Informática forense

El desarrollo alcanzado por la tecnología de información ha comenzado a plantear nuevos desafíos y la Policía Nacional y nuestro aparato jurídico, se están quedando rezagados, ya que los criminales también hacen uso de los ordenadores y por ende se hace necesario utilizar nuevos tipos de investigación.

La aplicación de la tecnología informática en la investigación de un ilícito cometido usando un ordenador , ha creado una nueva especialización, la **informática forense**, la cual abarca cuatro partes fundamentales que son:

1.- La identificación de evidencia digital.- Sabiendo qué evidencia está presente, dónde y como se guarda, es vital determinar qué procesos serán empleados para efectuar su recuperación. No solo los ordenadores son el centro de la informática forense, en la realidad el concepto puede extenderse a cualquier dispositivo electrónico que sea capaz de almacenar información, como los teléfonos celulares, las agendas electrónicas, las tarjetas flash, reproductores de mp3 y mp4 ya que ellas también son capaces de almacenar información.

2.- Preservación de la evidencia digital.- El examen de los datos electrónicamente guardados se debe llevar a cabo de la manera menos intrusiva posible, es por ello por lo que se trabaja sobre imágenes o copias de la data.

3.- El análisis de la evidencia digital.- La extracción, procesamiento e interpretación de los datos digitales, se consideran generalmente como los elementos principales de la informática forense. Una vez obtenida, la evidencia digital, normalmente requiere de un proceso, antes que pueda ser legible por las personas.

4.- La presentación de evidencia digital.- Incluye la manera formal de la presentación y la credibilidad de los procesos que se emplearon para producir la evidencia ya que si se usa un programa que no interpreta cada dato con precisión y exactitud, el significado entero del documento puede cambiar.

La informática forense utiliza muchas disciplinas como la Ingeniería de software, la criptografía, ingeniería electrónica, comunicaciones, derecho, matemática y otros y comprende, entre otras, las siguientes actividades:

Análisis de soportes y dispositivos electrónicos.- Como los discos, almacenamientos removibles (disquetes, discos ZIP, CD-ROMs, DVD, etc.), y se requiere entender completamente la estructura física y el funcionamiento de los medios almacenamiento, así como, la forma y la estructura lógica de cómo se almacenan los datos.

El análisis de la comunicación de datos.- Esto abarca la intrusión en una red de computadoras o mal uso de la misma y la interceptación de datos, para ello, debemos detectar la intrusión, conseguir la evidencia, capturarla y preservarla; y reconstruir la actividad específica.

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para poder supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal.

Hay que desarrollar nuevas técnicas y herramientas para estar actualizado frente a los cambios en la tecnología, no sólo hay que desarrollar las soluciones a los problemas existentes, sino también para reconocer problemas futuros y hallar las soluciones más adecuadas.

Desgraciadamente, los recursos y habilidades necesarios para mantener una investigación eficaz y un programa de desarrollo están más allá de la capacidad financiera de muchos grupos forenses.

El especialista en informática forense no debe emprender un examen más allá de su nivel de conocimiento y habilidad, es esencial que el perito sea consciente del límite de su conocimiento y habilidad y por ello, hasta que sean debidamente capacitados, deben buscar la ayuda de personal más experimentado y con conocimientos del tema, sobre todo de los hackers, tal y como sucede en países mas avanzados que el nuestro.

Leonardo Donaire Perales
“Dr. Software”
www.hacha.org