La Forensia como Herramienta en la Pericia Informática

Darío A. Piccirilli
Facultad Regional Buenos Aires. Universidad Tecnológica Nacional
Facultad de Informática. Universidad Nacional de La Plata
dpiccirilli@unlp.edu.ar, dariopiccirilli@gmail.com

—Abstract—Este documento contiene una descripción de los aportes que realiza la Forensia en Informática, contemplando las nuevas tecnologías que hoy día aplican en los procesos judiciales y que derivan en Pericias muy específicas y complicadas, tareas técnicas sobre las que no se puede generar ninguna duda en el tratamiento de la prueba. Es decir, el proceso de generación de la prueba, desde el secuestro de la misma hasta el análisis pericial, debe ser indubitable, de manera tal que quien deba impartir justicia pueda contar con elementos claros, contundentes y útiles. La informática puede considerarse que se encuentra relacionada en forma transversal con gran parte de la problemática judicial, aplicando en los distintos fueros de la Justica Argentina, tanto en lo Laboral, Comercial, Civil, Contencioso Administrativo Federal, Penal Económico, Criminal y también para la Corte Suprema.

***Palabras Clave*—Forensia, Pericia Infromática**

I. INTRODUCCION

Hoy día la informática se ha convertido en una herramienta o vehículo para la comisión de un delito., pero también esta ciencia es objeto de delitos. Dicho de otra manera, hoy es posible aplicar la informática para realizar una estafa, enviar una amenaza (intentando quedar en el anonimato), para obtener claves secretas de cuentas bancarias y así conseguir ilegalmente fondos dinerarios de otras personas, para realizar robo de datos de una empresa con distintos fines, acceso indebido a la información de la cía., daños en las páginas WEB, violación de la confidencialidad y secretos de la cía., entre otros.

A esto debemos sumarle casos vinculados con delitos sociales como la pedofilia o delitos federales como el Lavado de Activos y demás delitos financieros.

Lo expuesto hace que cuando se tenga que realizar una pericia informática, se deban considerar distintos aspectos a saber:

- El perfil del problema o del delito a peritar
- El procedimiento científico a aplicar
- La presencia de peritos de parte
- El procedimiento protocolar a aplicar, en relación a la situación procesal
- Las herramientas de forensia informática a aplicar o la combinación de más de una herramienta
- La posibilidad de nuevas pruebas
- La posibilidad de aclarar los puntos de pericia requeridos por el Juez que interviene en la causa
- La existencia de cadena de custodia de la prueba informática
- Las condiciones en que la prueba ha sido preservada

Sobre la base de lo mencionado, es de destacar que la forensia informática es un componente muy importante dentro de las Pericias Informáticas. No obstante lo expuesto, existe una novedosa aplicación de las herramientas de forensia para situaciones privadas, para pre constituír pruebas en forma previa a un pleito. Esto se aplica básicamente en los fueros Civil, Laboral o Comercial. Pues en el fuero Penal, generalmente la prueba ocurre ante un secuestro.

II. DESARROLLO

Considerando lo planteado en la introducción al tema, se desarrollan a continuación los puntos que caracterizan la temática planteada.

A. Perfil del problema o del delito a peritar

Es necesario saber que nunca existe una pericia informática igual a otra, a pesar que se encuentren caracterizadas por el mismo tipo de delito. Siempre varía:

- el escenario
- las pruebas y la modalidad en que han sido obtenidas
- las partes que intervienen en el pleito o en la investigación
- las herramientas que deben usarse
- el conocimiento que el perito debe aplicar, como así también su experiencia

Por ello, a veces es necesario integrar más de un perito a la tarea pericial. Pues a pesar que tengan todos la misma especificidad, es muy probable que no todos cuenten con la misma especialidad, experiencia y grado d conocimiento sobre la tarea a realizar.

B. Procedimiento científico a aplicar

Es el protocolo que se debe aplicar al momento de realizar una pericia informática, y parte del mismo es la herramienta de forensia a utilizar.

En el caso de existir peritos de parte, esta tarea debe ser consensuada entre todos los participantes, con el objetivo de obtener una prueba clara y útil para impartir justicia por la autoridad competente.

La tarea pericial debe ser debidamente comunicada a los especialistas de parte, debido a que la tarea no puede ser realizada en forma exclusiva por peritos de oficio, existiendo técnicos de parte que deban participar.

C. Herramientas de Forensia

Conforme lo establece el FBI, "*la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional"*. Por lo tanto, al momento de seleccionar es necesario conocer claramente lo que el Juez requiere para completar su investigación. Pues una investigación forense puede integrarse de las siguientes etapas que se describen en la siguientes subsecciones.

C.1. Objetivo a cumplir – investigar durante la pericia

En primer lugar se debe analizar el dispositivo objeto de la pericia. Por ejemplo: si es un disco rígido o un teléfono celular. En el caso de un disco rígido, es posible que se necesite investigar sobre:

- las características del sistema operativo instalado en el disco rígido
- si existen archivos borrados en un disco rígido secuestrado
- verificar las fechas de creación, modificación, borrado o último acceso a os archivos
- buscar archivos en espacios liberados por el sistema operativo que posee el disco rígido
- analizar si los discos fueron cambiados
- buscar en archivos que poseen claves y que no han sido provistas en forma previa al análisis de la información

En el caso de un teléfono celular, es posible que se necesite investigar sobre:

- mensajes de texto enviados y recibidos
- correos electrónicos enviados y recibidos
- contactos guardados en el dispositivo
- imágenes
- mensaje de voz
- georeferenciación de los archivos

Es de señalar que no todos las marcas y modelos de teléfonos celulares tienen las mismas posibilidades de búsqueda y hallazgos, particularmente los de origen chino, que en algunos casos llegan a poseer hasta seis (6) chips.

C.2. Protocolo a seguir una vez clarificado el objetivo

Una vez evaluado el dispositivo celular o elemento óptico o magnético a estudiar, es necesario definir:

- si se va a aplicar sobre un teléfono celular, se debe analizar sobre las herramientas de forensia que se disponen, si se aplican aquellas que se encuentran con hardware y software integrado o aquellas que se aplican a través de software solamente
- si se va aplicar sobre elementos magnéticos – comunes o de estado sólido (por ejemplo pendrives, discos rígidos), se debe aplicar duplicadores forenses, que permiten generar una copia imagen del disco origen, sin alterarlo. También se aplican elementos de protección contra escritura o bloqueadores, con el objetivo de evitar contaminar la prueba. Esta protección de escritura puede ser por hardware o software.
- existe la posibilidad de tener que realizar la forensia informática in situ, es decir en el momento del allanamiento. Para ello existen soluciones de herramientas "portables", que permiten obtener pruebas bajo protocolos de forensia, sin contaminar la prueba y sin retirar o secuestrar los elementos del lugar que se allana.

Esto permite aplicar criterios prácticos al momento del procedimiento del pedido de secuestro, pues existen situaciones que el parque de computadoras que se investiga es muy grande (por ejemplo, mas 50 equipos), y sería muy complicado retirar todos los elementos, cuando se sospecha que solamente en alguno de ellos puede existir información de interés para la causa que se investiga.

C.3. Aspectos a considerar una vez obtenida la evidencia digital

Es fundamental evaluar la forma en que se le va a entregar la evidencia digital obtenida. Es decir, como el propio FBI plantea cuando expresa que se debe considerar la forma de "presentar" dicha evidencia, se hace clara referencia a que una vez obtenidos los hallazgos, es importante evaluar la manera de estructurar los mismos para que el Juez pueda entenderlos y considerarlos. Pues normalmente las herramientas de forensia informática producen reportes que no son intuitivos de entender por alguien que no trabaja a diario con estos elementos. Si esta parte no se respeta, la pericia puede haber sido muy bien hecha, pero no le sirve de mucho al Juez, si no la puede entender bien.

Por ello, muchas veces se solicita separar los mensajes de texto de las imágenes, de los documentos en Word o de las planillas en Excel. También, que los correos electrónicos sean enviados en una interfase de fácil comprensión para el administrador de justicia. En muchos casos se aplica el "mailnavigator".

Se recomienda que, de ser posible y según la problemática que se investigue, se apliquen mas de una herramienta de forensia, combinando la potencia que cada una pueda tener. Por ejemplo, para copia de forensia al duplicar un disco rígido, se puede usar un dispositivo de un determinado proveedor y luego para realizar las búsquedas sobre la evidencia digital generada, se puede aplicar uan herramienta que pertenezca a otro proveedor.

Hoy día, existen en el mercado varios proveedores reconocidos de herramientas de forensia informática, como ser Guidance, Cellebrite, Access Data, a los que debe sumársele varios productos del estilo "free" o libres de licenciamiento, y por supuesto sin costo alguno. Es de aclarar que el hecho de no tener costo, no sacrifica la calidad del producto.

Teniendo en cuenta el amplio mercado que existe sobre herramientas de forensia informática, es de aclarar que no es que una sea mejor que otra, todo depende del escenario que se debe investigar y del dominio o experiencia que se tenga sobre cada una de ellas.

Como resultado de las tareas de investigación, en algunas situaciones, surge la necesidad de requerir nuevas pruebas digitales. En estos casos, el perito cuenta con la posibilidad de relevar bien el escenario en que se encuentran esas nuevas evidencias, y por ende, puede prepararse mejor para la obtención de las mismas.

Al momento de ordenar una pericia informática, existe la posibilidad o tal vez la necesidad de aclarar los puntos de pericia requeridos por el Juez. Ello debido a que muchas veces se le pide al perito la búsqueda de evidencia digital en forma

amplia o genérica. Es decir, no se definen por ejemplo las "palabras clave" sobre las que se debe realizar el análisis digital. Pues para realizar esta tarea, sobre la copia o imagen forense obtenida anteriormente, es necesario ser muy preciso en lo que se debe analizar, ya que guarda directa relación sobre el objeto. Por ejemplo, se puede especificar el número de una cuenta bancaria, una dirección de IP, la especificación de un correo electrónico, la especificación de una imagen, etc.

Esto es fundamental que se encuentre especificado en los puntos de pericia, pues de lo contrario puede quedar librado al criterio del perito que realiza la tarea, y probablemente dicho criterio puede no coincidir con la estrategia de investigación que se sigue.

C.4. Cadena de custodia de la prueba informática

Se debe analizar su existencia. Este es un procedimiento que muy pocas veces se aplica y que debe originarse en el primer contacto con la evidencia digital, generalmente durante el secuestro. Esta parte del protocolo es considerada como una simple formalidad, pero en realidad es de vital importancia llevar una especie de "historia clínica" de todos los pasos que se siguen con dicha evidencia.

No debemos olvidar que muchas veces del momento que se accede a la prueba o evidencia digital hasta el momento que llega al perito informático, no sólo pasa un considerable tiempo, sino que pasa por distintas etapas (del allanamiento a la comisaría, de allí al juzgado, de allí al perito).

D. Condiciones en que la prueba ha sido preservada

Al momento de recibir los elementos a peritar, debe verificar si ha sido resguardada con franjas de secuestro, si ha sido sellada en todos sus puertos de acceso, si viene en bolsas de nylon transparentes o de color, si viene en cajas de cartón, si tienen protección en papel especial contra golpes, si vienen resguardados en protecciones de espuma anti estática, entre otros aspectos.

En otro orden conceptual, y al sólo efecto ilustrativo de la potencialidad y variedad de herramientas que hoy día existen en e mercado, es de señalar a modo informativo algunas de ellas:

Disk Jockey: se utiliza para la duplicación de discos en paralelo

Tableau Dead Collection: se utiliza para prevenir la escritura sobre aquellos dispositivos de almacenamiento que fueron secuestrados o aportados como prueba

EnCase: posee varios módulos de aplicación, entre ellosla realización de una copia forense o imagen de discos o dispositivos mganeticos, ya sea desde un disco secuestrado o en el momento de un allanamiento (conocido como Dead/Live Collection)

Linen CrossOver Acquisition: permite realizar copias de información almacenada en dispositivos mganético, de manera segura y en vivo

F-Response - Network Acquisition - Write Blocker Dead Collection: permite la protección de escritura sobre dispositivos con conexión del tipo USB

Zero View: permite leer las cabeceras de los discos rígidos

FTK: permite realizar copias imagen de dispositivos magnéticos secuestrados o en el momento del allanamiento (módlo conocido como Dead/ive Collection)

Cellebrite – UFED: permite realizar un análisis forense del contenido de una gran variedad de teléfonos celulares sobre todos los modelos existentes en el mercado internacional. Incluye gran variedad de teléfonos de origen chino, ue generalmente son muy clejos de estudiar. Esta herramienta permite identificar la información contenida en el dispositivo, incluyendo mensajes entrantes – salientes, lista de contactos, llamadas entrantes – salientes, correos electrónicos entrantes = salientes.

III. Conclusiones Preliminares

A modo de reflexión preliminar, es de señalar que cada herramienta cumple una finalidad específica con más eficiencia que otras. Por ejemplo, existen herramientas que son muy intuitivas para realizar búsqueda información sobre palabras clave que generalmente ordena un Juez, pero no son tan efectivas en el bloqueo de escritura por hardware. Otras que permiten un excelente bloqueo de escritura para preservar la prueba de contaminación digital, pero no son ágiles para búsqueda y análisis sore pañabras clave.

Generalmente, y dependiendo del problema a analizar, se sugiere aplicar una combinación de herramientas, para asegurar la efectividad que se debe tener en estos casos donde la libertad de las personas puede estar comprometida, y ello podría depender del resultado de una pericia informática aplicando herramientas de forensia.

Referencias

[1] Código Procesal Penal de la Nación Argentina. http://www.infojus.gov.ar

[2] Código Procesal Civil de la Nación Argentina. http://www.infojus.gov.ar

[3] Argentina: Ley 24.766 de Confidencialidad (30/12/1996) http://www.infojus.gov.ar

[4] Argentina: Ley 24.769 Penal Tributaria (15/01/1997). http://www.infojus.gov.ar

[5] Argentina: Ley 25.036 Propiedad. Intelectual (15/11/1998) http://www.infojus.gov.ar

[6] Argentina: Ley 25.236 Habeas Data (02/11/2000) http://www.infojus.gov.ar

[7] Alvarado Lemus, J. 2008. "Cibercrimen", Artemis Edinter, De Museo,

[8] [Mikel Gatesi – Dani Creus, "El cibercrimen y las guerras de robots: Search & Destroy", 2012

[9] Phil Williams, "Crimen Organizado y Cibernético" Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon, 2008

[10] Argentina: Ley 25.891 Servicio de Comunicaciones Móviles (25/05/2004) http://www.infojus.gov.ar

[11] Argentina: Ley 25.930 Modificación Código Penal / Incluye Inc. 15 Art. 173 y Modificación Art. 285 http://www.infojus.gov.ar

[12] [12] Argentina: Artículo 44 Código Contravencional de la Ciudad Autónoma de Buenos Aires

http://www.infojus.gov.ar

[13] Argentina: Ley 26.388 Delitos Informáticos (24/06/2008) http://www.infojus.gov.ar

[14] Wilson 2003,Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E y Liederbach, J. 2006

[15] Forensic Toolkit http://www.accessdata.com/products/utk

[16] WinHex http://www.x-ways.net/forensics/index-m.html

[17] [White,D., Rea, A., Mckenzie, B y Glorfled, L 2004, Cano 2006

[18] US Department of Justice, Electronic Crime Scene Investigation: “A Guide for First Responders”, 2001

[19] Fernando Miró Linares: “El Cibercrimen: Fenomenología y Criminología de la Delincuencia en el Ciberespacio”, Marcial Pons Ediciones Jurídicas y Sociales S.A., 1ra. Edición, 12/2012

[20] Misha Glenny. “El lado oscuro de la Red, el CiberCrimen, la Ciberguerra y TU, 2013

[21] Rina Begum, “Connect More”, KPMG Infrastructure Survey 2013, KPM LLC, 09/201

Dario Piccirilli. Licenciado en Sistemas de la Universidad Tecnológica Nacional (1979), con estudios de Posgrado como magister en Ingeniería de Software en el Instituto Tecnológico de Buenos Aires (Argentina) y Master en Ingeniería de Software en la Universidad Politécnica de Madrid (España). Profesor Titular en la Cátedra de Pericias Informáticas (Carrera de grado en Ingeniería en Sistemas de Información) y Profesor Titular en la Cátedra Auditoría, Seguridad y Pericias Informáticas (Carrera de Maestría en Sistemas de Información) en la Facultad Regional Buenos aires de la Universidad Tecnológica Nacional. Profesor Titular en Pericias Informáticas (Especialización de Posgrado en Redes) En la Facultad de Informática de la Universidad Nacional de La Plata (Argentina). Especialista en Pericias Informáticas en fueros Penal, Civil, Comercial y Laboral del Poder Judicial de la Nación de la Republica Argentina (desde 1989 a la fecha).