Práctica 2. Análisis forense de sistemas Linux.

Volcado de memoria.

Cuando en nuestra práctica forense nos enfrentemos a un sistema operativo “vivo”, procederemos a extraer todas las evidencias posibles por medio de un script como el que se realizó en la práctica número 1.

Los siguientes pasos a tener en cuenta serían realizar un volcado de memoria y obtener una imagen del disco duro. La imagen del disco duro no presenta mayor dificultad, realizaremos un procedimiento de clonado haciendo uso del comando “dd” similar al que hicimos en las prácticas del tema 2.

En cuanto al volcado de memoria, decir que no es una tarea fácil en el sentido de que no existe una herramienta “estándar”, como ocurría en los sistemas operativos Windows, que sirva para todas las distribuciones Linux. En la mayoría de los escenarios de Linux se hace necesario compilar las herramientas de extracción de memoria con la versión exacta del kernel de la máquina de la que se desea adquirir el volcado.

Objetivo:

- Aprender a realizar volcados de memoria en Linux utilizando diversas herramientas.

Materiales

- Distribución Debian 10.9.0 de 64 bits con kernel version 4.9.0-16-amd
- Herramientas de extracción de memoria: memdump, fmem, LiME y avml. Descargarlas de aquí

Se pide crear una máquina virtual con la distribución mencionada anteriormente y documentar con ejemplos de uso como tiene lugar el proceso de volcado de memoria con las herramientas mencionadas anteriormente.