Investigación informática forense basada en Emacs

José Luis Jerez Guerero

Madrid, Julio 2015

Tutor:

Fernando Pérez Costoya (fperez@fi.upm.es)

La composición de este documento se ha realizado con Emacs LaTeX.
Diseño de Oscar Cubo Medina adaptado por José Luis Jerez.

- Los testimonios del personal afectado no debe de condicionar en modo alguno al analista.
- En ningún caso el analista debe seguir un impulso por llegar a obtener conclusiones que le haga actuar sobre las infraestructuras afectadas sin respetar el procedimiento adecuado para ello.

La evidencia digital, o prueba documental:

- Es la información relevante que permite a un analista establecer los motivos y fundamentos en los que se basan sus conclusiones.
- Se puede presentar como medio de prueba.
- Consiste básicamente en información digitalizada, codificados y alojados en un elemento contenedor digital (equipos, dispositivos periféricos, unidades de memoria, unidades virtualizadas, tramas de red y otros). Su valor es independiente del:
    - Formato de la misma (la codificación que permite guardar, tratar, recuperar o almacenar la información).
    - Dispositivo físico o virtual en el cual se encuentra contenida.
- Puede encontrarse en distintos estados que requieren procedimientos y herramientas distintas para garantizar la integridad de la misma:
    - Almacenada estáticamente en un contenedor digital.
    - Almacenada dinámicamente o en procesamiento en un elemento volátil.
    - En movimiento por la red en forma de trama de información que puede ser capturado y almacenado.
- Nunca debe de ser tratada directamente.
    - Se debe de realizar una copia bit a bit de modo que ésta sea idéntica a la original original, y sin alterar la integridad de la información original ni contaminarla
    - La copia puede ser copiada tantas veces como se precise, con métodos que garantizan que se está accediendo a la información en modo único de lectura, evitando su contaminación o modificación, la que permite desde el punta de vista de la cadena de custodia preservar integro el valor probatorio del original.

La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil establece en el capítulo V, 'De la prueba: disposiciones generales', en su:

- SECCIÓN 3: 'DE OTRAS DISPOSICIONES GENERALES SOBRE PRÁCTICA DE LA PRUEBA', expone que:
    - Las pruebas se practicarán en vista pública, si bien, excepcionalmente, el Tribunal podrá acordar, mediante providencia, que determinadas pruebas se celebren fuera del acto de juicio o vista.
    - Será inexcusable la presencia judicial en el interrogatorio de las partes y de testigos, en el reconocimiento de lugares, objetos o personas, en la reproducción de palabras, sonidos, imágenes y, en su caso, cifras y datos, así como en las explicaciones impugnaciones, rectificaciones o ampliaciones de los dictámenes periciales.