Worcester Polytechnic Institute
Department of Computer Science

Module 1: Partition Table

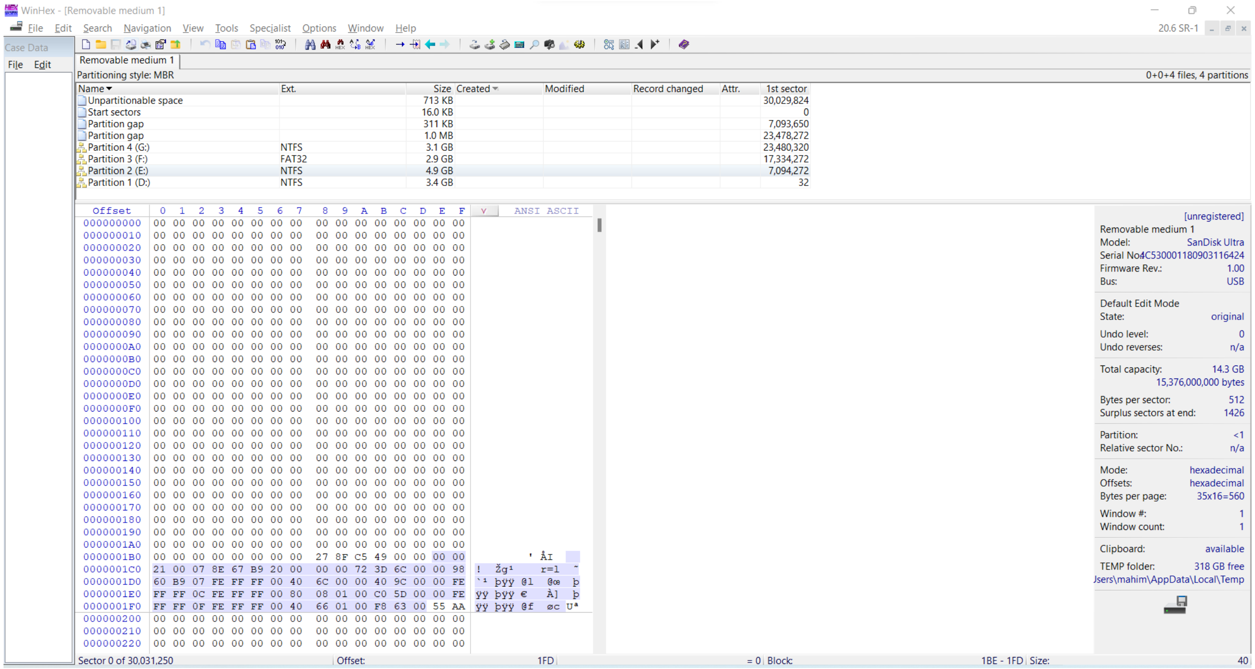
Objectives

- Use WinHex to examine the partition table in the Master Boot Record
- Locate partition table in the Master Boot Record
- Find information about all partitions on the disk, including hidden partitions

Tasks

Task 1: Locate partition table in the Master Boot Record

1. Open WinHex, click “Tools”, “Open Disk” from the menu. In the “Select Disk” menu, select the drive which you want to examine and click “OK”.
2. The partition table is in the **Master Boot Record (MBR)** Located at sector 0 of the disk drive. In the hexadecimal editor, the first partition is at offset 0x1BE. The partition table is 64 bytes in length (four 16 bytes entries). Disks can have no more than four Primary partitions, up to three Primary partitions plus one Extended partition



Partitioning style: MBR

0+0+4 files, 4 partitions

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Unpartitionable space		713 KB					30,029,824
Start sectors		16.0 KB					0
Partition gap		311 KB					7,093,650
Partition gap		1.0 MB					23,478,272
Partition 4 (G:)	NTFS	3.1 GB					23,480,320
Partition 3 (F:)	FAT32	2.9 GB					17,334,272
Partition 2 (E:)	NTFS	4.9 GB					7,094,272
Partition 1 (D:)	NTFS	3.4 GB					32

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0  00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00           ' ÅI
0000001C0  21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98   !  Žg¹    r=l  ˜
0000001D0  60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE   `¹ þÿÿ @l  @œ  þ
0000001E0  FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE   ÿÿ þÿÿ €   À]  þ
0000001F0  FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA   ÿÿ þÿÿ @f  øc U ª
000000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

[unregistered]
Removable medium 1
Model: SanDisk Ultra
Serial No.: 4C530001180903116424
Firmware Rev.: 1.00
Bus: USB

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Total capacity: 14.3 GB
15,376,000,000 bytes

Bytes per sector: 512
Surplus sectors at end: 1426

Partition: <1
Relative sector No.: n/a

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 35x16=560

Window #: 1
Window count: 1

Clipboard: available

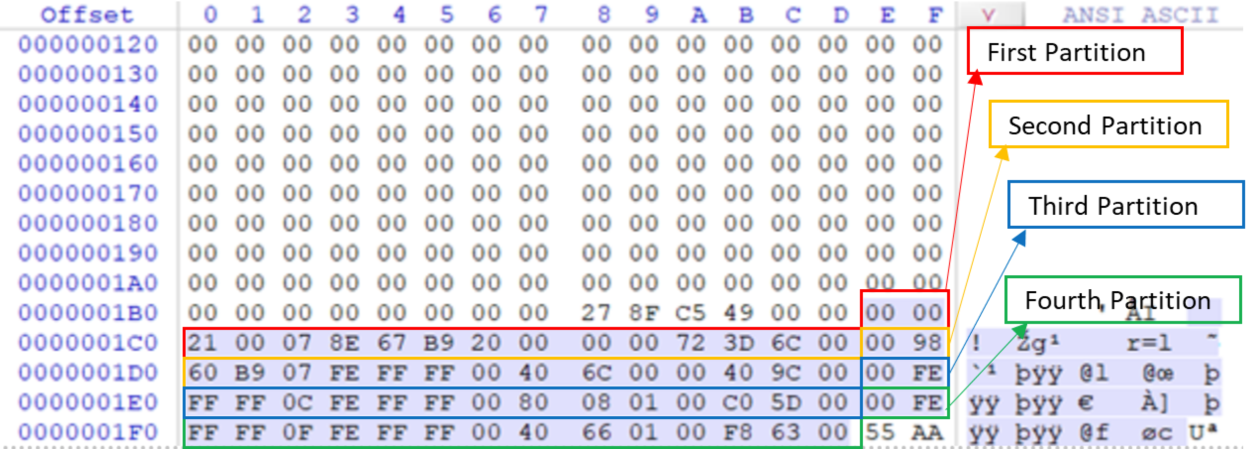
TEMP folder: 318 GB free
Jsers\mahim\AppData\Local\Temp

Sector 0 of 30,031,250 | Offset: 1FD | = 0 | Block: 1BE - 1FD | Size: 40

Task 2: Examine the information available on each partition in the Master Boot Record

3. Partitions on Master Boot Record:
   a) **First partition**: Click on the record 0x1BE and then drag down till the offset reaches 0x1CD on the Master Boot Record.
   b) **Second partition:** Click on the record 0x1CE and then drag down till the offset reaches 0x1DD on the Master Boot Record.
   c) **Third partition:** Click on the record 0x1DE and then drag down till the offset reaches 0x1ED on the Master Boot Record.

d) **Fourth partition:** Click on the record 0x1EE and then drag down till the offset reaches 0x1FD on the Master Boot Record.

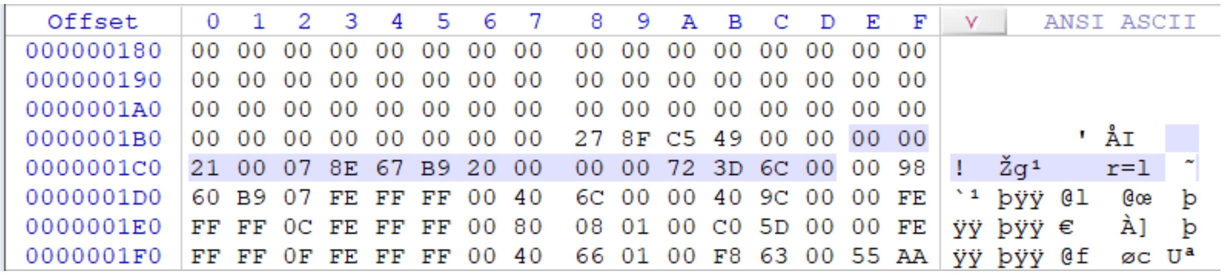


```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
000000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0  00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00          ' ÅI
0000001C0  21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98   !  Žg¹     r=l  ˜
0000001D0  60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE   `¹ þÿÿ @l  @œ  þ
0000001E0  FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE   ÿÿ þÿÿ €   À]  þ
0000001F0  FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA   ÿÿ þÿÿ @f  øc Uª
```

4. Let's analyze the information in a partition, such as Boot Indicator, File System, Starting sector and Partition size.
   - **Boot Indicator:** Located at 1st offset of each partition. If the byte value is 00, then the partition is non-bootable. If the byte value is 80, then the partition is bootable.
   - **File System type:** Its single byte. It indicates the type of partition. Compare the value from common partition value references https://en.wikipedia.org/wiki/Partition_type , and the Hexadecimal codes for file types at the end of this report. (For a hexadecimal code that is not included in the mentioned references, simply google it)
   - **Starting Sector:** Its value is of 4 bytes. It is stored on disk in Little endian, so the byte order must be reversed. For example: If the byte value is 0x3F000000, the reverse value is 0x3F (i.e., 0x0000003F, starting 0's can be ignored)
   - **Partition Size:** Its value is of 4 Bytes. It represents the size of each partition and is stored on disk in Little-endian, so the byte order must be reversed. For example: If the byte order is 0x00019941, the reverse order is 0x41990100

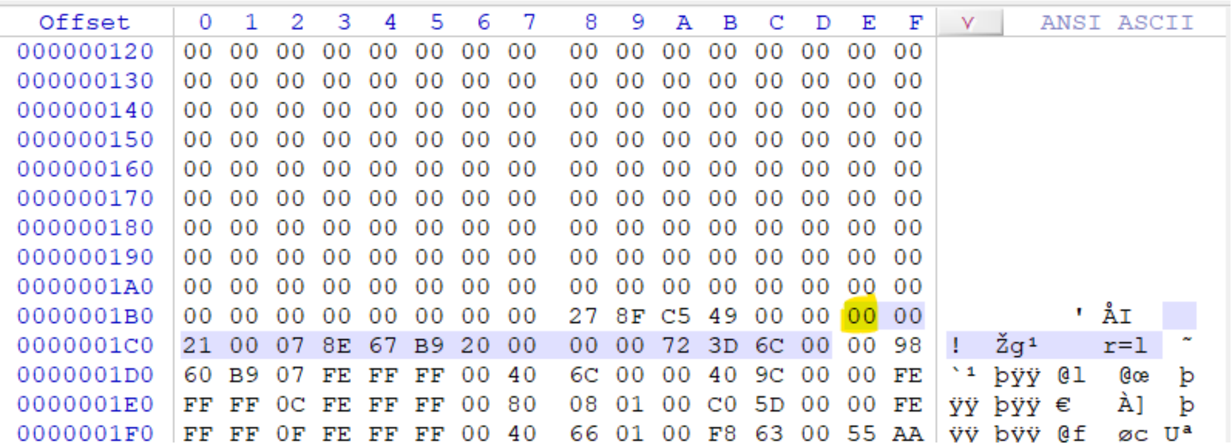
Task 3: Fetch disk information from Partition

5. Click on the record 0x1BE and then drag down till the offset reaches 0x1CD. This is the first partition on the Master Boot Record.



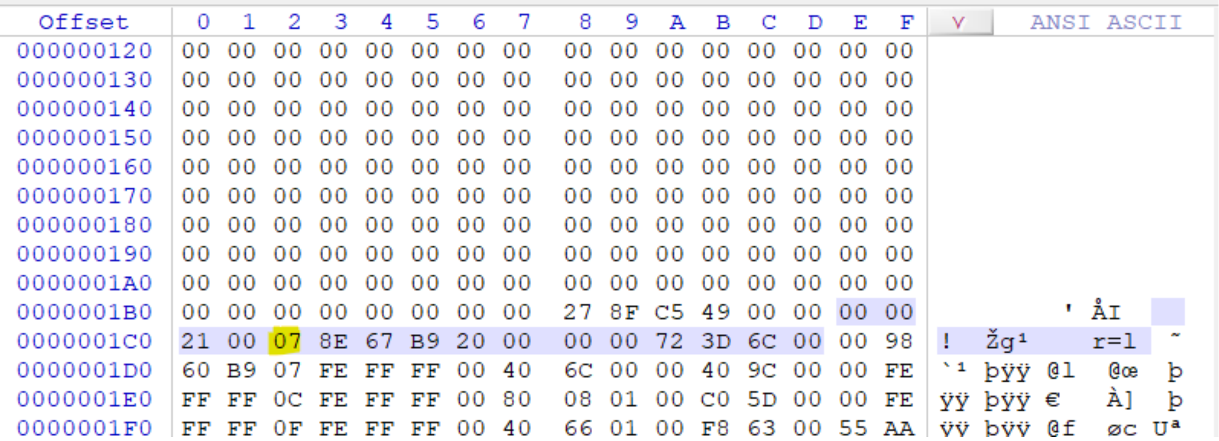
```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
000000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0  00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00          ' ÅI
0000001C0  21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98   !  Žg¹     r=l  ˜
0000001D0  60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE   `¹ þÿÿ @l  @œ  þ
0000001E0  FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE   ÿÿ þÿÿ €   À]  þ
0000001F0  FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA   ÿÿ þÿÿ @f  øc Uª
```

6. The Boot Indicator at offset 0x1BE (i.e., the first offset position of the partition) is 0x00. This indicates that the partition is non-bootable.



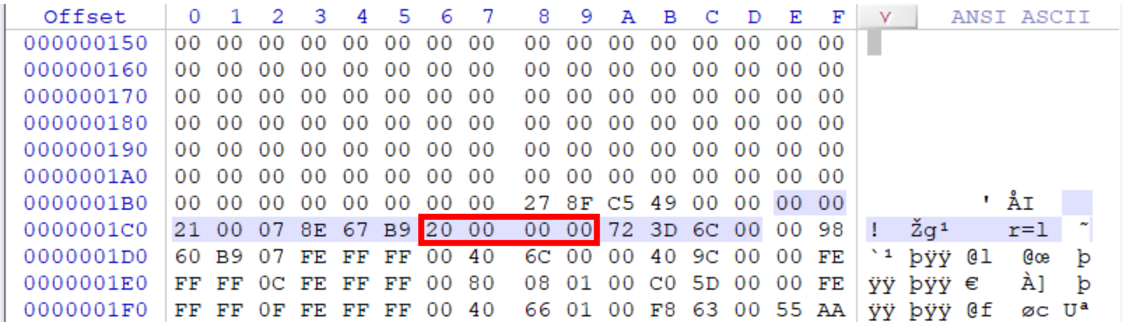
```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000120 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000130 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000140 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000150 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000160 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000170 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000180 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0 00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00           ' ÅI
0000001C0 21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98   !  Žg¹     r=l   ˜
0000001D0 60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE   `¹ þÿÿ @l   @œ  þ
0000001E0 FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE   ÿÿ þÿÿ €    À]  þ
0000001F0 FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA   ÿÿ þÿÿ @f   øc Uª
```

7. Compare the hexadecimal code at offset 0x1C2 with the File system types (Please refer to this link for different file types https://en.wikipedia.org/wiki/Partition_type and the Hexadecimal table of codes at the end of this report). Partition 1 is of type NSFT, the hexadecimal code at offset 0x1C2 is 0x07



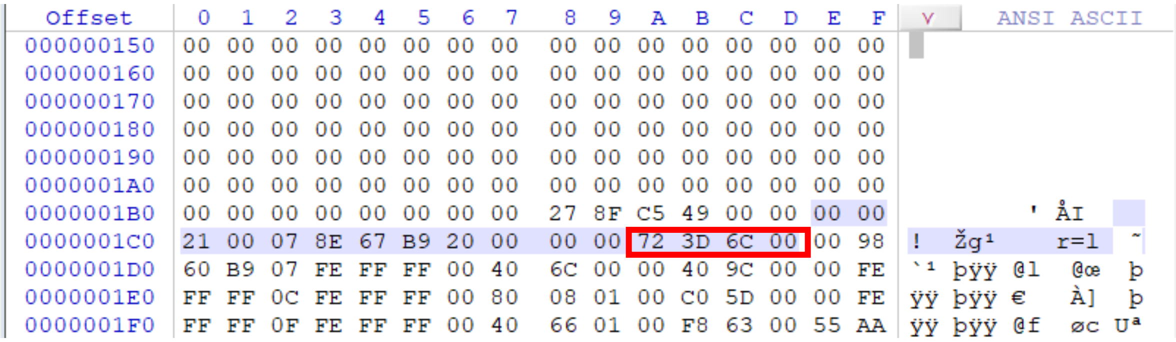
```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000120 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000130 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000140 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000150 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000160 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000170 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000180 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0 00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00           ' ÅI
0000001C0 21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98   !  Žg¹     r=l   ˜
0000001D0 60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE   `¹ þÿÿ @l   @œ  þ
0000001E0 FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE   ÿÿ þÿÿ €    À]  þ
0000001F0 FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA   ÿÿ þÿÿ @f   øc Uª
```

8. Click on offset 0x1C6 and drag to the right till the offset reaches 0x1C9. 0x20000000 is the hexadecimal code to find the starting sector of the partition.
    - First, the byte order must be reversed which is 0x00000020 hexadecimal code (**Please note**: Here you need to reverse the hex code in byte format not in decimal formal. For example: if the original hex code is 40 FF 00 00, the reversed hex code will be 00 00 FF 40 and not 00 00 FF 04).
    - Second, convert the reversed hexadecimal code into decimal, so when 0x00000020 hex code is converted to decimal we get 32. This means that our first partition begins at absolute sector 32.



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0  00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00          ' ÅI
0000001C0  21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98  !  Žg¹    r=l  ˜
0000001D0  60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE  `¹ þÿÿ @l  @œ  þ
0000001E0  FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE  ÿÿ þÿÿ €   À]  þ
0000001F0  FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA  ÿÿ þÿÿ @f  øc Uª
```

9. Click on offset 0x1CA and drag to the right till the offset reaches 0x1CD. 0x723D6C00 is the hexadecimal code to find the size (total sectors) of the partition. Start Notepad, and in a new document, press Ctrl+V to paste the hex code. Leave this window open for all the calculations you will be doing in this activity.
   - First, the byte order must be reversed which is 0x006C3D72 hexadecimal code (**Please note**: Here you need to reverse the hex code in byte format not in decimal formal. For example: if the original hex code is 40 FF 00 00, the reversed hex code will be 00 00 FF 40 and not 00 00 FF 04).
   - Second, convert the reversed hexadecimal code into decimal, so when 0x006C3D72 hex code is converted to decimal we get 7093618 sectors.
   - Third, convert total sectors to bytes, to do so, multiply total number of sectors with 512 bytes/sector. So, 7093618 * 512 => 3.63 bytes => 3.63 GB. This means that our first partition is of size 3.63 GB.

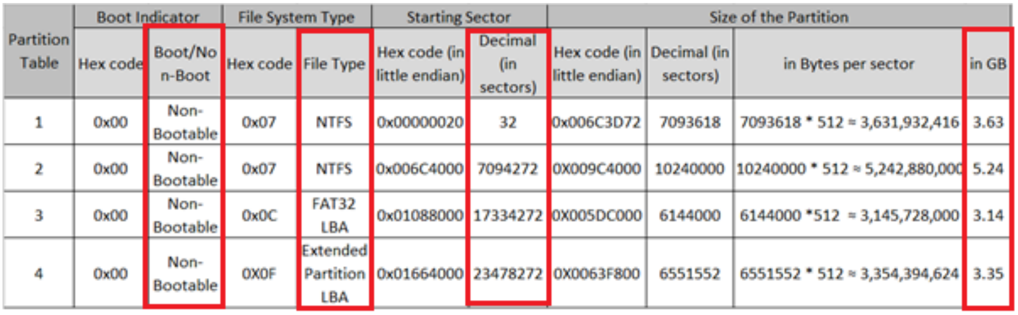


```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001B0  00 00 00 00 00 00 00 00  27 8F C5 49 00 00 00 00          ' ÅI
0000001C0  21 00 07 8E 67 B9 20 00  00 00 72 3D 6C 00 00 98  !  Žg¹    r=l  ˜
0000001D0  60 B9 07 FE FF FF 00 40  6C 00 00 40 9C 00 00 FE  `¹ þÿÿ @l  @œ  þ
0000001E0  FF FF 0C FE FF FF 00 80  08 01 00 C0 5D 00 00 FE  ÿÿ þÿÿ €   À]  þ
0000001F0  FF FF 0F FE FF FF 00 40  66 01 00 F8 63 00 55 AA  ÿÿ þÿÿ @f  øc Uª
```

10. To summarize, from the first partition table in master boot record we found below information:
    Boot Indicator: Non- bootable
    File system type: NTSF
    Starting Sector: 32
    Size of the partition: 3.63 GB
11. Repeat Step 6-10 for the partitions 2,3, and 4 to fetch the disk information w.r.t their offset positions mentioned below:

Partition	Information	Offset position
Partition 1: Click on the offset 0x1BE and then drag down till the offset reaches 0x1CD. This is the first partition on the Master Boot Record	Boot Indicator	0x1BE
	File system type	0x1C2
	Starting Sector	0x1C6 to 0x1C9
	Size of the partition	0x1CA to 0x1CD
Partition 2: Click on the offset 0x1CE and then drag down till the offset reaches 0x1DD. This is the second partition on the Master Boot Record	Boot Indicator	0x1CE
	File system type	0x1D2
	Starting Sector	0x1D6 to 0x1D9
	Size of the partition	0x1DA to 0x1DD
Partition 3: Click on the offset 0x1DE and then drag down till the offset reaches 0x1ED. This is the third partition on the Master Boot Record	Boot Indicator	0x1DE
	File system type	0x1E2
	Starting Sector	0x1E6 to 0x1E9
	Size of the partition	0x1EA to 0x1ED
Partition 4: Click on the offset 0x1EE and then drag down till the offset reaches 0x1FD. This is the fourth partition on the Master Boot Record	Boot Indicator	0x1EE
	File system type	0x1F2
	Starting Sector	0x1F6 to 0x1F9
	Size of the partition	0x1FA to 0x1FD

12. To summarize, below is the example calculation for four partitions on the Master Boot Record after completing steps 6-10 for each given partition:



Partition Table	Boot Indicator		File System Type		Starting Sector		Size of the Partition			
	Hex code	Boot/Non-Boot	Hex code	File Type	Hex code (in little endian)	Decimal (in sectors)	Hex code (in little endian)	Decimal (in sectors)	in Bytes per sector	in GB
1	0x00	Non-Bootable	0x07	NTFS	0x00000020	32	0x006C3D72	7093618	7093618 * 512 = 3,631,932,416	3.63
2	0x00	Non-Bootable	0x07	NTFS	0x006C4000	7094272	0X009C4000	10240000	10240000 * 512 ≈ 5,242,880,000	5.24
3	0x00	Non-Bootable	0x0C	FAT32 LBA	0x01088000	17334272	0X005DC000	6144000	6144000 *512 = 3,145,728,000	3.14
4	0x00	Non-Bootable	0X0F	Extended Partition LBA	0x01664000	23478272	0X0063F800	6551552	6551552 * 512 ≈ 3,354,394,624	3.35

References: Different types of File system

Hexadecimal Code	File System
01	DOS 12-bit FAT (floppy disks)
04	DOS 16-bit FAT for partitions smaller than 32MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32MB
07	NTFS and exFAT
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
0F	Extended partition with Logical Block Address (LBA)
17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT 32 partition
1E	Hidden VFAT partition

Questions:

1. What is the size of an offset (in bytes) in the master boot record?
2. What is the size (in bytes) of each partition in the master boot record?
3. What is the offset position to find boot indicator information in the first partition?
4. How to convert total sectors to bytes?
5. What is the offset position to find the starting sector in the second partition?