

Plan de Becas en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT Análisis Forense

## **Programa particiones**

Para la realización de está práctica se tuvo que montar otro disco duro externo, el programa se desarrolló en Python, la ejecución del programa se muestra en la figura 1, donde se crean 3 particiones primarias.

```
cio-leal -> /h/s/D/p/practica2
# python practica2.py /dev/sdc
p primaria
e extendida
s salir
Seleccione una opcion (default p): p
Sistemas de archivos:
82 Linux swap
83 Linux
06 FAT16
07 HPFS/NTFS
Numero de particion (1-4): 1
Unidad de medida M (MegaBytes), G (GigaBytes): 200M
Guardar (w), salir (q), regresar (Enter): w
Particion 1 sistema de archivos FAT16
p primaria
e extendida
s salir
Seleccione una opcion (default p): p
Sistemas de archivos:
82 Linux swap
83 Linux
06 FAT16
07 HPFS/NTFS
Selecciona el sistema de archivos a utilizar (Valor): 82
Numero de particion (1-4): 2
Unidad de medida M (MegaBytes), G (GigaBytes): 150M
Guardar (w), salir (q), regresar (Enter): w
Particion 2 sistema de archivos Linux swap
p primaria
e extendida
s salir
Seleccione una opcion (default p): p
Sistemas de archivos:
82 Linux swap
83 Linux
06 FAT16
07 HPFS/NTFS
Selecciona el sistema de archivos a utilizar (Valor): 83
Numero de particion (1-4): 3
Unidad de medida M (MegaBytes), G (GigaBytes): 250M
Guardar (w), salir (q), regresar (Enter): w
Particion 3 sistema de archivos Linux
p primaria
e extendida
s salir
Seleccione una opcion (default p):
```

Figura 1. Ejecución del programa desarrollado.



Plan de Becas en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT Análisis Forense

Utilizando *fdisk*, verificamos que se crearon de manera correcta las particiones, como se muestra en la figura 2.

```
-> /h/s/D/p/practica2
  fdisk -l /dev/sdc
Disk /dev/sdc: 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: 0x00000000
            Boot Start
                              End Sectors Size Id Type
Device
/dev/sdc1
                    2048
                          411647
                                    409600
                                             200M 6 FAT16
                                             150M 82 Linux swap / Solaris
                  309248 616447
dev/sdc2
                                    307200
                                    512000
                                             250M 83 Linux
```

Figura 2. Tabla de particiones.

## **Conclusiones**

Para realizar el programa, fue de mucha utilidad el haber realizado la práctica 1 ya que me permitió conocer como se compone la tabla MBR, lo cuál fue de mucha utilidad para saber como ir guardando los valores hexadecimales en la tabla MBR del dispositivo que le pasamos como parámetro, cabe recordar que se utiliza el formato Little endian, lo cuál al no utilizarlo tendremos errores a la hora de tratar de guardar los datos en la tabla MBR, donde se tuvo mayores problemas fue en la hora de especificar el inicio del sector de las particiones.

## Referencias

https://docs.python.org/2/library/binascii.html