SEGURIDAD EN SISTEMAS OPERATIVOS
4º Grado en Informática – Complementos de Ing. del Software
Curso 2018-19

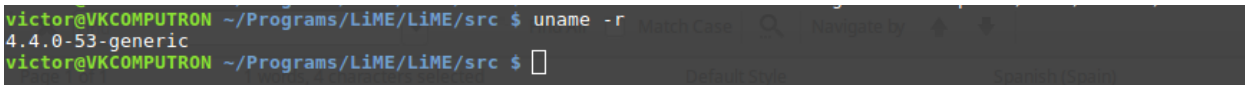
Práctica 3. Auditoría Informática e Informática forense

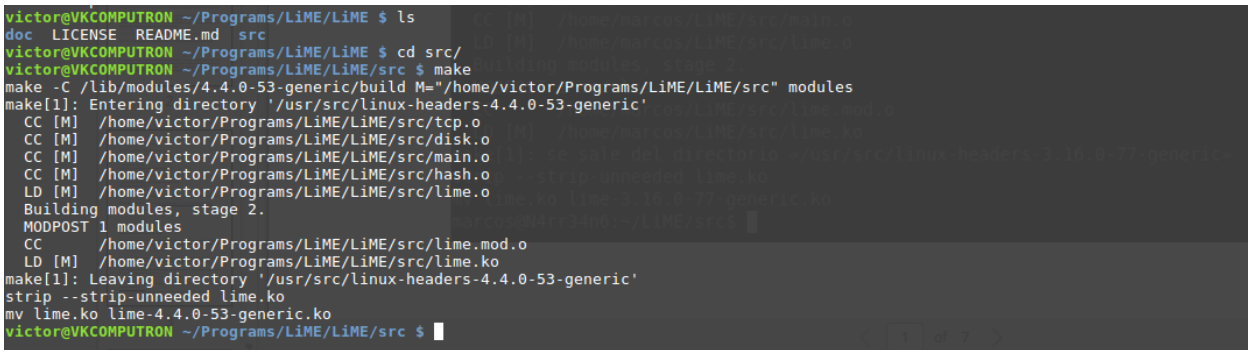
Sesión 2. Análisis forense en Linux (ii)

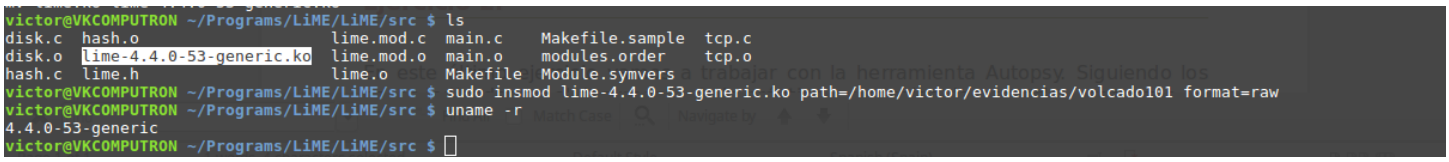
Autor[1]: Víctor García Carrera

Ejercicio 1.

Comenzamos esta última práctica realizando un volcado de memoria RAM en formato .lime de mi sistema. Para ello utilizamos la herramienta open source *LiME* (*Linux Memory Extractor*) que realiza el volcado de la memoria volatil tanto en Linux como en Android. Tras clonar el repositorio y compilar el modulo de *LiME*, podemos observar en la carpeta */src* que aparece un archivo con el nombre *lime-4.4.0-53-generic.ko*, donde la versión que aparece es la del kernel nuestro sistema (podemos obtener esta información mediante el comando *uname -r*).



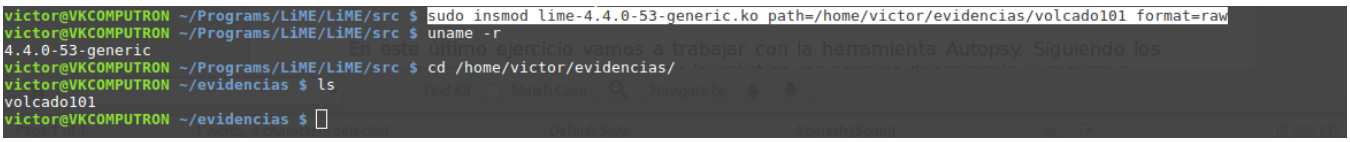




A continuación, realizamos el volcado local de nuestra memoria RAM mediante el siguiente comando:

sudo insmod lime-4.4.0-53-generic.ko path=/home/victor/evidencias/volcado101 format=raw

Tras esperar a que termine el volcado, si accedemos al directorio */home/victor/evidencias* podemos ver que efectivamente se ha realizado el volcado de la memoria volatil al aparecer el fichero *volcado101*.



---

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

Tras realizar este volcado, si formara parte de un análisis forense, podríamos ejecutar time para conocer el momento en el que se realizó este volcado, realizar una copia de seguridad para trabajar con ella y no con el volcado original y calcular la firma SHA-1 para garantizar que los datos no han sido modificados.

Ejercicio 2.

En este último ejercicio trabajamos con la herramienta volatility para analizar la imagen de la RAM obtenida en el ejercicio anterior, utilizando 3 plugins para ver la diversa información específica que nos aporta.