Construyendo una Guía Integral de Informática Forense

Ana H. Di Iorio*, Hugo Curti**, Fernando Greco**, Ariel Podestá*, Martín Castellote*, Juan Iturriaga**, Santiago Trigo**, Bruno Constanzo*, Gonzalo Ruiz de Angeli*, Sabrina Lamperti***
InFo-Lab
Universidad FASTA, Ministerio Público de la Provincia de Bs.As., Municipalidad de General Pueyrredón
**{diana, arieluf, tinchocapoeira, bconstanzo}@ufasta.edu.ar*
***{hcurti, fmartingreco, juaniturriaga, santiago.trigo, gonzalo.ruizdeangeli}@gmail.com*
****slamperti@mpba.gov.ar*

Abstract

Con la creciente inserción de la informática en la vida diaria, cada vez es más común que se encuentren involucrados en cuestiones judiciales elementos informáticos, directa o indirectamente. Es entonces necesario el desarrollo y la adopción de un método científico y probado para guiar la actuación informático-forense. No sólo se le necesita como guía para la validación y verificación de las pericias que se realicen, sino también para poder referir a jueces, fiscales, instructores, abogados y nuevos peritos sobre las correctas prácticas en la disciplina.

1. Introducción

En la sociedad moderna es cada vez mayor la prevalencia de dispositivos informáticos y sistema de información para cada vez más aspectos de la vida de las personas. Desde las computadoras que se utilizan a diario para trabajar, hasta los teléfonos inteligentes que cada vez más personas llevan consigo, pasando por tarjetas de crédito, tarjetas de transporte público, relojes inteligentes, autos inteligentes, o incluso cámaras de video, la interacción de las personas con la informática es cada vez mayor, y más sutil que en otras épocas. De esta interacción, los sistemas informáticos se convierten en fuentes de información objetiva, organizada y confiable sobre las personas y sus actividades. Esto es de suma importancia para instancias legales en las cuáles pueda ser necesario utilizar, verificar o correlacionar la información que recuperan diversos sistemas informáticos sobre un individuo.

Esta información debe recuperarse de forma organizada, coherente, y siguiendo un proceso que sea repetible y replicable, tratando de no alterar los objetos de pericia, o alterarlos lo menos posible, para que la información recuperada por el perito o experto informático ser incluida en un proceso judicial.

Sin embargo, la velocidad del desarrollo tecnológico, la diversidad de tecnologías y la reciente irrupción de la informática en la sociedad conspiraron para generar una situación en donde hay expertos con un alto grado de conocimiento informático pero poca experiencia judicial forense, o expertos judiciales con pocos conocimientos de informática. Los individuos que reúnen el conocimiento técnico y legal para afrontar la situación actual son una pequeña minoría, y hay poco soporte formal para su actuar.

Aunque existen guías de recomendaciones, sugerencias, buenas prácticas y algunos protocolos provisorios para afrontar la realidad, es claro que se necesita la propuesta de protocolos o guías que puedan enmarcarse en la situación legal e institucional de nuestra región, para brindar a los expertos informáticos un marco de actuación, y al sistema judicial una herramienta con la cual guiar, capacitar y medir el desempeño de sus peritos informáticos.

2. Marco Teórico y Trabajo Previo

A lo largo de los años diversas instituciones han propuesto guías de recomendaciones y buenas prácticas [1-5] que orientan a los profesionales en la realización de pericias, informes de juicio experto y procesos de recuperación de información en ambientes no judicializados o con fines privados. También se formularon diversos *Request For Comments* [6] con respecto a cuestiones de la informática forense, y luego la norma ISO/IEC 27037 [7] sobre la adquisición y preservación de evidencia digital, junto con la norma ISO/IEC 27043 que está en preparación [8] sobre los principios y procesos de una investigación digital. La problemática con estos documentos es que son acotados

en su alcance, difíciles de adaptar a la normativa de nuestro país y nuestra situación institucional, o no están terminados y evaluados por la comunidad científica. Por estas razones es necesario tomarlos como base, generalizar un proceso abarcador y adaptarlo a la realidad de nuestro país.

Un primer paso en ésta dirección fue dado por Podestá et al. [9], y luego profundizaron algunos aspectos de la problemática de Cloud Computing [10]. Sin embargo, estos trabajos asumen que los objetos y equipos sobre los que debe trabajar el perito ya se encuentran secuestrados o disponibles en el laboratorio, es decir, no indican el correcto proceder al momento de recolectar las fuentes de evidencia digital. Tampoco se definen roles ni responsabilidades, como se hace en las Normas ISO, y quedan pendientes las cuestiones de una implementación y práctica real del proceso propuesto en ambientes e instituciones reales. A continuación se verán algunos conceptos de Informática Forense & Respuesta a Incidentes (IFRI) que sentarán la base para el Desarrollo y Propuesta de este trabajo.

Las guías de recomendaciones existentes plantean, a grandes rasgos, el mismo proceso, con mayor o menor nivel de detalle y con distintas consideraciones sobre el proceso legal. Algunos de los conceptos que manejan todas las guías son:

- **Evidencia digital:** es información o datos, almacenada o transmitida en un medio informático, que puede ser utilizado como evidencia en un proceso judicial. La evidencia digital se caracteriza tanto por su fragilidad como por la facilidad con que puede realizarse una copia fiel de la misma[1].
- **Fuente de evidencia digital:** es un medio o dispositivo del puede obtenerse evidencia digital.
- **Relevamiento:** es el proceso de buscar, reconocer y documentar potencial evidencia digital.
- **Recolección:** es el proceso de secuestrar o reunir elementos físicos pasibles de contener evidencia digital.
- **Adquisición:** es el proceso de generar una copia de datos de un conjunto definido.
- **Preservación:** es el proceso de mantener y resguardar la integridad y/o condición original de la potencial evidencia digital.

El cálculo de *hashes* o digestos matemáticos se realiza inmediatamente luego de la Adquisición, y es una de las tareas principales para la correcta Preservación de la evidencia digital. Por lo general, se utilizan hashes MD5 o SHA-1. Si bien hay discusiones respecto de la validez criptográfica de MD5 o SHA-1, la utilización de ambos digestos en conjunto, digestos por segmento de archivo, u otros digestos criptográficamente seguros, como SHA-2 o SHA-3, son suficiente medida para brindar el respaldo necesario

Además de los conceptos recién vistos, pueden considerarse algunos otros conceptos adicionales:

- **Extracción:** es el proceso de extraer información particular de las fuentes de evidencia digital. Se separa del análisis propiamente dicho porque en ocasiones los procesos de extracción generan mucha información que luego no resulta ser evidencia digital, y no merece análisis.
- **Análisis:** es el proceso de interpretar la información extraída en el contexto de los puntos periciales y el interés de los investigadores del caso.

Estas definiciones hacen al modelo de proceso, pero brindan poca información en cuanto a las cuestiones técnicas propiamente dichas. En este punto hay que tener cuidado, si bien deberían brindarse secuencias de pasos o recomendaciones sobre cómo trabajar, si se es demasiado específico se corre el riesgo de especializar demasiado el protocolo sobre una tecnología.

3. Modelo Propuesto

El modelo que se plantea para la "Guía Integral de Empleo de la Informática Forense en el Proceso Penal" se basa en las fuentes citadas anteriormente, y otras guías y procesos existentes, buscando obtener un modelo extensivo que cubra la totalidad del proceso pericial e investigativo, y lo integre adecuadamente en el proceso penal, cumpliendo con sus requerimientos y exigencias. Además de contemplar las guías existentes y los modelos académicos presentados en distintos congresos, conferencias y revistas, se tuvo en cuenta para el desarrollo de esta guía su inserción en instituciones reales y el marco legal de la Provincia de Buenos Aires. Varias diferencias y modificaciones con respecto a otras guías surgen de este análisis y del trabajo realizado para adaptar de la teoría a la realidad.

En primer lugar, se dan definiciones de conceptos y glosario, similares a las planteadas por las Normas ISO/IEC 27037 y 27043. Luego, se plantean tres roles definidos para los expertos, en lugar de los dos roles que plantea la Norma ISO:

- **Especialista en Recolección:** es un rol básico, entrenado con el mínimo conocimiento técnico para manejar adecuadamente la recolección de evidencia digital, y resguardar la escena y los objetos para evitar la contaminación o eliminación de información en las fuentes de evidencia digital presentes. Este rol también es

[1] Por esta razón, en algunas guías se define la "copia de la evidencia digital" como una copia fiel, idéntica al original, y que puede verificarse mediante digestos matemáticos. En esta característica fundamental de la informática forense, surgen algunas de las diferencias con respecto a otras ciencias forenses.

ideal para fuerzas de seguridad, que en ocasiones son las primeras en llegar a una escena del hecho.

- **Especialista en Adquisición:** es un rol más avanzado, que puede manejar también tareas de adquisición y preservación de fuentes de evidencia digital. Debería presentarse en la escena del hecho si es necesario realizar tareas de adquisición, ya sea de medios de almacenamiento volátiles como de información volátil.
- **Especialista en Evidencia Digital:** es el rol del perito informático propiamente dicho, quien realiza la restauración de las imágenes y volcados, el análisis, y los informes periciales y presentación de los resultados.

Si bien los roles se definen distintos entre sí, una misma persona puede asumir más de un rol de ser necesario. La separación de los roles en distintos individuos permite optimizar los recursos,

Para organizar las tareas, se proponen 6 fases que el experto informático recorre a medida que va avanzando la investigación o pericia. Cada fase tiene Tareas, Actividades, Técnicas y Herramientas asociadas. Las Tareas guían a un nivel macro, mientras que las Actividades explican y particularizan el actuar. Las Técnicas y Herramientas se brindan como sugerencias para resolver una Actividad en particular. Algunas tareas especiales abarcan más de una fase, o la totalidad del modelo o proceso. Las fases propuestas son:

1. Fase de Relevamiento.
2. Fase de Recolección.
3. Fase de Adquisición.
4. Fase de Preparación.
5. Fase de Extracción y Análisis.
6. Fase Presentación.

En el Gráfico del Anexo I, puede verse cómo se organizan las Fases y las Tareas dentro de cada una de ellas. Si bien el gráfico parece indicar un cierto orden o secuencialidad de las fases y las tareas, debemos destacar que no es un orden estricto, ya que dependiendo cómo se desarrolle la investigación y la tarea pericial, puede ser necesario que se vuelva a Fases o Tareas anteriores, para realizar nuevamente Actividades[2].

Se detallarán a continuación las Fases, con una breve explicación de su propósito y las tareas que la componen, pero sin llegar a los niveles de granularidad más finos.

La Fase de Relevamiento abarca la investigación para conocer el caso e identificar los posibles objetos de interés. Esta fase puede identificarse con las tareas investigativas de una investigación judicial, o con una entrevista de "reconocimiento" en el caso de un trabajo privado no judicial. Las tareas que la componen son:

- **Identificación de documentación legal y técnica:** consiste en identificar toda la documentación, ya sea legal, de infraestructura, diseño, hardware, software o cualquier otra documentación relevante para conocer el caso en profundidad y poder tomar las decisiones adecuadas. Si no hay documentación sobre la cual trabajar, o no hay consideraciones legales que deban tenerse en cuenta, no es necesario profundizar en esta tarea.
- **Identificación de infraestructura IT:** consiste en identificar la infraestructura de red y/o hardware sobre la cual se va a trabajar. En investigaciones donde se involucran redes de computadoras, servidores, o sistemas Cloud es muy importante identificar correctamente los objetos que intervienen para preparar adecuadamente las fases de Recolección y Adquisición.

La Fase de Recolección abarca las acciones y medidas necesarias para obtener los equipos sobre los cuales se deberá trabajar posteriormente. En una investigación judicial se corresponde con etapas de allanamiento, o trabajo sobre una escena del hecho, mientras que en trabajos particulares contempla el primer contacto con las fuentes de evidencia digital. Las tareas que la componen son:

- **Detección de Infraestructura IT:** esta tarea se compone de actividades relacionadas con inspeccionar y evaluar el lugar para detectar todos los objetos de interés para la investigación.
- **Recolección de Objetos:** esta tarea se compone de las actividades relacionadas con el correcto levantamiento de los objetos de la escena, y su correcta preservación de acuerdo a los protocolos de cadena de custodia.

La Fase de Adquisición abarca todas las tareas en las que se obtienen las copias del contenido que se irá a analizar. Esta fase puede realizarse tanto en el lugar del hecho, durante un allanamiento o procedimiento judicial, o en un laboratorio forense luego de haber recolectado los objetos. Las tareas que componen esta fase son:

- **Adquisición de Medios de Almacenamiento Persistente:** consiste en adquirir una copia bit a bit de los medios de almacenamiento persistentes de un dispositivo, ya sean discos, CD/DVD/Blu-Ray, tarjetas de memoria, pen drive, etc.
- **Adquisición de Datos Volátiles:** consiste en adquirir una copia, con la menor alteración posible, de la memoria RAM de los equipos.
- **Adquisición de Tráfico de Red:** consiste en adquirir un volcado del tráfico de una red. Esta

[2] Nótese que hablamos de "modelo" en lugar de "proceso", como hacen otras guías y protocolos, por esta razón.

tarea es especial porque requiere una duración en el tiempo mayor que los otros tipos de adquisición.

- **Adquisición de Smartcards:** consiste en adquirir una copia de la información contenida en algún tipo de Smartcard. Esta tarea se distingue de la Adquisición de Medios de Almacenamiento Persistentes por la arquitectura e interfaz marcadamente distinta de las Smartcards con respecto a los otros.
- **Validación y Resguardo:** consiste en generar digestos matemáticos (MD5, SHA-1, SHA-2, etc) para las imágenes y volcados generados en la adquisición.
- **Transporte no supervisado:** consiste en el cifrado de la información para asegurar que durante su transporte no pueda realizarse una copia que pueda comprometer el caso.

La Fase de Preparación involucra las tareas técnicas en las que se prepara el ambiente de trabajo del informático forense, la restauración de las imágenes y volcados forenses, junto con su correspondiente validación, y la selección de las herramientas apropiadas para trabajar en la extracción y el análisis. Las tareas que componen esta fase son:

- **Preparación de Extracción:** consiste en preparar el entorno de trabajo para recomponer, descomprimir y validar las imágenes de dispositivos, y mapearlos a dispositivos, montar las imágenes como particiones o generar máquinas virtuales para el trabajo de análisis.
- **Identificación:** consiste en identificar las particiones, sistemas de archivos y sistemas operativos que puedan encontrarse presentes en las imágenes a analizar.
- **Preparación del Ambiente:** consiste en instalar y configurar las aplicaciones necesarias para el trabajo de análisis.

La Fase de Extracción y Análisis comprende las tareas de extracción de la información de las imágenes, selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales o requerimientos de un particular.

Con el fin de abstraer lo mejor posible el Análisis y no atarlo a ninguna tecnología o plataforma en particular, se separa en 3 niveles abstractos, el nivel de Aplicación, el nivel de Plataforma y el Bajo Nivel. Esta separación es un modelo simple permite separar adecuadamente las actividades específicas de análisis de acuerdo al objeto de análisis y su dependencia con técnicas y herramientas específicas.

Esta fase se compone de las siguientes tareas:

- **Extracción a Nivel de Aplicación:** esta tarea reúne las actividades de análisis particularizado a nivel de aplicación. En esta tarea se extrae información de las aplicaciones instaladas en los equipos que se analizan, para obtener información de uso de las mismas, archivos abiertos, historiales y registros de utilización, archivos de datos, etc. El objetivo es conocer qué se hizo con las aplicaciones con el mayor grado posible, en la medida que resulte relevante para el caso.
- **Extracción a Nivel de Plataforma:** esta tarea consiste en la extracción de información relacionada con el sistema operativo, sistemas de archivos, y su configuración. Es de un nivel inferior que la Extracción a Nivel de Aplicación, pero también permite un análisis más profundo. En esta tarea encontramos actividades como la extracción de información del registro de Windows, de un volcado de memoria, de un sistema de archivos particular, etc.
- **Extracción a Bajo Nivel:** en esta tarea se concentran las actividades de recuperación de información al nivel lógico más bajo, cuestiones como *data carving* y *file carving*, búsqueda de información por medio de expresiones regulares, búsqueda de información en las áreas de paginado o bases de datos en particiones sin formato, por citar algunos ejemplos. Toda actividad en donde se esté trabajando a un nivel inferior al sistema operativo y sus mecanismos puede considerarse una actividad de bajo nivel.
- **Análisis de Contenidos:** es una tarea de alto nivel que engloba el análisis del contenido, la información propiamente dicha que se almacena en los datos extraídos en las tareas anteriormente mencionadas.
- **Análisis de Relaciones:** es una tarea de alto nivel que engloba el análisis de la relación de los distintos elementos y el contenido recuperado entre sí y con los elementos del caso, para poder descubrir la relevancia de los datos que se recuperan o los objetos que intervienen en un caso.

Como un comentario adicional, las tareas de Análisis son especiales en el sentido que tienen un alcance mayor que solamente la Fase de Extracción y Análisis. La tarea de Análisis de Relaciones puede extenderse por la totalidad del proceso

Finalmente la Fase de Presentación comprende el armado de los informes necesarios y la presentación del caso en un juicio o a los solicitantes, sus tareas son:

- **Armado del Informe:** es una tarea de alto nivel, que corresponde con la documentación de las tareas y actividades realizadas y el armado de un informe pericial que sea claro, preciso y

permita reproducir y replicar el proceso de análisis llevado a cabo.

- Preparación de la Información a Presentar: esta tarea consiste en la preparación para una eventual presentación, ya sea en juicio o a los solicitantes de la pericia. En ocasiones es posible que el perito deba brindar una presentación donde explique el trabajo realizado, además del informe correspondiente.

Se han explicado las Fases y sus Tareas, tratando de mantener breve la exposición. Como se dijo anteriormente, las Tareas se componen de Actividades de menor nivel, particulares a un trabajo determinado. Por una cuestión de brevedad, no se explicará ese nivel con el mismo detalle, sin embargo haremos algunas consideraciones.

Las Actividades tienen asociadas Técnicas y Herramientas. Por ejemplo, la Actividad de "Extracción de archivos en espacio no asignado", se refiere a las técnicas de *file carving* y *data carving* que permiten recuperar información en situaciones de extrema adversidad. Para estas Técnicas, se sugieren herramientas que nuestro grupo de investigación ha evaluado, utilizado y comparado. Debido a que las técnicas, y las herramientas que implementan dichas técnicas, están sujetas a cambios y desarrollos tecnológicos, éstas se incorporan en nuestra Guía dentro de Anexos Técnicos y Hojas de Datos. Esto permite actualizar estas secciones sin modificar la Guía, lo que brinda estabilidad al modelo planteado para no tener que validarlo y auditarlo cada vez que se quiera sugerir una nueva técnica o herramienta para resolver una Actividad determinada.

4. Conclusiones y Trabajo Futuro

El modelo propuesto en la "Guía Integral de Empleo de la Informática Forense en el Proceso Penal" es una propuesta para formalizar y enmarcar la actividad en un proceso científico, evaluado, probado y mejorado a lo largo de los años. Se basa en guías y estándares internacionales, trabajos del ámbito nacional y regional, y además se combina con la experiencia de criminalistas, peritos informáticos, abogados, instructores judiciales y fiscales con experiencia real.

El trabajo en un equipo interdisciplinario además logró una unión entre academia y práctica, reuniendo a los investigadores universitarios con los practicantes tanto de la actividad pericial como de las actuaciones judiciales, y eso generó una sinergia en la cual ambas partes aprendieron del otro. Este aprendizaje contribuyó a mejorar los modelos iniciales de PURI, que eran demasiado abstraídos de las problemáticas judiciales y las situaciones que suceden en una investigación real. También sirvió de oportunidad para discutir temas de ocultamiento de información, técnicas anti-forenses y técnicas forenses de alta complejidad a los expertos de Ministerio Público, y discutir con ellos la necesidad de actuar siguiendo determinados protocolos, técnicas, y la importancia de las distintas formas y fuentes de evidencia digital para poder trabajar con una imagen completa de los hechos.

El trabajo a futuro consiste principalmente en la actualización de las Hojas de Datos y Anexos en donde se ubican los contenidos particularizados de la Guía, que contienen la información sobre técnicas y herramientas que cambia más rápidamente. Además se buscará la inserción del protocolo en ambientes apropiados, para su utilización, evaluación y mejora tanto desde las sugerencias y desarrollos que puedan venir del ámbito académico, como aquellas que vengan desde la práctica en su utilización e implantación.

5. Referencias

[1] "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", Reporte Especial del NIJ, Departamento de Justicia de los Estados Unidos. Disponible en: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[2] "Good Practice Guide for Computer-Based Electronic Evidence. Oficial release version", ACPO (Association of Chief Police Officers) – England, Wales and North Ireland, disponible en http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[3] "Guidelines for the Management of IT Evidence", APEC Telecommunications and Information Working Group, disponible en http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[4] Álvarez Galarza, M. D., Guamán Reiman, V. A., "Metodologías, Estrategias y Herramientas de la Informática Forense Aplicables para la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional", Universidad Politécnica Salesiana, Sede Cuenca, Ecuador, Febrero 2008.

[5] Yussof, Y., Ismail, R., Hassan, Z., "Common phases of computer forensics investigation models", *International Journal of Computer Science & Information Technology* (IJCSIT), 2011, Vol 3, No 3.

[6] Brezinski, D., Killalea, T., "RFC 3227: Guidelines for Evidence Collection and Archiving", The Internet Society, Febrero 2002, disponible en http://www.normes-internet.com/normes.php?rfc=rfc3227

[7] "ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence".

[8] "ISO/EIC 27043 — Digital evidence investigation principles and processes"

[9] Podestá, A., Constanzo, B., Waimann, J., Castellote, M., Sansevero, R., "PURI: Proceso Unificado de Recuperación de

Información", Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática 2012, Mar del Plata, Argentina, Abril 2012.

[10] Podestá, A., Castellote, M., Constanzo, B., Waimann, J., Iturriaga, J., "Dificultades de Investigaciones Penales en Cloud Computing", Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática 2014, Mar del Plata, Argentina, Mayo 2014.

6. Anexo I – Gráfico de Modelo