INSTITUTO POLITÉCNICO NACIONAL
COMUNICADO DE PRENSA
COORDINACIÓN DE COMUNICACIÓN SOCIAL

México, D.F., a 28 de diciembre de 2015

IPN PRIMERA INSTITUCIÓN CON EQUIPO DE ESPECIALISTAS EN INFORMÁTICA FORENSE DEL PAÍS

- **Esta técnica detecta evidencia sobre ataques informáticos para presentar datos válidos en un proceso legal**
- **Cualquier equipo electrónico o de memoria puede ser un elemento a analizar en una investigación digital**

C-311

El Instituto Politécnico Nacional (IPN) cuenta con el único grupo de especialistas forenses en México que se dedica a elaborar análisis técnicos en redes (sociales e internet), sistemas operativos y controles de seguridad con el propósito de reunir información que pueda ser utilizada en una corte como evidencia digital.

El equipo del Centro de Investigación en Computación (CIC) del IPN, a cargo del investigador Eleazar Aguirre Anaya y especialistas en informática de posgrado, tienen la meta de proteger la transmisión de información digital porque se ha convertido en un punto vulnerable para los ataques cibernéticos que permiten el fácil acceso a datos financieros, documentos familiares, laborales, médicos, bancarios, personales y fotográficos.

En México, la Comisión Nacional de Seguridad (CNS), informó que del 2010 al 2015 se recibieron 30 mil reportes telefónicos, de los cuales 53 por ciento ocurrieron contra dependencias gubernamentales, 26 a recintos académicos y 21 al sector privado. La suplantación y robo de identidad ocuparon el 68, fraude 17 y hackeos el 15. Estas cifras colocan a nuestro país en el tercer lugar mundial por crímenes cibernéticos, debajo de China y Sudáfrica.

Para hacer frente a estos delitos surge el análisis forense digital, con el propósito de aplicar técnicas científicas y analíticas especializadas en instrumentos tecnológicos que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal, por este motivo fue creado el Laboratorio de CiberSeguridad del CIC.

La metodología forense almacena datos de diferentes medios digitales sin alterar los de origen, por ejemplo, conversaciones en redes sociales, emails y chats, donde su finalidad es que las evidencias digitales recabadas permitan elaborar un dictamen claro, breve y fundamentado que funcione como prueba ante un litigio. El procedimiento se basa en los requerimientos legales para no vulnerar los derechos de terceros.

Cualquier equipo electrónico o memoria puede ser un elemento a analizar en una investigación digital. Esto incluye servidores, cámaras fotográficas, dispositivos GPS, unidades USB de almacenamiento, smartphones y tabletas, donde aunque la información sea borrada permanece en la red y para suprimirla definitivamente debe pasar por un proceso especializado.

Existen modelos y protocolos de protección anticipados que evitan ataques informáticos, como la defensa preventiva, si esta fuera evadida se utilizaría un conjunto de controles que identifican y detectan la evasión; en caso de ser burlado, se realiza un análisis forense para contrarrestar estas acciones.

La importancia radica en mantener su integridad, ya que la evidencia digital es sumamente frágil, ya que con dar doble clic a un archivo se modifica la fecha de último acceso. Es importante mencionar que esta disciplina no tiene como objeto prevenir delitos, de ello se encarga la seguridad informática.

“Existen herramientas especializadas en informática que permiten analizar sin alterar la información, como en una escena del crimen física, donde los peritos forenses utilizan lo necesario para evitar contaminar la evidencia”, informó Eleazar Aguirre.

Los ataques cibernéticos procesados en México contaron con evidencia y se relacionan con el acceso no autorizado de equipos informáticos, violación de propiedad intelectual, sexting, delitos financieros, robo y suplantación de identidad, los cuales están legislados en el artículo 211 bis fracción I del Código Penal Federal.

===000===