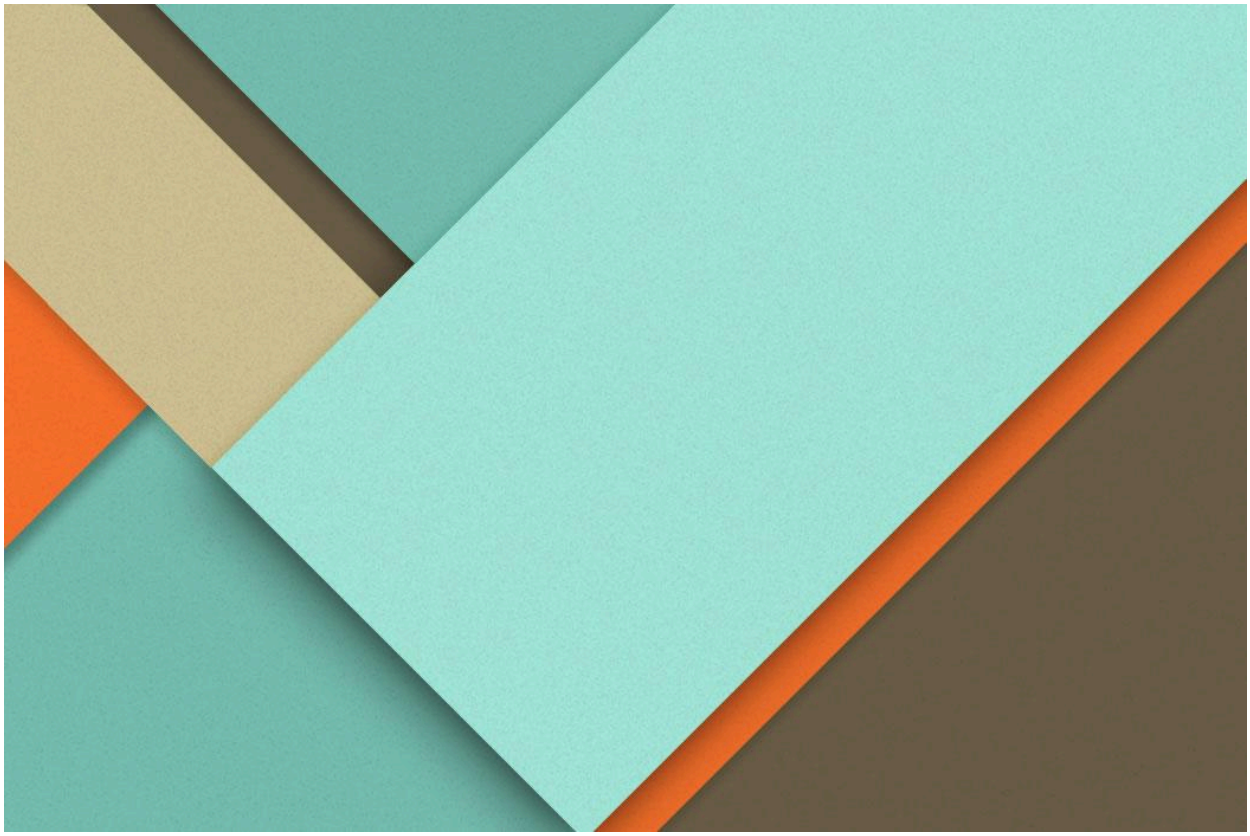


1. Análisis de las tablas de particiones

25/11/2025

—

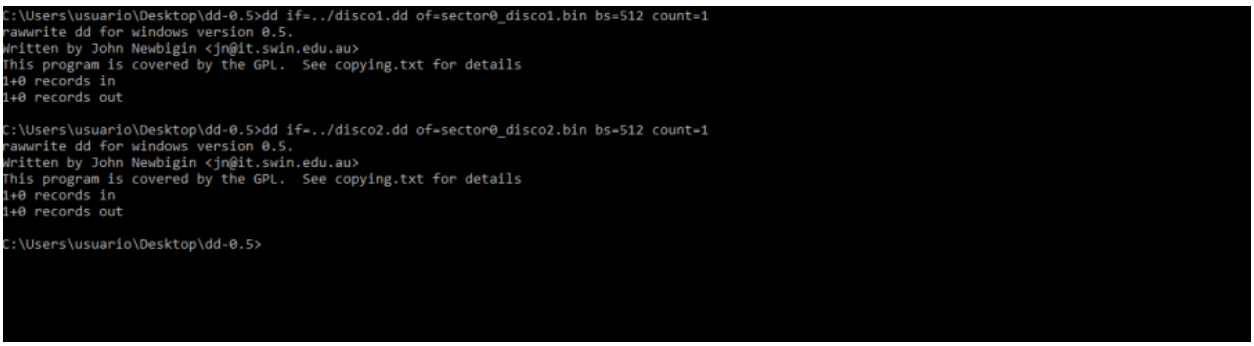
Ramón Javier Romero Montilla
Granada
Análisis Forense

1. Crear una máquina virtual Windows y practicar los comandos de extracción de sectores

Para el desarrollo de la práctica se ha procedido a la creación de una máquina virtual con el sistema operativo Windows 10 utilizando un entorno de virtualización. Una vez configurado el entorno, se descargaron las imágenes forenses disco1.dd y disco2.dd para su análisis.

Con el objetivo de verificar el acceso a los discos y extraer la información inicial, se utilizó la herramienta dd for Windows a través de la consola de comandos. Se ejecutaron los comandos necesarios para volcar los primeros 512 bytes correspondientes al Sector 0 de cada imagen en archivos con extensión .bin.

La ejecución de dichos comandos arrojó un resultado exitoso de lectura y escritura de registros, lo que confirma que las imágenes son accesibles y que la extracción del sector de arranque se realizó correctamente para su posterior análisis con editores hexadecimales.



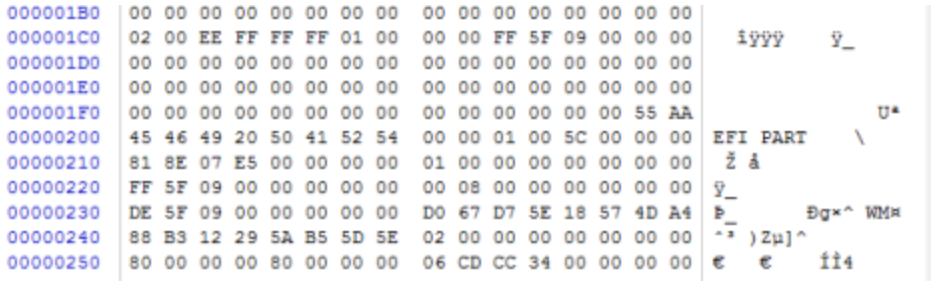
2. Obtener toda la información de los discos que puedas

Disco 1: Es **GPT**.*Evidencia:* Presencia de la firma "EFI PART" en el Sector 1 (Offset 512).

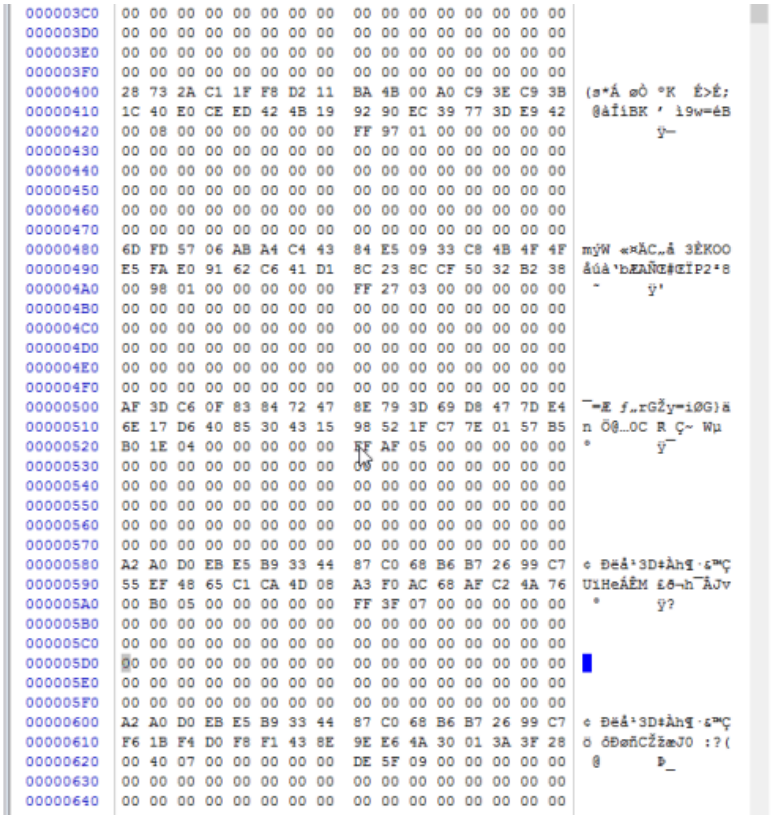
- **a. Dirección de la cabecera GPT:** LBA 1 (Offset 512 / 0x200)
- **b. Tamaño de la cabecera:** 92 bytes (5C 00 00 00)
- **c. Primer LBA usable:** 34 (22 00 00 00)
- **d. Último LBA usable:** 614.366 (DE 5F 09 00)

- **e. GUID del disco:** D0 67 D7 5E 18 57 4D A4 88 B3 12 29 5A B5 5D 5E
- **f. Sector que contiene la tabla de particiones:** LBA 2 (Offset 1024 / 0x400)

Datos	Partición 1	Partición 2	Partición 3	Partición 4	Partición 5
i. Tipo de partición	EFI System (28 73 2A...)	Linux Swap (6D FD 57...)	Linux Filesystem (AF 3D C6...)	Basic Data (A2 A0 D0...)	Basic Data (A2 A0 D0...)
ii. GUID Único	1C 40 E0...	84 E5 09...	8E 79 3D...	87 C0 68...	87 C0 68...
iii. LBA Inicio	2048	104,448	270,000	372,736	475,136
iv. LBA Fin	104,447	206,847	372,735	475,135	614,366
v. Nombre	(Vacío)	(Vacío)	(Vacío)	(Vacío)	(Vacío)



```
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0  02 00 EE FF FF FF 01 00  00 00 FF 5F 09 00 00 00    îÿÿÿ     ÿ_
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA                U*
00000200  45 46 49 20 50 41 52 54  00 00 01 00 5C 00 00 00  EFI PART     \
00000210  81 8E 07 E5 00 00 00 00  01 00 00 00 00 00 00 00   Ž å
00000220  FF 5F 09 00 00 00 00 00  00 08 00 00 00 00 00 00  ÿ_
00000230  DE 5F 09 00 00 00 00 00  D0 67 D7 5E 18 57 4D A4  Þ_       Ðg×^ WM¤
00000240  88 B3 12 29 5A B5 5D 5E  02 00 00 00 00 00 00 00  ^³ )Zµ]^
00000250  80 00 00 00 80 00 00 00  06 CD CC 34 00 00 00 00  €   €     ÍÌ4
```

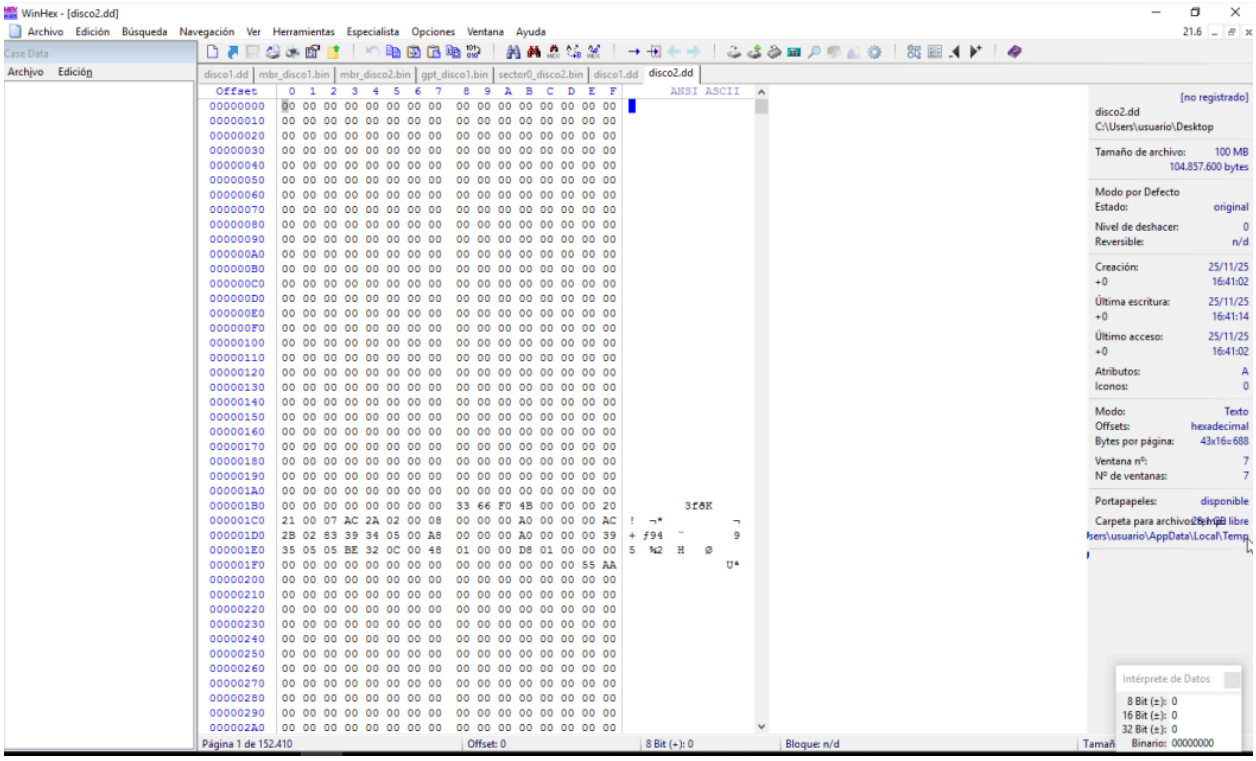


```
000003C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000003D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000003E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000003F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000400  28 73 2A C1 1F F8 D2 11  BA 4B 00 A0 C9 3E C9 3B  (s*Á øÒ ºK  É>É;
00000410  1C 40 E0 CE ED 42 4B 19  92 90 EC 39 77 3D E9 42   @àÎíBK ' ì9w=éB
00000420  00 08 00 00 00 00 00 00  FF 97 01 00 00 00 00 00          ÿ—
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000440  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000450  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000460  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000470  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000480  6D FD 57 06 AB A4 C4 43  84 E5 09 33 C8 4B 4F 4F  mýW «¤ÄC„å 3ÈKOO
00000490  E5 FA E0 91 62 C6 41 D1  8C 23 8C CF 50 32 B2 38  åúà'bÆAÑŒ#ŒÏP2²8
000004A0  00 98 01 00 00 00 00 00  FF 27 03 00 00 00 00 00   ˜       ÿ'
000004B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000004C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000004D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000004E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000004F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000500  AF 3D C6 0F 83 84 72 47  8E 79 3D 69 D8 47 7D E4  ¯=Æ ƒ„rGŽy=iØG}ä
00000510  6E 17 D6 40 85 30 43 15  98 52 1F C7 7E 01 57 B5  n Ö@…0C R Ç~ Wµ
00000520  B0 1E 04 00 00 00 00 00  FF AF 05 00 00 00 00 00  °       ÿ¯
00000530  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000540  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000550  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000570  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000580  A2 A0 D0 EB E5 B9 33 44  87 C0 68 B6 B7 26 99 C7  ¢ ÐëÅ¹3D‡Àh¶·&™Ç
00000590  55 EF 48 65 C1 CA 4D 08  A3 F0 AC 68 AF C2 4A 76  UïHeÁÊM £ð¬h¯ÂJv
000005A0  00 B0 05 00 00 00 00 00  FF 3F 07 00 00 00 00 00   °       ÿ?
000005B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000005C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000005D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000005E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000005F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000600  A2 A0 D0 EB E5 B9 33 44  87 C0 68 B6 B7 26 99 C7  ¢ ÐëÅ¹3D‡Àh¶·&™Ç
00000610  F6 1B F4 D0 F8 F1 43 8E  9E E6 4A 30 01 3A 3F 28  ö ôÐøñCŽžæJ0 :?(
00000620  00 40 07 00 00 00 00 00  DE 5F 09 00 00 00 00 00   @       Þ_
00000630  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000640  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Disco 2: Es **MBR**. *Evidencia:* Firma 55 AA en el Sector 0 y 3 particiones definidas con tipos estándar (07, 83) sin MBR de protección (EE).

Dato	Partición 1	Partición 2	Partición 3
a. Número de partición	1	2	3
b. Indicador de arranque	00 (No arrancable)	00 (No arrancable)	00 (No arrancable)
c. CHS del primer sector	20 21 00	AC 2B 02	39 35 05
d. Tipo de partición	07 (NTFS / Windows)	83 (Linux)	05 (Extendida)
e. CHS del último sector	AC 2A 02	39 34 05	BE 32 0C
f. LBA del primer sector	2048	43008	83968

g. Longitud (sectores)	40960	3232	120832




```
000001B0  00 00 00 00 00 00 00 00  33 66 F0 4B 00 00 00 20          3fðK
000001C0  21 00 07 AC 2A 02 00 08  00 00 00 A0 00 00 00 AC  !  ¬*          ¬
000001D0  2B 02 83 39 34 05 00 A8  00 00 00 A0 00 00 00 39  + ƒ94  ¨          9
000001E0  35 05 05 BE 32 0C 00 48  01 00 00 D8 01 00 00 00  5  ¾2  H   Ø
000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA                  U*
00000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

3. Contrasta la información que has obtenido de forma manual con las que te ofrecen herramientas forenses del tipo Sleuthkit

Para verificar la integridad y exactitud de los datos obtenidos manualmente mediante el análisis hexadecimal, se utilizó la herramienta forense de línea de comandos **mmls** (*The Sleuth Kit*) que permite listar la estructura de particionamiento de forma automatizada y recursiva.

Comparativa de Resultados:

- **Disco 1 (GPT):** La herramienta confirma las 5 particiones identificadas manualmente en WinHex. Los sectores de inicio (*Start*) coinciden exactamente con nuestros cálculos (2048, 104448, 270000, 372736, 475136).

```
C:\Users\usuario\Desktop>mmls -t gpt disco1.dd
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0000104447   0000102400
005:  001       0000104448   0000206847   0000102400
006:  -------   0000206848   0000269999   0000063152   Unallocated
007:  002       0000270000   0000372735   0000102736
008:  003       0000372736   0000475135   0000102400
009:  004       0000475136   0000614366   0000139231
010:  -------   0000614367   0000614399   0000000033   Unallocated
```

- **Disco 2 (MBR):** El análisis confirma las 3 entradas primarias en la tabla de particiones (Slots 002, 003 y 004). Los tamaños coinciden con la conversión manual (40960 sectores para las dos primeras).

```
C:\Users\usuario\Desktop>mmls -t dos disco2.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000043007   0000040960   NTFS / exFAT (0x07)
003:  000:001   0000043008   0000083967   0000040960   Linux (0x83)
004:  Meta      0000083968   0000204799   0000120832   DOS Extended (0x05)
005:  Meta      0000083968   0000083968   0000000001   Extended Table (#1)
006:  -------   0000083968   0000086015   0000002048   Unallocated
007:  001:000   0000086016   0000126975   0000040960   Win95 FAT32 Hidden (0x1c)
008:  Meta      0000126976   0000204799   0000077824   DOS Extended (0x05)
009:  Meta      0000126976   0000126976   0000000001   Extended Table (#2)
010:  -------   0000126976   0000129023   0000002048   Unallocated
011:  002:000   0000129024   0000204799   0000075776   Linux Swap / Solaris x86 (0x82)
```

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

Durante el análisis forense se han detectado anomalías y estructuras que no corresponden a un particionamiento estándar lineal:

1. Zona de datos vacía (Gap) en el Disco 1: La herramienta mmls (Slot 006) y el análisis manual confirman la existencia de un "agujero" de datos no asignados entre la Partición 2 y la Partición 3.

- La Partición 2 termina en el sector 206.847.

- La Partición 3 comienza en el sector 270.000.
- Existe un bloque **Unallocated** de **63.152 sectores** (aprox. 32 MB). En un escenario real, este espacio es crítico porque podría utilizarse para ocultar información (*data hiding*) fuera del sistema de archivos visible.

2. Estructura recursiva en el Disco 2 (Partición Extendida): El análisis del MBR reveló una partición de tipo 0x05 (Extendida) en el Slot 004.

- Aunque en el Sector 0 (MBR) aparece como una sola entrada de 120.832 sectores, la herramienta mmls revela que **es un contenedor**.
- Dentro de ella, existen unidades lógicas que no son visibles en la tabla principal: una partición **"Win95 FAT32 Hidden"** (Slot 007) y una **"Linux Swap"** (Slot 011).
- La presencia de una partición marcada como *Hidden* (Oculta, tipo 0x1c) es una peculiaridad forense importante, ya que el sistema operativo normal podría no montarla automáticamente, ocultando su contenido al usuario.