Proceso Unificado de recuperación de Información en SmartPhones.

Ing. Fausto Viscaino.
Universidad Regional Autónoma de los Andes "UNIANDES", Km 5 ½ vía a Baños, Ambato – Ecuador.
Faustov_zh1@hotmail.com

Ing. Ana Aide di Lorio
Universidad de Fasta, Mar del Plata-Argentina
anadiiorio@gmail.com

Ing. Freddy Baño N.
Universidad Regional Autónoma de los Andes "UNIANDES", Km 5 ½ vía a Baños, Ambato – Ecuador.
freddybn@gmail.com

RESUMEN.

La Universidad de FASTA y su grupo de investigación de Informática Forense, generó el proyecto PURI (Proceso Unificado de Recuperación de la Información) que permite dar un marco de formalidad y define un conjunto de fases, tareas, técnicas y herramientas que definen esta actividad, con el fin de guiar al Informático Forense en su labor.

En Ecuador en general, en la ciudad de Ambato provincia de Tungurahua en particular, no existen antecedentes de investigaciones ni expertos que trabajen en esta temática, muchos menos utilizando procesos formales aplicables a las pericias informáticas en Smartphones.

El presente estudio tomo como punto de partida el trabajo realizado por la universidad de Fasta y se lo adecuo en una pericia en Smartphone con el fin de tener un PURI adaptado a las necesidades de los dispositivos mencionados.

Como resultado de este proceso surge la propuesta del PURI para Smartphone, resaltando los nichos carentes, total o parcialmente, de herramientas para el desarrollo de determinadas tareas.

Palabras Clave: Proceso**,** Unificado, Recuperación, Información, Informática, Forense, Smartphone

1. INTRODUCCIÓN.

Los teléfonos inteligentes vienen día a día ganando mercado. Los usuarios están migrando a Smartphones tareas que anteriormente solían realizarse desde un computador personal. Si consideramos que la información es actualmente el activo más importante de una organización, no podemos estar ajenos a estos cambios sociales.

En países latinoamericanos existen algunas instituciones específicas en el cibercrimen, como es el caso de Colombia que posee una página web de la policía con información sobre delitos informáticos, pero en particular no existe ningún documento que posea el respaldo de un estudio en el cual se defina un proceso o algún tipo de instructivo que se deba seguir para poder realizar una pericia en un SmartPhones en un caso judicial.

El delito informático se empezó a considerar legalmente en el Ecuador desde que en 1999 se puso en el tapete la discusión del proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas

Electrónicas, en el país se empezaron a realizar cursos, seminarios, encuentros, se conformaron comisiones para la discusión de la Ley para que se formulen observaciones, aquí intervinieron organismos que se encontraban directamente interesados como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, entidades que veían en el comercio electrónico una buena oportunidad de hacer negocios y de paso hacer que el país entre en este nuevo auge y no se quede retrasado.

Por el lado de la Función Judicial no ha existido la suficiente preparación por parte de Jueces y Magistrados, en este sentido puede darse el caso que los llamados a impartir justicia se encuentran confundidos con la particularidad de estos delitos y tienden a confundirlos con los delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.[1]

Con esto lo que se evidencia es que se hace necesario que se formen unidades investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática e informática forense. Estas unidades también pueden servir de base para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. [2]

A pesar de la existencia de peritos informáticos, cabe recalcar que para el caso de SmartPhones no existen guías formales establecidas como estándares dentro de la función judicial.

Hoy en día existen algunas herramientas forenses para recuperar información de dispositivos móviles, pero la mayoría de ellas son aplicaciones cerradas, que se desconoce internamente como trabajan. Además, los altos costos de las propuestas comerciales, sumado a las deficiencias de las herramientas gratuitas, hacen que no exista en la actualidad una guía para el profesional forense que le sugiera la herramienta apropiada para utilizar ante determinada tecnología, o al menos, que le indique las características que debiera tener en cuenta al momento de seleccionar una herramienta.

2. OBJETIVOS DE LA INVESTIGACIÓN.

2.1. OBJETIVO GENERAL.

Desarrollar una investigación sobre las herramientas, técnicas y métodos disponibles en el mercado para la recuperación de la información en dispositivos móviles mediante la adopción del proceso PURI y su validación en base a prototipos.

2.2. ESPECÍFICOS.

- ✓ Desarrollar el relevamiento y estado del arte.
- ✓ Realizar al estudio y análisis de las fases a seguir para la recuperación de la información según las buenas prácticas sugeridas por organismos internacionales.
- ✓ Adaptar el Estudio del Proceso PURI "Proceso Unificado de Recuperación de Información" para SmartPhones.
- ✓ Desarrollar la propuesta de Nuevas Técnicas a utilizar en fases carentes.
- ✓ Desplegar el Desarrollo de Nuevas Herramientas.

3. JUSTIFICACIÓN.

Es evidente que día a día el ser humano va adaptándose con un ritmo creciente a la utilización de sistemas informáticos para llevar a cabo sus actividades cotidianas. Pero si se presta atención a este punto, puede notarse que estas actividades crecen no solo en número sino en criticidad. Cada vez realizamos operaciones más complejas y decisivas para nuestras vidas a través de sistemas

[1] Pino, Dr. Santiago Acurio Del. «Los Delitos Informáticos en el Ecuador (parte II).» 29 de 02 de 2012. 10 de 01 de 2013 <http://www.cavaju.com/2012/02/29/los-delitos-informaticos-en-el-ecuador-parte-ii/>.

2 Acurio, Dr. Santiago. INFORMÁTICA FORENSE, INSERCIÓN JURÍDICA. Quito, s.f.

informáticos. Por ejemplo, hoy en día se ven frecuentemente grandes transacciones bancarias, que sin duda son de importancia para quien las realiza, hasta operaciones críticas médicas que dependen de un software. [3]

Es sabido que, en todo sistema informático, el crecimiento en complejidad va de la mano con el aumento de vulnerabilidades. Estas vulnerabilidades pueden ser aprovechadas por personas malintencionadas que accionan explotándolas con el fin de obtener algún beneficio propio. Eventualmente estos tipos de fraude podrían dejar vestigios que permitan reconstruir los hechos y determinar que realmente se trata de un fraude y no del resultado de la actividad normal de un usuario de buena fe. Éste es uno de los tantos casos en los que interviene la informática forense, en donde un experto intenta obtener evidencias a fin de reconstruir la real sucesión de hechos. Por ende, la recuperación de la información, tanto visible como oculta, es fundamental en esta actividad.

Existen también otros contextos en los que la informática forense es de suma importancia. A pesar de la evolución de la informática en sí, no todo fraude o delito será realizado a través de ella; pero, sin embargo, su rama forense podría aportar pruebas decisivas en la culpabilidad de la persona. Estamos hablando, en este caso, de eventualmente un agresor o estafador que podría dejar evidencia de sus intenciones en algún medio informático a pesar de que la acción no sea llevada a cabo a través del mismo. Entonces, allí también tomaría presencia un experto en informática forense, quien realizaría pericias que aporten a la resolución del caso. Es indudable que aquí también es sumamente valiosa la correcta recuperación de toda información relacionada al hecho.

Como puede observarse, las aplicaciones de la informática forense son incontables pero aun así existe un punto en común para llevarlas a cabo que es la recuperación de la información. La correcta extracción de información es crucial en la obtención de evidencias y es justamente el objetivo de este proyecto.

El contexto de esta actividad que forma parte de la informática forense es ciertamente complejo y velozmente cambiante. Es sabido que existen muchas dificultades a sortear en la realización de esta tarea, y estas incrementan la labor y el estudio de los informáticos forenses. Algunas de estas problemáticas serán tratadas, con el fin de presentarlas y eventualmente de aportar posibles soluciones. [4]

4. DESARROLLO.

4.1. LA INFORMÁTICA FORENSE

La ciencia digital forense comprende la recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital que se define como información de valor almacenado o transmitido en una forma binaria, para ayudar a determinar el origen de incidentes, tal como los delitos informáticos. Es decir, la informática Forense es una rama de la ciencia forense que trabaja con datos que han sido procesados electrónicamente y guardados en un medio computacional.[5]

A su vez, como disciplina demanda de personal entrenado en la materia, que pueda actuar metódicamente, mantener la cadena de custodia y no contaminar la prueba, principios forenses básicos. Existen varias guías y procedimientos de trabajo en informática forense de dependencias policiales y judiciales de distintos países con el fin de unificar criterios en el trabajo con evidencia digital. No conocemos la existencia de este tipo de guías en nuestro país, así como tampoco indicaciones en los códigos procesales de los diferentes foros sobre como preservar la evidencia

3 UNIVERSIDAD DE FASTA. «CIIDDI.ORG.» 01 de 09 de 2010. http://www.ciiddi.org/congreso2012/papers/PURI%20Proceso%20Unificado%20de%20Recuperacion%20de%20Informacion%20%28Podesta%20et%20al%29.pdf (último acceso: 03 de 08 de 2013).

4 UNIVERSIDAD DE FASTA. «CIIDDI.ORG.» 01 de 09 de 2010. http://www.ciiddi.org/congreso2012/papers/PURI%20Proceso%20Unificado%20de%20Recuperacion%20de%20Informacion%20%28Podesta%20et%20al%29.pdf (último acceso: 03 de 08 de 2013).

5 Blog PUPC. «Informática Forense.» 2009. 05 de 07 de 2013 <http://blog.pucp.edu.pe/item/53067/informatica-forense>.

digital. Sería interesante reflexionar sobre este punto y hacer saber a nuestros legisladores al respecto, dado que los departamentos de informática forense, tanto públicos como privados, precisan contar con estándares, guías, procedimientos y metodologías que los asistan en el proceso bajo el principio de mantener la integridad de los datos y no alteración de la prueba.

El establecimiento de procedimientos debería guiar el proceso técnico de adquisición, examinación y análisis de la evidencia, así como la forma de preservar la evidencia en el tiempo y su forma de presentación. Los procedimientos deben estar testeados previo a su implementación para asegurar que los resultados obtenidos sean válidos y reproducibles en forma independiente. Con el objeto del armado de un proceso unificado, y sus procedimientos particulares deben documentarse los pasos en su desarrollo y validación con el fin de permitir la adaptabilidad del proceso a medida que surjan nuevos aspectos que permitan su crecimiento. Los aspectos que se documentaran a lo largo de este proyecto son:

- Identificación de la tarea o problema a resolver
- Soluciones propuestas
- Testeo de cada solución con un ejemplo de control
- Evaluación del resultado del testeo
- Finalización del procedimiento.

Es importante destacar que el uso principal de la informática forense se da en ambientes judiciales, pero hoy en día también es utilizado en empresas.

4.2. PROCESO DE RECUPERACIÓN DE LA INFORMACIÓN

Un proceso de recuperación de la Información, en líneas generales, consta de cuatro grandes etapas que nombraremos Identificación, Adquisición - Examinación, Análisis y Presentación.

Este proyecto se centra en las etapas de adquisición - Examinación y Análisis, dado que la identificación y la presentación son etapas más relacionadas al actuar judicial, lo que excede el marco de este proyecto.

a. Identificación

En esta etapa se identifica la información a recuperar y los equipos o dispositivos objetos de esta tarea. La evaluación de los medios sobre los que se actuará es determinante del curso de la acción. Por este motivo, el estudio del ambiente es fundamental, dado que de acuerdo al hecho a investigar y a la información que se desea obtener son las etapas, fases y tareas que se seguirán del proceso general definido.

Algunos puntos a considerar en la etapa de identificación son:

- La necesidad de realizar otros procesos forenses sobre la evidencia (ej: origen y validez del documento, audio o video, análisis de huellas dactilares sobre el equipo, entre otros).
- Posibilidad de obtener datos fuera del equipo que puedan colaborar con la obtención de evidencias (Identificar la presencia o no de una red, identificar medios de almacenamiento externos o remotos(nube), tarjetas extraíbles, usb, cd, tarjetas de memoria, entre otros)
- Evaluar las posibles habilidades técnicas de los usuarios del equipo para determinar la posibilidad de uso de estrategias para destruir u ocultar evidencia (uso de encriptación, esteganografía, booby traps, entre otros)

b. Adquisición y Examinación de la Información

Con el fin de recolectar la evidencia digital, los procedimientos forenses tradicionales examinan soportes y dispositivos electrónicos. La etapa de adquisición consiste entonces, en la extracción de datos de medios digitales, manteniendo su integridad.

Para los dispositivos electrónicos, es decir cualquier dispositivo capaz de guardar información que posea valor como evidencia (teléfonos celulares, agendas, organizadores electrónicos, dispositivos de comunicaciones de red como routers, hubs, etc.), el tratamiento es más específico.

Por ejemplo, en cuanto a la telefonía móvil, la investigación de la tarjeta SIM es valiosa por el hecho de que el cliente de un sistema de telefonía móvil en esencia necesita un medio de comunicación que

implica un intercambio de información (voz y datos) potencialmente útil. Además todos los sistemas de telefonía móvil rastrean la posición de los terminales y en la mayoría de los casos existe una relación unívoca entre los usuarios y sus móviles y en consecuencia con el tipo de información que almacena una SIM. [6]

Sin embargo, intentos de manipulación de una tarjeta inteligente para la extracción de sus datos, podrían conducir a un bloqueo irreversible de la misma pudiendo sólo resolverse mediante la sustitución con una nueva tarjeta inteligente emitida por el mismo proveedor. Por lo tanto, dado que la única información que ofrece una tarjeta inteligente con el mundo exterior son los datos de su sistema de archivos, la mayoría de las herramientas aplicadas para la adquisición de datos de una SIM, tratan de leerlos y reconstruir un árbol con la estructura de datos que contiene.

- Adquisición en medios de almacenamiento persistentes

El primer paso en un proceso de recuperación de información es la adquisición, es decir, la realización de una imagen fiel del original, con el fin de preservar la prueba y trabajar sobre la copia. Existen varios formatos específicos y cerrados en los que puede ser almacenada una imagen, los cuales dependerán de la herramienta utilizada para realizar esta acción.

Los tipos de Imagen RAW (dd), SMART y E01 son los más utilizados. Actualmente un grupo de trabajo del DFRW (Digital Forensic Research WorkShop)[7] se encuentra trabajando en la definición de un formato abierto y aceptado por la comunidad, denominado CDESF (Common Digital Evidence Storage Format). Esto se debe a la gran variedad de formatos de imágenes existentes

Se debe bloquear el disco o el dispositivo para prevenirlo de escritura, con el objeto de preservarlo y proteger el original. El disco puede bloquearse por hardware, con dispositivos específicos, o por software, funcionalidad que debe proveer la herramienta forense utilizada; por otro lado, dispositivos de hard para realizar las imágenes, internamente ya realizan el bloqueo del disco.

La adquisición de la evidencia puede realizarse con:

- Software de duplicación específico
- Software Forense específicos
- Dispositivos de hardware dedicados

- Adquisición en medios de almacenamiento volátil (memoria)

La recolección de pruebas se centra en la obtención de evidencia digital en una forma aceptable. Cómo vimos precedentemente hay dos enfoques para la adquisición de imágenes: orientado a software o a hardware.

Herramientas de adquisición de Memoria Física orientadas a hardware:

La idea principal es evitar al sistema operativo por medio de un dispositivo físico. El dispositivo abrirá una comunicación a través de un puerto dedicado para copiar el contenido de la memoria física. Dos tecnologías principales se emplean:

4.3. SamrtPhones (Teléfonos Inteligentes).

Desde hace aproximadamente diez años, el empleo de dispositivos móviles se ha incrementado notablemente. “El uso de sistemas de telecomunicaciones móviles en todo el mundo ha llegado a

[6] UNIVERSIDAD DE FASTA. «CIIDDI.ORG.» 01 de 09 de 2010. 03 de 08 de 2013 <http://www.ciiddi.org/congreso2012/papers/PURI%20Proceso%20Unificado%20de%20Recuperacion%20de%20Informacion%20%28Podesta%20et%20al%29.pdf>.

7 http://www.dfrws.org/

proporciones casi epidémicas"[8], principalmente por su facilidad de uso y la propiedad de mantener en contacto permanente a sus usuarios, por lo cual se ha generado un cambio significativo en la forma en que las personas se comunican, pero también por su proliferación se ha incrementado su uso en actividades de orden delictivo.

Existe gran variedad de gamas de dispositivos móviles, dentro de los cuales el mayor crecimiento en popularidad y uso se presenta en los dispositivos móviles inteligentes, debido a su capacidad tanto para realizar llamadas como para navegar por Internet con el objetivo de intercambiar información a través de diferentes enlaces y además porque permiten desarrollar y ejecutar aplicaciones que no necesariamente son incluidas por el fabricante.

Actualmente la información almacenada en cualquier computador y/o dispositivo móvil puede considerarse como el activo de información más valioso para cualquier organización e incluso para cualquier persona del común. Con los métodos de comunicación que existen actualmente como la red wireless o tecnologías de corto alcance como Bluetooth se puede hacer uso de la información y compartir la misma de manera eficiente sin necesidad de encontrarse en una estación de trabajo fija conectada a algún medio físico.

Por consiguiente, el constante desarrollo de las tecnologías móviles ha permitido aumentar la portabilidad de la información. Esto se ve reflejado con la llegada de dispositivos móviles, que en esencia tiene las mismas características de un computador y permite almacenar y transferir varios tipos de información en el momento y lugar deseado por el usuario.

Por otra parte debido a su gran popularidad y la importancia de la información que almacenan y transmiten, estos dispositivos pueden ser víctimas de ataques criminales que buscan afectar la integridad, confiabilidad y disponibilidad de la información que estos administran, como mensajes de texto, mensajes multimedia, historial de páginas web visitadas, contactos telefónicos, imágenes, registro de llamadas, sonidos y correos electrónicos, información valiosa al momento de realizar un análisis forense en una escena del crimen donde se encuentre un SmartPhone.

Uno de los retos que enfrenta actualmente la computación forense es realizar análisis forense sobre dispositivos móviles, esto debido a que se tiene como base los procedimientos realizados en la informática forense clásica, pero no existen procedimientos formalizados para realizar este tipo de análisis específicamente sobre dispositivos móviles.

A nivel latinoamericano existen estudios sobre análisis forense y técnicas forenses en diferentes dispositivos como es el caso de Análisis Forense en dispositivos Móviles con Symbian OS, de C. Agualimpia y R. Hernandez de la Universidad Javeriana de Colombia, o el proyecto Guía Metodológica para el Análisis Forense orientado a incidentes en dispositivos moviles GSM, de Carlos Castillo y Rafael Romero.

4.4. METODOLOGÍA DE TRABAJO.

En la primera etapa se realizó una investigación del tipo exploratorio donde se recopilo y analizó los documentos con el fin de conocer el estado del arte.

Luego, se procedió a sintetizar y formalizar este conocimiento, chequeándolo con el proceso PURI desarrollado por la Universidad Fasta de Mar de Plata Argentina, proponiendo modificaciones de ser necesario con el fin de adaptarlo a los requerimientos de los Smartphones.

Se validó el proceso propuesto en la etapa anterior, con dos casos de uso típicos a diseñar en la etapa 1, preferentemente uno por cada plataforma tecnológica (Android, Blackberry).

8 Mellar, B. «Forensic examination of mobile.» 01 de 05 de 2013. <http://faculty.colostate-pueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf>.

Una vez validado el proceso, en la etapa 3 se prevé estudiar, analizar y proponer, sobre los nichos carentes, el desarrollo de nuevas técnicas y herramientas, sobre las cuales, en la etapa 4 se trabajará en el desarrollo y validación del prototipo.

4.5. HERRAMIENTAS Y TÉCNICAS DISPONIBLES PARA CUMPLIMENTAR CADA UNA DE LAS TAREAS PROPUESTAS.

Es primordial recalcar que la mayoría de la información aquí recabada es procedente de internet de páginas especializadas sobre el tema, debido a que en nuestro país no existe información sobre herramientas forenses para dispositivos móviles.

A continuación mostramos el listado de herramientas que se utilizará para la validación del PURI para SmartPhones; la mayoría de las herramientas son multiplataforma, esto quiere decir que se puede acceder a dispositivos Android, Blackberry, Windows Phone, entre otros, lamentablemente hasta el momento no se ha logrado encontrar herramientas específicas para dispositivos Iphone.

En esta recopilación también se enlistan herramientas que permiten obtener datos de las tarjetas de almacenamiento, aquí es importante mencionar que las que se ha escogido son herramientas OpenSource que funcionan sobre el sistema operativo LINUX la gran mayoría. Existe una gran controversia debido a que al momento de utilizar herramientas OpenSource en un juicio, algunos abogados apelan los veredictos basados en estas herramientas debido a que manifiestan que no tienen el 100% de veracidad ya que cualquier persona especializada en el área de la informática podría modificar su código fuente a la conveniencia del caso.

- Modelos para la recuperación de la Información

Primero que nada vamos a definir lo que es un modelo de recuperación de la información. El diseño de un SRI se realiza bajo un modelo, donde queda definido "cómo se obtienen las representaciones de los documentos y de la consulta, la estrategia para evaluar la relevancia de un documento respecto a una consulta y los métodos para establecer la importancia (orden) de los documentos de salida"[9]

Existen varias propuestas de clasificación de modelos, una de las síntesis más completas la realiza Dominich en cinco grupos:

Modelo	Descripción
Modelos clásicos	Incluye los tres más comúnmente citados: booleano, espacio vectorial y Probabilístico
Modelos alternativos	Están basados en la Lógica Fuzzy
Modelos lógicos	Basados en la Lógica Formal. La recuperación de información es un proceso inferencial.
Modelos basados en la Interactividad	Incluyen posibilidades de expansión del alcance de la búsqueda y hacen uso de retroalimentación por la relevancia de los documentos recuperados.
Modelos basados en la Inteligencia Artificial	Bases de conocimiento, redes neuronales, algoritmos genéticos y procesamiento del lenguaje natural.

Tabla 1. Clasificación de los Modelos de Recuperación de Información según Dominich.
Fuente: Dominich, S. 'A unified mathematical definition of classical information retrieval'. Journal of the American Society for Information Science, 51 (7), 2000. p. 614

Actualmente con los dispositivos móviles se hace necesario la adaptación de los modelos existentes o la creación de un modelo que satisfaga las necesidades que emiten los SmartPhones.

[9] Villena, Román, J. Sistemas de Recuperación de Información. 1997, Valladolid: Departamento Ingenierías Sistemas Telemáticos, Universidad.
<http://www.mat.upm.es/~jmg/doct00/RecupInfo.pdf> 20 de 01 de 2003

LISTADO DE HERRAMIENTAS UTILIZADAS.						
nombre	**Licencia**	**S.O.**	**plataforma**	**fuente**	**dispositivo**	**memoria**
encase forensic	trial- propietaria	windows	multiplataforma		X	
mobiledit forensic	trial-propietaria	windows	multiplataforma	http://www.mobiledit.com/mef-overview.htm	X	
winmofo	trial-propietaria	windows	multiplataforma	http://winmofo.com/	X	
filescavenger	Propietaria	windows		http://www.es.quetek.com/prod02.htm		x
oxygen forensic suite 2013	Freeware	windows	multiplataforma	http://www.oxygen-forensic.com/en/download/freeware	X	
cellebrite (ufed physical analyzer)	trial- propietaria	windows	multiplataforma	http://go.cellebrite.com/lp=77	X	
open source android forensics toolkit	Opensource	linux	multiplataforma	http://osaf-community.org/	X	
open source forensics	Opensource	windows	multiplataforma	http://www2.opensourceforensics.org/tools	X	x
digital forensics framework	Opensource	windows/ linux	multiplataforma	http://www.digital-forensic.org/		x
digital forensics association	Opensource	windows	multiplataforma	http://www.digitalforensicsassociation.org/opensource-tools/	X	x
the coroner's toolkit (tct)	Opensource	linux		http://www.porcupine.org/forensics/tct.html		x
live view	Opensource	windows/ linux		http://liveview.sourceforge.net/		x
computer aided investigative environment c.a.i.n.e.	Opensource	linux	multiplataforma	http://www.caine-live.net/	X	
portable linux auditing cd	Opensource	linux	independiente	http://plac.sourceforge.net/	X	x
phomebase2	Propietaria	windows	independiente	http://www.phonebase.info	X	
photorecoverypro	Propietario	windows	independiente	http://www.photorecoverypro.net/?gclid=coxh-nw_zbccfwvo7aodahyasa	X	x
sd card recovery software	Propietario	windows	independiente	http://www.photorecoverypro.net/?gclid=coxh-nw_zbccfwvo7aodahyasa		x
mjm freephotorecovery	Gratis	windows/ linux	independiente	http://www.ukdatarecovery.com/data-recovery/forensic-data-recovery.html		x
diskinternalsrecovery	Gratis	windows	independiente	http://www.diskinternals.com/	X	x

softperfect file recovery	Gratis	windows	independiente	http://www.softperfect.com/products/filerecovery/	X	x
mac data recovery wizard trial	Trial	mac	mac	http://www.easeus.com/download.htm	X	x
datarecovery wizard	Trial	windows	independiente	http://www.easeus.com/download.htm		x
photorecovery	Trial	windows y mac	independiente	http://www.wondershare.net/ad/photo-recovery/?gclid=clkczqi4y7ccfwdo7aoddq0agq	X	x
galeryundelete	Gratis	windows	windows	http://www.glarysoft.com/glary-undelete/download/	X	x
photorec	Gnu	windows /linux / mac	independiente	http://www.cgsecurity.org	X	x
device seizure	trial-propietaria	windows	independiente	http://www.paraben.com/device-seizure.html	X	x

5. CONCLUSIONES

El rápido avance tecnológico ha producido la inserción de dispositivos de alta tecnología en el común de la población con ello es fácil encontrar teléfono inteligentes en el uso diario de millones de personas en nuestro país.

Los SmartPhones o teléfonos inteligentes actualmente son dispositivos de gran ayuda tanto en el ámbito laboral como estudiantil, pero muchas veces la falta de conocimiento, o la falta de precaución al momento de instalar aplicaciones en nuestros dispositivos nos hace vulnerables ante los delincuentes.

Actualmente los delitos informáticos se están produciendo con mayor frecuencia en nuestro país, es importante tratar de dar soluciones que ayuden a la función judicial a resolver delitos en los cuales la tecnología es una evidencia trascendental al momento de dar un veredicto.
En la actualidad existen variedad de dispositivos tanto en marcas, modelos y sistemas operativos móviles para los mismos, en consecuencia es importante analizar y estudiar la estructura de cada uno de los sistemas móviles para poder tratar de recuperar información útil en un caso judicial.
Es necesario estandarizar procesos independiente mente de la tecnología móvil para que sean aceptados por los entes encargados de emitir justicia y que permitan dar valides legal a la precia informática que se realice sobre los SmartPhones.

BIBLIOGRAFÍA/ LITERATURA CITADA.

1. Acurio, Dr. Santiago. *INFORMÁTICA FORENSE, INSERCIÓN JURÍDICA.* Quito, s.f.
2. Blog PUPC. «Informática Forense.» 2009. http://blog.pucp.edu.pe/item/53067/informatica-forense (último acceso: 05 de 07 de 2013).
3. Mellar, B. «Forensic examination of mobile.» 01 de 05 de 2013. http://faculty.colostate-pueblo.edu/dawn.spencer/Cis462/Homework/Ch4/Forensic%20examination%20of%20mobile%20phones.pdf.
4. http://www.mobiledit.com/mef-overview.htm
5. Pino, Dr. Santiago Acurio Del. «Los Delitos Informáticos en el Ecuador (parte II).» 29 de 02 de 2012. http://www.cavaju.com/2012/02/29/los-delitos-informaticos-en-el-ecuador-parte-ii/ (último acceso: 10 de 01 de 2013).
6. http://www.glarysoft.com/
7. Dominich, S. 'A unified mathematical definition of classical information retrieval'. Journal of the American Society for Information Science, 51 (7), 2000. p. 614
8. UNIVERSIDAD DE FASTA. «CIIDDI.ORG.» 01 de 09 de 2010. http://www.ciiddi.org/congreso2012/papers/PURI%20Proceso%20Unificado%20de%20Recuperacion%20de%20Informacion%20%28Podesta%20et%20al%29.pdf (último acceso: 03 de 08 de 2013).
9. Villena, Román, J. Sistemas de Recuperación de Información. 1997, Valladolid: Departamento Ingenierías Sistemas Telemáticos, Universidad. <http://www.mat.upm.es/~jmg/doct00/RecupInfo.pdf> 20 de 01 de 2003
10. Dragonjar. S.f. 04 de 01 de 2014< http://www.dragonjar.org/>.
11. Carlos Castillo 30 de 11 de 2013 < http://www.carlosacastillo.com/>.
12. yodot. yodot. s.f. 01 de 03 de 2014 <http://www.yodot.com/es/androide-de-recuperacion-de-datos/>.
13. Remo Software S.f. 02de 02 de2014 http://www.android-photo-recovery.net/es/software-para-samsung-galaxy-s3.html/.
14. Advanced Data Recovery S.f. 10 de 04 de 2014 http://www.adrdatarecovery.com/ smartphones/
15. Krollontrck S.f. 11 de 04 de 2014 <http://www.krollontrack.com/data-recovery/data-recovery-services/mobile-device-recovery/>