Informática Forense

Introducción y Concepto.-

El cómputo forense, también llamado informática forense, computación forense, análisis forense digital, examinación forense digital o Forensic es la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. La importancia de éstos conocimientos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Adicionalmente, un examinador forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo.

Introducción a la Informática Forense a nivel mundial y en Bolivia.-

La informática forense a nivel mundial es la ciencia dedicada a la recolección, preservación, análisis y presentación de la evidencia digital en casos judiciales, arbitrales o procesos internos disciplinarios.

De igual manera en Bolivia se han dado grandes pasos para cubrir la brecha del tratamiento de la evidencia digital ante la ausencia de una ley que la incluya como medio probatorio directo estando actualmente bajo la figura de la Pericia. La ponencia tiene como objetivo compartir estos pasos recorridos y mostrar el estado del arte en Bolivia tanto en métodos como en herramientas de software y hardware para el fuero legal y también académico.

Generalidades.-

Se reconoce generalmente a Dan Farmer y Wietse Venema, los creadores del Forensics Toolkit, como los pioneros de la informática forense. Actualmente, Brian Carrier es probablemente uno de los mayores expertos mundiales en el tema.

La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

La Informática Forense es una ciencia relativamente nueva y no existen estándares aceptados, aunque algunos proyectos están en desarrollo, como el C4PDF (Código de Prácticas para Digital Forensics), de Roger Carhuatocto, el Open Source Computer Forensics Manual, de Matías Bevilacqua Trabado y las Training Standards and Knowledge Skills and Abilities de la International Organization on Computer Evidence, que mantiene online varias conferencias interesantes.

- ¿Para qué sirve?

  Para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.

- ¿En qué consiste?

  Consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas.

- ¿Cuál es su finalidad?

  Cuando una empresa contrata servicios de Informática forense puede perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.

- ¿Qué metodologías utiliza la Informática forense?

  Las distintas metodologías forenses incluyen la recogida segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas.

- ¿Cuál es la forma correcta de proceder? Y, ¿por qué?

Todo el procedimiento debe hacerse teniendo en cuenta los requerimientos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados. Ello, para que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio, para alcanzar un resultado favorable.

Objetivos.-

- Finalidad preventiva, en primer término. Como medida preventiva sirve a las empresas para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes. Asimismo, permite detectar las vulnerabilidades de seguridad con el fin de corregirlas. Cuestión que pasa por redactar y elaborar las oportunas políticas sobre uso de los sistemas de información facilitados a los empleados para no atentar contra el derecho a la intimidad de esas personas.
- Por otro lado, cuando la seguridad de la empresa ya ha sido vulnerada, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa para determinar las actividades realizadas desde uno o varios equipos concretos.

Cuestiones técnicas y legales de la Informática Forense.-

Para realizar un adecuado análisis de Informática forense se requiere:

- Un equipo multidisciplinar que incluya profesionales expertos en derecho de las TI y expertos técnicos en metodología forense. Esto es así porque se trata de garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

Herramientas de Informática Forense (a nivel mundial).-

Sleuth Kit -Forensics Kit, Py-Flag - Forensics Browser, Autopsy - Forensics Browser for Sleuth Kit, dcfldd - DD Imaging Tool command line tool and also works with AIR, foremost - Data Carver command line tool, Air - Forensics Imaging GUI, md5deep - MD5 Hashing Program, netcat - Command Line, cryptcat - Command Line, NTFS-Tools, qtparted - GUI Partitioning Tool, regviewer - Windows Registry, Viewer, X-Ways WinTrace, X-Ways WinHex, X-Ways Forensics, R-Studio Emergency (Bootable Recovery media Maker), R-Studio Network Edtion, R-Studio RS Agent, Net resident, Faces 3 Full, Encase 4.20, Snort, Helix, entre otras.

Uso de las herramientas en Bolivia.-

La Informática Forense puede ser usada para descubrir evidencia potencial en una variedad de casos, incluyendo:

- Delitos contra la Propiedad Intelectual, en caso de Software Pirata o documentos con el debido registro de derechos de Autor. LEY No. 1322 DE 13 DE ABRIL DE 1992.
- Robo de Propiedad Intelectual y Espionaje industrial (que aunque no se crea, sí existe en nuestro país).
- Lavado de Dinero, vía transferencia de fondos por Internet.
- Acoso Sexual (vía e-mail); Chantaje o amenazas (vía e-mail).
- Acceso no autorizado a propiedad intelectual.
- Corrupción.
- Destrucción de Información Confidencial.
- Fraude (en apuestas, compras, etc. Vía e-mail).
- Pornografía en todas sus formas, inclusive en la más devastadora: Pornografía infantil.

Uso de las herramientas en España.-

- Protección al menor: producción, distribución y posesión de pornografía infantil.
- Fraude en las comunicaciones: locutorios telefónicos clandestinos.
- Dialers: modificación oculta del número de teléfono de destino.
- Producción y distribución de decodificadoras de televisión privada.
- Fraudes en Internet: estafas, subastas ficticias y ventas fraudulentas.
- Carding: uso de tarjetas de crédito ajenas o fraudulentas.
- Phising: redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas).
- Cartas nigerianas (segunda fuente de ingresos del país, según el FBI; después del petróleo).
- Seguridad lógica: virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico.
- Delitos de injurias, calumnias y amenazas a través del e-mail, news, foros, chats o SMS.
- Propiedad intelectual: piratería de programas de ordenador, de música y de productos cinematográficos.
- Robos de código: como en el caso de los juegos Dark Age of Camelot, y Half-Life 2, o de los sistemas Cisco IOS y Enterasys Dragon IDS

Técnicas de detección de evidencias.-

La Informática Forense combina técnicas especializadas con el uso de software sofisticado para ver y analizar información a la que no puede acceder el usuario ordinario. Esta información pudo haber sido "borrada" por el usuario meses o años antes de la investigación o inclusive pudo no haber sido guardada, pero puede aún estar presente en todo o en parte, en el disco duro de la computadora.

Es siempre recomendable para precautelar el interés del abogado, del cliente y de otros aspectos legales que se está tratando, el encontrar a un especialista que nos asista en todas las etapas, en la preparación de un proceso judicial, incluyendo aspectos como: