Metodología de análisis forense orientada a incidentes en dispositivos móviles

***Diego Pinto*[1,2]**
[1] Universidad de las Fuerzas Armadas - ESPE, Departamento de Ciencias de la Computación, Sangolquí, Ecuador.
[2] Universidad de las Américas - UDLA, Facultad de Ingeniería y Ciencias Agropecuarias, Quito, Ecuador.

Autores para correspondencia: pintoauz@hotmail.com, djpinto@espe.edu.ec

Fecha de recepción: 21 de septiembre de 2014 - Fecha de aceptación: 17 de octubre de 2014

RESUMEN

En el presente artículo se tratan temas relacionados con el análisis forense aplicado a dispositivos móviles, así como la propuesta y prueba de una metodología que apoye efectivamente estas actividades. Se describen los objetivos a seguir en dicho estudio, y se plantea la búsqueda de evidencia almacenada en los dispositivos móviles bajo un escenario en el que se ha cometido un delito. Se hace énfasis en la evolución y multiplicidad de usos que poseen actualmente los dispositivos; y finalmente se aborda la necesidad de tener estándares que permitan garantizar la integridad de las evidencias encontradas, para ello se describe la metodología desarrollada, la cual permite realizar de manera adecuada el proceso forense sobre dispositivos móviles, por lo que se aspira a que se constituya en un estándar para realizar este tipo de investigaciones.

Palabras clave: Dispositivos móviles, forense en celulares, teléfonos inteligentes, evidencia digital, derecho informático, metodología, análisis forense, informática forense.

ABSTRACT

The article addresses issues related to forensic analysis applied to mobile devices, as well as a proposal and test of a methodology that effectively support these activities. We describe the objectives of the study, and the search for evidence stored on mobile devices under a scenario in which a crime has been committed. Emphasis is on the evolution and multiplicity of uses currently on devices, and finally addresses the need for standards to ensure the integrity of the found evidence, describing the methodology developed which enables the complete forensic process on mobile devices. The presented approach could establish itself as a standard for this type of research.

Keywords: Mobile devices, forensic phones, smartphones, digital evidence, computer law, methodology, forensics, computer forensics.

1. INTRODUCCIÓN

Las tareas de análisis forense (Lázaro, 2013) en dispositivos móviles pueden volverse en muchas ocasiones una ardua labor, y bajo ciertas circunstancias como: condiciones internas de la organización, falta de conocimiento o inexistencia de estándares o buenas prácticas; y condiciones como: el desconocimiento o falta de leyes, hacen que el estudio se pueda volver incluso imposible.

Esta imposibilidad no siempre viene determinada por la capacidad técnica sino por los requisitos legales exigibles a las evidencias (Acurio, 2009) que procedan de este tipo de dispositivos. Por ejemplo una de las condiciones clave en la recolección de evidencias es la asepsia, práctica que asegura que las pruebas recogidas no estén contaminadas, y que por tanto sean válidas para ser

utilizadas en procesos judiciales, siguiendo una rígida cadena de custodia en todos sus pasos y complemente documentada.

En otras ocasiones las dificultades sí están causadas por aspectos técnicos, ya que para conservar adecuadamente una prueba esta debe ser previamente recolectada con éxito, es decir efectuar la recolección de evidencias bajo parámetros legales así como en la forma de proceder para su recolección, lo que garantiza la integridad de las evidencias; teniendo como principal inconveniente la inexistencia de un estándar mundial que rija este tipo de tareas. Otro aspecto a considerar es la multiplicidad de marcas y sistemas operativos de los dispositivos móviles. Esto lleva a dejar insubsistente la evidencia recopilada sea por vacíos normativos o por la pérdida de integridad de la información por la inadecuada manipulación de la misma.

El Análisis Forense Digital (Ariza & Ruíz, 2009) es un campo de investigación excitante y dinámico que tiene cada vez más un poderoso impacto en una variedad de situaciones, incluyendo ambientes corporativos, investigaciones internas, litigación civil, investigaciones criminales, investigaciones de inteligencia, e incluso asuntos de seguridad nacional. El Análisis Forense en dispositivos móviles es sin duda el de mayor crecimiento y desarrollo en la disciplina forense digital, y ofrece ventajas significativas así como también muchos retos.

1.1. Problemática actual

Los dispositivos móviles a medida que pasa el tiempo son indispensables para la comunicación y manejo de información a nivel mundial. De igual manera como paso con las computadoras, estos dispositivos han dejado de ser un lujo para convertirse en una necesidad; la brecha y funcionalidad entre los dispositivos se ha vuelto cada vez más delgada, siendo actualmente una distinción únicamente el tamaño, si hablamos por ejemplo de las tablets y los smartphones. La mayoría de estos dispositivos cuentan con funciones entre las que encontramos: el envío de mensajes de texto cortos (SMS), mensajes de texto multimedia (MMS), mensajes instantáneos (IM), correos electrónicos tanto en cuentas corporativas como personales, acceso a Internet, administrar información personal, cámaras fotográficas sofisticadas, conexión en la nube con ayuda de ciertas aplicaciones, localizadores geo referenciales, videoconferencia, entre muchas otras; todo esto se traduce en más poder para capturar, mantener, acceder y modificar información.

Cuando un dispositivo móvil está involucrado en un delito o en un incidente se debe analizar y tomar en cuenta que el dispositivo contiene información personal, laboral, e incluso puede reflejar costumbres o hábitos de la persona, convirtiéndose así en información muy sensible para ser tomada para una investigación.

Para realizar una investigación, los analistas forenses requieren seguir una metodología adecuada, una cadena de custodia bien definida, normas de preservación de evidencia físicas (por ejemplo huellas dactilares en el dispositivo), así como evidencias digitales que pueden ser recogidas a través de herramientas que permitan obtener una apropiada y rápida recuperación de la información almacenada en el dispositivo. La información obtenida será analizada, y servirá para redactar un reporte detallado de las actividades efectuadas, con la finalidad de buscar evidencias que revelen la causa y forma en la que se llevó a cabo un posible delito; en algunos casos ésta información puede obtenerse incluso luego de haber sido borrada del dispositivo.

El poseer dispositivos móviles incrementa la frecuencia con la que se navega por la red, ya sea utilizando planes de datos, redes inalámbricas tanto corporativas como en el hogar, permitiendo el uso de redes sociales, transacciones bancarias, etc., lo que causa el incremento de vulnerabilidades. La problemática se incrementa al poder elegir entre las miles de aplicaciones gratuitas de proveedores de aplicaciones legítimos y externos. Sin embargo, descargar aplicaciones gratuitas suele tener un precio: servicio gratuito a cambio de información personal, se solicitan registros con ingreso de datos personales en formularios para acceder al servicio. Estadísticas muestran que la mayoría de consumidores (73%) están dispuestos a facilitar información personal si reciben algo a cambio, por ejemplo: algún servicio para móviles gratuito.

Por último hay que tomar en cuenta estadísticas que indican que tres de cada cuatro empresas permiten a sus empleados utilizar dispositivos personales tales como: portátiles, mini portátiles, smartphones y tablets, para actividades relacionadas con el trabajo, sin contar con normas y políticas

de seguridad adecuadas. Esta tendencia continúa en expansión y motiva a los ciberdelincuentes a traspasar sus defensas para acceder a información personal y laboral.

1.2. Estado del arte

El análisis forense digital tradicionalmente involucra las siguientes fases: identificación, preservación (no modificar la evidencia), obtención, documentación y análisis de la información. Existen ciertas metodologías y procedimientos bien definidos que pueden ser adaptados al análisis forense en dispositivos móviles. Dichas metodologías consisten generalmente en la ejecución de los siguientes puntos:

- Preparar una copia de la evidencia digital.
- Examinar la copia obtenida con la finalidad de recuperar la información.
- Analizar la información recuperada.
- Crear un reporte describiendo los datos obtenidos en el procedimiento de análisis.

Las herramientas (Larry & Lars, 2012) de análisis forense intentan facilitar el trabajo en cada uno de estos pasos, enfocados hacia la generación de un reporte final veraz y de calidad, que permita revelar detalles de actividades realizadas en el dispositivo móvil, contestando las mismas preguntas en las que se basa el análisis forense clásico: ¿qué se hizo?, ¿cómo se hizo? y ¿cuándo se hizo? (Cano, 2009).

Existen diferencias entre el análisis forense sobre dispositivos móviles y el análisis forense de computadoras, debido a varios factores entre los que se incluyen:

- El diseño orientado a la facilidad de transporte.
- Almacenamiento en una memoria volátil contra memorias no volátiles.
- La facilidad de acceso para modificar o eliminar remotamente la información.
- El comportamiento de hibernación, la suspensión de procesos cuando se apaga y se vuelve a activar el dispositivo.
- Los diversos tipos de seguridad que poseen los dispositivos móviles.
- La diversidad de sistemas operativos embebidos (Hoog, 2011).
- Ciclos cortos de producción para introducir nuevos dispositivos móviles con mayores prestaciones y nuevas funcionalidades.
- Riesgos de seguridad por la cantidad de aplicativos existentes.

Estos factores muestran la necesidad de investigar nuevas propuestas en el campo de la informática forense relacionada con dispositivos (Ariza *et al*., 2009).

Entre las metodologías existentes podemos citar:

Metodología del Departamento de Justicia (DOJ) de los Estado Unidos

El modelo del DOJ (Eloff *et al*., 2008) no hace distinción entre los métodos forenses aplicados a computadores o a algún otro dispositivo electrónico. Intenta construir un modelo general para aplicarlo a la mayoría de dispositivos electrónicos. Se ha desarrollado un análisis de la metodología en la Tabla 1.

Tabla 1. Metodología DOJ.

Particularidades	Ventajas	Desventajas
Especifica un flujo bien definido para la realización de cada una de las etapas que propone	Es muy claro el procedimiento que se debe de seguir gradas al diagrama de flujo que proporciona para cada una de las etapas.	No cubre las etapas generales necesarias para realizar una investigación forense. Se enfocada a la investigación de computadoras que cuenten con un sistema operativo Windows. No propone metodologías para realizar análisis en grandes volúmenes de información. No se establece una cadena de custodia. No da resultados para mejorar el sistema.

Metodología del Instituto SANS

El instituto SANS (Sans, 2011) es una organización cooperativa de investigación y educación para profesionales de la seguridad. El manejo adecuado de una investigación forense es clave para luchar contra los delitos informáticos, requiriendo un profundo conocimiento de muchas áreas para una investigación adecuada. El análisis de la metodología se lo puede observar en la Tabla 2.

Tabla 2. Metodología SANS.

Particularidades	Ventajas	Desventajas
Formatos para establecer la cadena de custodia. Define lugares en donde se puede encontrar información oculta dentro de los sistemas operativos Windows y Linux.	Cubre con todas las etapas para hacer una investigación forense. Toma en cuenta el cuidado de la cadena de custodia.	No propone métodos para realizar la adquisición de evidencia de grandes volúmenes de datos. No propone métodos de análisis para volúmenes grandes de datos. Es específica para dispositivos que cuenten con sistemas operativos Windows o Linux. Esto deja fuera la posibilidad de que se pueda aplicar está metodología en dispositivos móviles.

Digital Forensics Research Workshop (DFRW)

DRFW (Carrier & Spafford, 2004; DFRW, 2001) es un grupo dirigido por la academia más que por el mundo legal, ayuda a definir y enfocar la dirección de la comunidad científica en relación al análisis forense digital. Un análisis de la misma lo podemos ver en la Tabla 3.

Tabla 3. Metodología DFRW.

Particularidades	Ventajas	Desventajas
Provee una lista de los lugares más comunes en los que se puede encontrar información oculta. Provee métodos y actividades para la localización de información oculta.	Cubre con todas las etapas requeridas para hacer una investigación forense. Define todo el universo de dispositivos y plantea formas que puedan ser analizadas dentro de una investigación de cómputo forense. Enfocada a conservar la integridad y mantener la cadena de custodia. Considera técnicas para la extracción de datos ocultos. Considera métodos para el análisis de grandes volúmenes de información. Es una metodología que se encuentra en constante actualización.	No propone un procedimiento específico para la realización de las actividades

Kevin Mandia y Chris Prosise

Mandia & Prosise (2003) definen el proceso de análisis forense como una metodología de respuesta a incidentes, un análisis sobre la misma podemos ver en la Tabla 4.

Tabla 4. Metodología Kevin Madia y Chris Prosise.

Particularidades	Ventajas	Desventajas
Propone un paso llamado pre-preparación en el cual el grupo encargado de reaccionar ante un incidente se anticipa a ellos preparando las herramientas	Cumple con todas las etapas generales de una investigación forense. Proporciona métodos para realizar	No propone métodos para el análisis de grandes volúmenes de información. Está enfocada para la investigación de plataformas

necesarias y conocimientos de la infraestructura. Proporciona una lista de los principales ataques que se presentan hacia una computadora y recomienda una estrategia de respuesta.	el análisis de datos.	Windows NT/2000, UNIX y routers Cisco. Dejando fuera todos los dispositivos que utilicen una plataforma diferente, y deja de lado cualquier otro dispositivo periférico y digital.

2. METODOLOGÍA Y MATERIALES

Dentro del análisis forense no existe una metodología universal que nos permita llevar a cabo una investigación, por tal motivo se decidió realizar el estudio de varias metodologías. A partir de ellas se escogió lo mejor de cada una, y alineado a las condiciones de la tecnología se desarrolló una propia.

Además se obtuvieron indicadores que sustentan la investigación, para lo cual se realizaron encuestas a oficiales de seguridad encargados de asesorar áreas y proyectos relacionados con Seguridad de la Información, Auditoría de Sistemas, Gestión de proyectos de Tecnologías de Información de instituciones públicas y privadas del Ecuador.

El cuestionario constó de 36 preguntas lo que permitió obtener 14 indicadores relacionados con: (i) evidencia digital e incidentes con dispositivos móviles, (ii) informática forense y metodologías en dispositivos móviles, (iii) seguridad informática y formación profesional; indicadores que sustentan el planteamiento del tema, así como el de la metodología propuesta.

Dentro de los resultados obtenidos podemos indicar:

- El 90% no conoce sobre procedimientos formales para administración de evidencia digital; y
- El 85% no conoce sobre metodologías relacionadas con informática forense para dispositivos móviles.

Otro indicador que sustenta la investigación está relacionado con los incidentes en los que intervienen dispositivos móviles (ver Fig. 1).

Con los indicadores hallados se evidencia que el 25% de la inversión dentro del área de seguridad informática está relacionada con la seguridad en dispositivos móviles, pero en lo referente al análisis forense tanto de computadores como de dispositivos móviles es del 0%.

Se realizó un análisis comparativo de las metodologías existentes versus las fases tradicionales del análisis forense digital (ver Tabla 5).

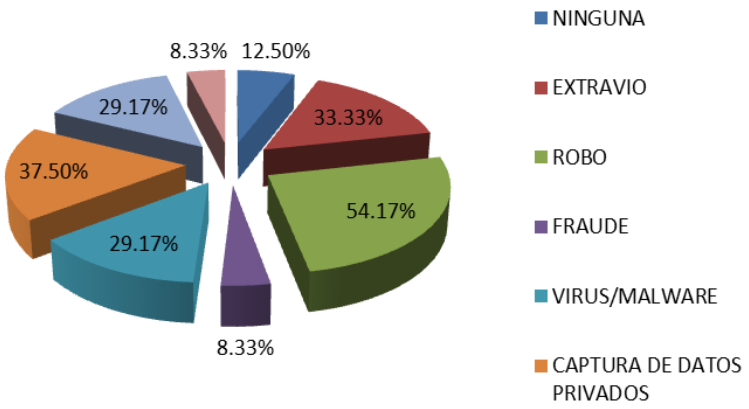

Figura 1. Incidentes de seguridad que involucran dispositivos móviles.

Posteriormente se efectuó una comparación entre 4 de ellas (ver Tabla 6), mismas que son las de mayor aceptación, difusión y creadas por instituciones que han alcanzado un reconocimiento internacional en el campo del Cómputo Forense.

Tabla 5. Análisis comparativo metodologías vs. Fases del análisis forense.

Etapas de la Investigación	Metodologías						
	Brian Carrier y Eugene Spafford	SANS	DOJ	DFRW	Reith, Carr y Gunsch	Mandia/ Prosise	Casey
Identificación		✓	✓	✓		✓	✓
Recolección	✓	✓	✓	✓	✓	✓	✓
Análisis	✓	✓	✓	✓	✓	✓	✓
Presentación	✓	✓		✓		✓	✓

Tabla 6. Análisis comparativo de metodologías.

Etapas de la investigación	Metodologías			
	SANS	DOJ	DFRW	Mandia y Prosise
Cubre con todos los pasos generales para realizar una investigación de cómputo forense	✓		✓	✓
Implementación en todos los dispositivos			✓	
Manejo de grandes volúmenes de información.			✓	
Respuesta a las técnicas para ocultar datos	✓		✓	✓
Procedimientos para la realización de actividades				

3. RESULTADOS

Como resultado de los análisis comparativos y de los indicadores, se planteó la siguiente metodología orientada al análisis forense en dispositivos móviles, la cual consta de 7 fases (ver Fig. 2).

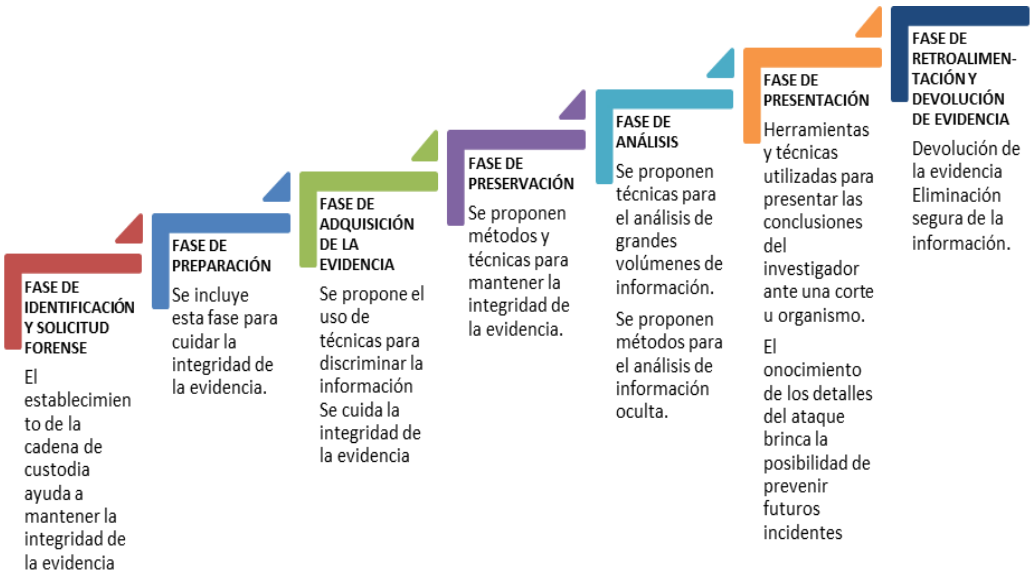

Figura 2. Metodología de análisis forense sobre dispositivos móviles.

A continuación se describen cada una de las fases de la metodología:

Fase 1: Se recopila la información necesaria para trabajar sobre el posible incidente. Permite adicionalmente detectar desviaciones del incidente y compararlos con acontecimientos similares en caso de existir, para lo cual se deben seguir las etapas que se muestran en la Fig. 3. Se tiene que responder a las siguientes preguntas: ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde?, ¿Por qué?, ¿Cómo?

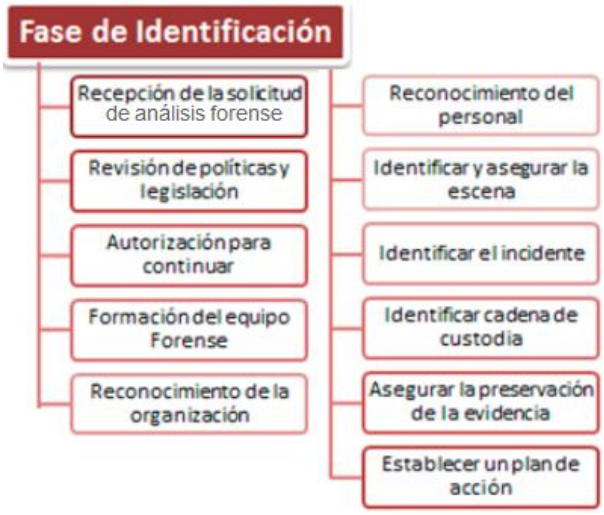

Figura 3. Etapas de la fase de identificación.

Fase 2: Se acondiciona el entorno de trabajo adecuado al estudio que se desee realizar, debiendo en la mayoría de los casos se recomienda no manipular los dispositivos originales implicados, y trabajar con imágenes, o mejor aún con una copia de éstas; hay que tener en cuenta que se necesitará montar estas imágenes tal cual estaban en el sistema comprometido, debiendo seguir las etapas que se muestran en la Fig. 4.

Fase 3: Se inicia la investigación y se procede a recopilar los datos respectivos, utilizando las herramientas analizadas, aprobadas y definidas en la fase anterior. Es importante revisar la legislación para el manejo y almacenamiento de evidencias, para ello se efectúan las etapas que se muestran en la Fig. 5.

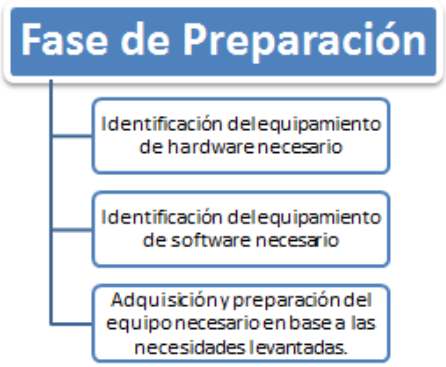

Figura 4. Etapas de la fase de preparación.

Figura 5. Etapas de la fase de adquisición.

Fase 4: Se documenta el cómo ha sido preservada la evidencia. 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" y como tal se deben asegurar. Para ello se siguen las siguientes etapas que se muestran en la Fig. 6.

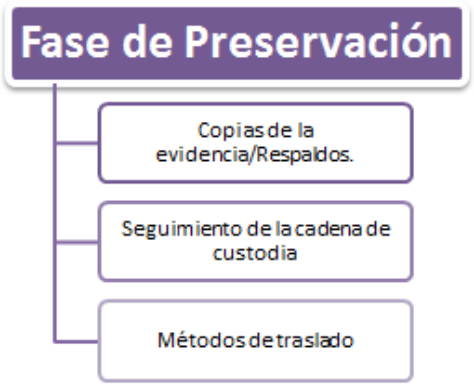

Figura 6. Etapas de la fase de preservación.

Figura 7. Etapas de la fase de análisis.

Fase 5: Se preparan las herramientas y técnicas para el análisis forense, sobre las evidencias obtenidas en la Fase 3, tomando el análisis de la Fase 2 y preservadas en la Fase 4; es importante tomar en cuenta las declaraciones de las personas involucradas en el incidente obtenidas en la Fase 1. El objetivo principal es reconstruir con todos los datos disponibles la cadena de acontecimientos que tuvieron lugar desde el inicio del incidente, hasta el pedido por parte de los interesados, para ello se siguen las etapas que se muestran en la Fig. 7.

Fase 6: Es de suma importancia 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, reduciendo al mínimo las posibilidades de error a la hora de gestionar el incidente. Se procede a documentar todas las acciones, eventos y hallazgos encontrados, lo que garantiza y asegura la cadena de custodia, para ello se siguen las etapas que se muestran en la Fig. 8.

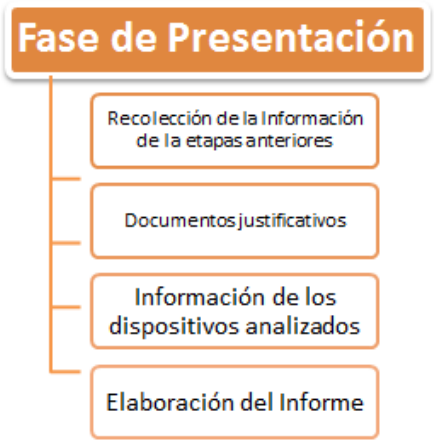

Figura 8. Etapas de la fase de preparación.

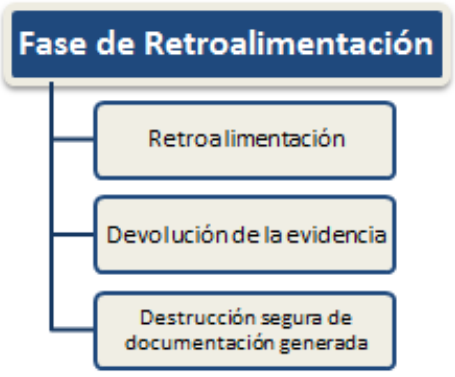

Figura 9. Etapas de la fase de retroalimentación.

Fase 7: Se brinda la retroalimentación del proceso efectuado, se procede a la devolución de documentos y de los dispositivos sujetos al análisis; también se realiza un borrado seguro de información digital almacenada, y la trituración de información impresa de carácter confidencial, para ello se siguen las etapas que se muestra en la Fig. 9.

Cada una de las sub fases (etapas) constituyen el puntal de la propuesta, lo que hace que la metodología trate a detalle un análisis forense sobre dispositivos móviles. Se concluye el estudio con un análisis comparativo entre la metodología forense de computadoras y la metodología planteada (ver Tabla 7).

Tabla 7: Metodología propuesta vs. Metodología de Informática forense tradicional.

Etapas de una investigación forense	METODOLOGÍA DESARROLLADA						
	Identifi-cación	Prepara-ción	Adquis-ición de evidencia	Preserva-ción	Análisis	Creación del reporte	Plan de retroali-mentación
Identificación	✓						
Preservación		✓	✓	✓			
Análisis					✓		
Presentación						✓	

4. DISCUSIÓN

La metodología propuesta es un método desarrollado en base a un estudio comparativo de varias metodologías existentes y en base al desarrollo actual de los dispositivos.

A continuación se probó la metodología, desarrollando las fases en un caso de estudio en el que está involucrado un celular (ver Fig. 10), y se comprobó la eficacia de su uso en tareas de análisis forense.

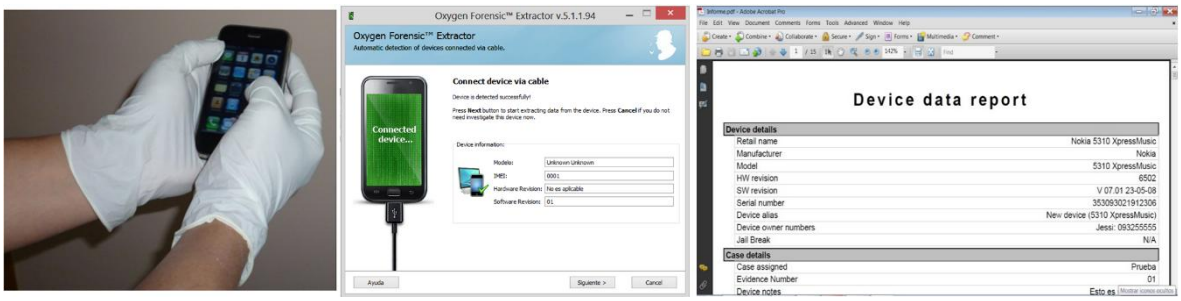

Figura 10: Caso práctico del proceso forense.

De manera experimental se efectuó el procedimiento a un teléfono celular, identificando toda la información almacenada en el dispositivo. Para llevar a cabo el proceso se utilizaron instrumentos como: solicitud del incidente, revisión de legislación, cadena de custodia, reportes detallados e informe final. Se validaron los resultados usando diferentes herramientas tanto de software libre como de software propietario.

La metodología permitió recolectar, manejar y analizar evidencias digitales almacenadas en el dispositivo móvil, garantizando el proceso forense. Para llevar a cabo éste proceso se identificaron varias herramientas, sin embargo ninguna de ellas resulta ser mejor que otra, incluso presentan deficiencias para interactuar con los dispositivos. Por lo tanto es importante utilizar varias de ellas para mejorar el proceso tanto de preservación, así como el de análisis. Se utilizó: Wodershare MobileGo para preservar la información, Hashcalc para la obtención del Hash que garantiza la integridad, y Oxygen Forensic Suite 2013 para el análisis; estas herramientas nos permitieron obtener un rendimiento promedio del 90% durante todo el proceso forense, sobre otras herramientas analizadas.

La metodología es una herramienta de apoyo y ayuda en la obtención de pruebas para esclarecer diferentes tipos de ilícitos; si se lo hace de manera adecuada, y manteniendo el respectivo asesoramiento jurídico, para no tener problemas legales o ser considerado violación de la privacidad.

Si bien los actuales dispositivos móviles inteligentes, tienen similitudes, y cada vez las tendrán en mayor medida con una computadora, la evidencia que eventualmente encontremos en estos dispositivos será similar (imágenes, archivos, correos intercambiados, sitios de internet visitados), pero existen una cantidad de elementos adicionales que pueden obtenerse y son específicos de este tipo de dispositivos como son:

- La agenda de contactos.
- Logs de llamadas realizadas y recibidas.
- SMS, MMS.
- Datos que permitan conocer la ubicación física en la que se encontraba el móvil al momento de su obtención (si el mismo se encontraba apagado) a partir del registro de la celda de comunicación empleada.

Aunque ambos son sistemas digitales, claramente existen diferencias entre ellos, desde la forma en que se ven, hasta en la forma en que operan internamente. Para entender mejor estas diferencias, se las puede separar en 4 categorías:

- Sistema de archivos.
- Estados de memoria.
- Capacidad de almacenamiento.
- Adquisición de datos.

La diversidad de marcas y modelos, sumado al corto ciclo de vida de los dispositivos móviles, representan un desafío para los investigadores forenses actuales; así como la estandarización de una metodología que permita evaluar todos los casos.

Posiblemente en los próximos años, las interfaces y sistemas operativos de estos dispositivos se estandaricen, facilitando la tarea investigativa, pero mientras tanto la diversidad de herramientas, y por sobre todo la experticia del investigador forense informático, son la clave para las investigaciones actuales.

5. CONCLUSIONES

Para efectuar las tareas de análisis forense existen metodologías que cumplen con los principios de la informática forense. El crecimiento de incidentes en los que intervienen dispositivos móviles plantea la necesidad de tener una metodología para estas tecnologías, ya que al existir diferentes fabricantes, cada uno tiene diversos criterios en el manejo de la información sin seguir ningún estándar. La metodología desarrollada tiene dentro de cada una de sus etapas un conjunto ordenado de 31 pasos a seguir, en cada etapa se plantea el objetivo a cumplir, las sub fases con sus respectivas indicaciones, y que productos se deben generar y entregar al finalizar la misma; a diferencia de otras metodologías donde si bien se tiene un marco general, no se indica que se debe hacer a detalle en cada una de sus etapas.

La fase 7 (de Retroalimentación) es otro de los aportes de la presente metodología, ya que aquí se considera la destrucción segura de documentos físicos y digitales del proceso forense que se está efectuando, garantizando la confidencialidad de la información encontrada. Además nos permite generar una base de conocimiento de lecciones aprendidas, lo que servirá para retroalimentar y mejorar al personal del equipo forense para futuros casos.

En la investigación se identificaron varias herramientas de análisis forense que no cubren por completo el proceso sobre dispositivos móviles, por tanto existe la necesidad de desarrollar nuevas herramientas de análisis forense por parte de las universidades, con la finalidad de que se conviertan en centros de investigación y apoyo en ésta área. La necesidad de generar convenios de investigación que involucren a la academia, al estado, y organismos nacionales e internacionales, tanto a nivel técnico como legal, para brindar entrenamiento y capacitación en análisis forense sobre dispositivos móviles a nivel de pregrado, Maestrías y personal involucrado con peritaje digital.

Para llevar a cabo una investigación forense no importa que metodología sea empleada, lo relevante es que cada actividad realizada debe estar perfectamente probada, documentada, sustentada y alineadas con la parte legal vigente.

REFERENCIAS

Acurio, S., 2009. Perfil sobre los delitos informáticos en el Ecuador. Pontificia Universidad Católica del Ecuador (Ecuador). Disponible en *http://www.criptored.upm.es/guiateoria/gt_m592d.htm.*

Ariza, A., J. Ruíz, 2009. iPhorensics: un protocolo de análisis forense para dispositivos móviles inteligentes. Pontificia Universidad Javeriana (Colombia). Disponible en *http://www.criptored.upm.es/guiateoria/gt_m142l1.htm*.

Ariza, A., J. Cano, J. Ruíz, 2009. iPhone 3G: Un nuevo reto para la informática forense. Bogotá, Colombia. Disponible en *http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6%284%29.pdf*.

Cano, J., 2009. Computación forense descubriendo los rastros informáticos. En: Computación forense descubriendo los rastros informáticos. Editorial: AlfaOmega, México, 1-7, 153-287.

Carrier, B., E. Spafford, 2004. An event-based digital forensic investigation framework. Center for Education and Research in Information Assurance and Security - CERIAS Purdue University, West Lafayette, Indianapolis, USA. Disponible en h*ttp://www.dfrws.org/2004/day1/Carrier-event.pdf*.

DFRW, 2001. A road map for digital forensic research. New York. Disponible en *http://www.dfrws.org/2001/dfrws-rm-final.pdf*.

Eloff, J.H.P., M. Kohn, M.S Olivier, 2008. Information and computer security architectures (ICSA). Research Group. Department of Computer Science, University of Pretoria, South Africa. Disponible en *http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/25.pdf*.

Hoog, 2011. *Android forensics: Investigation, analysis, and mobile security for Google Android*. Syngress, 364 pp.

Larry, D., D. Lars, 2012. *Digital forensics for legal professionals, understanding digital evidence from the warrant to the courtroom*. Syngress, 321 pp.

Lázaro, 2013. *Introducción a la informática forense*. España: RA-MA, 340 pp.

Mandia, K., C. Prosise, 2003. Incident response & computer forensics (2ª ed.). McGraw-Hill, 491 pp.

Sans, I., 2011. Disponible en *http://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652*.