PURI: Proceso Unificado de Recuperación de Información

Ariel Podestá[1], Bruno Costanzo[2], Julián Waimann[3],
Martín Castellote[4], Rita Sansevero[5]

***1**: Ingeniero Informático. Investigador de la Facultad de Ingeniería de la Universidad FASTA. Programador/Analista de la Municipalidad del Partido de General Pueyrredón. {arielpodesta@gmail.com}*

***2**: Técnico en Informática. Auxiliar de Investigación Alumno, Facultad de Ingeniería de la Universidad FASTA. {bru.constanzo@gmail.com}*

***3**: Técnico en Informática. Auxiliar de Investigación Alumno, Facultad de Ingeniería, Universidad FASTA. Desarrollador .Net, Common Sense {julianw@ufasta.edu.ar}*

***4**: Ingeniero Informático. Investigador de la Facultad de Ingeniería de la Universidad FASTA. Bioinformático en INTA EEA Balcarce. Desarrollador web. {castellotemartin@yahoo.com.ar}*

***5**: Ingeniera en Informática. Docente e investigadora de la Facultad de Ingeniería de la Universidad FASTA. Programador/Analista de la Municipalidad del Partido de General Pueyrredón. {resansevero@gmail.com}*

Abstract: En el presente documento se trata la problemática que existe en la informática forense durante la actividad de la obtención de evidencias. Aquí se analiza el complejo contexto en el que esta actividad debe llevarse a cabo poniendo atención a numerosas dificultades como la diversidad de tecnologías, métodos de ocultamiento de información, tiempos ajustados, falta de guías de operación, legislación vigente, intereses de fabricantes, entre otras. Toda esa serie de obstáculos que tiene que enfrentar un informático forense determina que el éxito de la tarea dependa de su habilidad profesional guiada por su criterio y no por un proceso formal.

Se requiere por lo tanto, un proceso formal que permita guiar y validar la actividad del informático forense en la obtención de evidencias llamado proceso unificado de recuperación de la información (PURI).

En este paper se analizan las distintas problemáticas de la recuperación de información en el contexto actual y próximo de la informática en el mundo, para poder concluir con fundamentos en la necesidad de la existencia de un PURI que valide la labor del perito y contemple tal diversidad de dificultades permitiendo tener una guía orientadora en la tarea de la obtención de evidencias.

Palabras clave: Informática forense, peritaje informático, recuperación de información.

Introducción

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 se realizan operaciones más complejas y decisivas a través de sistemas informáticos. Por ejemplo, hoy en día se ven grandes transacciones bancarias que sin duda son de importancia para quien las realiza y hasta intervenciones médicas con alto nivel de criticidad que dependen de un software.

Tomando en cuenta lo anterior podemos deducir que los sistemas crecen en complejidad al mismo ritmo que se va dando esta rápida evolución en la sociedad. Esta complejidad se debe no solo a lo funcional sino también a las medidas de seguridad que se requieren proporcionalmente con el aumento de la importancia de las operaciones.

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 acciones 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. Por ejemplo, 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 en los distintos contextos tiene como punto en común la recuperación de la información. La correcta extracción de la información es crucial en la obtención de evidencias y es justamente el objeto de análisis de este proyecto.

Pero dado el contexto de esta actividad, complejo y velozmente cambiante, existen muchas dificultades a sortear en la realización de la tarea que incrementan la labor y

el estudio de los informáticos forenses. Algunas de las problemáticas se tratan a continuación, con el fin de presentarlas y eventualmente aportar posibles soluciones:

Diferentes de tecnologías: La recuperación podría requerirse en distintos tipos de dispositivos. Con el correr del tiempo ingresan al mercado nuevos productos, lo que nos lleva a tratar con diferentes equipos (servidores, notebooks, tabletas, celulares, etc.) para los cuales no siempre se encuentra disponible la herramienta apropiada de obtención de la información.

Diversidad de métodos de almacenamiento: Existen técnicas de almacenamiento y tratamiento de la información que son ampliamente conocidas. Con lo cual, obtener la información de un dispositivo que utilizó tales métodos no sería una tarea demasiado compleja. Pero no siempre es así, eventualmente puede existir un fabricante que utilice su propia técnica de administrar la información en sus dispositivos y que, a su vez, no la de a conocer. Éste, es un problema complejo para los informáticos forenses dado que si no es posible sobrellevar esta dificultad entonces muy probablemente no sea posible hallar evidencias.

Localización de la información: Cuando se tiene un dispositivo personal transportable, como ser un celular, es fácil acceder a él para luego intentar obtener evidencias. Pero si se trata de, por ejemplo, un servidor ya la tarea puede tornarse más compleja. Tal servidor, muy probablemente no sea de la propiedad de la persona en cuestión y hasta quizás ni siquiera se encuentre en la misma zona geográfica. Esto dificulta mucho la tarea de recuperación de la información dado que involucra el traslado de los peritos al lugar donde se encuentran los equipos y no siempre es posible.

Heterogeneidad de leyes que aplican en el planeta: Siempre que se tiene un caso a resolver se requiere del aval legal para realizar pericias sobre los dispositivos relacionados al hecho en cuestión. Este aval debe ser provisto por una entidad que tenga jurisdicción en la zona geográfica donde se encuentran tales dispositivos. Entonces, es claro que el problema ocurre cuando los equipos se encuentran en una zona geográfica en la cual tal entidad no tiene jurisdicción. Por ende es posible que no se sea posible realizar pericias sobre los equipos.

Tecnologías que naturalmente eliminan evidencias: El dejar evidencias de información eliminada no es interés de los fabricantes de dispositivos y menos cuando eso va en contra de la performance de los mismos. Ciertamente, por ejemplo, los medios de almacenamiento de tipo SSD que hoy en día pueden observarse cada vez más en computadoras personales, son dispositivos que necesitan mantener limpios los espacios libres para maximizar su eficiencia, lo que va en claro desmedro de la posibilidad de recuperar información.

Mecanismos internos de protección de la información: Es atractivo para los usuarios que el dispositivo que adquieran no revele información sin su consentimiento. Los fabricantes, aprovechando esta tendencia, pueden ofrecer equipos

que garanticen tal propiedad. Este hecho puede ser un importante impedimento para el forense de acuerdo a que tan robusta e inviolable sea la tecnología con la cual se fabricó el dispositivo a analizar.

Falta de herramientas: Se conoce que los fabricantes proveen herramientas forenses que aplican a sus propios productos. Pero la distribución de tales herramientas se ve directamente afectada por los intereses de los mismos. Solo y exclusivamente si es rentable producirlas y distribuirlas, entonces lo harán. De otra manera, las mismas no se encontrarán disponibles en el mercado, agregando otra dificultad al desempeño de los peritos informáticos.

Criptografía: A medida que los sistemas ganan más y más interconexión las medidas de seguridad crecen por necesidad. Una de ellas es el encriptado. De esta manera, cuando un forense informático realiza un estudio es muy probable que se encuentre con información encriptada. Si el método de encriptado es conocido y se tiene lo necesario para desencriptar tal información, entonces no debería haber mayores problemas para tratar con tal información. Pero no siempre es así. Existen mecanismos de encriptado propios de algunos productores de dispositivos que no son dados a conocer y que pueden, obviamente, dificultar mucho la tarea de recuperación de la información.

Herramientas que cubren solo una parte del proceso: En el proceso de obtención de evidencias sería deseable que mediante una sola herramienta de software se pudieran realizar todas las tareas que son demandadas. Pero lo cierto es que raramente esto ocurre así. Con lo cual es necesario que eventualmente que el resultado de una herramienta pueda ser tomado por otra como punto de partida para continuar el proceso, lo que no siempre es posible.

Desconocimiento de la efectividad y cota de error de las herramientas: Cuando las herramientas utilizadas no son específicamente las provistas por los fabricantes de los dispositivos analizados, y aun cuando sean las provistas, es probable que no tengan una efectividad absoluta. Por ejemplo, un software podría ser capaz de obtener solo ciertas secciones de la información. Así entonces se llevarían a cabo inspecciones, con información resultante incompleta. Es importante conocer la efectividad y cota de error de la herramienta utilizada, con el fin de considerar la posibilidad de utilizar otras que brinden la misma funcionalidad.

Falta de guías y mecanismos de validación: Al presente aún no existe un modelo universal a seguir en el proceso de recolección de evidencias informáticas y su validación. Entonces en un contexto tan complejo como el comentado se hace evidente que el éxito de la extracción de evidencias termina dependiendo de la destreza, experiencia e inventiva del forense.

La complejidad del Proceso de Recuperación de Información

Como punto de partida es necesario tener claro que la finalidad de la informática forense es el hallazgo de evidencias digitales las cuales se definen como información de valor almacenado o transmitido en una forma binaria, para ayudar a determinar el origen de incidentes como los delitos cibernéticos.

La obtención de este tipo de evidencias no es un proceso simple. Este proceso comprende la adquisición, validación, análisis, interpretación, documentación y presentación de las mismas. Como puede verse, entonces, es un proceso compuesto de varias etapas de distintas naturalezas que por consiguiente presentan diferentes problemáticas y dificultades a sobrellevar.

Para dar una noción de la magnitud de este proceso, a continuación se mencionan algunas de las posibles técnicas y herramientas utilizadas, comentando las dificultades que pueden presentarse.

Adquisición y validación de datos

Con el fin de recolectar la evidencia digital, los procedimientos forenses tradicionales examinan gran diversidad de dispositivos electrónicos y soportes de almacenamiento manteniendo la integridad de la información original.

Es claro que la complejidad de la tarea de adquisición dependerá esencialmente de la naturaleza del dispositivo a analizar y se puede diferenciar en:

Adquisición en soportes de almacenamiento extraíble

Si hablamos de soportes como ZIP, CD-ROM, o DVD bastaría con realizar una lectura exacta de la unidad completa utilizando el lector correspondiente y finalmente validar la copia con algún mecanismo de “Hash#”. Esta validación es uno de los puntos que PURI tendrá en cuenta y propondrá como un paso formal ineludible a realizar en dicha tarea.

Adquisición en dispositivos de almacenamiento masivo

En caso de tratarse de un medio de almacenamiento más complejo como ser un pendrive o un disco rígido pueden presentarse ciertas complicaciones. Debido a algoritmos de optimización de tiempos, ocultamiento de espacio, encriptado de información y balanceo de frecuencia de uso de sectores, estos dispositivos, en donde la controladora se encuentra embebida junto al hardware propio del medio de almacenamiento dentro del mismo producto, suelen ser un problema dado que sin la controladora no es posible acceder al hardware pero con ella no se tiene la plena

seguridad de que la información obtenida sea la copia fiel de lo realmente almacenado. Las principales dificultades detectadas son:

Algoritmos automáticos de optimización: Es conocido que ciertas controladoras de discos de almacenamiento de estado sólido, con fines de optimizar escrituras futuras, realizan periódicamente barridos de verificación de los bloques en donde establecen a ceros aquellos que encuentren en desuso. El inconveniente aquí es que tales bloques podrían contener información que sirva de evidencia para el forense, que es eliminada en cada barrido. A su vez, otro problema a sobrellevar es que el barrido puede comenzar en el mismo instante en el que el dispositivo es conectado a una fuente de energía. Con lo cual normalmente el sistema operativo poco puede hacer para impedir esta actividad.

Mecanismos de ocultamiento de espacio: Actualmente existen técnicas soportadas por las controladoras de medios de almacenamiento para informar que el mismo dispone de menos capacidad de la que realmente tiene. Esta funcionalidad tiene diversas aplicaciones. Los fabricantes, comúnmente, con el fin de alojar en el espacio oculto información de resguardo del sistema, utilizan esta técnica que les permite recuperar el sistema de sus clientes en tiempos reducidos. Pero del mismo modo, una persona con conocimientos suficientes podría ocultar información de evidencia en esta sección oculta. PURI nuevamente viene a proponer que la detección de áreas ocultas sea un paso formal obligatorio en el proceso de recuperación de la información.

Encriptado de la información: Ciertamente el encriptado de la información es un recurso muy accesible para quien desee ocultarla. Pero el problema no solo se acota a archivos encriptados por software sino que existen mecanismos que involucran al hardware del mismo equipo que realizan cifrados de toda la unidad siendo virtualmente imposible recuperar la información sin disponer del equipo en cuestión. Por otra parte, también existen medios de almacenamiento removibles que en su misma controladora ejecutan algoritmos de encriptado de la información dificultando en gran medida la extracción de la misma sin conocer las claves de acceso. Entonces es claro que un paso inevitable sería verificar las dependencias que la unidad de almacenamiento puede llegar a tener con el hardware antes de removerla y devolver el resto del equipo.

Balanceo de frecuencia de uso de sectores: Las tecnologías de almacenamiento en estado sólido presentan limitaciones en tiempo de vida útil que obligan a distribuir la utilización del espacio a fin de que cada bloque tenga el mismo desgaste que el resto. Esto hace que la controladora deba ser un componente inteligente capaz de ejecutar los algoritmos que permiten realizar esta tarea; y con ello capaz de mostrar al sistema operativo la información que espera y no la que realmente contiene el medio de almacenamiento en los sectores solicitados. El inconveniente aquí es que si para evitar el problema, previamente mencionado, de eliminación de sectores en desuso se

reemplaza la controladora, probablemente tampoco sería posible leer la información dado que solamente la primera conoce la forma en que está distribuida la información en el medio.

Particularidades con servidores: No siempre es posible remover el dispositivo de almacenamiento del equipo donde se halla. La realidad es que cada vez más frecuentemente se deberán realizar pericias sobre equipos funcionando como servidores donde mantener una alta disponibilidad es crucial en todo momento. Con lo cual la detención de sus servicios para realizar la adquisición de su información debe ser acotada en el tiempo.

Dado que los medios de almacenamiento crecen en capacidad vertiginosamente y con ello el tiempo necesario para la copia de sus datos, es necesario entonces tener bien en claro cuál es el método más óptimo y confiable para realizar la adquisición en un escenario como el planteado. PURI estudia las diferentes variantes que existen en la actualidad esperando proponer un método de adquisición lo más eficiente posible.

Adquisición en Telefonía Móvil

Un punto importante de la investigación en este área es la extracción de evidencias situadas en la tarjeta SIM 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.

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. En este punto es visible una contrapartida de utilizar tal método la cual es que al leer la información que la SIM entrega consultando su sistema de archivos, se desestiman los espacios no utilizados que también podrían contener restos de evidencias. En el proyecto PURI se analizarán las posibles alternativas para evitar este tipo de pérdidas de información.

Una situación similar se encuentra al tratar con el teléfono móvil en sí más allá de la tarjeta SIM. Hoy en día dada la veloz evolución de estos dispositivos, en cuanto a espacio de almacenamiento y funcionalidades, se hace cada vez más necesario su análisis dado que pueden contener cualquier tipo de evidencia en su memoria.

Respecto a la memoria estos dispositivos, así como también las tabletas y otros similares, suelen tener un soporte removible (por ejemplo una tarjeta SD), así como también una memoria interna la cual no es fácilmente accesible sino a través del mismo dispositivo. Nuevamente el problema aquí es que el dispositivo actúa como filtro de tal información impidiendo una copia limpia y completa de todo lo realmente almacenado. En este proyecto entonces se intentará hallar la mejor alternativa para esta tarea.

Adquisición de datos volátiles en Computadoras Personales y Servidores

Toda la información volátil como las conexiones de red, historial de comandos o información relacionada con la ejecución de aplicaciones, es sumamente útil también dado que complementa a la estática obtenida de los medios de almacenamiento. Tal información reside en la memoria RAM y no es posible acceder a ella por medio de análisis forense del disco. Es necesario realizar la extracción en pleno funcionamiento y según el estado del equipo pueden presentarse varias dificultades. En este proyecto se analizarán las dos vías posibles a utilizar, por software y por hardware, y se introducen brevemente a continuación:

Por hardware: La idea de utilizar hardware es lograr pasar por alto al sistema operativo y acceder directamente a la controladora de la memoria RAM. Por ejemplo, es posible utilizar una tarjeta PCI dedicada a tal operación, que teniendo acceso directo a memoria (DMA) realiza una lectura completa de la misma. La desventaja de esta técnica es que requiere que la placa esté previamente instalada al momento en el que se realiza la pericia.

Por software: Las alternativas por software requieren que el sistema operativo provea algún mecanismo de volcado de memoria. Por ejemplo, existen ciertos sistemas que contemplan este tipo de funcionalidad con el fin de realizar un volcado en caso producirse un error. Esto facilita mucho la recuperación del estado del sistema, previo al error producido. Tal funcionalidad es aprovechada entonces por aplicaciones que solicitan su ejecución y obtienen una copia del contenido de la RAM en un determinado instante.

Análisis e interpretación de datos

Esta es una etapa subsiguiente a la de adquisición y consiste en interpretar los datos adquiridos y validados para determinar su importancia en el caso intentando hallar evidencias que lleven a la revolución del mismo. Probablemente sea la etapa más extensa en todo el proceso de peritaje dada la diversidad de métodos, técnicas y procedimientos posibles a aplicar. Pero no solo es la variedad de recursos a utilizar lo que hace tan compleja esta etapa sino también las innumerables formas de ocular

información que existen. Es principalmente aquí donde se hace evidente la necesidad de una guía que oriente al forense en su labor, a fin de que se efectúen todos los pasos necesarios que lleven a la correcta extracción de las evidencias, y que el éxito de la tarea no recaiga en su destreza y memoria exclusivamente.

Esta etapa requiere una comprensión completa tanto de la estructura física y del funcionamiento de los medios de almacenamiento y dispositivos, como de la forma y la estructura lógica en la que almacenan los datos. A continuación se introducen algunas técnicas de análisis a fin de dar una idea de la diversidad de recursos que el forense podría aplicar:

Búsqueda de cadenas: es una de las técnicas más tradicionales en el análisis forense, consiste es la búsqueda de cadenas significativas como contraseñas o direcciones de red que son relevantes para la investigación. Ventajas: facilidad de uso. Desventajas: proporciona información sin un contexto global que en su mayoría se infiere por el investigador.

Recupero de archivos eliminados: Ciertamente en los sistemas actuales, los archivos no son eliminados físicamente sino en su forma lógica. Esto implica que la información permanece aún después de ser eliminada del sistema. Siendo así, el informático forense puede intentar reconstruir la estructura de los archivos que la contenía a fin de buscar evidencias en la misma. Existe una gran variedad de métodos de recuperación de archivos eliminados (y herramientas que los implementan) que trae a consecuencia que sea confuso conocer previamente cual es el más óptimo de ellos para el caso particular que se presente al forense.

Análisis de la cola de impresión: Normalmente los sistemas operativos de hoy en día utilizan una cola de impresión que en su implementación utiliza archivos alojados en forma estática en disco. Estos archivos son eliminados usualmente con la frecuencia que el sistema determina en un proceso que el usuario no percibe. Con lo cual, independientemente de que el usuario elimine completamente el archivo original, la información podría existir aún alojada. Es evidente entonces que el análisis de la cola de impresión debe proponerse como un paso necesario en la pericia.

Búsqueda de objetos de procesos en Windows: un proceso de Windows tiene asociada una estructura EPROCESS. De la misma manera, un subproceso de Windows tiene asociada una estructura ETHREAD. Uno o más hilos pertenecen a un proceso. Estas técnicas buscan en estructuras EPROCESS. Desventaja: los tamaños y los valores de las estructuras cambian entre los sistemas operativos Windows y las versiones de service packs.

Búsqueda en firmas de objetos: se pueden utilizar firmas específicas de objetos (palabras claves de los objetos, como nombres de propiedades o campos) para identificarlos en la memoria. El enfoque principal es analizar el conjunto de firmas para identificar los objetos ocultos.

Conclusión

La idea esencial es tratar de obtener información fiable del estado del sistema, a partir de la adquisición y análisis de los datos obtenidos de memorias y dispositivos. Para tal fin, como cualquier otra ciencia, la informática forense hace uso de herramientas especializadas para obtener información significativa del objeto de estudio. El uso de técnicas correctas y herramientas, es decisivo para lograr dicho objetivo.

Las metodologías empleadas en la Informática Forense pueden ser diversas e independientes de la plataforma o sistema operacional donde se efectúen las actividades de los investigadores, pero deben cumplir ciertos requisitos con la información o evidencia identificada.

Surge entonces la necesidad de contar con un Proceso Unificado de Recuperación de la Información (PURI) que guíe al profesional forense en este proceso, indicándole las fases a seguir, el objetivo de cada fase, que tareas incluye y las técnicas y herramientas a aplicar para cumplir cada fase.

El proyecto PURI consiste en el estudio de las técnicas y herramientas disponibles en el mercado con el fin de generar un proceso unificado para recuperar información, y presentar propuestas de desarrollo de nuevas técnicas y herramientas.

Bibliografía

1. Forensic Examination of digital Evidence: A Guide for law enforcement, NIJ Report, US Department of Justice, Office of Justice Programs, disponible en *http://www.ojp.usdoj.gov/nij*
2. Survey of Disk Image Storage Formats Version 1.0, Common Digital Evidence Storage Format Working Group, Digital Forensic Research Workshop, 2006. Disponible en www.dfrws.org/CDESF/survey-dfrws-cdesf-diskimg-01.pdf
3. "An overview of mobile embedded memory and forensics methodology "
4. "FACE: Automated digital evidence discovery and correlation"
5. "Steganalysis in Computer Forensics"
6. Volatility and RegRipper User Manual, Mark Morgan: Mark.Morgan@iarc.nv.gov.
7. Help de la herramienta RegRipper.
8. ACPO (Association of Chief Police Officers) – England, Wales and North Ireland. Good Practice Guide for Computer-Based Electronic Evidence. Oficial release version. Disponible en www.acpo.police.uk (accedido el 3 de julio de 2011)

9. A guide to basic computer forensics – TechNet Magazine, Marzo de 2008. Disponible en www.technet.microsoft.com/en-us/magazine/2007.12.forensics.aspx (accedido el 11 de julio de 2011)
10. NIJ (National Institute of Justice) Report – United States of America, Department of Justice. Forensic Examination of Digital Evidence: A guide for Law Enforcement. Disponible en http://www.ojp.usdoj.gov/nij (accedido el 3 de Julio de 2011)
11. [12] Law Enforcement Investigations - Active Army, Army National Guard, and US Army Reserve. FM 3-19.13. Disponible en www.armystudyguide.com (accedido el 4 de Julio de 2011)
12. María Daniela Álvarez Galarza, "METODOLOGÍAS, ESTRATEGIAS Y HERRAMIENTAS DE LA INFORMÁTICA FORENSE APLICABLES PARA LA DIRECCIÓN NACIONAL DE COMUNICACIÓN Y CRIMINALÍSTICA DE LA POLICÍA NACIONAL". Ecuador. Disponible en www.dspace.ups.edu.ec/bitstream/123456789/546/5/CAPITULO4.pdf (accedido el 4 de Julio de 2011)
13. BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. Disponible: http://www.normes-internet.com (accedido el 4 de Julio de 2011)
14. IOCE, Guidelines for the best practices in the forensic examination of digital technology, 2002. Disponible: http://www.ioce.org (accedido el 5 de Julio de 2011)
15. INFORMATION SECURITY AND FORENSICS. Computer forensics. Part2: Best Practices, 2009 Disponible: http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part2.pd (accedido el 5 de Julio de 2011)
16. Guía Para El Manejo De Evidencia En IT - Estándares de Australia. APEC Telecommunications and Information Working Group. Disponible en http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf (accedido el 6 de Julio de 2011) 26