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-

ricial incluye todo lo relacionado con las partes judicial y legal. A la hora de hacer un análisis forense hay que hacer cumplir las leyes.

3. Entrevista aclaratoria

Como su nombre lo indica, la entrevista aclaratoria consiste en el encuentro del perito con los personajes involucrados. Con el objetivo de evitar malentendidos, en este paso se dan a conocer varios tipos de conceptos: "quién soy", "qué hago", "cuál es mi código ético". Esta acción debe estar regida por el concepto de imparcialidad, aunque el perito haya sido contratado por una primera o tercera empresa. Por ejemplo, si en los ficheros borrados o eliminados de un ordenador se encuentra pornografía infantil, el perito tiene la obligación de realizar la denuncia respectiva.

¿Qué son los personajes? Se considera así a las personas que actúan o que están dentro del proceso de investigación, ya sean los empleados de los que se sospecha, el representante de los trabajadores o de la empresa. En un mismo proceso de investigación pueden confluir diferentes personajes o escenarios.

4. Inspección ocular

Se aplicaría en la zona donde están los servidores, ordenadores, pero si ya se ha hecho la identificación del incidente, está de más efectuar este paso.

5. Recopilación de evidencias

Si continuamos con la analogía, obtener las evidencias consistiría en algo parecido a lo que se hace en la escena de un crimen: comprobar los valores de la víctima, si está viva o no, si necesita atención. En la informática, se recogen un conjunto de pruebas de la máquina que luego se compararán con una línea base.

6. Preservación de la evidencia

Las cadenas de custodia están enfocadas a la conservación de la información para evitar su manipulación.

7. Análisis de la evidencia

Una vez recopilada y preservada la evidencia, se puede empezar a trabajar con las copias obtenidas anteriormente. Es el momento de realizar el análisis y la exploración de la información, para obtener las conclusiones definitivas que serán presentadas en la documentación y la presentación.

8. Documentación y presentación de los resultados

Los resultados de la investigación se presentarán en dos informes: uno ejecutivo y otro técnico.

1.4.1. Principales puntos de la Metodología de análisis forense digital

Entre los principales puntos de la metodología para el análisis forense de evidencias digitales se pueden destacar los siguientes:

1. **Identificación**

Es muy importante conocer los antecedentes del bien informático, su identificación, su uso dentro de la red, el inicio de la cadena de custodia, el entorno legal que protege al bien y el apoyo para la toma de decisiones con respecto al siguiente paso.

2. **Preservación**

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta que permita mantener la integridad de la evidencia y la cadena de custodia que se requiere.

3. **Análisis**

En este proceso se aplican técnicas científicas y analíticas que permiten ejecutar la indagación sobre cadenas de caracteres, acciones específicas de los usuarios de la máquina como el uso de dispositivos USB (marca, modelo), sitios visitados ,además de la búsqueda de archivos específicos, la recuperación e identificación de correos electrónicos y del caché del navegador de internet.

4. **Presentación**

Es la recopilación de toda la información que se obtuvo a partir del análisis para realizar el informe y la presentación de resultados (Fig. 1.1).