La Informática Forense y el proceso de recuperación de información digital.

Ana Haydée Di Iorio[1]

a Universidad FASTA, Gascón 3145, B7600FNK, Mar del Plata, Argentina

Abstract

Con la irrupción de la Sociedad de la Información, las nuevas tecnologías alcanzan practicamente todos los aspectos de nuestra vida. Al ser la información que se almacena digitalmente cada vez más importante, su recuperación pasa a ser considerada un aspecto crítico. Desde el punto de vista de la resolución de conflictos judiciales e investigación penal, una de las mayores problemáticas es la falta de un proceso unificado que guíe a los expertos forenses en esta tarea tan compleja, ya sea por la variedad de plataformas tecnológicas que pueden encontrarse, como por la diversidad de evidencias digitales. Se presenta en éste trabajo una propuesta de "Proceso Unificado de Recuperación de la Información", resultado de un Proyecto de Investigación de la Facultad de Ingeniería de la Universidad FASTA – Mar del Plata – Argentina, que pueda colaborar con los informáticos forenses y con los organismos de justicia.

Keywords: Recuperación de Información, PURI, Informática forense, Evidencia Digital;

Introducción

Ya a fines del siglo XX comenzamos a vivir el paso de la Era Industrial a la Era del Conocimiento, caracterizada entre otras cosas por la denominada “Sociedad de la Información”.

Este cambio de paradigma implica modificaciones en los conceptos y formas de ver el mundo, así por ejemplo, pasamos de pensar una economía donde la riqueza se encontraba en los bienes de capital, bienes tangibles, a una economía donde la riqueza está dada por el acceso a la información y el conocimiento. En ese orden de ideas la creatividad, la innovación y las nuevas ideas se convierten en el combustible de la nueva economía.

A su vez, con la llegada del siglo XXI, específicamente en los últimos diez años, la sociedad ha estado experimentado un proceso gradual de despapelización, que trajo aparejado una dependencia prácticamente total de los sistemas informáticos para manipular información. Es así que nos encontramos debatiendo temas como e-justicia, e-gobierno y recientemente e-democracia.

Por otro lado, tareas cada vez más críticas son realizadas por software, desde intervenciones médicas hasta complejas operaciones militares.

Esta realidad hace que tanto los particulares, como las organizaciones, y los gobiernos, deban esforzarse por aumentar los mecanismos de resguardo, seguridad, auditoría y control de la información digitalizada, sobre todo si esta información precisa luego ser utilizada como medio de prueba en una actuación judicial.

Los cambios en las tecnologías, plataformas, medios de almacenamiento, legislaciones y aplicaciones de sofware, hace cada vez más necesario el uso de procesos, métodos, estándares y buenas prácticas, que brinden algún tipo de garantías en la recuperación de información almacenda digitalmente, y sobre todo, que permitan asegurar que se realizaron todas las tareas posibles con los mecanismos adecuados.

De esta manera, existiría algún medio para creer que si una información no es recuperada es porque no es posible hacerlo con la tecnología vigente y disponible al momento.

[1] Grupo Informática Forense. Facultad de Ingeniería. Universidad FASTA. Tel.:(+54-223)499-0418 ; diana@ufasta.edu.ar

En el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA se detectó la necesidad de los profesionales Informáticos Forenses que actúan judicialmente, de contar con un proceso de recuperación de información que sirva de guía en las tareas a realizar, que conste de una metodología, que haya sido probado, evaluado, y que sea capaz de reproducirse en instancias de juicio.

La Informática Forense y su papel en la investigación judicial

Según el FBI, la informática forense es la ciencia de "Adquirir, Analizar, Preservar y Presentar datos que han sido procesados electrónicamente en un medio computacional"

La Informática Forense nace como una rama de las ciencias forenses, una disciplina auxiliar a la justicia, que consiste en la aplicación de técnicas que permiten adquirir, validar, analizar y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

Las tareas de informática forense pueden llevarse a cabo tanto en procesos judiciales, como en cuestiones extra judiciales, sin embargo, la importancia de contar con un proceso unificado que auxilie en estas tareas está relacionada con la existencia de un aval científico que le permita a un oficial de justicia confiar en las tareas desarrolladas dentro de un proceso judicial.

El Dr. Julio Téllez Valdés define al Delito Informático como "una conducta típica, antijurídica y culpable en que se tiene a las computadoras como instrumento o fin", es decir, como instrumento para cometer cualquiera de los delitos ya tipificados, o como un fin en si mismo. Por ejemplo, en una estafa a través de sistemas informáticos, la informática es el medio; en cambio, en el caso de la distribución de virus informáticos, la informática es el fin.

En Argentina, la ley de delitos informáticos, ley 26.388 es sancionada en Junio del año 2008.

Es así que, a pesar del carácter correctivo que demarcan las bases de la informática forense, orientadas en forma casi exclusiva al marco legal, hoy en día su alcance es mucho más amplio, considerando que la presencia de las tecnologías de la información y la comunicación en la sociedad es una tendencia irreversible.

Si nos focalizamos en el ámbito penal, el Agente Fiscal, durante la etapa de instrucción, es quien dirige las acciones tendientes al desarrollo de la investigación, siguiendo las disposiciones establecidas en el ordenamiento procesal pertinente. En este proceso puede suceder que para la comprobación o explicación de ciertos hechos controvertidos, requiera de conocimientos ajenos a su saber específico. De allí surge la necesidad de ser auxiliado por personas que posean conocimientos específicos en alguna ciencia, técnica, industria o arte, con el fin de enriquecer la capacidad de juzgar.

El art. 244 del Código Procesal Penal (CPP) de la provincia de Buenos Aires, Argentina establece que "Se podrán ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinentes a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, técnica o arte".

Dentro de este marco, el Agente Fiscal es quien determinará la necesidad de producción de la pericia, y, como dispone el art. 248 del CPP, también será quien: dirija la pericia, formule los puntos periciales, fije el plazo de expedición del perito, asista a las operaciones, autorice al perito a examinar las actuaciones y asistir a determinados actos procesales y procure con el perito que las cosas a examinar sean

en lo posible conservadas de modo que la pericia pueda reproducirse.

El artículo expuesto precedentemente, entiende que el fiscal que dirige la instrucción tiene el conocimiento suficiente como para dirigir la pericia y formular las preguntas que integran el cuestionario pericial, todas y cada una de las cuales el perito deberá contestar. A su vez, las partes también podrán proponer puntos de pericia, los que tendrán que ser admitidos por el Fiscal, en tanto sean distintos a los indicados por él y conducentes para el proceso. En este orden de ideas, es conducente el pedido de un informe preeliminar, que permita esclarecer al Agente Fiscal el caso y le sirva de base para luego formular los puntos periciales que considere pertinentes.

Es así que, surge la necesidad de un profesional informático con conocimientos en criminalística y tareas de informática forense, que pueda colaborar con los organismos de justicia, tanto desde el área investigativa como desde el área forense.

En la República Argentina no se exige para la actuación como perito informático el estudio de una especialización, a diferencia de otras profesiones forenses, tales como médicina u otras carreras que si lo exigen. Cabe aclarar incluso, que los establecimientos de Educación Superior no ofrecen cursos o especializaciones para informáticos donde se pueda estudiar esta temática.

Por otro lado, la evidencia digital no está mencionada en los Códigos de Procedimiento, de ahí que no existe una actuación indicada por ley para la preservación de esta prueba.

El Proyecto de Investigación para la creación de un Proceso Unificado de Recuperación de la Información

El proyecto PURI nace en la conjunción de dos cátedras docentes de la facultad de Ingeniería de la Universidad FASTA, la cátedra de Sistemas Operativos y la de Informática y Derecho.

Tiene como objetivo general la generación de un proceso unificado para recuperar información y la presentación de propuestas de desarrollo de nuevas técnicas y herramientas, a partir de la detección de carencias.

Los objetivos específicos derivados del objetivo general propuesto son:

- El estudio y análisis de las fases a seguir para la recuperación de la información según las buenas prácticas sugeridas por organismos internacionales.
- La generación de un proceso unificado de recuperación de la información, donde para cada una de las fases se indique: el objetivo, las tareas que la componen, las técnicas disponibles y las herramientas.
- La propuesta de nuevas técnicas a utilizar en áreas carentes.
- La propuesta de desarrollo de nuevas herramientas y el desarrollo de prototipos funcionales

Para alcanzar los objetivos mencionados, se definen entonces cinco etapas bien identificadas, que conforman el plan de trabajo del proyecto con una duración estimada en veinticuatro meses.

En la primer etapa se propone realizar una investigación del tipo exploratorio para recopilar y analizar toda la documentación obtenida sobre recuperación de información con el fin de conocer el estado del arte. Luego, se procede a sintetizar y formalizar este conocimiento en un

proceso unificado divido por fases, cada una con sus objetivos, técnicas y tareas específicas. El proceso luego se valida con al menos dos casos de uso típicos en distintas técnologías base.

En esta etapa se realiza también el estudio de las técnicas y herramientas disponibles en el mercado con el fin de generar un proceso accesible al profesional forense actual.

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

Finalizado el proyecto se espera obtener el diseño de un proceso, las propuestas de las técnicas y herramientas efectivas al efecto de las fases carentes de ellas y los prototipos correspondientes.

En la redacción propuesta de proceso se sugieren ciertas herramientas hoy existentes en el mercado. Se han considerado las siguientes variables para determinar que herramientas sugerir: las pruebas de efectividad técnica realizadas por el equipo, el tipo de licencia (es decir, si se trata de software libre o propietario, si es open source o no), la compañia de respaldo, y el grado de madurez de la técnica.

Este proyecto propone entonces un proceso, hoy inexistente, que sirva de base y guía en la compleja tarea de recuperación de la información, que pueda ser utilizado como método formal para validar la labor del perito forense en su tarea de extracción de evidencias informáticas.

Desde el año 2001 diferentes autores y organizaciones han estado trabajando en guías de buenas prácticas en informática forense, muy buenas en lo suyo pero que no cumplían el papel de un proceso formal unificado, entre las que se pueden mencionar las siguientes:

- ACPO (Association of Chief Police Officers) – England, Wales and North Ireland. Good Practice Guide for Computer-Based Electronic Evidence. Oficial release version.
- A guide to basic computer forensics – TechNet Magazine
- NIJ (National Institute of Justice) Report – United States of America, Department of Justice. Forensic Examination of Digital Evidence: A guide for Law Enforcement.
- Law Enforcement Investigations - Active Army, Army National Guard, and US Army Reserve. FM 3-19.13. Chapter 11: Computer Crimes
- Metodologías, Estrategias y Herramientas de la Informática Forense aplicables para la dirección nacional de comunicación y criminalistica de la policia Nacional de Ecuador.
- RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving)
- Guía de la IOCE (International Organization on Computer Evidence) "Guía para las mejores practicas en el examen forense de tecnología digital"
- Guía de Mejores prácticas de la ISFS (Information Security and Forensic Society (Sociedad de Seguridad Informatica y Forense) Hong Kong .
- Guía Para El Manejo De Evidencia En IT - Estándares de Australia. APEC Telecommunications and Information Working Group.

De estas guías de buenas prácticas o recomendaciones, muchas abarcan solo una parte del proceso, otras son muy generales, otras focalizan únicamente en los temas delictivos, y ninguna de ellas aborda las técnicas existentes para realizar ciertas tareas, las herramientas disponibles en el mercado en la actualidad, así como tampoco las diferentes alternativas de acuerdo a la plataforma de software del equipo a periciar.

Este proceso PURI entonces, se define como una secuencia de fases compuestas por etapas que involucran tareas a llevar a cabo aplicando técnicas implementadas por herramientas

concretas que permiten ejecutar dichas tareas. Este modo de definir el proceso, brindará una visión detallada y abarcadora de todo lo concerniente a esta actividad, que inmersa en un entorno judicial requiere de una estricta formalidad, claridad y una excelsa ilustración detallada de las operaciones realizadas.

Fases Básicas de un Proceso PURI

Fases básicas del Proceso Unificado de Recuperación de la Información:

1) Fase de Adquisición

Esta fase comprende toda actividad vinculada con la generación de una réplica exacta de todo el contenido digital alojado en el dispositivo original. El motivo de realizar una copia de tal información viene originado por distintas razones que se mencionan a continuación:

1) La ciencia forense debe respetar tres principios básicos: No contaminación, actuar metódicamente y mantener la cadena de evidencia. Justamente en las ciencias informáticas la no contaminación se garantiza a través de la copia bit a bit del original, de esa manera, al trabajar sobre la copia se resguarda el original y se garantiza la no contaminación de la evidencia.

2) Además, el proceso de recuperación de información demanda cierto tiempo, durante el cual el dispositivo quedaría inutilizado para otras actividades. Al trabajar sobre la copia, se podría entregar el original al dueño.

3) Eventualmente el dispositivo que almacena la información en cuestión puede no ser siempre el más indicado para llevar a cabo las pruebas requeridas, debido a problemas de accesibilidad o velocidad. Esta es otra razón que fundamenta la obtención de una copia exacta de los datos a fin de trabajarlos eficientemente en un entorno apropiado.

4) En escenarios donde la justicia se encuentra involucrada es de crucial importancia exista un modo de reproducir las tareas efectuadas por el perito informático sobre la información original y obtener los mismos resultados. Esto no se lograría si no es contando con una réplica exacta del contenido del dispositivo.

Esta fase de adquisición comprende etapas que de acuerdo al entorno en el que se deba llevar a cabo la recuperación de la información, aplicará o no involucrarlas en el proceso. Es así que se procedió a dividir la adquisición de dispositivos móviles de otros dispositivos por sus características altamente diferenciadoras a todo nivel, tanto físico (hardware), cómo lógico (software).

2)Fase de Preparación

Esta fase involucra todos los procedimientos necesarios para generar el entorno de pruebas preciso para llevar a cabo en primer lugar la inspección, y eventualmente la recuperación de evidencias digitales.

Como primera etapa, la fase de preparación contempla la restauración de la imagen. Esto significa que si la misma se encontrara dividida, encriptada o comprimida deberá realizarse el proceso contrario, a fin de lograr el original.

A continuación se deberá validar que la restauración ha sido exitosa mediante un algoritmo de hash, como se mencionó previamente.

Si la imagen que se obtuvo es de un sistema de archivos de un determinado sistema operativo, entonces será útil generar una máquina virtual que tome dicha imagen como su disco principal. Al hacerlo se debería realizar una copia a fin de no alterar la imagen original.

Opcionalmente puede montarse la imagen a fin de tratar los datos contenidos en la misma como un dispositivo de almacenamiento conectado al equipo de trabajo.

Finalmente esta etapa contempla la identificación de tipos de sistemas de archivos y sistemas operativos contenidos en los medios de almacenamiento originales.

3)Fase de Análisis

Esta fase comprende el fuerte del trabajo en donde se analiza el contenido adquirido en busca de vestigios de lo que se quiere hallar. El objetivo final de la fase de análisis en el caso de un proceso judicial o pre-judicial es encontrar la denominada Evidencia Digital, es decir, aquello que relaciona el hecho ocurrido con el "imputado" y la "victima". Entonces, se piensa en la evidencia digital como en un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

La fase de análisis comprende las siguientes etapas:

1. Extracción lógica
2. Extracción física
3. Análisis de relaciones

La extracción lógica representa la recuperación de información eliminada a partir del sistema de archivos. Por esa razón se denomina "lógica", ya que no se accede en forma directa a los bloques, sino a través del Sistema de Archivos, y del Sistema Operativo como intermediario. La mayoría de los sistemas operativos no eliminan la información en el momento en el que un Usuario solicita el borrado de un archivo determinado, sino que , de alguna manera, dejan registrado que el espacio que ocupaba dicho archivo ahora se encuentra disponible. De esta manera, por ejemplo, si fuese posible hallar tal espacio entonces sería posible reconstruir la información original.

La extracción física comprende la búsqueda de la información directamente en el espacio de datos omitiendo todo tipo de estructura de sistema de archivos. Con lo cual se da caso omiso a los metadatos y se aplican diferentes técnicas sobre el contenido puro del bloque en el dispositivo de almacenamiento.

La etapa de análisis de relaciones trata justamente de identificar relaciones entre conjuntos de archivos, con el fin de obtener una conclusión. Esto involucra puntualmente la Identificación de relaciones entre conjunto de archivos vinculados a una actividad en particular (ej: archivos relacionados a la navegación por internet) y la verificación de aplicaciones instaladas, entre otros. A continuación se presenta el detallado del proceso, con las técnicas existentes y herramientas recomendadas. Indicando "Nicho Carente" en aquellas áreas donde aún no hay soluciones disponibles.

Reflexiones y Conclusiones

El proceso propuesto presentado se validó para las plataformas de escritorio Linux Ubuntu, Microsoft Windows y Mac OSX, y en Android para dispositivos móviles.

A partir de esta validación, y de la búsqueda de técnicas propuestas por investigadores y herramientas específicas es que se detectaron áreas carentes con potencialidad de ser resueltas desde la academia, en beneficios de las ciencias forenses en general, y de la sociedad en particular.

Es así que se trabajó en dos prototipos de aplicaciones para llenar estos nichos carentes, especificamente vinculados con tecnologías de carving: Proyecto CIRA, y en recuperación de la información de perfil de usuario, Proyecto PRIP.

Por las características propias de las tecnologías de la información y la comunicación, su gran dinamismo y diversidad, es necesario contar con algún proceso que sea lo suficientemente amplio, como para adaptarse a cualquier tecnología, y a su vez, tuviera guías concretas de implementación en plataformas específicas con herramientas actuales y a disposición.

Entendemos que esta primer propuesta de un proceso unificado de recuperación de la información, su difusión y uso, pueden ser el puntapié para que este proceso siga madurando y fortaleciéndose.

Agradecimientos

Quiero agradecer al Ing. Roberto Giordano Lerena, decano de la Facultad de Ingeniería de la Universidad FASTA por confiar en nosotros, y ayudarnos en la elaboración de este proyecto; a la Lic. Mónica Pascual, Secretaria de Investigación, por su excelente predisposición en todo momento, y a todos los integrantes, pasados y actuales, del grupo de Informática Forense y Sistemas Operativos.

References

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 accedido el 10 de Enero de 2013
2. Computer-Based Electronic Evidence. Oficial release version. Disponible en www.acpo.police.uk (accedido el 3 de Enero de 2013)
3. 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 Enero de 2013)
4. NIJ (National Institute of Justice) Report – United States of America, Department of Justice. Forensic
5. Examination of Digital Evidence: A guide for Law Enforcement. Disponible en http://www.ojp.usdoj.gov/nij (accedido el 3 de Enero de 2013)
6. 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 Enero de 2013)
7. María Daniela Álvarez Galarza, "METODOLOGÍAS, ESTRATEGIAS Y HERRAMIENTAS DE LAINFORMÁTICA 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 Enero de 2013)
8. 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 3 de Enero de 2013)
9. IOCE, Guidelines for the best practices in the forensic examination of digital technology, 2002. Disponible:
10. http://www.ioce.org (accedido el 5 de Julio de 2011)
11. INFORMATION SECURITY AND FORENSICS. Computer forensics. Part2: Best Practices, 2009 Disponible: http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part2.pdf (accedido el 5 de Julio de 2011)
12. 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 Enero de 2013)
13. Carrier B D, Spafford E H (2003) "Getting Physical with the Digital Investigation Process" International Journal of Digital Evidence, Volume 2, Issue 2

14. Casey E, Palmer G (2004) "Digital Investigation Process" Chapter 4 in Digital Evidence and Computer Crime, 2nd Edition. Academic Press
15. Ó Ciardhuáin S (2004) "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, Volume 3, Issue 1
16. Beebe and Clark (2005) "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process" Digital Investigation Journal, Volume 2, Issue 2
17. - Casey E & Schatz B (2011) "Conducting Digital Investigations" Chapter 6 in Digital Evidence & Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition, Academic Press.