Práctica 1

Análisis de las Tablas de Particiones

Índice

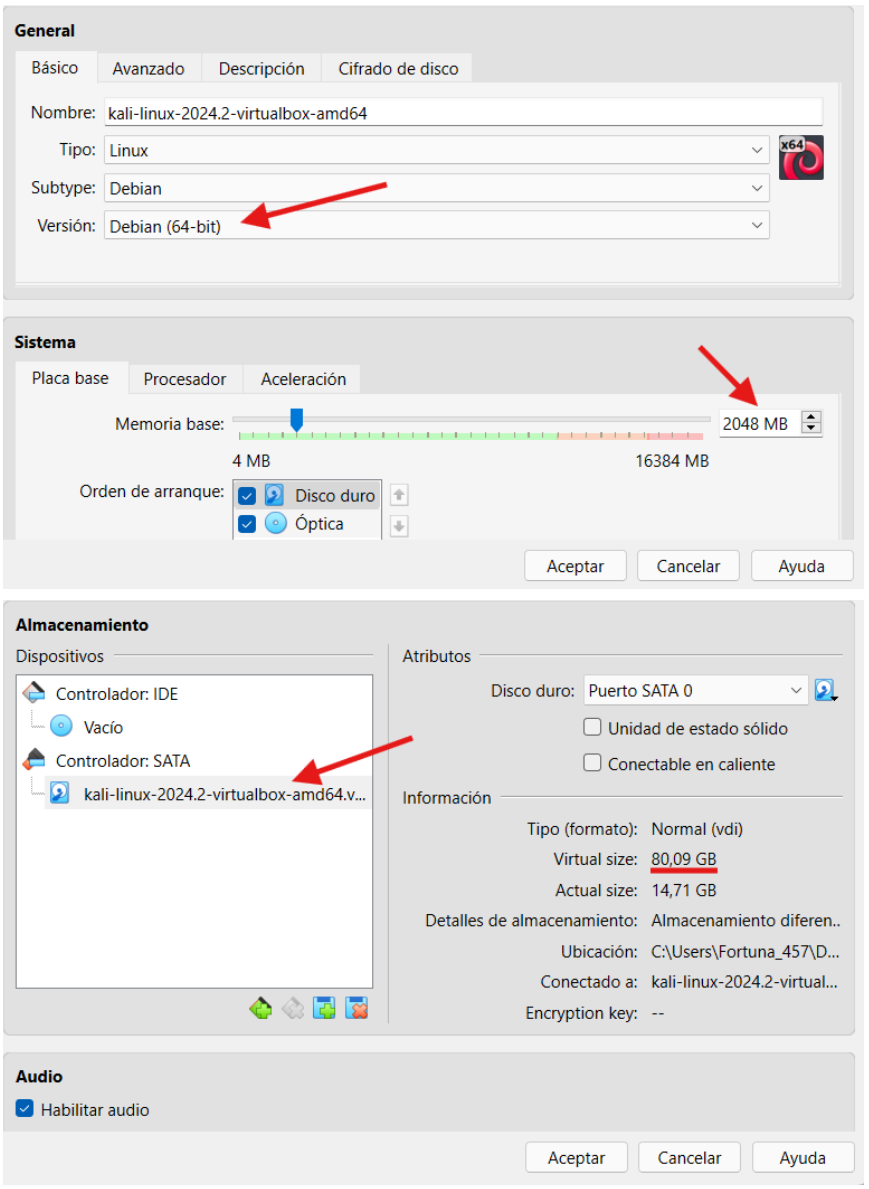
Pasos Previos:

1. Creación de Máquinas Virtuales (VM):

   a. Kali Linux:

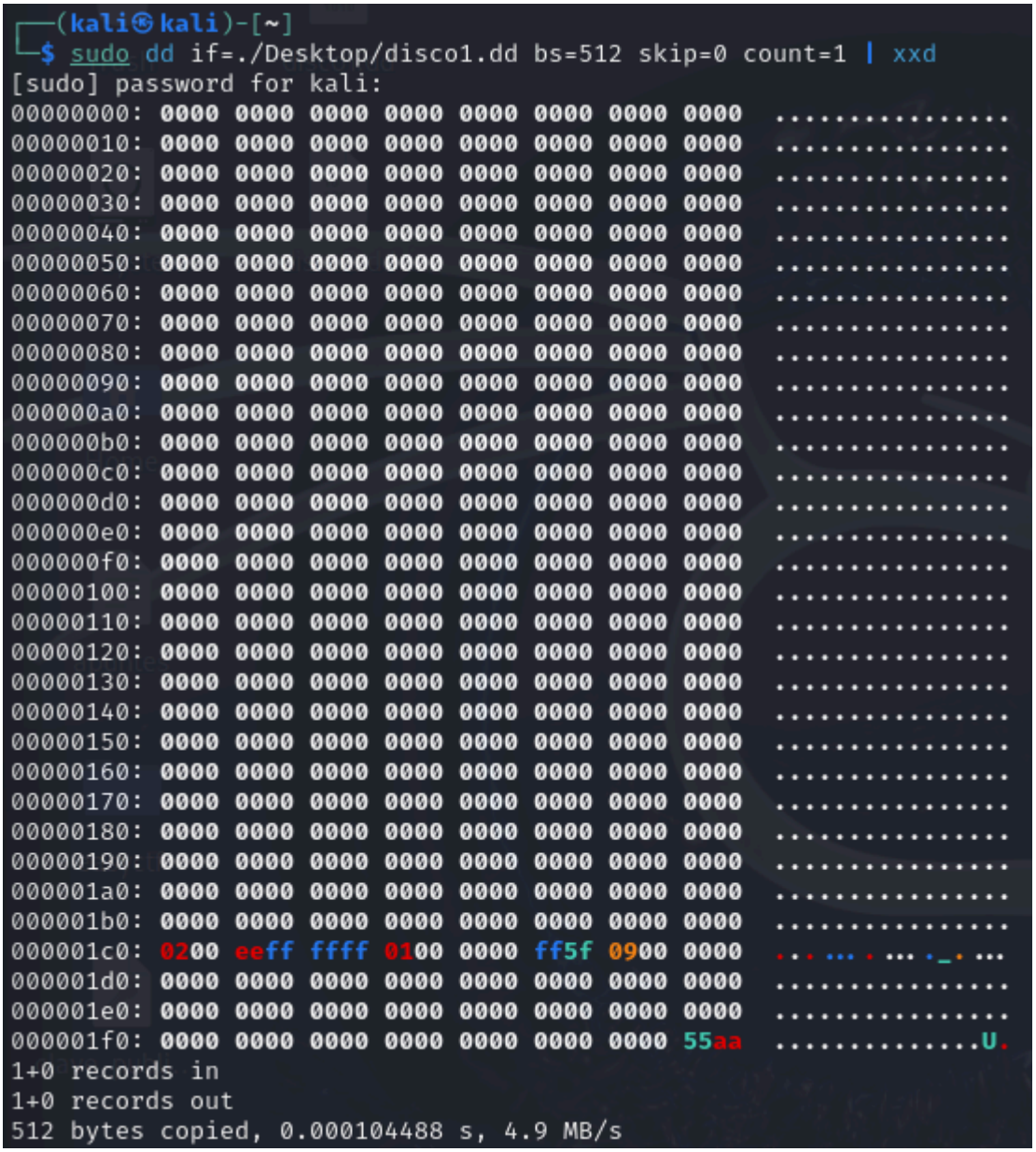
   Configuramos la máquina virtual para que tenga 2GB de memoria Ram y 80 GB de disco duro.

   Usamos una ISO de Kali Linux 2024.3 x64.



Extraemos los sectores con la herramienta dd:

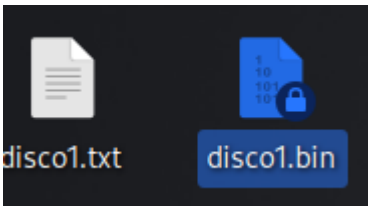
1. disco1.dd



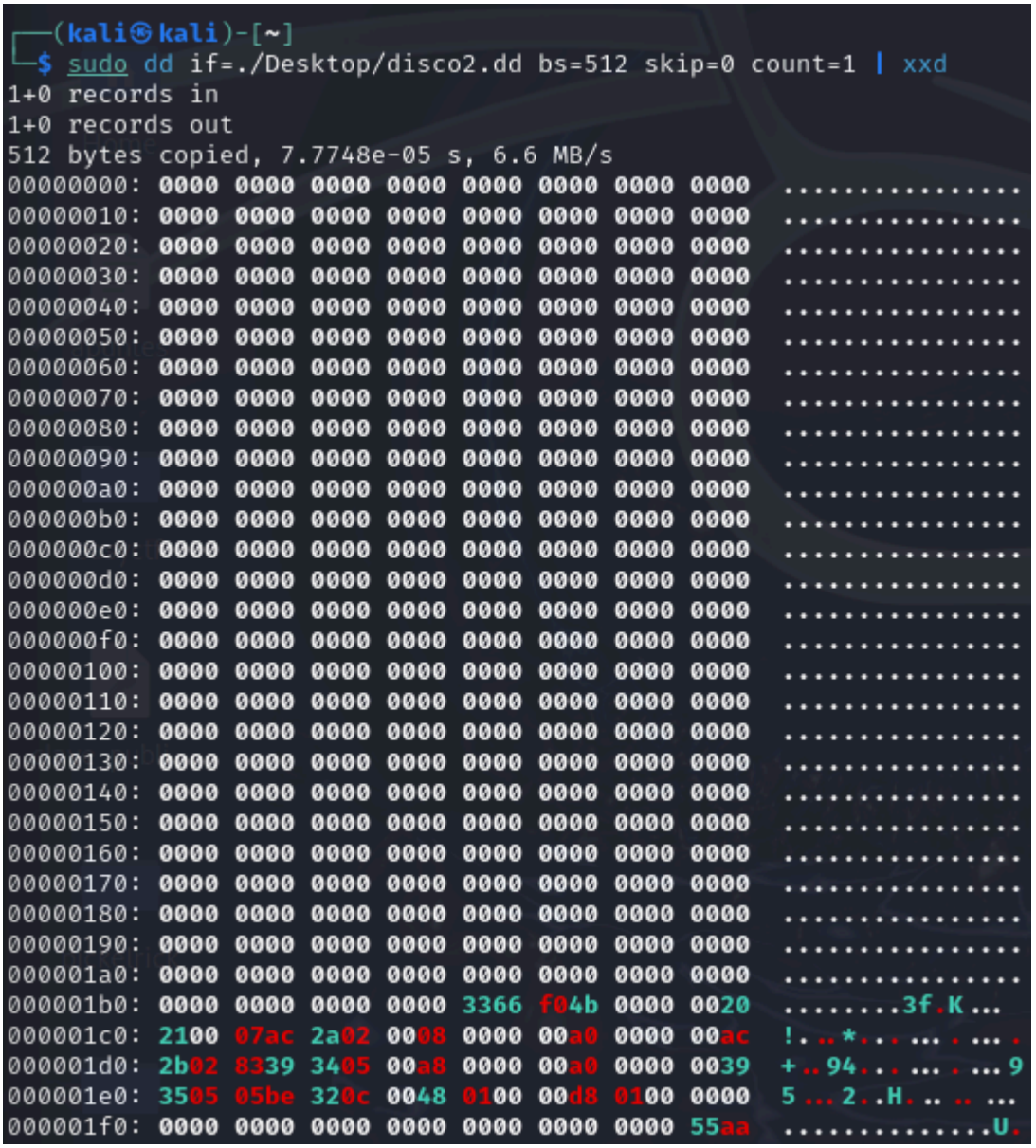
sudo dd if=./Desktop/disco1.dd bs=512 skip=0 count=1 | xxd > ./Desktop/disco1.txt

sudo dd if=./Desktop/disco1.dd bs=512 skip=0 count=1 of=./Desktop/disco1.bin

```
┌──(kali㉿kali)-[~]
└─$ sudo dd if=./Desktop/disco1.dd bs=512 skip=0 count=1 | xxd > ./Desktop/disco1.txt
1+0 records in
1+0 records out
512 bytes copied, 0.00738298 s, 69.3 kB/s

┌──(kali㉿kali)-[~]
└─$ sudo dd if=./Desktop/disco1.dd bs=512 skip=0 count=1 of=./Desktop/disco1.bin
1+0 records in
1+0 records out
512 bytes copied, 3.6085e-05 s, 14.2 MB/s
```



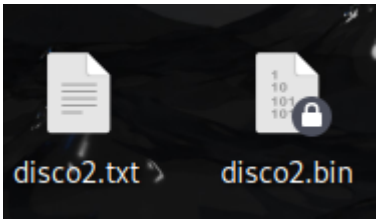
2. disco2.dd


┌──(kali㉿kali)-[~]
└─$ sudo dd if=./Desktop/disco2.dd bs=512 skip=0 count=1 | xxd
1+0 records in
1+0 records out
512 bytes copied, 7.7748e-05 s, 6.6 MB/s
00000000: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000010: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000100: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000110: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000120: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000130: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000140: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000150: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000160: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000170: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000190: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000001b0: 0000 0000 0000 0000 3366 f04b 0000 0020 ....3f.K ...
000001c0: 2100 07ac 2a02 0008 0000 00a0 0000 00ac !...*... ... .
000001d0: 2b02 8339 3405 00a8 0000 00a0 0000 0039 +..94... 9
000001e0: 3505 05be 320c 0048 0100 00d8 0100 0000 5 ... 2..H. .. ..
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa ....U.

sudo dd if=./Desktop/disco2.dd bs=512 skip=0 count=1 | xxd > ./Desktop/disco2.txt

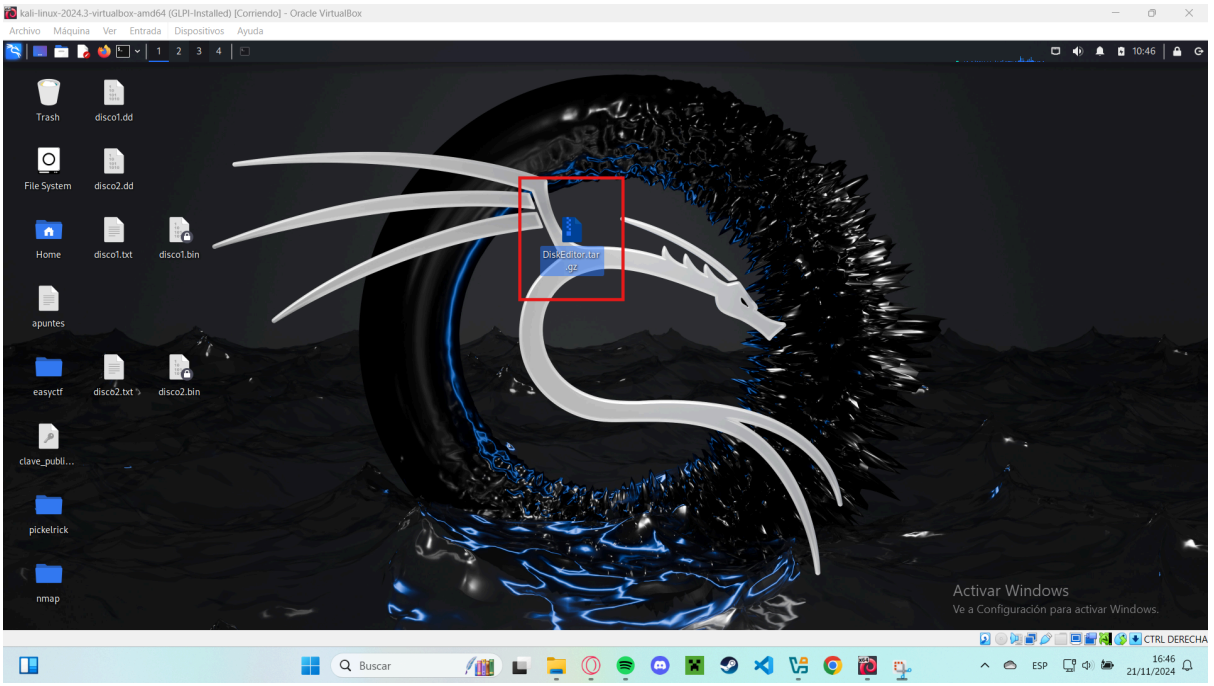
sudo dd if=./Desktop/disco2.dd bs=512 skip=0 count=1 of=./Desktop/disco2.bin

```
┌──(kali㉿kali)-[~]
└─$ sudo dd if=./Desktop/disco2.dd bs=512 skip=0 count=1 | xxd > ./Desktop/disco2.txt
1+0 records in
1+0 records out
512 bytes copied, 6.6981e-05 s, 7.6 MB/s

┌──(kali㉿kali)-[~]
└─$ sudo dd if=./Desktop/disco2.dd bs=512 skip=0 count=1 of=./Desktop/disco2.bin
1+0 records in
1+0 records out
512 bytes copied, 3.4724e-05 s, 14.7 MB/s
```



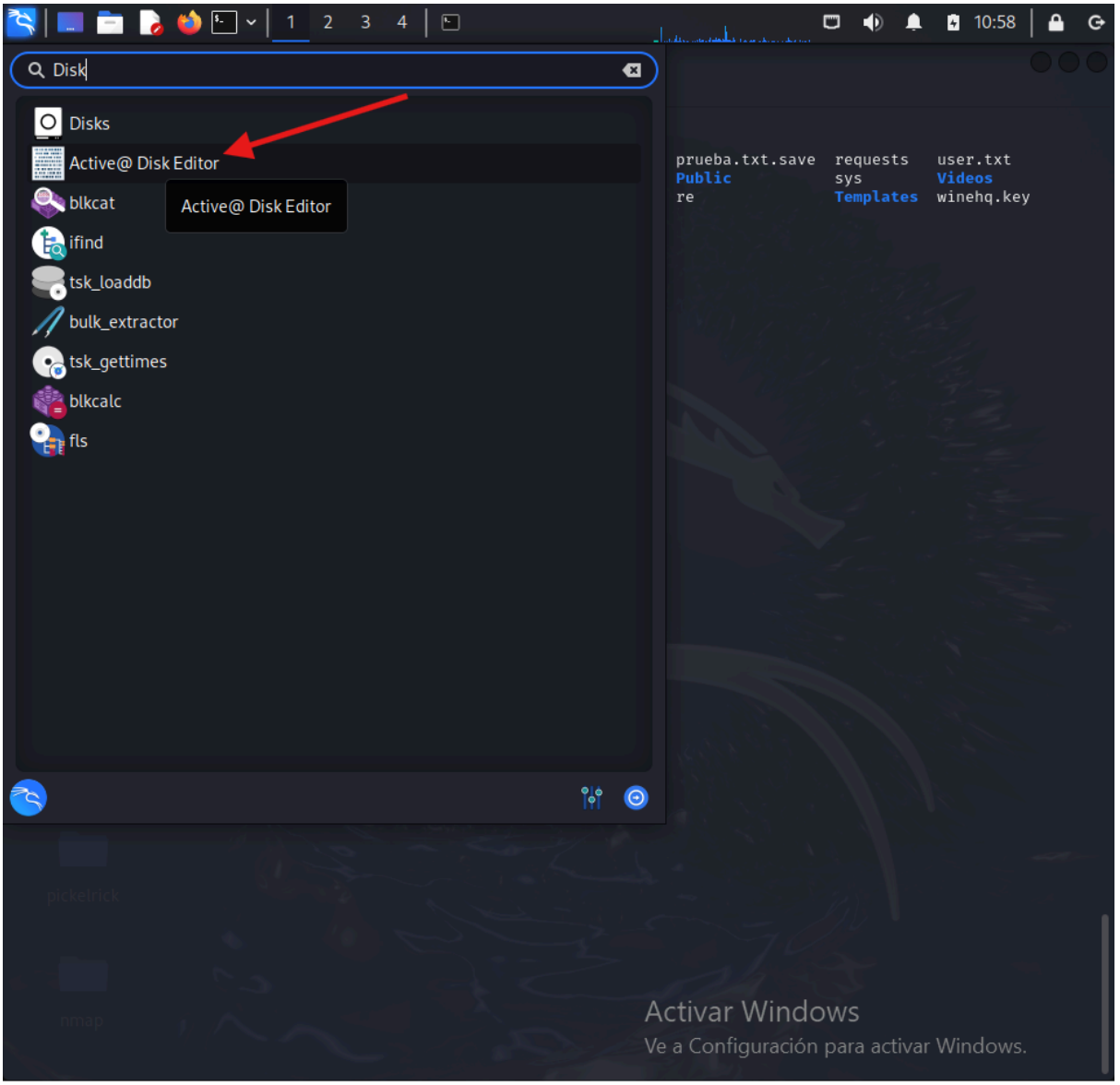
Active Disk Editor:

1. Instalación de Active Disk Editor.

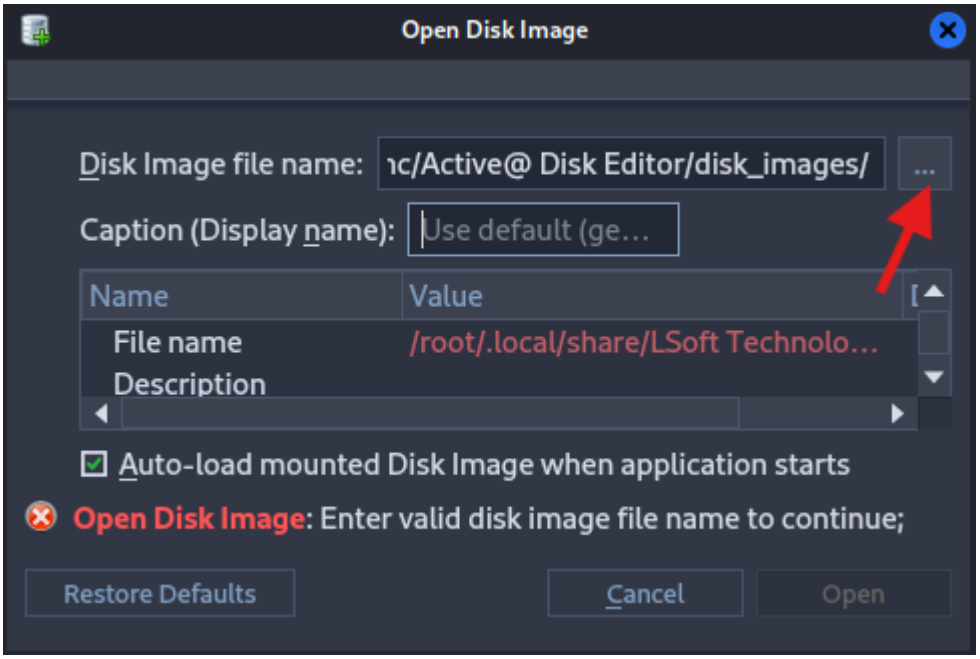


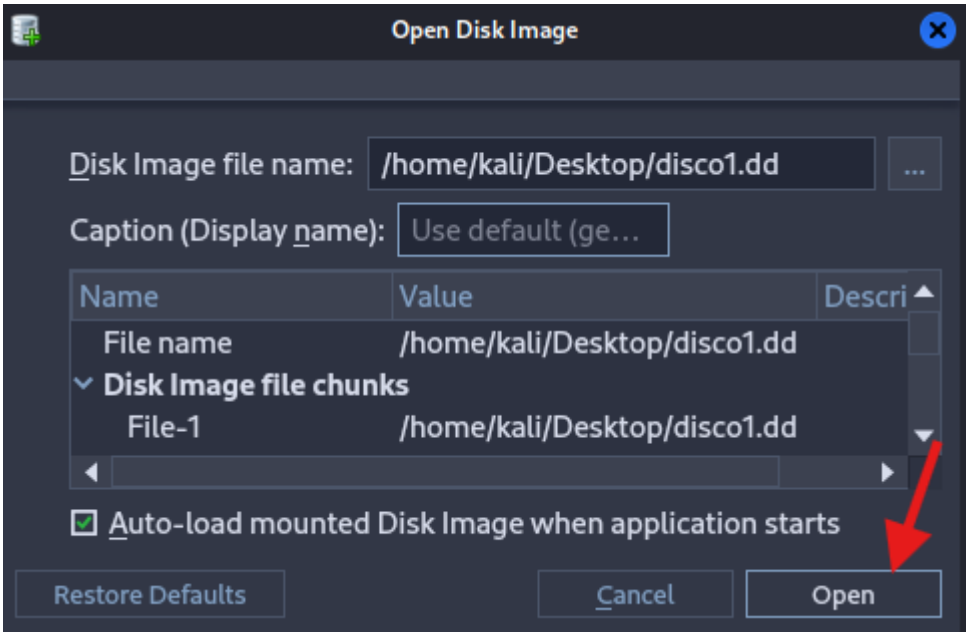

```
┌──(kali㉿kali)-[~]
└─$ tar -xvzf ./Desktop/DiskEditor.tar.gz
DiskEditor_Linux_Installer.run
```

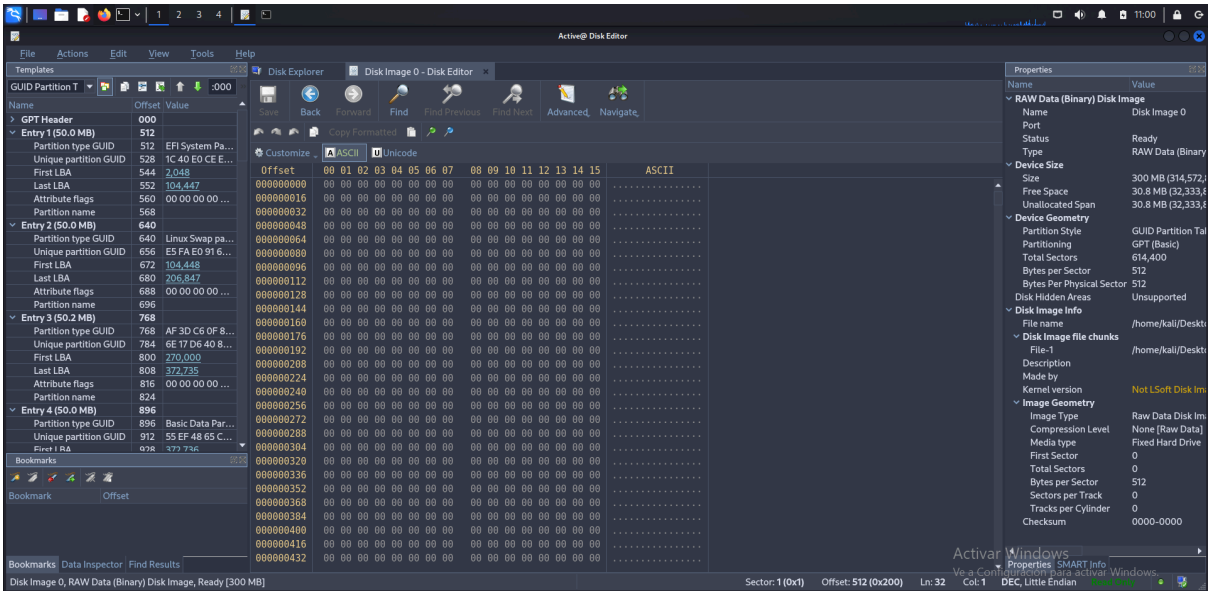
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop                     Downloads   fakeInstagram   Music     prueba.txt.save  requests   user.txt
DiskEditor_Linux_Installer.run  dvwa        getopt          os        Public           sys        Videos
Documents                   exploit.py  glpi-10.0.0.tgz Pictures  re               Templates  winehq.key

┌──(kali㉿kali)-[~]
└─$ ./DiskEditor_Linux_Installer.run
Verifying archive integrity...  100%   All good.
Uncompressing Active@ Disk Editor  100%
[sudo] password for kali:
```


Disk
Disks
Active@ Disk Editor
blkcat
ifind
tsk_loaddb
bulk_extractor
tsk_gettimes
blkcalc
fls
Active@ Disk Editor
prueba.txt.save
Public
re
requests
sys
Templates
user.txt
Videos
winehq.key
Activar Windows
Ve a Configuración para activar Windows.


Active@ Disk Editor
Active
Disk Editor
Version 24.0
Getting Started
Support
Version Info
Here are some commonly used actions when working with Active@ Disk Editor on a regular basis.
Open Disk
Open physical disk, Partition or Volume in Disk Editor.
Open File...
Open File in Disk Editor.
File Browser
Browse Local Computer and open Files or File Records in Disk Editor.
Open Disk Image...
Open Disk Image file as virtual disk.
Show this view on startup
Close
Activar Windows
Ve a Configuración para activar Windows.


Open Disk Image
Disk Image file name:
ıc/Active@ Disk Editor/disk_images/
...
Caption (Display name):
Use default (ge...
Name
Value
File name
/root/.local/share/LSoft Technolo...
Description
Auto-load mounted Disk Image when application starts
Open Disk Image: Enter valid disk image file name to continue;
Restore Defaults
Cancel
Open


Open Disk Image
Disk Image file name:
/home/kali/Desktop/disco1.dd
...
Caption (Display name):
Use default (ge...
Name
Value
Descri
File name
/home/kali/Desktop/disco1.dd
Disk Image file chunks
File-1
/home/kali/Desktop/disco1.dd
Auto-load mounted Disk Image when application starts
Restore Defaults
Cancel
Open


Active@ Disk Editor
File Actions Edit View Tools Help
Templates
Disk Explorer
Disk Image 0 - Disk Editor
Properties
Bookmarks
Data Inspector
Find Results
Disk Image 0, RAW Data (Binary) Disk Image, Ready [300 MB]

2. disco1.dd

- Tabla de particiones: GPT.
- Dirección de la cabecera GPT: 45 46 49 20 50 41 52 54.
- Tamaño de la cabecera: 92.
- Primer LBA usable: 2,048.
- Último LBA usable: 614,366.
- GUID del disco: D0 67 D7 5E 18 57 4D A4 88 B3 12 29 5A B5 5D 5E.
- Sector que contiene la tabla de particiones: 2.
- Partición 1:
    - Tipo de partición: EFI System Partition.
    - GUID: 1C 40 E0 CE ED 42 4B 19 92 90 EC 39 77 3D E9 42.
    - LBA donde empieza: 2,048.
    - LBA donde acaba: 104,447.
    - Nombre: .
- Partición 2:
    - Tipo de partición: Linux Swap partition.
    - GUID: E5 FA E0 91 62 C6 41 D1 8C 23 8C CF 50 32 B2 38.
    - LBA donde empieza: 104,448.
    - LBA donde acaba: 206,847.
    - Nombre: .
- Partición 3:
    - Tipo de partición: AF 3D C6 0F 83 84 72 47 8E 79 3D 69 D8 47 7D E4.
    - GUID: 6E 17 D6 40 85 30 43 15 98 52 1F C7 7E 01 57 B5.
    - LBA donde empieza: 270,000.
    - LBA donde acaba: 372,735.
    - Nombre: .

- Partición 4:
    - Tipo de partición: Basic Data Partition.
    - GUID: 55 EF 48 65 C1 CA 4D 08 A3 F0 AC 68 AF C2 4A 76.
    - LBA donde empieza: 372,736.
    - LBA donde acaba: 475,135.
    - Nombre: .
- Partición 5:
    - Tipo de partición: Basic Data Partition.
    - GUID: F6 1B F4 D0 F8 F1 43 8E 9E E6 4A 30 01 3A 3F 28.
    - LBA donde empieza: 475,136.
    - LBA donde acaba: 614,366.
    - Nombre: .

3. disco2.dd

- Tabla de particiones: MBR.
- Partición 1:
    - Número de partición: 1.
    - Indicador de arranque: 0x00.
    - Cilindro, Cabezal, Sector (CHS) del primer sector en la partición:
        - Cilindro: 0x00.
        - Cabezal: 32.
        - Sector: 0x21.
    - Tipo de partición: NTFS.
    - Cilindro, Cabezal, Sector (CHS) del último sector de la partición:
        - Cilindro: 0x02.
        - Cabezal: 172.
        - Sector: 0x2A.
    - Logical block address del primer sector de la partición: 2.048.
    - Longitud de la partición, en sectores: 40.960.

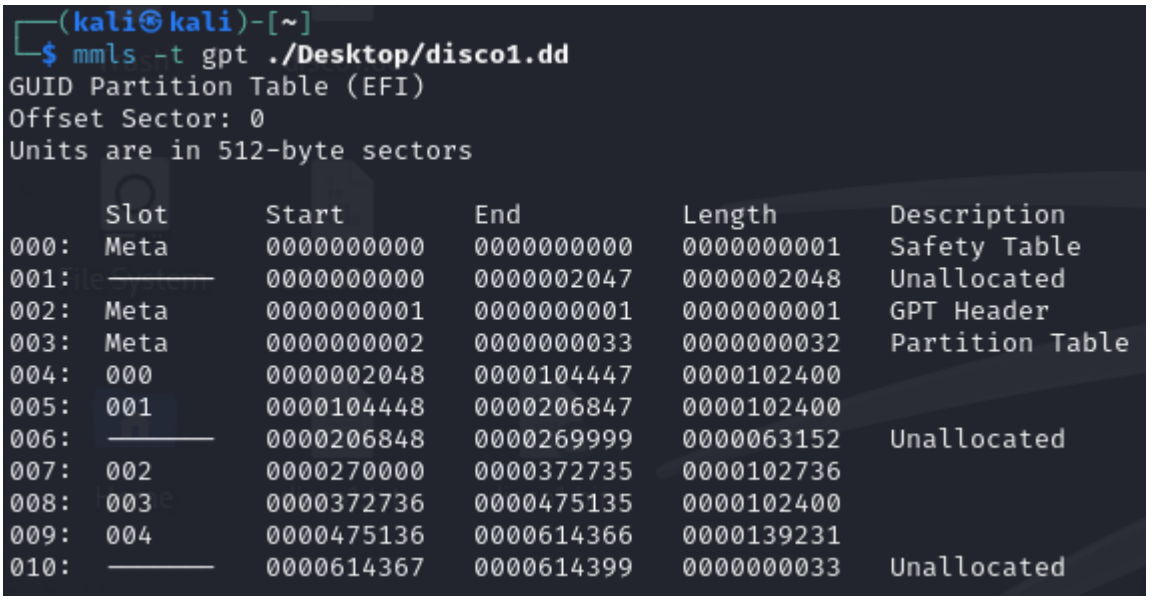
- Partición 2:
    - Número de partición: 2.
    - Indicador de arranque: 0x00.
    - Cilindro, Cabezal, Sector (CHS) del primer sector en la partición:
        - Cilindro: 0x02.
        - Cabezal: 172.
        - Sector: 0x2B.
    - Tipo de partición: Ext2.
    - Cilindro, Cabezal, Sector (CHS) del último sector de la partición:
        - Cilindro: 0x05.
        - Cabezal: 57.
        - Sector: 0x34.
    - Logical block address del primer sector de la partición: 43.008.
    - Longitud de la partición, en sectores: 40.960.
- Partición 3:
    - Número de partición: 3.
    - Indicador de arranque: 0x00.
    - Cilindro, Cabezal, Sector (CHS) del primer sector en la partición:
        - Cilindro: 0x05.
        - Cabezal: 57.
        - Sector: 0x35.
    - Tipo de partición: Extended.
    - Cilindro, Cabezal, Sector (CHS) del último sector de la partición:
        - Cilindro: 0x0C.
        - Cabezal: 190.
        - Sector: 0x32.
    - Logical block address del primer sector de la partición: 83.968.
    - Longitud de la partición, en sectores: 120.832.

- Partición 4:
    - Número de partición: 4.
    - Indicador de arranque: 0x00.
    - Cilindro, Cabezal, Sector (CHS) del primer sector en la partición:
        - Cilindro: 0x00.
        - Cabezal: 0.
        - Sector: 0x00.
    - Tipo de partición: Unused.
    - Cilindro, Cabezal, Sector (CHS) del último sector de la partición:
        - Cilindro: 0x00.
        - Cabezal: 0.
        - Sector: 0x00.
    - Logical block address del primer sector de la partición: 0.
    - Longitud de la partición, en sectores: 0.

Sleuthkit:

1. disco1.dd

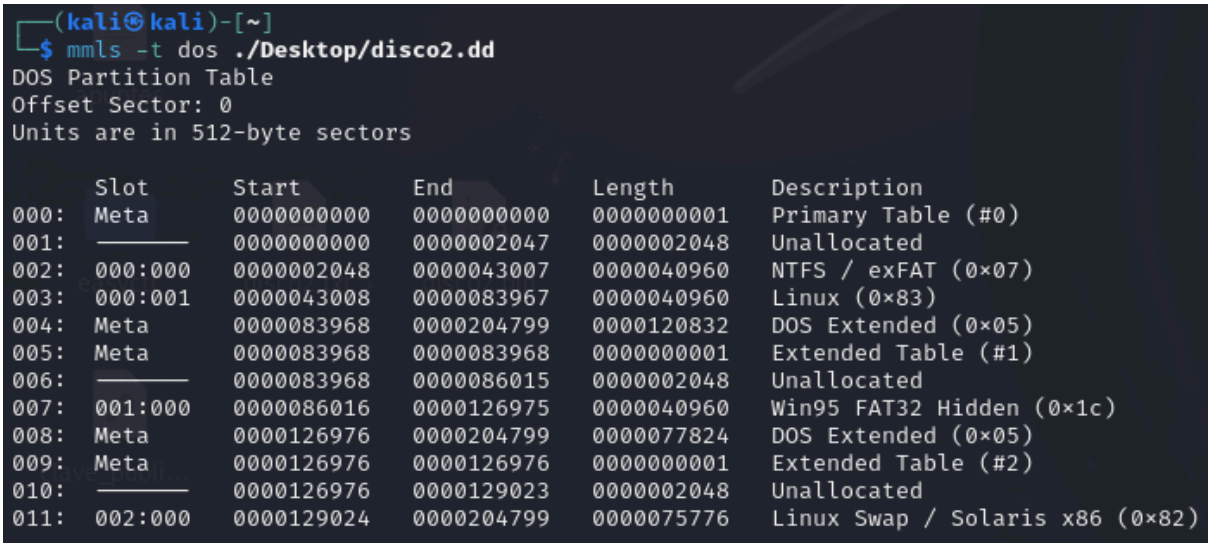
mmls -t gpt ./Desktop/disco1.dd



```
┌──(kali㉿kali)-[~]
└─$ mmls -t gpt ./Desktop/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
```

2. disco2.dd

mmls -t dos ./Desktop/disco2.dd



```
┌──(kali㉿kali)-[~]
└─$ mmls -t dos ./Desktop/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 (0×07)
003:  000:001   0000043008   0000083967   0000040960   Linux (0×83)
004:  Meta      0000083968   0000204799   0000120832   DOS Extended (0×05)
005:  Meta      0000083968   0000083968   0000000001   Extended Table (#1)
006:  ————————  0000083968   0000086015   0000002048   Unallocated
007:  001:000   0000086016   0000126975   0000040960   Win95 FAT32 Hidden (0×1c)
008:  Meta      0000126976   0000204799   0000077824   DOS Extended (0×05)
009:  Meta      0000126976   0000126976   0000000001   Extended Table (#2)
010:  ————————  0000126976   0000129023   0000002048   Unallocated
011:  002:000   0000129024   0000204799   0000075776   Linux Swap / Solaris x86 (0×82)
```

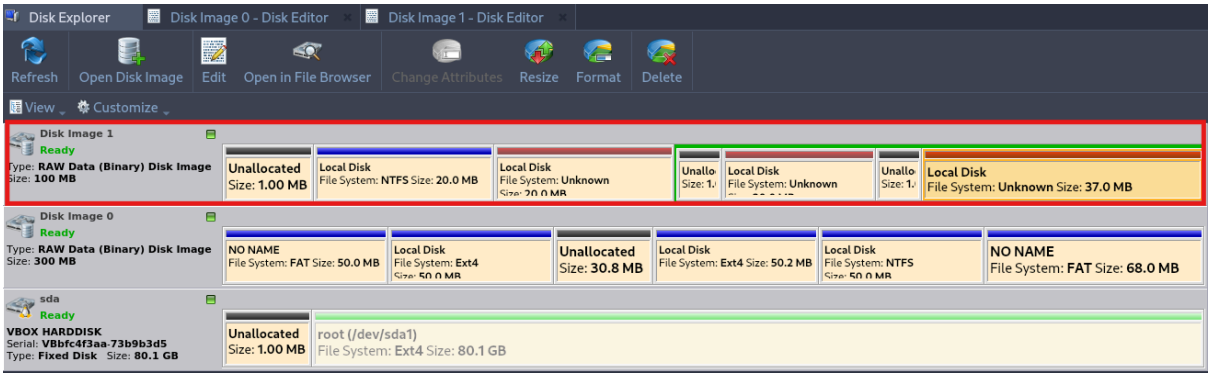
Peculiaridades encontradas:

Si nos fijamos en esta imagen:

```
┌──(kali㉿kali)-[~]
└─$ mmls -t dos ./Desktop/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)
```

Podemos observar qué hay elementos que no aparecen en Active Disk Editor. Tales como, una partición FAT32 oculta. De hecho, Active Disk Editor solo nos muestra tres particiones en el editor de disco.

Sin embargo, si nos vamos al Disk Explorer, observaremos que hay más de tres particiones:



Las dos primeras particiones mostradas tanto en la ventana de Disk Explorer, como en la de Disk Editor, coinciden con las dos primeras particiones de la tabla primaria mostradas con el comando mmls.

```
┌──(kali㉿kali)-[~]
└─$ mmls -t dos ./Desktop/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)
```

Cuyos IDs del sistema de archivos coinciden con los mostrados en el Disk Editor:

Partition 1 (NTFS, 20.0 MB)	446	
Active partition flag (80 = active)	446	0x00
Start head	447	32
Start sector (bits 0-5), cylinder (bit…	448	0x21
Start cylinder (lower 8 bits)	449	0x00
File system ID	450	0x07
End head	451	172
End sector (bits 0-5), cylinder (bits …	452	0x2A
End cylinder (lower 8 bits)	453	0x02
First sector	454	2,048
Total sectors	458	40,960

Partition 2 (Ext2, 20.0 MB)	462	
Active partition flag (80 = active)	462	0x00
Start head	463	172
Start sector (bits 0-5), cylinder (bit…	464	0x2B
Start cylinder (lower 8 bits)	465	0x02
File system ID	466	0x83
End head	467	57
End sector (bits 0-5), cylinder (bits …	468	0x34
End cylinder (lower 8 bits)	469	0x05
First sector	470	43,008
Total sectors	474	40,960

Además, si hacemos el cálculo con los sectores de la Tabla primaria:

Tabla primaria (#0): 81920 sectores

81920 × 512 / 1024^2 = 40MB

Que es la suma de las dos particiones de 20MB mostradas en Active Disk Editor.

Mientras que la tercera partición, es la suma del resto de particiones del disco:

Tabla extendida (#1): 40960 sectores

40960 × 512 / 1024^2 = 20MB

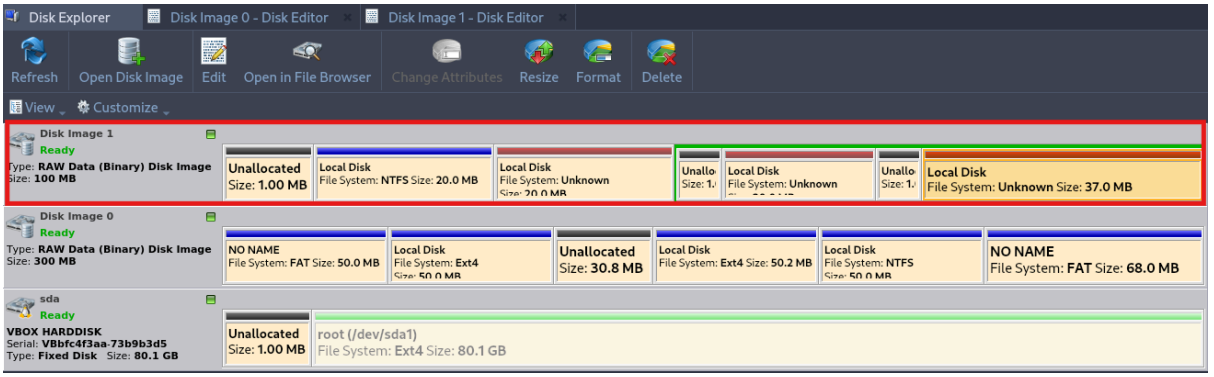
Tabla extendida (#2): 75776 sectores

75776 × 512 / 1024^2 = 37.02MB

Suma de las tablas: 20MB + 37.02MB = 57.02MB

57.02MB + 2MB (Son los dos sectores unallocated) = 59.02MB

De hecho, si volvemos a visualizar la imagen anterior:



Veremos que hay una línea verde que rodea las particiones mencionadas anteriormente, que conforman la tercera partición.

Y muestra el sistema de archivos Extended, ya que el sistema de archivos de la partición anterior tiene el atributo “Hidden”.