U.N.A.M. – C.E.R.T.

Forense

Alumno: Luis Fernando Resendiz Cruz

Creacion de la particion 1 Linux.

```
lresendiz@luis-resendiz:~$ 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 0x5aafea79.

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 (2048-2097151, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-2097151, default 2097151): +50M

Created a new partition 1 of type 'Linux' and of size 50 MiB.
```

Creación de la partición 2 SWAP.

```
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):
First sector (104448-2097151, default 104448):
Last sector, +sectors or +size{K,M,G,T,P} (104448-2097151, default 2097151): +50M

Created a new partition 2 of type 'Linux' and of size 50 MiB.

Command (m for help): t
Partition number (1,2, default 2): 2
Hex code (type L to list all codes): 82

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

Creacion de la partición 3 Windows.

```
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 (206848-2097151, default 206848):
Last sector, +sectors or +size{K,M,G,T,P} (206848-2097151, default 2097151): +50M

Created a new partition 3 of type 'Linux' and of size 50 MiB.

Command (m for help): t
Partition number (1-3, default 3):
Hex code (type L to list all codes): 7

Changed type of partition 'Linux' to 'HPFS/NTFS/exFAT'.
```

Creación de la partición 4 Datos (Extended)

```
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 (309248-2097151, default 309248):
Last sector, +sectors or +size{K,M,G,T,P} (309248-2097151, default 2097151): +50M

Created a new partition 4 of type 'Extended' and of size 50 MiB.
```

Verificación de las particiones que contiene el volumen de almacenamiento.

```
Command (m for help): p
Disk /dev/sdb: 1 GiB, 1073741824 bytes, 2097152 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: 0x5aafea79

Device     Boot  Start    End Sectors Size Id Type
/dev/sdb1         2048 104447  102400  50M 83 Linux
/dev/sdb2       104448 206847  102400  50M 82 Linux swap / Solaris
/dev/sdb3       206848 309247  102400  50M  7 HPFS/NTFS/exFAT
/dev/sdb4       309248 411647  102400  50M  5 Extended
```

Vizualisacion de el MBR.

```
lresendiz@luis-resendiz:~$ sudo dd if=/dev/sdb count=1 | hd
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  4a 7f fb 86 00 00 00 20  |........J...... |
000001c0  21 00 83 7f 39 06 00 08  00 00 00 90 01 00 00 7f  |!...9...........|
000001d0  3a 06 82 df 13 0c 00 98  01 00 00 90 01 00 00 df  |:...............|
000001e0  14 0c 07 3f 2c 13 00 28  03 00 00 90 01 00 00 3f  |...?,..(.......?|
000001f0  2d 13 05 9f 06 19 00 b8  04 00 00 90 01 00 55 aa  |-.............U.|
1+0 records in
1+0 records out
512 bytes copied, 0.019558 s, 26.2 kB/s
00000200
```

Para un análisis mas sencillo se decidió mover la salida a un archivo y limpiar lo que no se necesita en estos momentos. Se aislaron los 64 bytes que preceden al identificador del MBR, cada 16 bytes representan una partición.

```
00 20 21 00 83 7f 39 06 00 08 00 00 00 90 01 00
00 7f 3a 06 82 df 13 0c 00 98 01 00 00 90 01 00
00 df 14 0c 07 3f 2c 13 00 28 03 00 00 90 01 00
00 3f 2d 13 05 9f 06 19 00 b8 04 00 00 90 01 00

55 aa
```

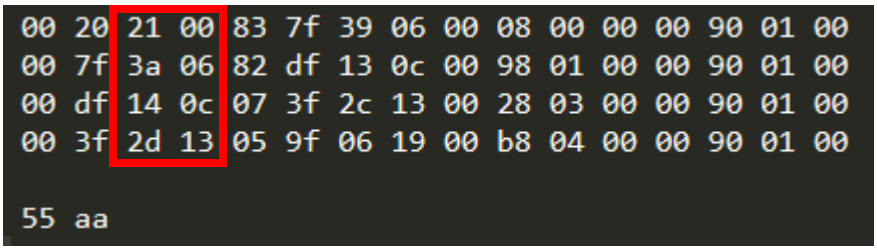
Partición de arranque: Ninguno debido a que todos están en 0.

```
00 20 21 00 83 7f 39 06 00 08 00 00 00 90 01 00
00 7f 3a 06 82 df 13 0c 00 98 01 00 00 90 01 00
00 df 14 0c 07 3f 2c 13 00 28 03 00 00 90 01 00
00 3f 2d 13 05 9f 06 19 00 b8 04 00 00 90 01 00

55 aa
```

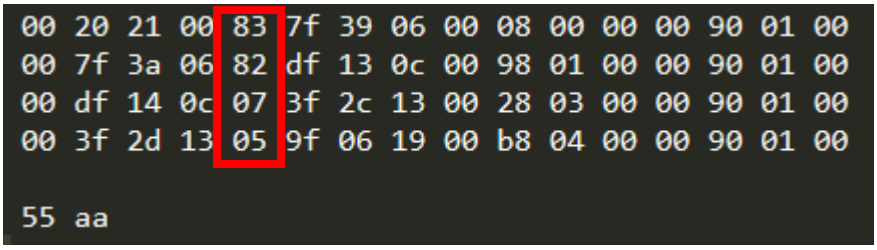
Cabezal donde inicia la partición:

Partición 1: 20
Partición 2: 7f
Partición 3: df
Partición 4: 3f



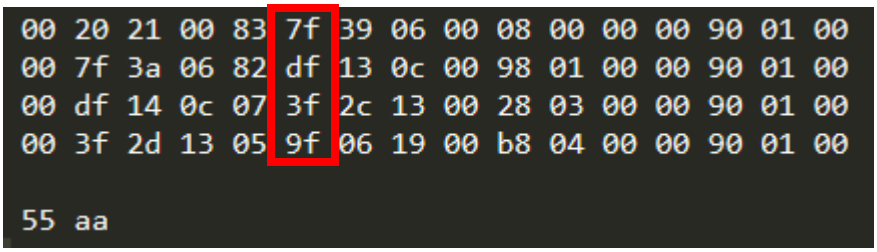
Sector y cilindró donde inicia la partición:

Partición 1: 21 00
Partición 2: 3a 06
Partición 3: 14 0c
Partición 4: 2d 13



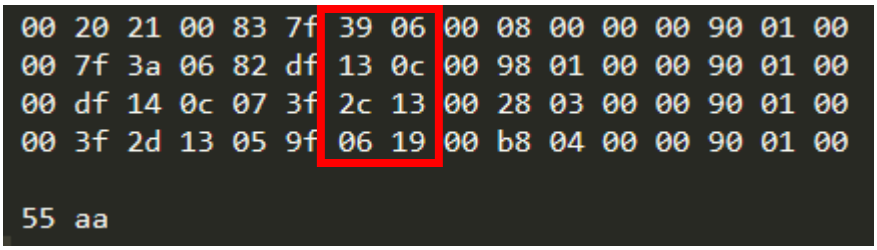
Tipo de partición:

Partición 1: 83 (Linux)
Partición 2: 82 (Linux SWAP / Solaris)
Partición 3: 07 (HPFS / NTFS)
Partición 4: 05 (Extended - Datos)



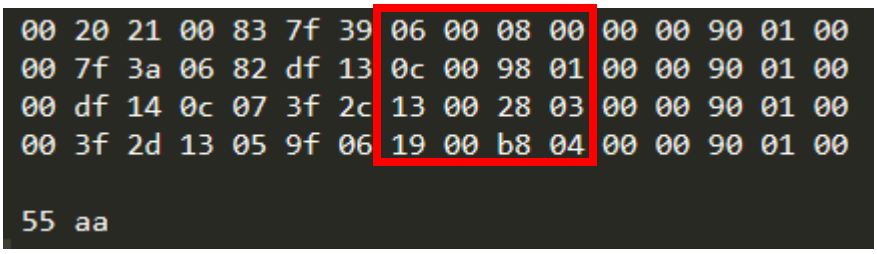
Cabezal donde finaliza la partición:

Partición 1: 7f
Partición 2: df
Partición 3: 3f
Partición 4: 9f



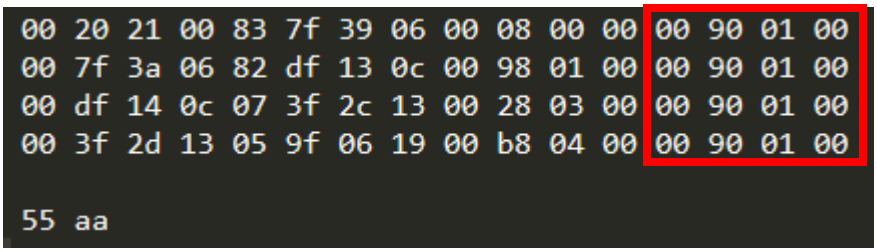
Sector y cilindró donde inicia la partición:

Partición 1: 39 06
Partición 2: 13 0c
Partición 3: 2c 13
Partición 4: 06 19



Distancia en sectores, desde la tabla de particiones al sector de la partición:

Partición 1: 06 00 08 00
Partición 2: 0c 00 98 01
Partición 3: 13 00 28 03
Partición 4: 19 00 b8 04



Tamaño de partición:

Numero en hexadecimal →	Numero de sectores →	Tamaño en Bytes →	Tamaño en Megas
Partición 1: 00 01 90 00	→ 102,400	→ 52,428,800	→ 52.4288 MB
Partición 2: 00 01 90 00	→ 102,400	→ 52,428,800	→ 52.4288 MB
Partición 3: 00 01 90 00	→ 102,400	→ 52,428,800	→ 52.4288 MB
Partición 4: 00 01 90 00	→ 102,400	→ 52,428,800	→ 52.4288 MB