PRÁCTICA 3. RECUPERACIÓN DE INFORMACIÓN

Los sistemas de archivo FAT, NTFS, ext2/ext3/ext4 guardan los archivos en bloques de datos o clusters. El tamaño de cluster ó bloque es constante luego de haber sido definido al formatear el sistema de archivos. En general, la mayoría de los sistemas operativos intentan guardar los datos de forma contigua para minimizar el nivel de fragmentación. Cuando un archivo es eliminado, los metatados del archivo (Nombre, fecha/hora, tamaño, ubicación del primer bloque ó cluster, etc.) se pierden; Esto significa que los datos siguen estando presentes, pero solamente hasta que sean sobreescritos en parte o por completo por un nuevo archivo.

PhotoRec es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDs así como imágenes perdidas (por eso el nombre PhotoRecovery) de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado.

TestDisk es un software gratuito de para ayudar a recuperar particiones perdidas y/o volver discos no booteables a booteables nuevamente cuando estos síntomas son causados por fallos software, virus o errores humano (como borrar accidentalmente su Tabla de Particiones).

Autopsy es una plataforma de análisis forense digital y la interfaz gráfica de Sleuthkit y otras herramientas forenses digitales. Es utilizado por gobiernos y entidades públicas y privadas, por fuerzas de seguridad como policiales y militares, además de profesionales y peritos informáticos para investigar lo que ocurrió en un ordenador. Después de algún incidente como un ataque o una falla se puede navegar en dispositivos de almacenamiento para recuperar archivos, buscar manipulaciones de sistema, recuperar fotos, imágenes o vídeos.

Objetivos principales de la práctica:

- **Practicar cómo recuperar información con diferentes herramientas forenses, desde el sistemas de archivos NTFS.**

Software a utilizar:

- FTK imager 4.3 o superior
- Active Disk Editor v7.0
- Photorec
- TestDisk
- Bulk Extractor
- Autopsy

Se pide:

1. Descargar la imagen de disco “recuperacion.dd”

2. Analiza el disco e intenta determinar la siguiente información:
    a. Sistema de particionado del disco (MBR/GPT)

b. Número de particiones válidas y tamaño de las mismas.
c. Investiga si es posible que exista algún sistema de archivos.

3. Utiliza la herramienta **Photorec** para recuperar toda información que te sea posible de la imagen del disco duro. Idem con las herramientas **Bulk Extractor y Autopsy.** Documenta brevemente el proceso.

4. Importa una máquina virtual multisistema (XP-ubuntu) desde la siguiente OVA. Estropea el MBR a propósito e intenta recuperarla con el disco de instalación de XP y con la herramienta TestDisk.

5. Importa una máquina virtual multisistema (W7-debian) desde la siguiente OVA. Estropea el MBR a propósito e intenta recuperarla con el disco de instalación de Windows 7.