CAPÍTULO 1. INTRODUCCIÓN AL ANÁLISIS FORENSE INFORMÁTICO

El Análisis Forense Informático se deriva del peritaje y cabe recalcar que son dos conceptos diferentes. Mediante el peritaje se buscan evidencias, pruebas y se efectúa en base a procedimientos técnicos y científicos que conforman el análisis informático. En la seguridad informática es importante tener en cuenta que la posibilidad de ver ciertos datos no significa necesariamente que esta exista en verdad; de acuerdo con esto, se puede asegurar que toda información puede provenir de muchos otros sitios (Hidalgo Cajo, 2014).

1.1. Análisis Forense Informático.

Se considera que el Análisis Forense Informático consiste en la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal (Santos Tello, 2013).

Cuando se requiere de servicios profesionales para ejecutar un análisis forense o peritaje, es prioritario salvaguardar toda la información que luego será o no judicializada.

El conocimiento del informático forense abarca aspectos no solo del *software*, sino también de *hardware*, redes, seguridad, *hacking*, *cracking*, recuperación de información.

Es muy importante tener clara la diferencia entre informática forense, seguridad informática y auditoría, para evitar confusiones como la que vincula a la primera con la prevención de delitos, cuando la que se encarga de esto es la seguridad informática.

1.2. El perito informático

1.2.1. Perito

Con la creación del Real Decreto del 17 de agosto de 1901 de Romanones surge una nueva profesión con el título de perito.Posteriormente aparecen los títulos de perito informático y perito forense (Delgado, 1994). Ejemplo: si un habitante

de una colina es experto en minerales o simplemente conoce bien la zona, podría actuar como perito judicial o forense en el caso de que ocurriera algún problema. No es imprescindible tener una titulación, pero sí experiencia en la actividad que se realiza a diario, aunque evidentemente lo más recomendable sería alcanzar certificaciones o titulaciones que potencien el trabajo que se lleva a cabo.

1.2.2. Perito judicial o perito forense

Es el profesional dotado de conocimientos especializados y reconocidos a través de sus estudios que suministra información u opinión con fundamentos a los tribunales de justicia, sobre cuestiones relacionadas con sus conocimientos en caso de ser requeridos como expertos. Se puede decir que es la persona que funciona como vínculo entre la parte técnica y la parte judicial (Sánchez Cordero, 2014).

Existen dos tipos de peritos: los nombrados judicialmente y los propuestos por una o ambas partes y luego aceptados por el juez o fiscal. Los peritos judiciales son capaces de ejecutar, aplicar y utilizar todas las técnicas y recursos de una forma científica para una adecuada administración de los requerimientos de su campo laboral (recolección de pruebas, aseguramiento, preservación, manejo de la cadena de custodia necesaria para esclarecer la verdad, etc.).

Peritos judiciales según la Ley de Enjuiciamiento Civil L.E.C. artículo 340.1

Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de este, por lo tanto, en la Ley de Enjuiciamiento Criminal, en su artículo 457 se contempla que los peritos judiciales pueden ser o no titulares.

Cuando no hay peritos judiciales se nombran a personas expertas sobre el tema, que pueden ser:

- Peritos que tienen título oficial en la naturaleza del peritaje requerida por el juzgado.
- En ausencia de peritos titulados, se puede nombrar personas entendidas o expertas sobre el tema que, a pesar de carecer de título oficial, posean conocimientos o prácticas especiales en alguna ciencia o arte.

El perito suministra al juez el peritaje u opinión sobre determinadas ramas del conocimiento que el juez no está obligado a dominar, a efecto de suministrarle argumentos o razones para la formación de su convencimiento (Arsuaga Cortázar, 2010).

Funciones de un perito informático

Entre las funciones que puede realizar un perito se encuentran (Hidalgo Cajo, 2014):

- Asesoría técnica contra el ciber-crimen, considerando que se pueden presentar problemas por la existencia de un *malware* que afecte una entidad financiera y, por ende, a sus clientes.
- Localización de evidencias electrónicas, es decir, de los ficheros que han sido borrados y cuya ubicación se requiere determinar.
- Auditorías y seguridad informática forense mediante test de penetración.
- Valoración y tasación de equipos tecnológicos.
- Certificaciones y homologaciones.
- Recuperación de datos.
- Asesoría informática y formación de profesionales del derecho, la administración pública, de cuerpos y fuerzas de seguridad del estado, y también como detectives privados.
- Contraespionaje informático.
- Supervisión de actividad laboral informática.
- Detección y asesoría en casos de infidelidad empresarial que se da cuando un trabajador se separa de una empresa y se lleva consigo información que no le pertenece como, por ejemplo, una base de datos de todos los clientes.
- Seguimiento de correos anónimos, autores de publicaciones, propietarios de páginas web.
- Análisis informático forense de videos, imágenes digitales y audio.
- Asesoría sobre falsificación de correos, imágenes, violaciones de seguridad, infiltraciones, doble contabilidad, fraude financiero y de sistemas informáticos, robo de claves, información sensible, secretos industriales, errores en la cadena de custodia.

Para realizar su labor, el perito debe entender bien la naturaleza del problema, en dependencia del tipo de organización. Es importante que tenga una formación adecuada porque se han observado casos de mal manejo de la información. Por ejemplo, se puede citar el caso específico de un perito que era electricista y, al realizar un peritaje informático, hizo copias de discos duros con el xCopy, lo que imposibilitó posteriormente la lectura o la copia del informe. Este tipo de inconvenientes son irreversibles.

Para lograr una buena formación es imprescindible contar con una buena preparación previa en informática que no implique solamente el manejo de la ofimática, sino los conocimientos básicos y generales sobre temas de desarrollo, ingeniería de *software*, base de datos y bases de sistemas.

Con esta base se impone la especialización en seguridad informática, la que está conformada por varios campos: la auditoría, el *hacking* ético, la parte de defensa y análisis forense; para hacer una analogía podría usarse el ejemplo de un médico general que, según la patología que detecte en su paciente, lo remite al médico especialista que pueda dar un diagnóstico y un tratamiento más fiable.

La seguridad es una especialización dentro de la informática y el análisis forense una sub-especialización de la misma, por lo tanto, se podrá contar con diferentes criterios y puntos de vista.

1.3. Forense informático

El forense informático es el experto en el campo informático que dirige la investigación orientado al descubrimiento de información cuando se ha cometido un mal proceso o crimen relacionado con el área de la informática (Navarro Clérigues, 2014). Inicialmente fue considerada como una materia, pero no está regulada; sin embargo, cuenta con una norma de metodología para el análisis forense de las evidencias electrónicas (http://www.ietf.org/rfc/rfc3227.txt) que apoyan al forense informático.

Se reconoce generalmente a los creadores del Forensics Toolkit, Dan Farmer y Wietse Venema, como los pioneros de la informática forense.

Actualmente, Brian Carrier es probablemente uno de los mayores expertos mundiales en el tema.

No existen estándares aceptados, aunque algunos proyectos están en desa-

rrollo, como el C4PDF (Código de Prácticas para Análisis Forense Digital), 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 en la web varias conferencias interesantes.

La norma internacional vigente no se usa mucho, sin embargo, en el caso de España, el analista forense cuenta desde junio de 2013, con la norma UNE (Una Norma Española), en la cual se define claramente cómo se debe realizar, tratar y gestionar un análisis forense de una evidencia digital. Hasta el 2013 se realizaba un procedimiento forense basado únicamente en conocimientos empíricos y sin la seguridad adecuada, lo que podía provocar inconvenientes como que se obtuvieran diferentes tipos de evidencias luego de realizar un mismo procedimiento. Para evitar estos problemas es muy importante disponer de una metodología, como la norma española (UNE-71506, 2013).

1.4. Metodología para el análisis forense de evidencias digitales

La metodología empleada se basa en el estudio de (Sánchez Cordero, 2014), la misma se desglosa en ocho puntos:

1. **Identificación del incidente**

Cuando se ingresa a una escena del crimen para ejecutar el peritaje correspondiente y se encuentra una persona abatida en el suelo, se procede a identificar valores como: si conserva la ropa en el cuerpo o no, si aún respira, si existe sangre en la escena, o si en la misma se detectan anomalías de otro tipo como cristales rotos.

En el mundo informático el proceder es similar. En el caso de un fraude es necesario observar aspectos como los ordenadores, su tipo, la sala en la que se encuentran y su sistema operativo. Esto permitirá identificar el contexto de la situación dada.

2. **Requisitoria pericial**

Si al contratar los servicios de una empresa se sospecha de un empleado, es obligatorio actuar mediante conceptos legales. No se puede intervenir deliberadamente el ordenador o el dispositivo de una persona y luego acusarla, sino que se debe contar con una serie de garantías procesales. Entonces la requisitoria pe-