PRÁCTICA 2: ADQUISICIÓN DE EVIDENCIAS. SISTEMA APAGADO (COLD-CLONE)

Estamos trabajando en una estación de trabajo del cliente, posiblemente una computadora portátil o una torre.

Usaremos herramientas como:

1) Comandos estándar de Unix: dd, nc, find

2) Distribuciones especializadas de Linux, o

3) Clonadora de discos

Objetivos principales de la práctica:

- **Recopilación de pruebas conservando su forma y contenido originales**

Se pide:

- Descargate el siguiente VHD, monta una máquina virtual simulando que se trata de un PC de un cliente. Añade un segundo VHD donde realizarás las clonación.
- Realiza una clonación del VHD haciendo uso de diversas técnicas.
    - ¿Qué requisitos debemos de cumplir para que la evidencia digital no se vea comprometida?
    - ¿Qué materiales/software necesitas?
- Calcula los HASH de original y copia (comando sha512sum)
- Documenta el proceso de clonación