Informática Forense

La Investigación en un Mundo Digital

Romel Rivas / romel.rivas@rrsecurityconsulting.com

La Informática Forense es una disciplina auxiliar de la criminalística o ciencia forense, que aplica conocimientos, métodos y técnicas informáticas, para el examen de evidencias de naturaleza digital, relacionada con un presunto hecho punible con el fin de determinar, en auxilio de los órganos encargados de administrar justicia, su existencia cierta, su reconstrucción o simplemente señalar y precisar la intervención de uno o varios sujetos en el mismo.

Sus inicios

En **1984**, se creó un programa del **FBI**, denominado "*Programa de Medios Magnéticos*", actualmente se conoce como "*Análisis Informático y Equipo de Respuesta*", donde la informática forense se considera la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional, con la finalidad de lograr el esclarecimiento de un presunto hecho punible.

Esta ciencia forense informática, es una de las disciplinas de la criminalística más innovadora, que en un principio se vio desde un punto de vista aislado, relacionada únicamente a la seguridad informática, y que excluía la naturaleza jurídica de los incidentes informáticos.

En el contexto venezolano

El 30 de octubre de **2001**, se promulga la primera ley venezolana, que busca la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, denominada "*Ley Especial Contra los Delitos Informáticos*".

Actualmente en Venezuela los procesos de Colección, Fijación, Preservación y Resguardo de evidencia de naturaleza digital, son regulados por el "*Manual Único de Procedimientos en Materia de Cadena de Custodia de Evidencias Físicas*", a los fines de que sea demostrada su integridad, desde la etapa de investigación, hasta la culminación del proceso, buscando mantener un criterio unificado de patrones criminalísticos y el valor probatorio de las pruebas electrónicas.

A su vez, existen guías de buenas prácticas internacionales como lo es la norma **ISO/IEC 27037:2012**, orientada a identificar las situaciones comunes que se encuentran en todos los procesos involucrados con la evidencia de naturaleza digital, así como su gestión.

Principales fuentes de evidencia digital

Entre las distintas fuentes, también llamadas pruebas electrónicas, que pueden llegar a determinar si un hecho tuvo o no lugar, se tienen las siguientes:

- Los medios de almacenamiento digital utilizados en equipos de computación estándar, como discos duros, disquetes, discos ópticos y magneto-opticos,

dispositivos de datos con funciones similares.

- Los teléfonos móviles, asistentes digitales personales (**PDA**), dispositivos electrónicos portátiles (**PED**), tarjetas de memoria.

- Los sistemas de navegación móviles.

- Las cámaras digitales y vídeo cámaras (incluyendo Circuito Cerrado de **TV**)

- Los equipos de computación estándar con conexiones de red, redes basadas en **TCP/IP** y otros protocolos comunicación digital.

- Así como cualquier otro dispositivo con funciones de almacenamiento y transmisión de datos.

Consideraciones

La evidencia digital es susceptible de sufrir alteraciones y/o modificaciones, por lo cual se debe utilizar un nuevo conjunto de herramientas, técnicas y métodos como la ejecución de funciones criptográficas o **HASH**. En tal sentido los expertos en Informática Forense o Peritos Informáticos deberán elegir el algoritmo que considere idóneo como **MD5, SHA-1**, entre otros; sobre los dispositivos de almacenamiento, generando una firma digital que permita la ulterior verificación que garantice la autenticidad, confiabilidad, suficiencia y no repudio de la evidencia colectada.

A su vez, los expertos en Informática Forense, a lo largo del desarrollo de los procesos de análisis deberán verificar las respectivas firmas digitales, documentando cualquiera de las acciones realizada sobre la evidencia analizada, dejando constancia si fuese el caso de alteraciones y/o modificaciones, tanto del resultado del **HASH** aplicado, como de la evidencia digital analizada y las pruebas electrónicas observadas.

Dichos expertos deberán poseer título en la materia de estudio y explicar de manera clara, precisa y por escrito, los resultados obtenidos, con sus debidas conclusiones conforme a los principios o reglas de su ciencia, asimismo deben presentarse para rendir declaración sobre éstos, de manera oral, si así fuese el caso.

La evidencia digital puede llegar a estar presente en cualquier investigación, sin importar su materia ya sea civil, mercantil, penal, laboral entre otras, sólo va depender de la pericia del Experto en Informática Forense y de las herramientas, métodos y técnicas utilizadas que permitan identificar sus principales fuentes, lo cual apoyará a los órganos encargados de administrar justicia en el esclarecimiento de los presuntos hechos que sean investigados.■