

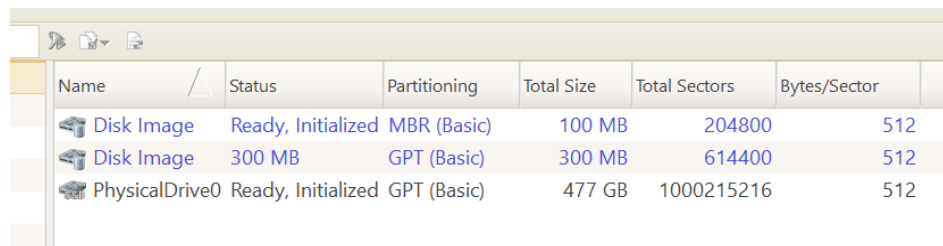
## Practica 1

# Analisis de las tablas de particiones

vamos a examinar las tablas de particiones de los discos que hemos descargado a través del Master Boot Record (MBR). Podemos obtener una cantidad significativa de información valiosa mediante este análisis. En este proceso, nos enfocaremos en dos discos específicos utilizando la herramienta Active Disk Editor.

### 1. Determinar si la tabla de particiones es MBR o GPT

Al examinar los discos descargados con Active Disk Editor, es evidente que el disco 1 (disco1.dd) posee una tabla de particiones GPT, mientras que el disco 2 (disco2.dd) cuenta con una tabla de particiones MBR.



Name	Status	Partitioning	Total Size	Total Sectors	Bytes/Sector
Disk Image	Ready, Initialized	MBR (Basic)	100 MB	204800	512
Disk Image	300 MB	GPT (Basic)	300 MB	614400	512
PhysicalDrive0	Ready, Initialized	GPT (Basic)	477 GB	1000215216	512

### 2. Ejemplo con una tabla de particiones MBR

En el caso de que la tabla de particiones sea MBR, como es el caso del disco 2 (disco2.dd), procederemos a obtener la siguiente información:

Numero de particion	Indicador de arranque	CHS primer sector	Tipo de particion	CHS ultimo sector	LBA primer sector	Longitud de la particion
1	0x00	0x00, 32, 0x21	NTFS	0x02, 172, 0x2A	2048	40960
2	0x02	0x02, 172, 0x2B	EXT2	0x05, 57, 0x34	43008	40960

3	0x05	0x05, 57, 0x35	Extended	0x0C, 190, 0x032	83968	120832
4	0x00	0x00, 0, 0x00	Unused	0x00, 0, 0x00	0	0

### 3. Ejemplo con una tabla de particiones GPT

En el caso de que la tabla de particiones sea GPT, como es el caso del disco 1 (disco1.dd), procederemos a obtener la siguiente información:

Dirección de la cabecera GPT	Tamaño de la cabecera	Primer LBA usable	Último LBA usable	GUID del disco	Sector que contiene la tabla de particiones
45 46 49 20 50 41 52 54	92	2.048	614.386	D0 67 D7 5E 18 57 4D A4 88 B3 12 29 5A B5 5D 5E	2

Además, debemos recopilar la siguiente información para cada partición:

Tipo de partición	GUID	LBA donde empieza	LBA donde acaba	Nombre
EFI	1C 40 E0 CE ED 42 4B 19 92 90 EC 39 77 3D E9 42	2.048	104.447	
Swap	E5 FA E0 91 62 C6 41 D1 8C 23 8C CF 50 32 B2 38	104.448	206.847	
	6E 17 D6 40 85 30 43 15 98 52 1F C7 7E 01 57 B5	270.000	372.735	
NTFS	55 EF 48 65 C1 CA 4D 08 A3 F0 AC 68 AF C2 4A 76	372.736	475.135	

NTFS	F6 1B F4 D0 F8 F1 43 8E 9E E6 4A 30 01 3A 3F 28	475.136	614.366	
------	--	---------	---------	--

#### 4. Contrasta la información que has obtenido de forma manual con las que te ofrecen herramientas forenses del tipo Sleuthkit. Ejemplo:

Con Autopsy, tenemos la capacidad de comparar la información obtenida manualmente con la que la aplicación nos ofrece directamente. En este contexto, examinamos los resultados generados por la herramienta en relación con el disco 1 (disco1.dd) con formato GPT

Listing

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol4 (Unknown: 2048-104447)	4	2048	102400	Unknown	Allocated
vol5 (Unknown: 104448-206847)	5	104448	102400	Unknown	Allocated
vol6 (Unallocated: 206848-269999)	6	206848	63152	Unallocated	Unallocated
vol7 (Unknown: 270000-372735)	7	270000	102736	Unknown	Allocated
vol8 (Unknown: 372736-475135)	8	372736	102400	Unknown	Allocated
vol9 (Unknown: 475136-614366)	9	475136	139231	Unknown	Allocated
vol10 (Unallocated: 614367-614399)	10	614367	33	Unallocated	Unallocated

Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

Page: 1 of Page Go to Page: 1 Jump to Offset Launch in HxD

```

0x00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Y además, podemos cotejar la información recopilada del disco 2 (disco2.dd) con un formato de tabla de particiones MBR utilizando la misma herramienta

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-43007)	2	2048	40960	NTFS / exFAT (0x07)	Allocated
vol3 (Linux (0x83): 43008-83967)	3	43008	40960	Linux (0x83)	Allocated
vol6 (Unallocated: 83968-86015)	6	83968	2048	Unallocated	Unallocated
vol7 (Win95 FAT32 Hidden (0x1c): 86016-126975)	7	86016	40960	Win95 FAT32 Hidden (0x1c)	Allocated
vol10 (Unallocated: 126976-129023)	10	126976	2048	Unallocated	Unallocated
vol11 (Linux Swap / Solaris x86 (0x82): 129024-204800)	11	129024	75776	Linux Swap / Solaris x86 (0x82)	Allocated

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences


Page: 1 of Page Go to Page: 1 Jump to Offset Launch in HxD

0x00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

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

Basándonos en la información obtenida sobre el disco MBR, podemos comentar sobre algunas peculiaridades encontradas:

1. Partición 3 - Tipo Extended: Esta partición tipo "Extended" podría considerarse como una partición oculta, ya que no almacena directamente datos visibles para el usuario. En cambio, sirve como un contenedor para particiones lógicas adicionales (en este caso, la Partición 4).
2. Partición 4 - Tipo Unused: La Partición 4 está etiquetada como "Unused", indicando que no se utiliza para almacenar datos. Es común encontrar particiones de este tipo en configuraciones de discos MBR, pero la razón específica para su existencia puede variar.
3. Zonas de Datos Vacías: Aunque no se ha especificado explícitamente, la presencia de particiones con el tipo "Unused" sugiere la existencia de zonas de datos vacías en el disco, áreas que no se asignan a ninguna partición específica.



Basándome en la información obtenida sobre el disco GPT, a continuación se destacan algunas peculiaridades encontradas:

1. Cabecera GPT:

- La dirección de la cabecera GPT está marcada como "EFI", indicando que el disco sigue el estándar de interfaz de firmware extensible.
- El tamaño de la cabecera es de 92 sectores, y el primer LBA usable comienza en el sector 2,048, lo que es consistente con las configuraciones típicas de discos GPT.
- La presencia de un GUID único para el disco (D0 67 D7 5E 18 57 4D A4 88 B3 12 29 5A B5 5D 5E) identifica de manera única este disco en particular.

2. Particiones GPT:

- Se observa la presencia de particiones con tipos específicos (por ejemplo, Tipo 1C 40 E0 CE ED, Tipo E5 FA E0 91 62) que indican la naturaleza de los datos almacenados en esas particiones.
- La existencia de particiones con GUIDs únicos (por ejemplo, GUID de la Partición 1: 42 4B 19 92 90 EC 39 77 3D E9 42) proporciona identificadores únicos para cada partición.
- No se menciona información sobre zonas de datos vacías directamente, pero la longitud de las particiones y los espacios entre ellas pueden indicar áreas no asignadas que podrían considerarse como zonas de datos vacías.

3. Partición Extendida:

- En el disco GPT no hay particiones extendidas como en el MBR. En cambio, se utiliza una tabla de particiones GPT que permite un mayor número de particiones directas sin la necesidad de particiones extendidas.