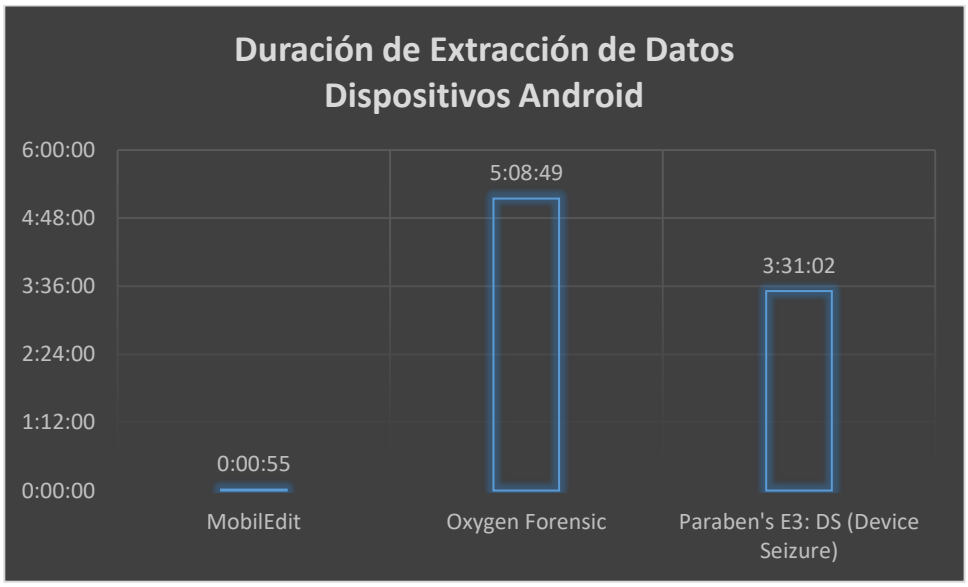


Figura 4. 64 Tiempo de Extracción según Aplicación Dispositivo Sony Xperia Z3

- **BlackBerry Torch 9800**

  Basándose en el cuadro comparativo de la tabla 4.8 se evidencia que existe información común que es importante y por lo tanto se repiten todas las aplicaciones, pero hay información recolectada que varía dependiendo del software utilizado la cual podría ser información no importante dependiendo del caso de estudio.

Tabla 4. 8 *Información Común Dispositivo BlackBerry Torch 9800*

Datos comunes			
BlackBerry Torch 9800			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Alias		x	
Fabricante	x	x	x
ICCID		x	x
Idioma		x	
IMEI	x	x	x
Modelo	x		x
Nombre de Venta		x	
Nombre del modelo			x
Nombre Interno		x	
Operador	x	x	
PIN		x	x
Plataforma	x	x	x
Redes	x		
Redes Soportadas		x	x
Resolución de fondo de pantalla	x		
Resolución de pantalla			x
Resolución del Display	x		
Revisión de Hardware	x	x	
Revisión de Software	x	x	x
Serie			x
Servicios		x	
SIM presente			x
Tarjeta de memoria presente			x
Tiempo del Teléfono	x		
Tipo de red			x
	11	14	14

Elaborado por: *Erika Guerra (2017)*

Como conclusión de la tabla 4.8 Información Común del Dispositivo Blackberry Torch 9800, se tiene la figura 4.61 que el software que más información común extrae del dispositivo analizado son Paraben Device Seizure y Oxygen Forensic ambas con 36%, frente a MobilEdit con 28%.

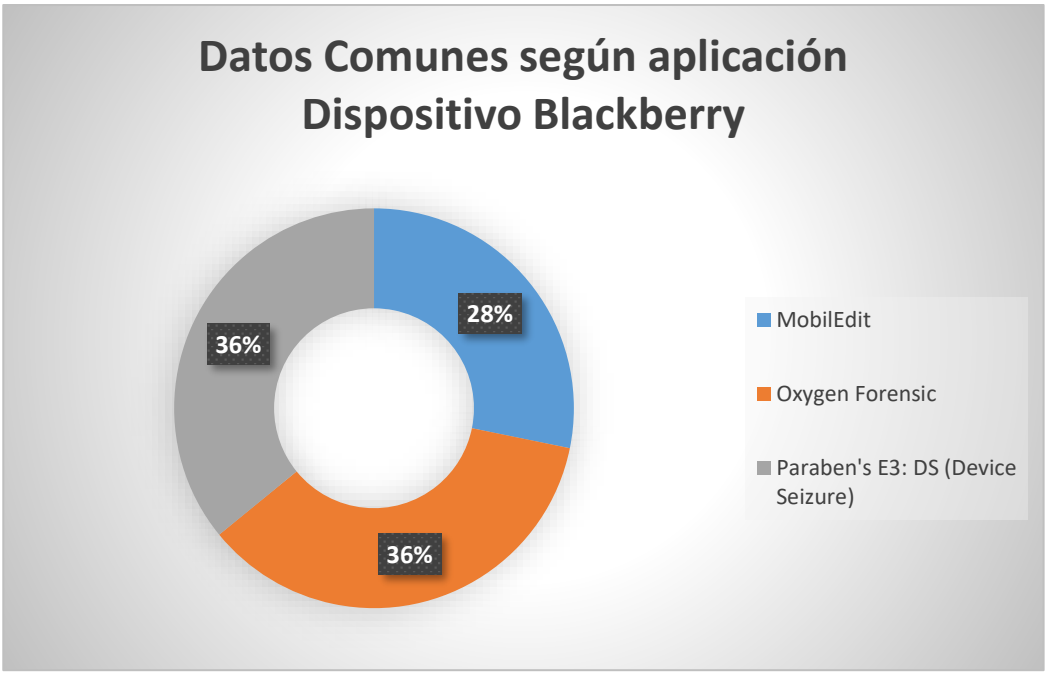


Figura 4. 65 *Datos Comunes según Aplicación Dispositivo BlackBerry Torch 9800*

Basándose en el cuadro comparativo de la tabla 4.9 se evidencia que los programas extraen información en común que sería la más importante en una investigación como, por ejemplo: mensajes, registro de llamadas y contactos y por lo tanto se repiten todas las aplicaciones, pero hay información recolectada que varía dependiendo del software utilizado la cual podría ser información no importante dependiendo del caso de estudio como el diccionario y datos de autentificación.

Tabla 4. 9 *Información Extraída según Aplicación Dispositivo BlackBerry 9800*

Información			
BlackBerry Torch 9800			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Aplicaciones		x	
Archivos	x	x	
Base de datos de BlackBerry		x	
Búsqueda		x	
Calendario	x	x	
Conexiones Web		x	
Contactos		x	
Contenido			x
Diccionario		x	
Directorio Telefónico	x	x	
E-mails	x		

Estado del teléfono	x		
Evidencia Importante		x	
Geo posición		x	
Gráfico Social		x	
Imagen de memoria			x
Imagen Lógica (Bases de datos)			x
Línea de tiempo		x	
Mensajes	x	x	
Notas	x	x	
Registro de llamadas	x	x	
Reportes	x	x	x
Tareas	x	x	
Vínculos y Status		x	
	10	19	4

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.9 Información Extraída según la Aplicación Dispositivo BlackBerry Torch 9800, se tiene la figura 4.65 en el que el software que más información extrae del dispositivo analizado es Oxygen Forensic con 58% frente a MobilEdit con 12% y Paraben con 30%.

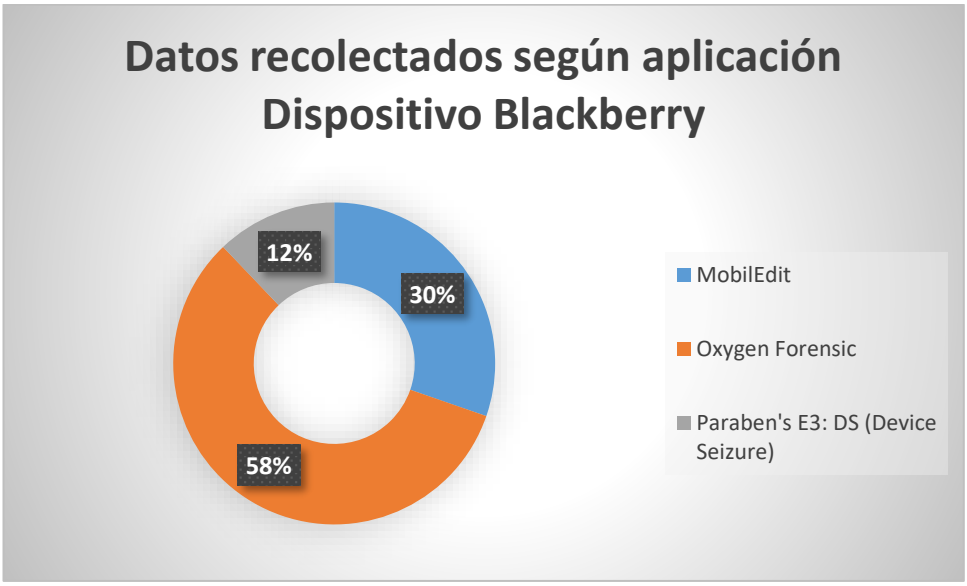


Figura 4. 66 *Datos recolectados según Aplicación Dispositivo BlackBerry Torch 9800*

Basándose en el cuadro comparativo de la tabla 4.10 se evidencia que dependiendo del software la extracción y análisis de datos puede ser menor o mayor entre si.

Tabla 4. 10 *Tiempo de Extracción según Aplicación Dispositivo BlackBerry Torch 9800*

Blackberry Torch 9800			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Comienzo	17:53:01	17:05:17	13:29:56
Final	18:01:57	17:08:14	13:57:17
duración	0:08:56	0:02:57	0:27:21

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.10 Tiempo de Extracción según Aplicación Dispositivo BlackBerry Torch 9800, se tiene la figura 4.66 en el que el software que menos se demora en extraer información del dispositivo estudiado es Oxygen Forensic con 2 minutos y 57 segundos seguido de MobilEdit con 8 minutos y 56 segundos y Paraben con 27 minutos y 21 segundos.

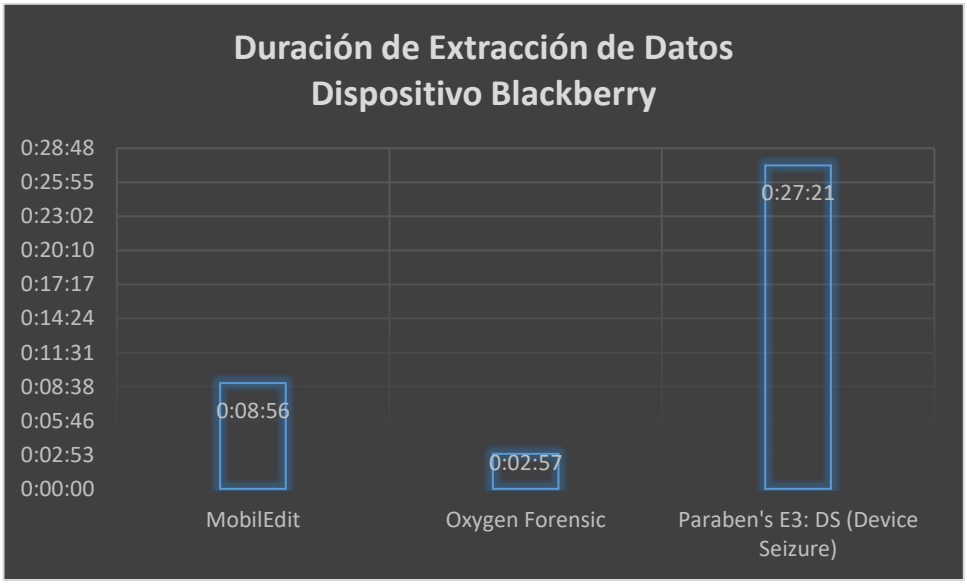


Figura 4. 67 *Duración de Extracción de Datos según Aplicación Dispositivo BlackBerry Torch 9800*

- **Nokia Lumia 520**

  Basándose en el cuadro comparativo de la tabla 4.11 se evidencia que existe información común que es importante y por lo tanto se repiten todas las aplicaciones, pero hay información recolectada que varía dependiendo del software utilizado la cual podría ser información no importante dependiendo del caso de estudio. Tomando en cuenta que el software Oxygen Forensic no cuenta con soporte para dispositivos Nokia.

Tabla 4. 11 *Datos Comunes según Aplicación Dispositivo Nokia Lumia 520*

Datos comunes			
Nokia Lumia 520			
	MobilEdit	Paraben's E3: DS (Device Seizure)	Oxygen Forensic
Fabricante	x	x	
Modelo	x	x	
Serie	x	x	
Operador	x		
Tiempo del teléfono	x		
Revisión de Hardware	x		
Revisión de Software	x	x	
Redes	x		
Plataforma	x		
Conexión	x		
Versión de Firmware		x	
Nombre de Venta		x	
Protocolo		x	
	10	7	0

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.11 Datos Comunes según Aplicación Dispositivo Nokia Lumia 520, se tiene la figura 4.67 que el software que más información común extrae del dispositivo analizado son MobilEdit con 59% frente a Paraben 41%.

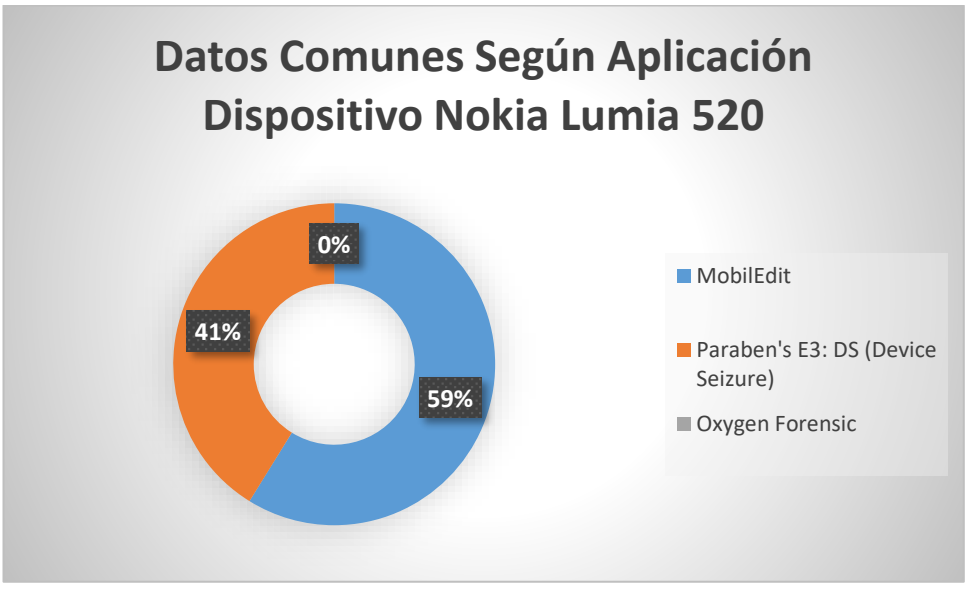


Figura 4. 68 *Datos Comunes según Aplicación Dispositivo Nokia Lumia 520*

Basándose en el cuadro comparativo de la tabla 4.12 se evidencia que los programas extraen información en común que sería la más importante en una investigación como, por ejemplo: mensajes, registro de llamadas y contactos y por lo tanto se repiten todas las aplicaciones, pero hay información recolectada que varía dependiendo del software utilizado la cual podría ser información no importante dependiendo del caso de estudio como el diccionario y datos de autentificación.

Tabla 4. 12 *Datos Recolectados según Aplicación Dispositivo Nokia Lumia 520*

Nokia			
	MobilEdit	Paraben's E3: DS (Device Seizure)	Oxygen Forensic
Archivos	x	x	
Aplicaciones		x	
Metadatos		x	
Servicio de librería multimedia		x	
Status	x	x	
Hints		x	
Información de almacenamiento		x	
Información de rendering		x	
Directorio telefónico	x		
Reportes	x	x	
	4	9	0

Elaborado por: *Erika Guerra (2017)*

Como resultado de la tabla 4.12 Datos Recolectados según Aplicación Dispositivo Nokia Lumia 520, se tiene la figura 4.68 en el que el software que más información extrae del dispositivo analizado es Paraben con 69% frente a MobilEdit con 31%.

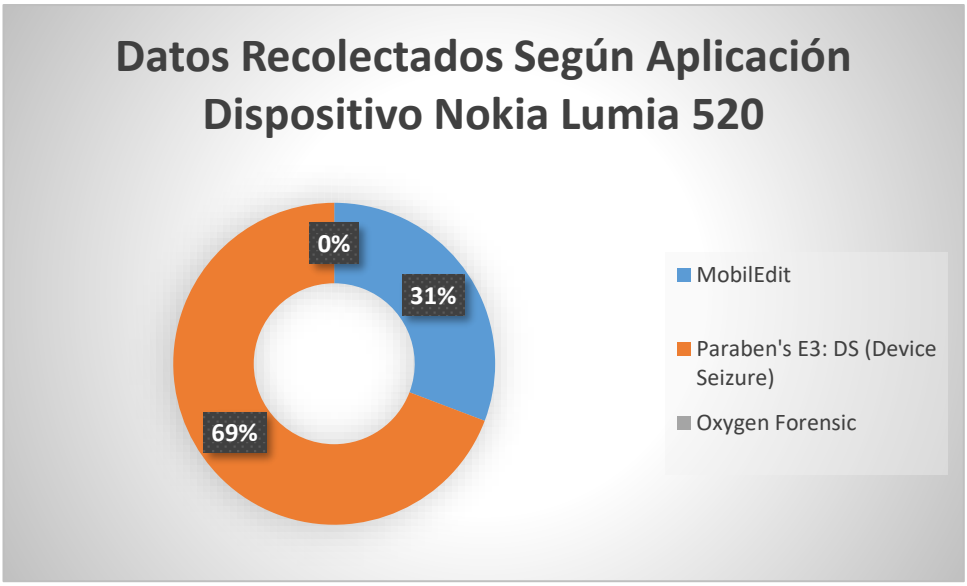


Figura 4. 69 *Datos Recolectados según Aplicación Dispositivo Nokia Lumia 520*

Basándose en el cuadro comparativo de la tabla 4.13 se evidencia que dependiendo del software la extracción y análisis de datos el tiempo puede ser menor o mayor entre si.

Tabla 4. 13 *Tiempo de Extracción según Aplicación Dispositivo Nokia Lumia 520*

Nokia Lumia 520			
	MobilEdit	Oxygen Forensic	Paraben's E3: DS (Device Seizure)
Comienzo	8:26:32		22:36:17
Final	8:30:31		22:37:07
duración	0:03:59	0:00:00	0:00:50

Elaborado por: *Erika Guerra*

Como resultado de la tabla 4.13 Tiempo de Extracción según Aplicación Dispositivo Nokia Lumia 520, se tiene la figura 4.69 en el que el software que menos se demora en extraer información del dispositivo estudiado es Paraben con 50 segundos seguido de MobilEdit con 3 minutos y 59 segundos.

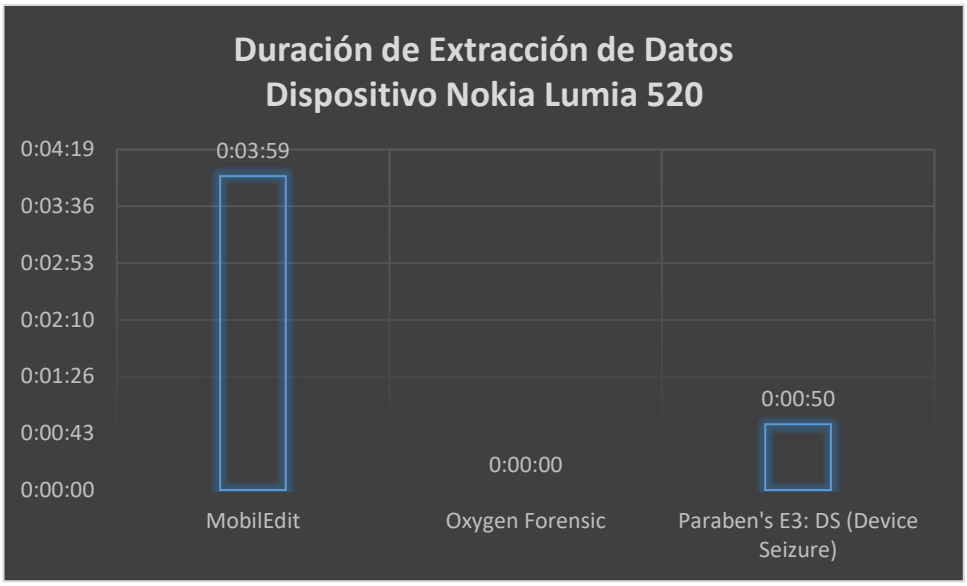


Figura 4. 70 *Tiempo de Extracción según Aplicación Dispositivo Nokia Lumia 520*

4.6 CUADROS COMPARATIVOS

La tabla 4.14, 4.15 y 4.16 muestra un resumen de todos los aspectos importantes en el software que fue evaluado siendo uno de los más importantes la información que es extraída de los dispositivos móviles.

Los *Datos Comunes* sirven para poder verificar la identidad del dispositivo móvil ya que en esta categoría está el IMEI que es un código de identificación irrepetible del dispositivo móvil.

La *Información* es la parte más importante de la extracción de información del dispositivo ya que dentro de esta opción están los mensajes, las llamadas, y los contactos del dispositivo móvil y dependiendo del software existen utilidades que permiten realizar gráficos de la información.

El *Tiempo* está determinado en algunos casos por horas, minutos y segundos es cuanto el software se demora en obtener y preparar la información del dispositivo.

El *Visor Hexadecimal* permite al investigador analizar archivos y bases de datos y buscar información dentro de estos.

La *Variedad de Reportes* brinda la facilidad de presentar toda la información del caso de manera clara y sencilla para que sea de fácil entendimiento para cualquier persona, dependiendo del software se brinda la posibilidad de presentar líneas de tiempo que pueden ayudar al investigador a mostrar fecha a fecha las actividades realizadas en el dispositivo.

La *Interfaz Intuitiva* ayuda al investigador a reducir tiempo en el aprendizaje del uso de la herramienta que se va a utilizar.

En la Tabla 4.14 se observa que el software que cumple con más requisitos es MobilEdit ya que cumple con 4 de 6 aspectos importantes en el software.

Tabla 4. 14 *Cuadro Comparativo Sony Xperia Z3*

SONY XPERIA Z3			
	MobilEdit	Paraben's E3: DS (Device Seizure)	Oxygen Forensic
Datos Comunes		x	
Información			x
Tiempo	x		
Visor Hexadecimal	x	x	x
Variedad de Reportes	x	x	
Interfaz Intuitiva	x		x
	4	3	3

Elaborado por: *Erika Guerra (2017)*

Como resultado para el dispositivo *Sony Xperia Z3* en la figura 4.70 se observa que el software que recolecta mayor información y presta más utilidades para trabajar con la información es *MobilEdit*, ya que este software presenta la información de una manera clara y sencilla para el investigador o cualquier usuario.

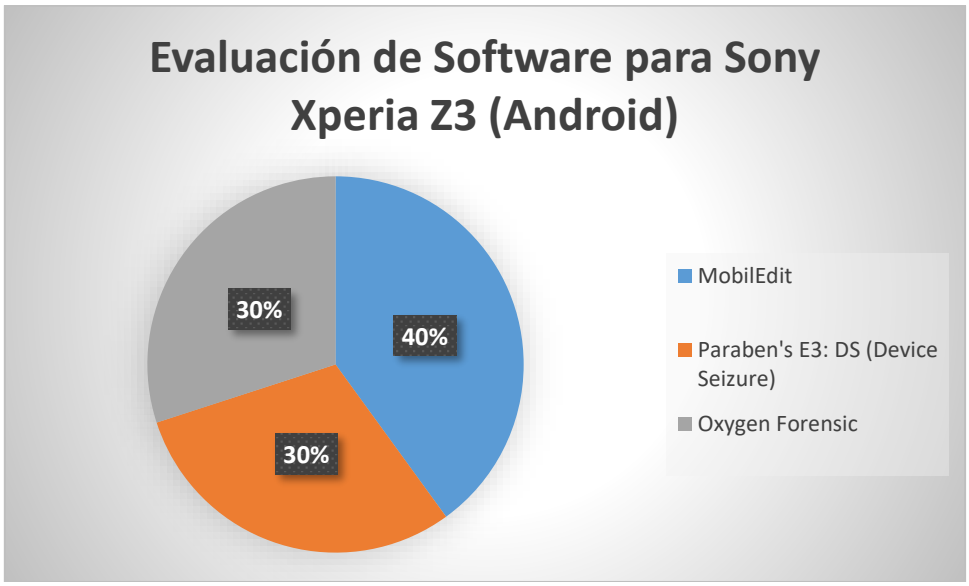


Figura 4. 71 *Evaluación de Software Sony Xperia Z3*

En la Tabla 4.15 se observa que el software que cumple con más requisitos es Oxygen Forensic ya que cumple con 5 de 6 aspectos importantes en el software.

Tabla 4. 15 *Cuadro Comparativo BlackBerry Torch 9800*

BLACKBERRY TORCH 9800			
	MobilEdit	Paraben's E3: DS (Device Seizure)	Oxygen Forensic
Datos Comunes		x	x
Información			x
Tiempo			x
Visor Hexadecimal	x	x	x
Variedad de Reportes	x	x	
Interfaz Intuitiva	x		x
	3	3	5

Elaborado por: *Erika Guerra (2017)*

Como resultado para el dispositivo *BlackBerry Torch 9800* en la figura 4.71 se observa que el software que recolecta mayor información y presta más utilidades para trabajar con la información es *Oxygen Forensic*, ya que este software presenta la información de una manera clara y sencilla para el investigador o cualquier usuario.

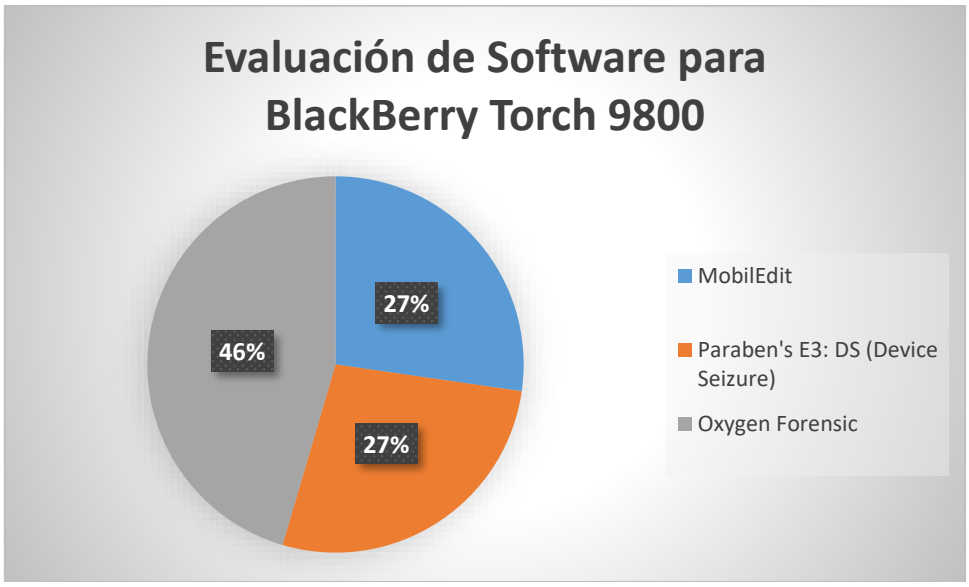


Figura 4. 72 *Evaluación de Software BlackBerry Torch 9800*

En la Tabla 4.16 se observa que el software que cumple con más requisitos es Paraben Device Seizure ya que cumple con 4 de 6 aspectos importantes en el software.

Tabla 4. 16 *Cuadro Comparativo Nokia Lumia 520*

NOKIA LUMIA 520

	MobilEdit	Paraben's E3: DS (Device Seizure)	Oxygen Forensic
Datos Comunes	x		
Información		x	
Tiempo		x	
Visor Hexadecimal		x	
Variedad de Reportes	x	x	
Interfaz Intuitiva	x		
	3	4	0

Elaborado por: *Erika Guerra*

Como resultado para el dispositivo *Nokia Lumia 520* en la figura 4.72 se observa que el software que recolecta mayor información y presta más utilidades para trabajar con la información es *Paraben Device Seizure*, ya que este software presenta la información de una manera clara y sencilla para el investigador o cualquier usuario.

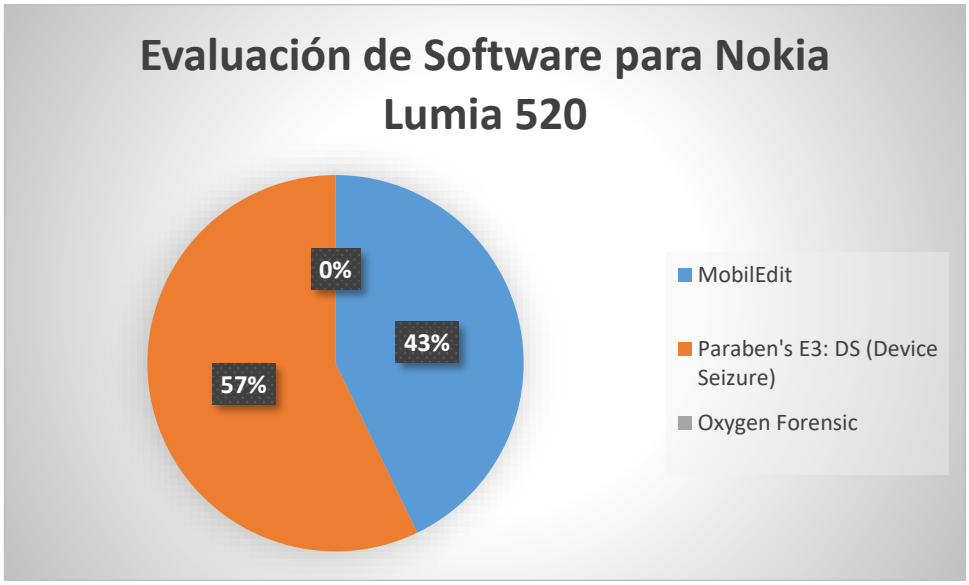


Figura 4. 73 *Evaluación de Software Nokia Lumia 520*

4.6 COMPARACIÓN DE LA EVALUACIÓN DE SOFTWARE

En la Tabla 4.17 se detallan las características que el software analizado cumplió en la fase de pruebas de software obteniendo como resultado que el software que mejor información básica del Smartphone extrae es Paraben, en la extracción de datos almacenados en las memorias del Smartphone y soporte para marcas y modelos están Paraben y MobilEdit y en tiempo de extracción el que menos tiempo se demora es MOBILedit.

Tabla 4. 17 *Evaluación de Características Generales*

	MobilEdit	Paraben's E3: DS (Device Seizure)	Oxygen Forensic
Información Básica del Smartphone	32%	45%	23%
Datos almacenados en las memorias del Smartphone	30%	30%	40%
Tiempo de extracción	68%	1%	31%
Soporte para Marcas y modelos	50%	50%	0%
Total	***45%***	***32%***	***24%***

Elaborado por: *Erika Guerra*

El la Figura 4.74 se puede observar que el software que mejor cumple con los aspectos de análisis del software fue MOBILedit en primer lugar ya que cumple con requisito importante como lo es el soporte para distintas marcas y modelos de Smartphones, pudiendo en las pruebas realizadas acceder a la información almacenada en los Smartphones de prueba.
MOBILedit al igual que el resto de software genera reportes con la evidencia adquirida de una manera muy sencilla, y muestra una interfaz fácil de manejar para el usuario a diferencia del software Oxygen el cual necesita un poco más de conocimiento del usuario para manejar la evidencia y generar reportes.

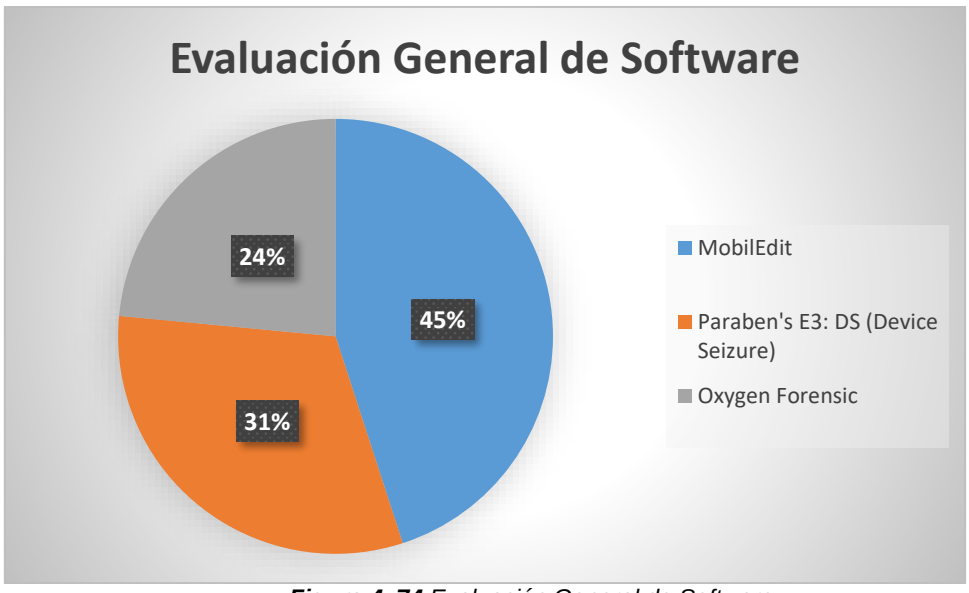


Figura 4. 74 *Evaluación General de Software*

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En la provincia de Tungurahua existen casos donde una de las evidencias de un delito son smartphones los cuales pueden contener información importante para resolver un posible delito y para eso se necesita de la Informática Forense por eso su importancia debido a que los usuarios pueden realizar cualquier tipo de acciones desde sus smartphones sean estas buenas o malas lo que convierte a este dispositivo en una poderosa fuente de evidencia dentro de un posible crimen.

- Oxygen Forensic es una herramienta muy potente en especial para dispositivos BlackBerry para la adquisición de evidencia realiza gráficos acerca de la información recolectada destacando su grafico social el cual ayuda a ver los vínculos del sospechoso con sus contactos, así como sus frecuencias de conversaciones.

- MobilEdit es una herramienta muy simple en su uso lo que ayuda al investigador a reducir tiempos en capacitación de uso de la herramienta y en dispositivos Android presenta más funcionalidades e información en comparación con los dispositivos BlackBerry y Nokia.

- Paraben Device Seizure no presenta una interfaz de usuario intuitiva y el investigador debe aprender del manejo de la herramienta para usar correctamente sus funciones; por otra parte, presenta un gran soporte para dispositivos de distintas marcas y sistemas operativos.

5.2 RECOMENDACIONES

- Se recomienda estar siempre actualizados acerca del uso de herramientas para análisis forense en smartphones, así como de la compatibilidad el software con los distintos dispositivos que hay en el mercado ya que los delincuentes cada día buscan técnicas avanzadas para cometer delitos.

- Se recomienda seguir detalladamente el proceso correspondiente a la cadena de custodia según el Manual De, Protocolos ,Instructivos Y Formatos Del Sistema Especializado Integral De Investigación Medicina Legal Y Ciencias Forenses [27] desde la página 210; como la documentación de la pantalla en caso de que el dispositivo esté encendido, el etiquetado de cables conectados al dispositivo, sellado de entradas del dispositivo, desconectar cables de red para impedir el acceso remoto y el embalaje (fundas y recipientes antiestáticos), sellado para que pueda ser entregado al custodio junto con el registro manual y automatizado, asegurando así la integridad del dispositivo y toda la información contenida en él.

- Se recomienda verificar y valorar cada etapa de análisis del dispositivo evidencia y sus resultados para que toda la información obtenida del proceso de extracción sea válida y pueda ser utilizada como prueba ante un tribunal. El mismo que acreditará y comprobará la veracidad ante el tribunal de la evidencia digital resultado del análisis del dispositivo no ha sido comprometida o alterada.

Bibliografía

[1] Revista Líderes, «Líderes,» 8 agosto 2016. [En línea]. Available: http://www.revistalideres.ec/lideres/usuarios-smartphones-economia-negocios-comunicacion.html. [Último acceso: 4 octubre 2017].

[2] Instituto Nacional de Estadisticas y Censos INEC, «Instituto Nacional de Estadisticas y Censos,» 2015. [En línea]. Available: http://www.ecuadorencifras.gob.ec//documentos/web-inec/Estadisticas_Sociales/TIC/2015/Presentacion_TIC_2015.pdf. [Último acceso: 15 octubre 2016].

[3] S. O. O. Oluwafemi Osho, «Modern Education and Computer Science Press,» enero 2016. [En línea]. Available: http://www.mecs-press.org/ijitcs/ijitcs-v8-n1/IJITCS-V8-N1-9.pdf. [Último acceso: octubre 2017].

[4] S. K. H. P. Maleza Jorge, «Repositorio Digital - EPN,» agosto 2012. [En línea]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/4903/1/Estudio%20y%20análisis%20de%20evidencia.pdf. [Último acceso: octubre 2017].

[5] S. S. a. O. P. Anobah, «The Journal of Digital Forensics Security and Law,» 2012. [En línea]. Available: http://ojs.jdfsl.org/index.php/jdfsl/article/view/281/226. [Último acceso: octubre 2017].

[6] W. J. N. C. R. D. Rick Ayers, «Cell Phone Forensic Tools: An Overview and Analysis,» Octubre 2005. [En línea]. [Último acceso: 31 mayo 2017].

[7] C. G. Castro, Analisis y Aplicación de Software para la Recuperación Forense, 2014. [En línea]. Available: http://repositorio.puce.edu.ec/bitstream/handle/22000/6373/9.21.001553.pdf?sequence=4&isAllowed=y. [Último acceso: enero 2016].

[8] Y. L. Li, Estudio y Evaluación de Aplicaciones para el Análisis Forense de Dispositivos Móviles bajo Android en la Ciudad de Ambato, 2013. [En línea]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/4957/1/Seminario_t824si.pdf. [Último acceso: enero 2016].

[9] S. S. a. O. P. Maxwell Anobah, «Academia,» [En línea]. Available: http://www.academia.edu/4697424/Evaluating_and_Comparing_T

ools_for_Mobile_Device_Forensics_using_Quantitative_Analysis. [Último acceso: octubre 2017].

[10] A. Ramos, Historia de la Informática Forense, 25 marzo 2011. [En línea]. Available: http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html. [Último acceso: febrero 2016].

[11] J. S. Cansado, «Hebe Global TECHONOLOGY,» Seguridad Informatica: Análisis Forense de Sistemas, 27 mayo 2015. [En línea]. Available: http://hebeglobal.blogspot.com/2015/05/seguridad-informatica-analisis-forense.html. [Último acceso: febrero 2016].

[12] C. Diaz, «Informática Forense,» Fases de la Informática Forense, [En línea]. Available: http://informaticaforenseunadcd.blogspot.com/p/frases-informatica-forense.html. [Último acceso: febrero 2016].

[13] ISACAC and RSA Conference Survey, «Information Systems Audit and Control Association,» State of Cybersecurity: Implication for 2015, 2015. [En línea]. Available: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf. [Último acceso: 12 mayo 2016].

[14] R. C. D. a. B. A. J. Sean E. Goodison, «Digital Evidence and the U.S. Criminal Justice System,» [En línea]. Available: https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf. [Último acceso: 3 Agosto 2016].

[15] C. Diaz, «Informatica Forense,» Recolección de Evidencia Digital, [En línea]. Available: http://informaticaforenseunadcd.blogspot.com/p/recoleccion-de-evidencia-digital.html. [Último acceso: febrero 2016].

[16] PWC, «PWC,» US cybercrime: Rising risks, reduce readiness, junio 2014. [En línea]. Available: https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf. [Último acceso: 12 mayo 2016].

[17] P. N. d. Ecuador, «Policia Nacional del Ecuador,» [En línea]. Available: http://www.policiaecuador.gob.ec/category/comunicamos/noticias/tungurahua/.

[18] H. A. R. L. Óscar López, «Informática Forense Generalidades, aspectos técnicos y herramientas,» 2010. [En línea]. Available: http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf. [Último acceso: 1 junio 2017].

[19] W. Jansen y R. Ayers, «Forensic Software Tools for Cell Phone Subscriber Identity Modules,» 2006. [En línea]. Available: http://search.proquest.com/docview/211493216/fulltextPDF/E9793C1C73F94460PQ/1?accountid=36765. [Último acceso: 30 mayo 2017].

[20] Oxygen Forensics, Inc, «Oxygen Forensic,» 2014. [En línea]. Available: https://www.oxygen-forensic.com/download/articles/Oxygen_Forensics_Ten_Reasons.pdf. [Último acceso: 20 enero 2017].

[21] COMPELSON Labs, «MOBILedit,» 2017. [En línea]. Available: http://www.mobiledit.com/mobiledit-forensic. [Último acceso: 10 abril 2017].

[22] «ProofPronto.com,» [En línea]. Available: http://www.proofpronto.com/device-seizure-by-paraben.html. [Último acceso: 15 abril 2017].

[23] Paraben Corporation, «Paraben Corporation,» 2016. [En línea]. Available: https://www.paraben.com/downloads/features/DS%20Feature%20Chart.pdf. [Último acceso: 10 abril 2017].

[24] Department of Homeland Security Science and Technology Directorate Cyber, «Test Results for Mobile Device Acquisition Tool: MOBILedit Forensic v8.6.0.20354,» noviembre 2016. [En línea]. Available: https://www.dhs.gov/sites/default/files/publications/MOBILedit%20Forensic%20v8.6.0.20354_Approved_508.pdf. [Último acceso: 20 abril 2017].

[25] COMPELSON Labs, «MOBILedit,» 2017. [En línea]. Available: http://www.mobiledit.com/forensic-express. [Último acceso: 4 abril 2017].

[26] E. Comercio, «El Comercio,» 7 septiembre 2014. [En línea]. Available: http://www.elcomercio.com/actualidad/marcas-telefonos-importadas-ecuador.html. [Último acceso: octubre 2017].

[27] F. G. d. E. Ecuador, «MANUALES, PROTOCOLOS,INSTRUCTIVOS Y FORMATOS DEL SISTEMA ESPECIALIZADO INTEGRAL DE INVESTIGACIÓN MEDICINA LEGAL Y CIENCIAS FORENSES,» 25 agosto 2014. [En línea]. Available: http://www.portal.dnpj.gob.ec/inicio/images/DOC_PUB/planificacion/registro%20oficial%20318.pdf. [Último acceso: 1 agosto 2017].

[28] La Hora, «La Hora,» Se disparan los delitos informáticos, 21 agosto 2011. [En línea]. Available: http://lahora.com.ec/index.php/noticias/show/1101191943#.VzNQnPl9600. [Último acceso: 11 mayo 2016].

[29] J. R. y. J. C. Andrea Ariza, «Facultad de Ingeniería Universidad de la Republica,» iPhone 3G: Un Nuevo Reto para la Informática Forense, [En línea]. Available: http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion6(4).pdf. [Último acceso: 11 mayo 2016].

[30] E. Guanopatín, Propuesta de un Modelo de Análisis Forense a Dispositivos con Sistema Operativo Andorid , mayo 2014. [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/9646/5/T-ESPE-048287.pdf. [Último acceso: enero 2016].

[31] Instituto Nacional de Estadisticas y Censos, «Ecuador en Cifras,» [En línea]. Available: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/Tecnologia_Inform_Comun_Empresas-tics/2012-2014_PRESENTACION_TIC.pdf. [Último acceso: 10 octubre 2017].

ANEXOS

Reportes del Software Paraben:

Reportes del Software MobilEdit: