Informática Forense como medio de pruebas

La Experticia es uno de los medios probatorios con más auge en los procesos civiles, mercantiles y penales, debido al incremento del desarrollo de la ciencia y tecnología en diversos campos del saber, lo que permite aplicar nuevos métodos de estudio en la búsqueda de la verdad.

La incorporación de las tecnologías de información a la vida personal cotidiana, procesos administrativos, de gestión y de telecomunicaciones ha marcado la necesidad de incluir a los medios informáticos como elementos de carácter probatorio, toda vez que los mismos pueden constituir fácilmente pruebas de manifestaciones de voluntad, consentimiento u consentimiento u otros hechos de relevancia jurídica.

Uno de los grandes problemas con los que nos encontramos al tratar de incorporar estos hechos al proceso, es el pensar que las pruebas informáticas son fácilmente creadas, modificadas o destruidas y que por ello difícilmente podrían ser utilizadas en un proceso judicial. La realidad es que dentro de la Criminalística o investigación científica judicial, se ha venido desarrollando una nueva disciplina denominada Informática Forense, la cual tiene como objeto el estudio de la Evidencia Digital. El término evidencia ha sido en principio adminiculado al de física dando como resultado el concepto de "Evidencia Física", lo cual parece ser contrastante con el término "Evidencia Digital", por cuanto, todo aquello relacionado con el término "digital" se ha asimilado al término "virtual", es decir, como no real o casí real. Es importante aclarar que los datos o Evidencia Digital, siempre estarán almacenados en un soporte real, como lo son los medios de almacenamiento magnéticos o magnetoópticos u otros que se encuentran en fase de desarrollo, siendo todos estos de tipo físicos por lo que este tipo de evidencia es igualmente física.
En innegable y evidente, que la aparición de la informática marcó el comienzo de la utilización de nuevos modus operandi para comisión de delitos convencionales, a través de las tecnologías de información, lo cual generó la aparición de novedosas legislaciones en los países anglosajones y de habla hispana, tipificando como delitos una gran cantidad de hechos en los cuales intervienen directa o indirectamente los ordenadores o computadoras. Son diversas las variantes de los delitos convencionales que por analogía en la forma de su comisión se han establecido doctrinariamente como delitos de tipo electrónico, como lo son por ejemplo, el delito de intersección y espionaje de comunicaciones electrónicas, asimilables a los delitos de intervenciones telefónicas y grabaciones ilícitas. La analogía entre el correo convencional y el electrónico, ha dado lugar al establecimiento de delitos de violación de correspondencia electrónica, así como el acceso indebido a información contenida en sistemas informáticos. La falsificación de documentos ya no es exclusiva de las falsificaciones materiales en soportes de papel, sino que ya existen como delitos, la falsificación de registros y documentos de tipo electrónico. La inclusión de los sistemas de comunicación electrónico, como el correo y transacciones a través de Internet en el mundo del comercio han terminado de impulsar la necesidad probatoria sobre los hechos que ocurren en este mundo informático del cual los abogados ya formamos parte.

Ahora bien, para decidir llevar este tipo de hechos por vía de pruebas al proceso, es necesario tener en cuenta conceptos básicos de la informática sin tener que ahondar en el exquisito mundo de los lenguajes de programación, códigos y algoritmos informáticos.

Características de la Evidencia Digital.
Tal como lo habíamos mencionado, la Evidencia Digital es un tipo de la evidencia física, que es menos tangible que otro tipo de evidencias, pero a diferencia de todas las demás evidencias físicas, esta presenta ciertas ventajas, debido a que puede ser duplicada de una forma exacta, por lo que es posible peritar sobre copias, tal cual como si se tratara de la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original.

En contraposición a lo que se piensa, es relativamente fácil determinar si una Evidencia Digital ha sido modificada o alterada a través de la comparación con su original o bien con el análisis de sus metadatos a los cuales haremos referencia más adelante.

La Evidencia Digital no puede ser destruida fácilmente, tal como piensan los usuarios de ordenadores o computadoras, que creen que con ejecutar un comando de borrado (delete), ya ha desaparecido un documento o archivo objeto del mismo de la máquina. El disco duro de un sistema informático, guarda los datos en sectores creados en el momento del formateo del mismo, lo cual equivale a cuadricular una hoja de papel para insertar números y hacer operaciones matemáticas. Es posible que para guardar un archivo se necesiten varios sectores del disco. Los sistemas operativos y hardware o parte física de los ordenadores, trabajan en conjunto en la ubicación de los archivos y programas para su visualización o ejecución, siendo los responsables especificos del acceso a los archivos, otros archivos denominados Meta Archivos con funciones de índice, que contienen la información necesaria para abrir o visualizar rápidamente datos específicos en el soporte magnético (Disco Duro). Lo que hace la ejecución de comando de borrado en la mayoría de los sistemas operativos es una eliminación de los datos de ubicación del archivo en el índice del disco duro sin borrar real y físicamente el archivo en si, por lo que el archivo objeto de la instrucción de borrado puede quedar en el disco duro sin que el usuario este consciente de ello.

Hechos Informáticos que pueden ser probados en juicios.
En principio, todo hecho acaecido en un sistema informático puede ser objeto de experticia y puede promoverse un medio probatorio a los efectos de su incorporación procesal. Los peritos en la materia, utilizan entre otros el método de la reconstrucción relacional, es decir, la ubicación en los ordenadores de los datos vinculados al caso, y de ser posible establecer el tiempo y concatenación de estos hechos a efectos de dar a conocer al sentenciador los elementos básicos de la investigación judicial, como lo son el ¿qué?, ¿cómo?, ¿cuándo?, ¿dónde? y el ¿por qué?.

Haciendo un breve recorrido por los diversos tipos de hechos informáticos, podemos señalar, que una de las posibilidades, que parece en principio no viable a los ojos de los usuarios informáticos convencionales, es el que se pueden obtener resultados periciales, en los cuales se establezca el origen o procedencia de los mensajes de datos (correo electrónico), los anexos o archivos adjuntos que se envían con los mensajes de datos,

pudiendo el experto determinar no solamente el país y/o ciudad de origen, sino que es posible también determinar e individualizar, entre varias máquinas de una misma marca, un mismo modelo, en cuál ha sido producido un archivo determinado.

Otros hechos acaecidos en el denominado espacio virtual o Internet, son de diversa naturaleza, pero es allí donde ocurren la mayoría de los nuevos delitos de violación de derechos de autor y contra la propiedad industrial más comunes. A través de la pericia informática es posible el rastreo y determinación de la propiedad, administración, y datos de contactos relacionados con un dominio en Internet y/o servidores de almacenamiento, así como la fecha de creación y modificaciones realizadas en página Web para establecer responsabilidades.

Debemos considerar dentro del ámbito de la Informática Forense, el análisis de los datos almacenados en todo tipo de artefactos electrónicos tales como: teléfonos móviles o celulares, agendas personales, grabadoras digitales, dispositivos de almacenamiento, cámaras, discos compactos en todas sus variedades, memorias no volátiles e inclusive fax.

La actividad en redes locales o externas puede ser igualmente analizadas a efectos de determinar las características y tráfico de datos, modus operandi, móviles y costumbre de los usuarios de informática.

Informática aplicada a la Investigación Forense.
La Evidencia Digital puede ser procesada conforme a los criterios de colección y manejo de evidencia que se manejan generalmente en Criminalística, por lo que el proceso se puede resumir en varias fases:

1. Reconocimiento.
2. Captura y Preservación.
3. Clasificación e Individualización.
4. Reconstrucción.

Reconocimiento: El reconocimiento de la Evidencia Digital incluye la fase de individualización del Hardware o equipos informáticos (cuando se pueda tener acceso físico a ellos), así como la descripción de sistemas operativos y aplicaciones instaladas en los mismos. La ubicación de los datos relevantes al caso es importante en esta fase, los cuales pueden ser de distinta naturaleza, dependiendo del programa que haya sido utilizado para realizar el hecho jurídico informático.

El perito o práctico en materia civil y afines, debe ser muy cauteloso en el ejercicio de sus funciones, regidas por el principio dispositivo, por cuanto la extralimitación en el encargo pericial puede traducirse fácilmente en un delito electrónico.

La captura y preservación de la Evidencia Digital en los casos penales, debe procurarse en su estado original. Para lograr efectivamente la preservación correcta de los datos, los expertos deben realizar copias exactas y fieles, a través del procedimiento conocido como copia bit a bit, el cual garantiza que los datos de un medio de almacenamiento, sean copiados de manera exacta desde su fuente de origen.

Los sistemas operativos instalados en los ordenadores utilizan en su mayoría los denominados archivos temporales, denominados también Memoria Virtual, que contienen trazas de las operaciones realizadas en los mismos, así como otro tipo de datos, imágenes y archivos susceptibles de ser recuperados, aún cuando se haya intentado borrarlos, por lo que el perito debe realizar las operaciones de copia con técnicas o herramientas especiales destinadas a tal efecto.

Como lo mencionamos anteriormente las operaciones técnicas de análisis que pasaremos a describir, nunca deben realizarse sobre los medios de almacenamiento originales sino sobre copias fieles y exactas.

Una de las garantías que debe ofrecer el perito a las partes y al juez, es la verificación de la identidad o correspondencia entre los archivos originales y sus duplicados, a través de la obtención de valores matemáticos de comprobación conocidos como “Hash”, que son valores numéricos, resultado de la suma de números tomados de los datos objeto del señalado proceso. El Hash o valor de comprobación debe ser idéntico entre los archivos originales y los copiados.

Clasificación e Individualización

La clasificación de la Evidencia Digital, es el proceso a través del cual el perito ubica las características generales de archivos y datos, que son utiles a su vez para realizar comparaciones entre archivos similares o bien para individualizar la evidencia, por lo que de esta forma se establecerán los tipos de archivos.

La individualización juega un papel determinante en la experticia informática, la cual se logra a través de la ubicación y análisis de los metadatos (metadata), es decir, los datos sobre los datos, información esta que se encuentra en embebida de forma oculta dentro de los archivos, siendo los metadatos típicos los relacionados con el título, tema, autor y tamaño de los archivos, incluyéndose también en esta categoría las fechas de creación, modificación e impresión de un documento electrónico. Los metadatos son incorporados a los documentos automáticamente sin que el usuario tenga que realizar ninguna operación destinada a el. Algunos programas toman datos del Hardware o de los equipos donde se encuentran instalados, lo cual en casos determinados puede constituir prueba inequívoca de que un archivo ha sido realizado en un ordenador determinado.

Reconstrucción:
La reconstrucción de los hechos informáticos incluye conceptualmente el establecimiento de la secuencia de producción de actividades en un computador o en redes. La recuperación de Evidencia Digital dañada entra también en esta categoría.

Es importante que en la pericia informática registre cada acción realizada durante su práctica a efectos de hacer posible la evaluación de los protocolos de manejo de evidencia o bien a efectos de confirmarse los resultados en ampliaciones y aclaratorias del dictamen.

La reconstrucción relacional de los hechos informáticos es importante a efectos de establecer su relación con otro tipo de evidencia del mismo caso. El perito debe tratar de

hacer una especie de línea del tiempo cuando la complejidad de los hechos que esta evaluando así lo requiera.

Valoración de la pericia informática.

Los hechos informáticos tienen su origen en procesos matemáticos por los cuales le son aplicables leyes científicas de carácter incuestionable, pero ello no significa en forma alguna que toda pericia informática sea certera y adecuada a las necesidades del proceso. Las pericias informáticas deben ser apreciadas siempre y cuando se desprenda del dictamen una estricta aplicación de las fases de preservación y manejo de evidencia, así como una correcta, sopesada y objetiva aplicación del método científico como garante único de la objetividad del perito, el cual no solo tiene el reto de realizar su labor de por sí compleja, sino que además debe preocuparse por utilizar un lenguaje digerible por mentes de corte eminentemente humanístico en las que a veces existe una predisposición en contra de la informática o bien una desconfianza sobre los posibles resultados de este nuevo tipo de aplicación de los medios probatorios periciales.

RAYMOND J. ORTA MARTINEZ: Abogado, Postgrado en Derecho Procesal, Perito en Documentología e Informática Forense, inscrito en el Registro de Peritos y Expertos del Tribunal Supremo de Justicia de Venezuela, Técnico Superior en Ciencias Policiales mención Grafotécnica y Dactiloscopia. lab@informaticaforense.com

Fuente del artículo: Tecnoiuris.com