Informática Forense

CONTENIDO

Introducción

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. El Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. bancos). Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de información forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

¿Qué es la Informática Forense?

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional [ReEx00].

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proce[Acis06].

Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Dentro de lo forense encontramos varias definiciones [Acis06]:

Computación forense (computer forensics) que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Forensia en redes (network forensics)
Es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.
Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Forensia digital (digital forensics)
Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Importancia de la Informática Forense

"High-tech crime is one of the most important priorities of the Department of Justice"[JaRe96]. Con esta frase podemos ver cómo poco a poco los crímenes informáticos, su prevención, y procesamiento se vuelven cada vez más importantes. Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática. (Ver [CERT06])
Sin embargo, la importancia real de la informática forense proviene de sus objetivos.

Objetivos de la Informática Forense

La informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

Usos de la Informática Forense [InfFor01]

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

1. Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
2. Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
3. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
4. Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
5. Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Ciencia Forense

La ciencia forense nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o

analizar la evidencia durante una investigación criminal forma parte de la ciencia forense. [ForIRT01]

Los principios científicos que hay detrás del procesamiento de una evidencia son reconocidos y usados en procedimientos como:

- Recoger y examinar huellas dactilares y ADN.
- Recuperar documentos de un dispositivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una huella digital con un algoritmo hash MD5 o SHA1 de un texto para asegurar que este no se ha modificado.
- Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Un forense aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplicando un método científico analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza pruebas, controles para confirmar o contradecir esas hipótesis. Esto puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir, esto es debido a que un forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por esto, sólo puede presentar posibilidades basadas en la información limitada que posee.

Un principio fundamental en la ciencia forense, que usaremos continuamente para relacionar un criminal con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (Edmond Locard, francés fundador del instituto de criminalistica de la universidad de Lion, podemos ver el esquema en la figura 1.

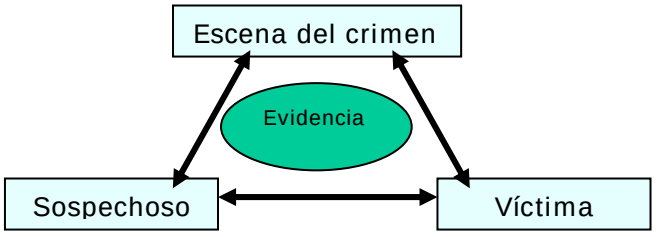

Figura 1: Principio de transferencia de Locard.

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y vice-versa (se lleva consigo), en otras palabras: “cada contacto deja un rastro”. En el mundo real significa que si piso la escena del crimen con toda seguridad dejaré algo mío ahí, pelo, sudor, huellas, etc. Pero también me llevaré algo conmigo cuando abandone la escena del crimen, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.

En este ejemplo hemos hablado de evidencias físicas, en la ciencia forense tradicional hay varios tipos de evidencias físicas:

- **Evidencia transitoria**: como su nombre indica es temporal por naturaleza, por ejemplo un olor, la temperatura, o unas letras sobre la arena o nieve (un objeto blando o cambiante).
- **Evidencia curso o patrón**: producidas por contacto, por ejemplo la trayectoria de una bala, un patrón de rotura de un cristal, patrones de posicionamiento de muebles, etc.
- **Evidencia condicional**: causadas por una acción o un evento en la escena del crimen, por ejemplo la localización de una evidencia en relación con el cuerpo, una ventana abierta o cerrada, una radio encendida o apagada, dirección del humo, etc.
- **Evidencia transferida**: generalmente producidas por contacto entre personas, entre objetos o entre personas y objetos. Aquí descubrimos el **concepto de relación**.

En la práctica las evidencias transferidas se dividen en dos tipos, conocidas como:

- Transferencia por **rastro**: aquí entra la sangre, semen, pelo, etc.
- Transferencia por **huella**: huellas de zapato, dactilares, etc.

Aunque en la realidad, estas últimas suelen mezclarse, por ejemplo una huella de zapato sobre un charco de sangre.

El principio de intercambio de Locard se puede resumir así:

1. El sospechoso se llevará lejos algún rastro de la escena y de la víctima.
2. La víctima retendrá restos del sospechoso y puede dejar rastros de si mismo en el sospechoso.
3. El sospechoso dejará algún rastro en la escena.

El objetivo es establecer una relación entre los diferentes componentes:

- la escena del crimen
- la víctima
- la evidencia física
- el sospechoso

Para la correcta resolución del caso, todos estos componentes deben estar relacionados. Esto se conoce como el **concepto de relación**, que es lo que nos faltaba para completar el principio de intercambio de Locard.

Las evidencias pueden, a su vez, ser transferidas de dos formas distintas:

1. Transferencia directa: cuando es transferida desde su origen a otra persona u objeto de forma directa.
2. Transferencia indirecta: cuando es transferida directamente a una localización y, de nuevo, es transferida a otro lugar.

Importante resaltar que cualquier cosa y todo puede ser una evidencia.

Brevemente, la ciencia forense facilita las herramientas, técnicas y métodos sistemáticos (pero científicos) que pueden ser usados para analizar una evidencia digital y usar dicha evidencia para reconstruir qué ocurrió durante
la realización del crimen con el último propósito de relacionar al autor, a la víctima y la escena del crimen.

Network Forensics

Forensia en redes, es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente [Acis06].

Es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente.