Limitaciones de las actuales herramientas de análisis digital forense para dispositivos móviles

G. A. Amsler (1), M.E. Casco (2), S. E. Roatta (3)

(1)Facultad Tecnología Informática / Universidad Abierta Interamericana
Ovidio Lagos 934, Rosario, 0341-4356510
santiago.roatta@gmail.com

(2) Dirección de Inteligencia Criminal Estratégica de la Dirección General de Policía de Investigaciones / Ministerio de Seguridad de la Prov. De Santa Fe
Primera Junta 2823, 0342-4505100
mecasco@gmail.com

(3)Facultad Tecnología Informática / Universidad Abierta Interamericana
Ovidio Lagos 934, Rosario, 0341-4356510
santiago.roatta@gmail.com

RESUMEN

Este informe describe la resolución de un problema de ingeniería de la asignatura Seguridad Informática de la Carrera de Ingeniería en Sistemas de la Universidad Abierta Interamericana. El objetivo del trabajo fue realizar una comparación cualitativa y cuantitativa de diferentes herramientas de adquisición de evidencia digital en dispositivos móviles. Las tareas se desarrollaron en el marco de una pasantía de un año realizada en el Laboratorio de Análisis Digital Forense de la Policía de Investigaciones de la Provincia de Santa Fe. En el presente trabajo, en primera instancia, presento un análisis comparativo de herramientas comerciales actuales y una de software libre desarrollada para su aplicación a dispositivos móviles; como así también de los distintos sistemas operativos difundidos en el mercado. Los datos analizados han sido obtenidos de la realidad, proporcionados por seis meses de trabajo pericial de un laboratorio forense, a partir de los cuales realizo una comparación numérica que ilustra el análisis propuesto. Para finalizar la investigación expongo la conclusión a la que he arribado tras el análisis de datos efectuados, permitiendo poner en consideración recomendaciones en base a la productividad generada por las herramientas forenses tras su implementación.

I. INTRODUCCIÓN

La Informática Forense o Análisis Digital Forense es un método probatorio consistente en una colección de evidencias digitales para fines de investigación o legales. Cada caso específico debe ser analizado como si fuera a juicio, así cualquier investigación informática soportará un escrutinio legal. Su propósito consiste en determinar los responsables de los delitos informáticos, esclarecer la causa original de un ilícito o evento particular para que no vuelva a repetirse. La consideración de cada elemento sometido a técnicas de análisis digital forense, como evidencia en un proceso judicial, requiere de asegurar credibilidad por medio de herramientas aceptadas mundialmente el entorno de profesionales reconocidos en el ámbito forense.

Se pone de manifiesto que el Análisis Digital Forense corresponde a un conjunto de principios y técnicas que comprenden el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales, sin alterar su estado original y que llegado el caso puedan ser presentadas en una instancia judicial [1][2]. Esta disciplina es relativamente nueva y se aplica tanto para la investigación de delitos "tradicionales" (homicidios, fraude financiero, narcotráfico, terrorismo, etc.), como para los propiamente relacionados con las tecnologías de la información y las comunicaciones, entre los que destacan piratería de software y comunicaciones, distribución de pornografía infantil, intrusiones y "hacking" en organizaciones, spam, phishing, etc. Por evidencia digital, se entiende a un conjunto de datos, que se encuentren en los soportes físicos, lógicos o sistema de archivos del sistema investigado o atacado.

II. HERRAMIENTAS UTILIZADAS

Existen numerosas herramientas de adquisición de evidencia digital [3][4], entre ellas es posible diferenciar aquellas del tipo comercial (con licencias de renovación periódica) y aquellas herramientas identificadas como software libre (debido al tipo de licencia con la que sus desarrolladores las han creado) como así también las de desarrollo privado o corporativas. Entre las herramientas comerciales de mayor difusión, compuestas por hardware y software específico que existen en mercado actualmente, se puede destacar XRY Office Complete de origen europeo y UFED Touch de fabricación israelí, siendo éstos con los cuales se desarrolla el presente trabajo.

UFED ("Dispositivo de Extracción Universal Forense") es un instrumento que permite obtención y creación de un archivo o colección de ellos con la información de equipos móviles y cualquier dispositivo de almacenamiento de datos. Esta herramienta cuenta con tres versiones: de campo, de laboratorio y para PC.

El fabricante ofrece además otras herramientas de software complementarias como UFED Cloud que permite obtener información de las cuentas asociadas a los dispositivos móviles analizados y datos guardados en la nube una vez realizada la extracción. También puede ampliarse el ambiente de software forense adquiriendo los complementos de análisis y cruce de datos para el trabajo con grandes volúmenes de datos para obtener resultados de extracción de información de varios dispositivos móviles sobre los cuales se deseará determinar la existencia de interacción.

UFED Touch permite además decodificar registros de llamadas, contactos, correo electrónico, bloqueo por patrón revelado de una imagen flash completa, marcadores, cookies SMS, MMS, chats, ubicaciones, historial web, archivos de vídeo, imagen y audio, archivos de texto, datos eliminados, Wi-Fi, Bluetooth e información Geotag.

En la versión de laboratorio, UFED Touch ofrece:

- Extracciones a profundidad, lógicas, físicas, de sistema de archivos y contraseñas, para obtener de datos de evidencias.

- Compatibilidad sin igual con la más amplia gama de los dispositivos móviles principales y versiones de sistemas operativos.

- Tecnología y gestores de arranque propietarios que aseguran extracciones válidas a nivel forense.

- Kit completo de conectores de punta compactos con cuatro cables maestros para extracción y carga durante el uso.

- Pantalla multitáctil de alta resolución e interfaz gráfica de usuario intuitiva.

• Actualizaciones frecuentes del software, que aseguran la compatibilidad con todos los nuevos teléfonos que ingresan en el mercado.

XRY Office Complete es un equipo compuesto por una unidad de hardware y una aplicación de software diseñada para Windows que permite realizar extracciones forenses seguras de los datos de una amplia variedad de dispositivos móviles. Esta extracción se realiza por medio de la conexión de un dispositivo móvil a un equipo de hardware electrónico que cumple las funciones de bloqueador de escritura, luego extrae y genera un archivo contenedor de la información obtenida del elemento analizado, manteniendo los datos inalterados en el dispositivo de origen.

XRY se presenta en cuatro versiones: la de Oficina, que permite a los investigadores acceder a todos los métodos posibles para recuperar datos de un dispositivo móvil; la de Campo, que posee un kit portátil robusto de fácil y rápido manejo, contiene hardware y software combinados para realizar un análisis completo y rápido para la gran mayoría de los dispositivos móviles disponibles en la actualidad; Quiosco, diseñada con un terminal táctil móvil para recuperar rápida y fácilmente datos de dispositivos móviles, está diseñada para realizar extracciones rápidas en un entorno controlado y Tablet, diseñada para realizar extracciones de manera fácil y rápida en cualquier lugar con solo conectar el dispositivo a la herramienta.

Ambas herramientas forenses estudiadas permiten realizar tres tipos principales de extracciones de información, como así también sus componente independiente dentro de cada una de las herramientas, los cuales requieren de su correspondiente licencia según corresponda, resultando 6 extracciones finales [5].

A) Extracción física, que proporciona una copia bit por bit de la memoria del dispositivo móvil, permitiendo no solo la adquisición de los datos existentes, sino también de aquellos ocultos o eliminados.

B) Extracción lógica, consiste en realizar una copia de los objetos almacenados en el dispositivo mientras el mismo se encuentra ejecutando sus funciones normales. Para ello, se utilizan los mecanismos implementados de manera nativa por el fabricante del dispositivo móvil o bien de la herramienta forense, utilizados para sincronizar el terminal con una computadora de modo que se solicita la información deseada al sistema operativo del dispositivo móvil.

A su vez cabe destacar que este tipo de extracción presenta dos opciones, por un lado se presenta la copia de seguridad, la cual realiza una extracción del BackUp de cada aplicación presente que almacene datos en el dispositivo y por el otro agente, el cual realiza un copiado de la información existente en el dispositivo a simple vista, que se realizan sobre el sistema del móvil en ejecución.

C) Extracción de sistema de archivos, permite obtener todos los ficheros del sistema del dispositivo móvil, no incluye archivos eliminados o particiones ocultas, este método posee una complejidad menor que la adquisición física, sin embargo permite recuperar los datos del patrón, pin y/o contraseña de desbloqueo en algunas marcas y modelos determinados de dispositivos móviles.

Para llevarlo a cabo se aprovecha de los mecanismos integrados en el sistema operativo para realizar el copiado de los ficheros, Android Device Bridge (ADB) en el caso de Android. Mediante este método es posible recuperar cierta información eliminada ya que algunos sistemas operativos como es el caso de Android e iOS se valen de una estructura que utiliza bases de datos SQLite para almacenar gran parte de la información. De este modo, cuando se eliminan registros

de los ficheros, únicamente se marcan como disponibles para sobrescritura, por lo que temporalmente siguen estando disponibles y por tanto es posible recuperarlos.

Cabe resaltar que la herramienta posee diversos subtipos de extracción de Sistema de Archivo, como ser:

- Sistema de Archivo, antes mencionado.
- Sistema de Archivo con desbloqueo, el cual es posible realizar una recuperación de los datos incluyendo del bloqueo que posea el dispositivo.
- Sistema de Archivo con Doungrade App, el cual realiza un copiado similar al de Copia de Seguridad mencionado con antelación. -

De acuerdo a lo mencionado cabe resaltar los complementos correspondientes a las herramientas:

D) Nube (Cloud) Mediante el complemento UFED Cloud o XRY Cloud es posible, recuperar información que se encuentra almacenada en la nube una vez realizada la extracción al dispositivo sin posesión física real del dispositivo móvil, ya que utiliza los tokens que utilizan los móviles para almacenar usuarios y contraseñas. Esto es particularmente útil cuando se buscan datos de medios sociales en línea y la información basada en aplicaciones para servicios como Facebook, Google, iCloud, Twitter, Snapchat, WhatsApp, Instagram y más.

E) PinPoint (PinPoint): esta herramienta es una solución avanzada compuesta de hardware y software. Permite a los usuarios extraer y descodificar datos de dispositivos móviles no estándar, generalmente estos son teléfonos “imitación” chinos. Esta solución está compuesta por un potente software que detecta automáticamente la configuración de pin-out y el hardware compacto, siendo requerida una licencia separada con permanente actualización.

XRY PinPoint está completamente integrado y utiliza la familiar y fácil de usar interfaz XRY Logical / Physical, pero requiere una licencia separada. Se actualiza continuamente para que se mantenga actualizado y mejore con el tiempo.

F) Cámara (Camera): Permite a los examinadores forenses capturar imágenes de dispositivos móviles y capturas de pantalla relevantes para complementar sus extracciones digitales.

SANTOKU Software dedicado al análisis y seguridad móvil, y está empaquetado en una plataforma de código abierto de fácil uso. Especializada en pruebas de seguridad, análisis de malware y análisis forenses para teléfonos móviles, válida para dispositivos con Android, BlackBerry, iOS y Windows Phone.

Es una distribución de linux desarrollada, para auditar celulares moviles a fin de captar vulnerabilidades y/o fallas. Además se utiliza para realizar análisis forenses. Cuenta con mucho software para llevar acabo todas las tareas, por ejemplo las herramientas de desarrollo son Android SDK Manager, Android Studio, Eclipse, FastBoot, SBF Flash, ACML Printer2, Heimdall y Google Play API. Para penetration testing incluye Zenmap, Nmap, Burp Suite, w3af Console/GUI, Ettercap, Zap, y SSLStrip. Las de análisis forense son Android Brute Force Encryption, Scalpel, Yaffey, ExifTool, Sleuth Kit, Iphone Backup Analuzers y AFLogical Open Source Edition. Las herramientas para ingeniería inversa son Jasmin, AndroGuard, radare2, Bulb Security SPF, JD-UI, Smali, Drozer, Baksmali, APKTool, Procyon, dex2jar y AntiVL.

Así mismo trae incorporada la herramienta denominada VIAEXTRACT; Es una herramienta de extracción lógica y física creada por NowSecure (antes conocido como ViaForensics). Permite en su versión libre, extraer toda información disponible a nivel lógico (incluyendo copias de

seguridad), mientras que la versión de pago agrega extracciones físicas. Se distribuye libremente dentro de un archivo de la máquina virtual (VMWare o formatos de la caja virtual) que funciona la distribución de Santoku Linux de NowSecure. Siendo requerida una conexión a Internet activa mientras se usa la versión gratuita.

III. SISTEMAS OPERATIVOS ANALIZADOS

Entre los diversos dispositivos que hoy día existen en circulación, encontramos diversos sistemas operativos móviles: Android, iOS, Windows Phone y Blackberry OS.

A) Android es un sistema operativo basado en Linux y diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tablets o tabléfonos; y también para relojes, televisores y automóviles inteligentes. Actualmente su sistema operativo se encuentra en la versión 7.1, conocida como Nougat. B) iOS es un sistema operativo móvil del tipo comercial desarrollado por Apple Inc. Originalmente utilizado para iPhone (iPhone OS), después aplicado a dispositivos tales como iPod touch y iPad. Su instalación sólo se ajusta a hardware de Apple Inc. Actualmente se encuentra en la décima versión, conocida como iOS 10. C) Windows Phone es un sistema operativo móvil desarrollado por Microsoft, como sucesor de Windows Mobile. A diferencia de su predecesor está enfocado en el mercado de consumo en lugar del mercado empresarial. Actualmente su sistema operativo se encuentra en la versión 10, diseñado para teléfonos inteligentes y tabletas, forma parte de las ediciones de Windows 10 y es sucesor de Windows Phone 8.1. Por último, D) Blackberry OS, que si bien es un sistema operativo conocido desde hace varias décadas, aún se encuentran dispositivos en el mercado, es de código cerrado únicamente para los dispositivos BlackBerry. Idéntica filosofía comercial que la expuesta para iOS. Actualmente su sistema operativo se encuentra en la versión 10.3.1.

IV. TAREAS REALIZADAS

Este trabajo fue posible gracias a una pasantía que realicé en la Dirección de Inteligencia Criminal de la Provincia de Santa Fe, cuyas herramientas de análisis forense fueron aplicadas para generar los datos que se exponen a continuación.

Durante ese transcurso del año 2016, desarrollé peritajes de dispositivos móviles y de almacenamiento a solicitud del Poder Judicial de la Provincia de Santa Fe. Para dar cumplimiento a los requerimientos judiciales se aplicaron las siguientes herramientas de hardware y software: UFED Touch, XRY Office Complete y Santoku Linux.

El proceso pericial aplicado en el laboratorio siguió los lineamientos recomendados por la Norma ISO/IEC 27.042:2015 (que proporciona orientación sobre el análisis e interpretación de la evidencia digital abordando cuestiones de continuidad, validez, reproducibilidad y repetibilidad. Incluye mejores prácticas para la selección, diseño e implementación de procesos analíticos y registro de información suficiente para permitir que tales procesos sean sometidos a un escrutinio independiente cuando sea necesario. Proporciona orientación sobre los mecanismos apropiados para demostrar competencia del equipo de investigación).

Los datos que fui recaudando son resultado de pericias realizadas por el laboratorio durante el año 2016, ascendiendo a un total general de 223 requerimientos judiciales para la aplicación de técnicas de análisis digital forense sobre un total general de 1034 dispositivos peritados, se toma una muestra de 20 requerimientos judiciales cumplimentados con la pericia de un total de 204 dispositivos que conforman la fuente de información utilizada para la elaboración del presente

análisis. Para lograr concretar el proceso de extracción forense fue imprescindible tener en cuenta el sistema operativo del dispositivo.

En Android es necesario habilitar el modo desarrollador y activar la depuración USB para facilitar que el equipo forense establezca conexión con el dispositivo móvil analizado. Un impedimento a solucionar son los dispositivos con patrón, contraseña, pin, huella dactilar o algún otro sistema de desbloqueo de pantalla. En estos casos es posible que las herramientas de extracción mediante su función de desbloqueo logren quitar el mismo (si la marca y modelo del dispositivo cuenta con esta opción habilitada en UFED Touch o XRY Office Complete) y en otros casos, mediante el tipo de extracción de sistema de archivos, sea obtenido el registro del patrón, pin o contraseña. En caso que la marca y modelo del dispositivo no contaran con la opción programada, las herramientas comerciales, permiten efectuar extracciones forenses para Android genéricos en cuyo caso se inicia una extracción física o de sistema de archivos con desbloqueo incluido, por medio del acceso vía bootloader.

En Windows Phone no es posible una conexión entre el sistema del dispositivo móvil y el de la unidad de extracción forense, y es tratado como un dispositivo de almacenamiento (pendrive, tarjeta de memoria, etc) En algunos modelos las herramientas permiten la obtención de registros de SMS y alguna información de llamadas entrantes y salientes. El desbloqueo de pantalla por medio de las herramientas no es posible.

En los dispositivos móviles con BlackBerry OS se presentan los mismos impedimentos que se describen para Windows Phone. Ambos sistemas son de código cerrado, propiedad de las empresas desarrolladoras, siendo posible realizar solo si este se encuentra desbloqueado una extracción de tipo lógica con la herramienta XRY o UFED Touch, facilitando esta última una extracción de tipo Física con un solo modelo de dicha marca.

Finalmente, en iOS se presenta la dificultad descripta para Windows Phone y BlackBerry OS respecto de la posibilidad de desbloqueo de pantalla, no es posible hasta el momento, sin embargo, si un dispositivo con sistema iOS se encuentra desbloqueado, en algunos casos permite obtener extracciones forenses del tipo física, recuperando datos eliminados y aquellos existentes al momento de la extracción y, en otros, sólo posibilita el acceso a los datos existentes mediante una extracción lógica.

Además, existen dispositivos encriptados para los cuales no se han desarrollado opciones hasta el momento entre las disponibles, en las herramientas forenses del mercado. Así también, es posible hallar los denominados “teléfonos móviles seguros”, un dispositivo de comunicación privada que cuenta con consola administrativa y entre otras funciones permite Remote Wipe (Borrado remoto del teléfono). Este tipo de dispositivo no cuenta con posibilidades de acceso mediante las herramientas forenses actuales.

Realizada las tareas mencionadas con las herramientas comerciales, se procede a realizar la correspondiente comparación con el software libre, siendo instalada la distribución SANTOKU en un dispositivo portátil, dentro de una partición de disco de 25 Gb. Si bien el peso del sistema operativo es menor a 3 Gb, se recomienda reservar algo de espacio para el correcto uso de las herramientas forenses. La instalación se puede realizar con la interfaz gráfica de la distribución UBUNTU, por lo cual es sencilla y amigable.

Se corre SANTOKU su distribución básica, sin incluir alguna aplicación adicional según lo indican las instrucciones de instación, AFLogical OSE, programa integrado que contiene esta distribución, se descarga el SDK (Software Developer Kit) correspondiente a la versión de

Android que dispone el celular, y se enchufa el dispositivo mediante cable USB, directo a la pc portátil para a posterior ejecutar la extracción. Al momento de que la misma se corre, observo que dicha aplicación instala dentro del celular un programa que permite elegir los datos a obtener; los mismos son Mensajes SMS, Llamadas, Contactos, Información del Dispositivo.

Finalizada la extracción los registros obtenidos se almacenan dentro de la memoria SD, con formato de archivo XML.

Se debe tener en cuenta que si el dispositivo presenta clave de bloqueo, la misma puede ser obtenida mediante línea de comandos de consola realizando un ataque de fuerza bruta con uso de diccionario.

V. DESCRIPCIÓN DE RESULTADOS

Retomando el análisis numérico de la muestra, en las siguientes tablas se expresa el ingreso al laboratorio de dispositivos discriminados por Sistema Operativo e indicando el porcentaje de extracciones exitosas concretadas por las herramientas de análisis forenses estudiadas.

En la tabla 1 se puede apreciar según discriminación de sistema operativo, la cantidad parcial y total de dispositivos extraídos con éxito con cada una de las herramientas comerciales y así mismo con la herramienta de software libre.-

Tabla 1

Dispositivos Analizados con cada Herramienta Forense

S.O	DISPOSITIVOS TOTAL	UFED	XRY	SANTOKU
Android	169	166	159	3
Windows Phone	18	10	9	
BlackBerry	5	3		
iOS	12	5		1
TOTALES	**204**	**184**	**168**	**4**

En las tablas siguientes se realiza una discriminación según tipo de extracción de cada herramienta y su resultado con éxito de acuerdo al sistema operativo soportado en cada una de ellas.-

Tabla 2

Comparación según Extracción por Sistema Operativo con Herramienta UFED Touch

HERRAMIENTA UFED TOUCH				
S.O	DISPOSITIVOS TOTAL	EXT FÍSICA	EXT LÓGICA	SIST. DE ARCHIVO
Android	169	140	169	100
Windows Phone	18	7	18	
BlackBerry	5	1	5	
iOS	12	6	6	1
TOTALES	**204**	**154**	**198**	**101**

Tabla 3

Comparación según Extracción por Sistema Operativo con Herramienta XRY

HERRAMIENTA XRY COMPLETE				
S.O	DISPOSITIVOS TOTAL	EXT FÍSICA	EXT LÓGICA	EXT LÓGICA AGTE-C. SEG
Android	169	155	169	160
Windows Phone	18	1	18	
BlackBerry	5		5	
iOS	12	1	1	
TOTALES	**204**	**157**	**193**	**160**

Tabla 4

Comparación según Extracción por Sistema Operativo con Software Santoku

HERRAMIENTA SANTOKU				
S.O	DISPOSITIVOS TOTAL	EXT FÍSICA	EXT LÓGICA	
Android	169		3	
Windows Phone	18			
BlackBerry	5			
iOS	12		1	
TOTALES	**204**		**4**	

En las tablas antes expuestas se muestran los resultados con las diversas herramientas forenses basados en casos reales del año 2016.

VI. DISCUSIÓN DE RESULTADOS

De acuerdo a lo antes expuesto en cada una de las tablas resulta de ellas que las marcas Samsung y LG permiten obtener registros abundantes, tanto datos existentes como borrados, estando bloqueados o no; posibilitando la concreción de extracción física con ambas herramientas comerciales (UFED - XRY), resultando sólo aquellos dispositivos marca Samsung con Santoku Linux, una extracción escueta y de tipo lógica.

Haciendo referencia a otras marcas difundidas en el mercado local, Motorola, presenta dificultades si se presenta bloqueo de pantalla, y en caso de contar con acceso al sistema permite configurarlo para obtener una extracción lógica. En algunos casos, es necesario completar algunos requisitos de los equipos forenses con el fin de obtener una extracción física, sin embargo, los dispositivos cuentan con fastboot bloqueado de fábrica impidiendo establecer conexión entre el dispositivo y el equipo forense utilizado. Los modelos con función Handy, del tipo iDen, para servicios de radiotelefonía, no son compatibles con las herramientas y no son detectados como dispositivos móviles, siendo necesario la utilización de la cámara USB UFED.

Aquellos dispositivos con sistema Operativo Microsoft, solo hacen posible realizar con las herramientas comerciales una extracción de tipo lógica solo obteniendo de ello resultados de memoria externa, no así lo almacenado en memoria interna del dispositivo.

Finalmente los dispositivos iOS, en la medida que ellos se encontraron desbloqueados (sin su pin de bloqueo) fue posible realizar una extracción de tipo lógica recuperando una moderada cantidad de información presente en el dispositivo, no así lo almacenado en la nube.

Como resultado de los sistemas operativos antes mencionados, respecto del software SANTOKU, se observa que a pesar de identificarse como compatible no se obtuvo un resultado positivo, observando que para la mayoría de las acciones requieren de los complementos adicionales para obtener alguna respuesta.-

Efectuando una comparación con las diversas herramientas comerciales y aquellas de software libre, solo hace posible una extracción lógica de dispositivos Samsung que poseen sistema operativo Android y dispositivos con sistema operativo iOS. Para lograr una extracción tipo física y ampliar la compatibilidad a otros sistemas operativos es necesario adquirir entre otros, un módulo comercial del software VIAEXTRACT, el cual requiere de la obtención de una licencia paga, no siendo posible obtener a simple instalación de la distribución el acceso a la totalidad de los datos como es difundido en su plataforma oficial.-

Por otra parte las herramientas comerciales, a pesar de no tener todos sus complementos, permiten un mayor margen de reconocimiento de dispositivos, como así también la obtención de una amplia información de cada uno de ellos, incluyendo datos eliminados adrede.

Cabe resaltar que las mencionadas herramientas comerciales, sin sus complementos antes mencionados tienen un costo que se aproxima a los U$360.000 ambas, sumando a ello cada complemento adicional, que uno quiera acceder, contemplando sus renovaciones anuales, no siendo obligatorio la compra de la totalidad de ellos y obteniendo grandes resultado simplemente con cada una de las herramientas en su versión principal.

Ambas herramientas comerciales, brindan un soporte postventa, como así también la entrega a cada cliente de todas las actualizaciones existentes con el paso del tiempo, las cuales se van efectuando a medida que se actualizan los dispositivos móviles, las cuales incorporan mayor franja de reconocimiento de dispositivos, tipos de extracción de los dispositivos, y actualización con cada uno de los Sistemas Operativos existentes en mercado.- La única desventaja es la dependencia constante de una licencia comercial de renovación periódica y la inminente caducidad de la vida útil del hardware forense cuya obsolescencia se pone en evidencia ante la constante actualización tecnológica.

Haciendo referencia a la distribución de Linux, que si bien se resalta que su versión es gratuita, la instalación de cada complemento requiere un costo mucho menor y más accesible a quienes presentan la necesidad de obtener información con un caudal inferior a un Laboratorio de Analisis Oficial, y prueba en su implementación y aplicación.-

A diferencia de las herramientas comerciales, esta distribución, no ofrece un soporte ni actualizaciones al alcance de cada usuario, siendo necesario por cada uno de ellos, la búsqueda y adaptación de actualizaciones de drivers según lo requiera y/o exista, por otra parte requiere mayor tiempo de instalación, oportunamente más complicado que una distribución comercial, siendo necesario el conocimiento de programadores para tal configuración.-

VII. CONCLUSIONES

La conclusión más evidente es que la actualización de licencias y software forense se efectúa al mismo ritmo con el que las terminales presentan sus nuevos teléfonos, de esta manera se mantiene la compatibilidad entre las marcas y modelos de dispositivos móviles más difundidos en el mercado local. Puedo resaltar a modo de ejemplo que la versión nueva y mejorada del UFED Touch es tres veces más rápida que la versión anterior, ofreciendo una gama de capacidades mejoradas diseñadas para aumentar el rendimiento, la facilidad de uso y la portabilidad.

La conclusión más relevante es -tal como muestran las tablas que las actuales herramientas de extracción de evidencia de dispositivos móviles y de almacenamiento de datos tienen sus limitaciones: algunos teléfonos no pueden ser peritados.

Finalmente cabe destacar que las herramientas comerciales no se presentan adecuadas para los peritos particulares porque son accesibles sólo a fuerzas de seguridad o poder judicial debido a su alto costo como ya fue mencionado con antelación. Son recomendables sólo en caso de contar con una fluida demanda pericial que requiera un mayor rendimiento (obviamente un menor tiempo para cada pericia permite realizar mayor cantidad de pericias).

Debido a lo antes expuesto, y en vista que la accesibilidad a las herramientas comerciales no es imposible para aquel que su uso pueda amortizar de acuerdo a la cantidad de pericias por dia para a realizar, como así también solventar todos sus costos; Se aconseja para peritos particulares no

descartar la implementación software opensource, como Santoku Linux u otras herramientas de software libre y sus complementos más accesibles al momento de ser gestionada su licencia, más alla de los resultados antes expuestos, los cuales no son alentadores, pero así y todo no presentan malas repercusiones de quienes lo implementan; Para quienes de forma habitual no tienen un caudal de pericias diarias, ni ellas son de alta trascendencia al requerir determinadas condiciones de seguridad, sino que ellas se efectúan de forma más prolongadas, como tengo conocimiento que hay (se reciben uno o dos dispositivos cada dos meses o mas) mayor libertad para el perito de configurar la máquina habilitada para realizarla pericia con los complementos y driver necesarios de forma manual para acceder a los datos de los dispositivos.-

VIII. BIBLIOGRAFÍA

[1] Lee Reiber, (2016), Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation. 1st Edition. Ed. McGraw-Hill Professional Publishing. ISBN 9780071843638. Developing Process for Mobile Device Forensics; C. A. Murphy

[2] Ayers, R., Dankar, A. & Mislan, R. (2009). Hashing Techniques for Mobile Device Forensics. Small Scale Digital Device Forensics Journal ,1-6.

[3] Brothers, S. (2011). How Cell Phone "Forensic" Tools Actually Work - Cell Phone Tool Leveling System. DoD Cybercrime

Conferece. 2011. Atlanta, GA

[4] Guide for Mobile Phone Seizure and Examination. APCO Good Practice Guide for Computer Based Electronic Evidence – Official Release Version 4.0, 45-51.

[5] Katz, Eric, "A Field Test of Mobile Phone Shielding Devices" (2010).College of

Technology, Purdue University.