PRÁCTICA 1. ANÁLISIS DE LAS TABLAS DE PARTICIONES

La tabla de particiones es una parte esencial en la computadora que, dependiendo de si es MBR o GPT, está físicamente ubicada en diferentes sectores del disco y controla el proceso de arranque. En la práctica de la pericial informática se hace necesario estudiar su estructura para asegurarse de que la computadora no esté infectada por programas maliciosos como malware que puede reemplazar el MBR y cargar archivos maliciosos software a la memoria de la computadora durante el proceso de arranque. Además, esto ayuda en las investigaciones forenses a extraer detalles del disco, así como el tipo de sistema de archivos utilizado por las particiones y su tamaño. Estos análisis también pueden utilizarse como evidencia digital o incluso pueden servir para recuperar datos perdidos. En cualquier caso se hace necesario comprender la estructura de los medios de almacenamiento lógicos y físicos que se utilizan para almacenar la información requerida en la computadora.

Objetivos principales de la práctica:

- **Estudiar las tablas de particiones de los sistemas MBR y GPT**

Software a utilizar:

- Windows X
- Winhex
- Sleuth kit
- dd

Se pide:

- Crear una máquina virtual Windows
- Descargar de aquí dos imágenes de discos duros
- Practicar los comandos de extracción de sectores donde residen las tablas de particiones. Recuerda que los comandos tienen pequeñas diferencias dependiendo del S.O. Ejemplos:

  # dd if=disk3.dd bs=512 skip=0 count=1 | xxd

  c:\>dd count=1 bs=512 if=\\.\PHYSICALDRIVE2 of=d:\mbr.dd skip=0

- Obtener toda la información de los discos que puedas:
  1. Determinar si la tabla de particiones es MBR o GPT
  2. Si es MBR, determinar para cada partición los siguientes datos:
     a. Numero de particion
     b. Indicador de arranque
     c. Cilindro, Cabezal, Sector (CHS) del primer sector en la partición
     d. Tipo de partición
     e. Cilindro, Cabezal, Sector (CHS) del último sector de la partición
     f. Logical block address del primer sector de la partición
     g. Longitud de la partición, en sectores

3. Si es GPT, determinar para cada partición los siguientes datos:
    a. Dirección de la cabecera GPT
    b. Tamaño de la cabecera
    c. Primer LBA usable
    d. Último LBA usable
    e. GUID del disco
    f. Sector que contiene la tabla de particiones
    g. Para cada partición
        i. Tipo de partición
        ii. GUID
        iii. LBA donde empieza
        iv. LBA donde acaba
        v. Nombre
4. Contrasta la información que has obtenido de forma manual con las que te ofrecen herramientas forenses del tipo Sleuthkit. Ejemplo:

    mmls -t gpt|dos <disco>

5. Comenta las peculiaridades que hayas encontrado en los discos del tipo: particiones ocultas, zonas de datos vacías, etc.