Informática forense, qué es, definición, significado

Esto de saber de informática o computación forense es algo que vale la pena explorar, no solo porque es útil de forma aislada, sino porque hace parte de la seguridad en entornos digitales, lo cual es nuestra rutina diaria en el trabajo.

Introducción

Voy a hacer una confesión, me agradaba mucho la serie Bones, de Fox. Claro, me apasiona la medicina y la misma antropología (que hacer, si soy un bicho raro) pero me agrada más la lógica y la estructura de un discurso. Ver cómo Brenan partía de un deceso o un crimen para reconstruir los hechos y llegar al culpable, cruzando información y saberes en el camino, me parecía lo máximo.

En la actualidad, siguiendo con esa línea, Coroner me tiene atrapado, si bien es otro enfoque, en últimas el resultado es, básicamente el mismo, resolver delitos.

Reconstruyendo escenarios

Pues bien, lo anterior para contarles que la informática forense es una especialidad de la seguridad computacional que permite, usando las huellas digitales que dejan todos nuestros actos en la web y en los dispositivos interconectados, reconstruir una escena de un cibercrimen para dar con los responsables del mismo.

Tal vez no tenga el rating que pudiera tener alguna de las series televisivas que mencioné al comienzo, porque, claro, es

una labor digamos que rutinaria, rastrear Ips, puntos de contacto, registros, envíos de correo, de mensajes en redes sociales, historiales de navegación.

Concepto de informática forense

El término forense significa literalmente el uso de algún tipo de proceso científico establecido para la recopilación, análisis y presentación de la evidencia que se ha recopilado. Sin embargo, todas las formas de evidencia son importantes, especialmente cuando se ha producido un ciberataque.

Si gestiona o administra redes y sistemas de información, debe comprender de manera general, lo que significa la informática forense. La ciencia forense es el proceso de utilizar el conocimiento científico para recopilar, analizar y presentar pruebas a los tribunales.La ciencia forense se ocupa principalmente de la recuperación y el análisis de evidencia latente.

Debido a que la informática forense es una disciplina nueva, hay poca estandarización y coherencia entre los tribunales y la industria. Como resultado, aún no se reconoce como un «Disciplina científica”.

Definimos la informática forense como la disciplina que combina elementos de derecho e informática para recopilar y analizar datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que sea admisible como evidencia en un tribunal de justicia. En el mundo de la ciberseguridad, este tipo de datos (también conocidos como “datos ambientales”) no se ven ni se pueden acceder fácilmente a primera vista en la escena de un ciberataque.

En otras palabras, se necesita un nivel mucho más profundo de

investigación por parte del experto en informática forense para descubrirlos. Obviamente, estos datos tienen muchos usos, pero se implementaron de tal manera que el acceso a ellos ha sido extremadamente limitado.

Entre los ejemplos de datos latentes se incluyen los siguientes: Información que se encuentra en el almacenamiento de la computadora pero que no se puede consultar fácilmente en las tablas de asignación de archivos; Información que el sistema operativo o las aplicaciones de software de uso común no pueden ver fácilmente; Datos que se eliminaron intencionalmente y que ahora se encuentran en: Espacios no asignados en el disco duro; Intercambiar archivos; Imprimir archivos de cola; Volcados de memoria; El espacio de holgura entre los archivos existentes y la caché temporal.

Que hace un analista forense digital

La informática forense, es un campo bastante nuevo. Los investigadores forenses informáticos, también conocidos como especialistas en informática forense, examinadores forenses informáticos o analistas forenses informáticos, están encargados de descubrir y describir la información contenida en, o el estado o existencia de, un artefacto digital.

Los artefactos digitales incluyen sistemas informáticos, discos duros, CD y otros dispositivos de almacenamiento, así como documentos y archivos electrónicos como correos electrónicos e imágenes JPEG.

El campo de rápido crecimiento de la informática forense incluye varias ramas relacionadas con firewalls, redes, bases de datos y dispositivos móviles. Los técnicos forenses digitales pueden encontrar trabajo en muchos tipos de organizaciones: gobierno (local, estatal y federal), firmas de contabilidad, firmas de abogados, bancos y empresas de

desarrollo de software. Esencialmente, cualquier tipo de organización que tenga un sistema informático puede necesitar un especialista en forense digital. Algunos especialistas en análisis forense digital optan por iniciar sus propios negocios, lo que les brinda la oportunidad de trabajar con una variedad de clientes.

¿Cuándo y cómo se usa la informática forense?

Hay pocas áreas de crimen o disputa donde no se puede aplicar la informática forense. Los organismos encargados de hacer cumplir la ley se encontraban entre los primeros y más habituales usuarios de la informática forense, como resultado, a menudo han estado a la vanguardia de los desarrollos en el campo.

Las computadoras pueden considerarse una «escena de un crimen», por ejemplo, con piratería o ataques de denegación de servicio . Pueden tener evidencia de delitos que ocurrieron en otros lugares, en forma de correos electrónicos, historial de Internet, documentos u otros archivos relevantes para delitos como asesinato, secuestro, fraude o tráfico de drogas.

Un examen informático forense puede revelar más de lo esperado Los investigadores no solo están interesados en el contenido de los correos electrónicos, documentos y otros archivos, sino también en los metadatos asociados con esos archivos. Los registros de las acciones de un usuario también pueden almacenarse en archivos de registro y otras aplicaciones en una computadora, como navegadores de Internet.

Por lo tanto, un examen forense informático podría revelar cuándo apareció un documento por primera vez en una computadora, cuándo se editó por última vez, cuándo se guardó o imprimió por última vez y qué usuario realizó estas acciones. Las organizaciones comerciales han utilizado la

informática forense para ayudar con todo tipo de casos, que incluyen: Robo de propiedad intelectual, Disputas laborales, Fraude de facturas, a menudo habilitado por correos electrónicos de phishing, Falsificaciones, Uso inadecuado de correo electrónico e Internet en el lugar de trabajo, Cumplimiento normativo, etc.

Leer también: ¿Qué es un Firewall como servicio, FWaaS? Ventajas ; ¿Edge Computing es una buena idea? ; Ransomware, mejores prácticas para prevenir daños irrecuperablesRansomware, mejores prácticas para prevenir daños irrecuperables