



Ciberdelitos: pericia forense, clave para detectar ilícitos

Tras los recientes casos donde la Justicia condenó el uso ilegítimo de software, el especialista Zacarías Leone explica cómo se realiza una investigación.

En muchos lugares del mundo el uso y abuso de licencias de software y aplicaciones crece día a día. Recientemente, se dio a conocer un operativo realizado en una mega corporación internacional que abusó del uso de licencias de programas, convirtiéndose en un caso de piratería informática.

En estas situaciones un investigador forense informático debe realizar un operativo de adquisición y preservación de evidencias basado en un riguroso procedimiento de trabajo, ya que el mínimo cambio o modificación en los datos adquiridos culminaría en la desestimación de dicha investigación frente a un juzgado.

Los investigadores forenses informáticos utilizan herramientas desarrolladas para tales fines, cuyo objetivo es adquirir evidencias sin modificarlas, garantizando su integridad mediante hashes o firmas digitales para su correspondiente preservación.

Las evidencias analizadas o “periciadas” se obtienen directamente de las computadoras y servidores en los cuales se sospecha están utilizando aplicaciones o sistemas operativos con licencias fraguadas o vulgarmente conocidas como “crackeadas”.

En la investigación se buscan los números ocultos de los sistemas operativos y aplicaciones instaladas, para luego ser volcadas en una base de datos que, mediante la Justicia, será comparada con el fabricante del producto a fin de corroborar su integridad y autorización para tales fines.

Una vez adquiridas y analizadas las evidencias, los resultados junto con los originales periciados son incluidos dentro de lo que se conoce como “cadena de custodia”, a fin de hacer llegar al juzgado los resultados, preservar los originales y sus correspondientes copias fieles y los resultados del investigador forense informático a cargo.

Este paso es de suma importancia para poder demostrar a terceros la integridad de las evidencias, en la forma en que las mismas fueron adquiridas e investigadas.

Toda la investigación, desde el momento en que el investigador forense informático se hace presente, deberá ser volcada en su totalidad con lujo de detalles en lo que se conoce como “acta notarial”.

Esa acta notarial es la que indica a los fiscales y jueces cómo trabajó y se desempeñó el profesional en dicho operativo, quiénes estuvieron colaborando, qué herramientas utilizó, cuál es el número de serie autorizado para dichas herramientas de análisis forenses, y cómo se inició la cadena de custodia de la información y evidencias.



Actualmente en la Argentina existen varias organizaciones destinadas a la investigación de estos ilícitos, con el objetivo de regular el correcto uso de los sistemas operativos y aplicaciones.