

Práctica 1

Pérez Martínez Josué Saúl

22 de Septiembre 2020

1. Particiones

1. Primero se verifica que el disco a modificar se encuentre en el sistema, además se visualiza el espacio con el que cuenta.

```
sansforensics@siftworkstation: ~  
$ sudo fdisk -l /dev/sdb  
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

2. Se crea la primera partición de tipo primaria, formato por default de linux, con un espacio de 512M.

```
sansforensics@siftworkstation: ~  
$ sudo fdisk /dev/sdb  
Welcome to fdisk (util-linux 2.31.1).  
Changes will remain in memory only, until you decide to write them.  
Be careful before using the write command.  
  
Device does not contain a recognized partition table.  
Created a new DOS disklabel with disk identifier 0x92d2e40b.  
  
Command (m for help): n  
Partition type  
  p   primary (0 primary, 0 extended, 4 free)  
  e   extended (container for logical partitions)  
Select (default p): p  
Partition number (1-4, default 1): 1  
First sector (2048-4194303, default 2048):  
Last sector, +sectors or +size[K,M,G,T,P] (2048-4194303, default 4194303): +512M  
Created a new partition 1 of type 'Linux' and of size 512 MiB.
```

3. Para la segunda partición, igual se indica que es de tipo primaria, con un espacio de 512M, como se crea por default de tipo linux, se cambia el formato a NTFS, indicando que es formato Windows.

```
Command (m for help): n  
Partition type  
  p   primary (1 primary, 0 extended, 3 free)  
  e   extended (container for logical partitions)  
Select (default p): p  
Partition number (2-4, default 2): 2  
First sector (1050624-4194303, default 1050624):  
Last sector, +sectors or +size[K,M,G,T,P] (1050624-4194303, default 4194303): +512M  
Created a new partition 2 of type 'Linux' and of size 512 MiB.
```

```

Command (m for help): t
Partition number (1,2, default 2): 2
Hex code (type L to list all codes): 86

Changed type of partition 'Linux' to 'NTFS volume set'.

```

4. Se realiza el mismo procedimiento para la tercera partición, ahora se elige un formato SWAP con un tamaño de 512M.

```

Command (m for help): n
Partition type
  p primary (2 primary, 0 extended, 2 free)
  e extended (container for logical partitions)
Select (default p): p
Partition number (3,4, default 3): 3
First sector (2099200-4194303, default 2099200):
Last sector, +sectors or +size{K,M,G,T,P} (2099200-4194303, default 4194303): +512M

Created a new partition 3 of type 'Linux' and of size 512 MiB.

Command (m for help): t
Partition number (1-3, default 3): 3
Hex code (type L to list all codes): 82

Changed type of partition 'Linux' to 'Linux swap / Solaris'.

```

5. Para el formato de datos, se elige el tipo extendido, con un tamaño de 500M.

```

Command (m for help): n
Partition type
  p primary (3 primary, 0 extended, 1 free)
  e extended (container for logical partitions)
Select (default e): e

Selected partition 4
First sector (3147776-4194303, default 3147776):
Last sector, +sectors or +size{K,M,G,T,P} (3147776-4194303, default 4194303): +500M

Created a new partition 4 of type 'Extended' and of size 500 MiB.

```

6. Para finalizar se sobrescribe la tabla de particiones, además se listan para poder verificar que efectivamente se crearon de manera correcta.

```

Command (m for help): p
Disk /dev/sdb: 2 GiB, 2147483648 bytes, 4194304 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x92d2e40b

Device Boot Start End Sectors Size Id Type
/dev/sdb1 2048 1050623 1048576 512M 83 Linux
/dev/sdb2 1050624 2099199 1048576 512M 86 NTFS volume set
/dev/sdb3 2099200 3147775 1048576 512M 82 Linux swap / Solaris
/dev/sdb4 3147776 4171775 1024000 500M 5 Extended

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

```

2. MBR

El análisis de MBR se usa el comando 'sudo dd if=/dev/sdb count=1 | hd', donde se observa las particiones creadas.

```

sansforensics@siftworkstation: ~
$ sudo dd if=/dev/sdb count=1 | hdmp
1+0 records in
1+0 records out
512 bytes copied, 0.000409412 s, 1.3 MB/s
00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
000001b0 00 00 00 00 00 00 00 00 0b e4 d2 92 00 00 00 20 |.....|
000001c0 21 00 83 65 24 41 00 08 00 00 00 00 10 00 00 65 |!..e$A.....e|
000001d0 25 41 86 aa 28 82 00 08 10 00 00 00 10 00 00 aa |%A..(.....|
000001e0 29 82 82 ef 2c c3 00 08 20 00 00 00 10 00 00 ef |).....|
000001f0 2d c3 05 ad 6a 03 00 08 30 00 00 a0 0f 00 55 aa |-...j...0....U.|
00000200

```

1. Para la partición linux, se observa desde la posición 0x1BE
 - byte 1 : Bandera arranque = 0x00 No activo
 - byte 2 : Número de cabezal inicial = 0x20
 - byte 3 : Número de sector inicial de boot = 0x21
 - byte 4 : Número de cilindro en el sector de boot = 0x00
 - byte 5 : Tipo de partición = 0x83 Linux
 - byte 6 : Número de cabeza final = 0x65
 - byte 7 : Número de sector final = 0x24
 - byte 8 : Número de cilindro final = 0x41
 - byte 9-12: Distancia al sector inicial = 0x00080000
 - byte 13-16: Número de sectores en la partición = 0x00001000
2. La partición Windows inicia desde 0x1CE.
 - byte 1 : Bandera arranque = 0x00 No activo
 - byte 2 : Número de cabezal inicial = 0x65
 - byte 3 : Número de sector inicial de boot = 0x25
 - byte 4 : Número de cilindro en el sector de boot = 0x41
 - byte 5 : Tipo de partición = 0x86 Linux
 - byte 6 : Número de cabeza final = 0xaa
 - byte 7 : Número de sector final = 0x28
 - byte 8 : Número de cilindro final = 0x82
 - byte 9-12: Distancia al sector inicial = 0x00081000
 - byte 13-16: Número de sectores en la partición = 0x00001000
3. Para SWAP inicia desde 0x1DE.
 - byte 1 : Bandera arranque = 0x00 No activo
 - byte 2 : Número de cabezal inicial = 0xaa
 - byte 3 : Número de sector inicial de boot = 0x29
 - byte 4 : Número de cilindro en el sector de boot = 0x82
 - byte 5 : Tipo de partición = 0x82 Linux
 - byte 6 : Número de cabeza final = 0xef
 - byte 7 : Número de sector final = 0x2c
 - byte 8 : Número de cilindro final = 0xc3
 - byte 9-12: Distancia al sector inicial = 0x00082000
 - byte 13-16: Número de sectores en la partición = 0x00001000
4. La partición de datos se encuentra desde 0x1EE

- byte 1 : Bandera arranque = 0x00 No activo
- byte 2 : Número de cabezal inicial = 0xef
- byte 3 : Número de sector inicial de boot = 0x2d
- byte 4 : Número de cilindro en el sector de boot = 0xc3
- byte 5 : Tipo de partición = 0x05 Linux
- byte 6 : Número de cabeza final = 0xad
- byte 7 : Número de sector final = 0x6a
- byte 8 : Número de cilindro final = 0x03
- byte 9-12: Distancia al sector inicial = 0x00083000
- byte 13-16: Número de sectores en la partición = 0x00a00f00