ECCI
Módulo Informática Forense.
Ejemplo 1

Perito:Ramiro José Nogales Ríos
Realizar prácticas de informática forense a una memoria USB.
Para realizarla se usó una memoria USB Kingston de 8GB. Se empleó un computador con sistema operativo BackTrack 5 R3, y las utilidades correspondientes a The Sleuth Kit.

Pasos Realizados:

1. Se ubica la memoria USB: *fdisk -l*, para saber como se reconoce.

root@medusa:~# fdisk -l
Disco /dev/sda: 320.1 GB, 320072933376 bytes
255 cabezas, 63 sectores/pista, 38913 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes
Tamaño de sector (lógico / físico): 512 bytes / 4096 bytes
Tamaño E/S (mínimo/óptimo): 4096 bytes / 4096 bytes
Identificador de disco: 0x07f2837e

Dispositivo Inicio Comienzo Fin Bloques Id Sistema
/dev/sda1 * 1 12167 97725440 83 Linux
/dev/sda2 12167 38914 214842369 5 Extendida
La partición 2 no se inició en el limite físico del sector
/dev/sda5 12167 38306 209960960 83 Linux
/dev/sda6 38306 38914 4880384 82 Linux swap / Solaris

Disco /dev/sdc: 8011 MB, 8011087872 bytes
247 cabezas, 62 sectores/pista, 1021 cilindros
Unidades = cilindros de 15314 * 512 = 7840768 bytes
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes
Identificador de disco: 0x00000000

Dispositivo Inicio Comienzo Fin Bloques Id Sistema
/dev/sdc1 * 1 1021 7817766 c W95 FAT32 (LBA)

La memoria USB está como /dev/sdc1.

2. Se verifica el sistema de archivos que presenta el dispositivo:

root@medusa:~# *df -T /dev/sdc1*
S.ficheros Tipo Bloques de 1K Usado Dispon Uso% Montado en
/dev/sdc1 vfat 7802508 587340 7215168 8% /media/0980-B2DE

3. Se identifica como *fls*, determina el sistema de archivos, correspondiente:

root@medusa:~# *fls -f list*
Supported file system types:
ntfs (NTFS)
fat (FAT (Auto Detection)) ext (ExtX (Auto Detection)) iso9660 (ISO9660 CD)
hfs (HFS+)
ufs (UFS (Auto Detection)) raw (Raw Data)
swap (Swap Space)
fat12 (FAT12)
fat16 (FAT16) fat32 (FAT32) ext2 (Ext2) ext3 (Ext3) ufs1 (UFS1)
ufs2 (UFS2)

4. Se crea la imagen de la memoria:

root@medusa:~# *dd if=/dev/sdc1 of=/home/rnogales/Descargas/forense/usbImagen.dd*
15635532+0 registros de entrada
15635532+0 registros de salida
8005392384 bytes (8,0 GB) copiados, 386,638 s, 20,7 MB/s

5. Se crea una copia de la imagen:

root@medusa:~/Descargas/forense# *cp usbImagen.dd usbImagenCopia.dd*

6. Se verifica los md5, de cada uno de los archivos.

root@medusa:~/Descargas/forense# *md5sum usbImagen.dd*
f36504ab14250778b0d5ad805a35f6d0 usbImagen.dd
root@medusa:~/Descargas/forense# *md5sum usbImagenCopia.dd*
f36504ab14250778b0d5ad805a35f6d0 usbImagenCopia.dd

Se puede comprobar que los archivos son iguales.

7. Se ejecua autopsy:

root@medusa:~/autopsy-2.24# *./autopsy*

==========
Autopsy Forensic Browser http://www.sleuthkit.org/autopsy/ver 2.24
==========

Evidence Locker: /home/rnogales/Descargas/forense

Start Time: Sun Jun 12 22:01:16 2011
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
Este es el modo gráfico de The Sleuth Kit.

8. Para ver los archivos borrados de la imagen.

root@medusa:~/Descargas/forense# *fls -f fat32 -d -r -p usbImagenCopia.dd > borrados1.txt*
Se envían a un archivo .txt, debido a la cantidad de información. Dicho archivo se adjunta a este informe.

9. Se ubica el archivo a recuperar y se obtiene el inodo del listado correspondiente:

r/r * 971938: Examen-Modulo-4-Seguridad-de Red_files/attribution_noncommercial.png, fila 1869 en el archivo borrados1.txt.

Se recupera entonces:

root@medusa:~/Descargas/forense# *icat -f fat32 -r -s usbImagenCopia.dd 971938 > icono.png*

Recuperándose el archivo correspondiente.