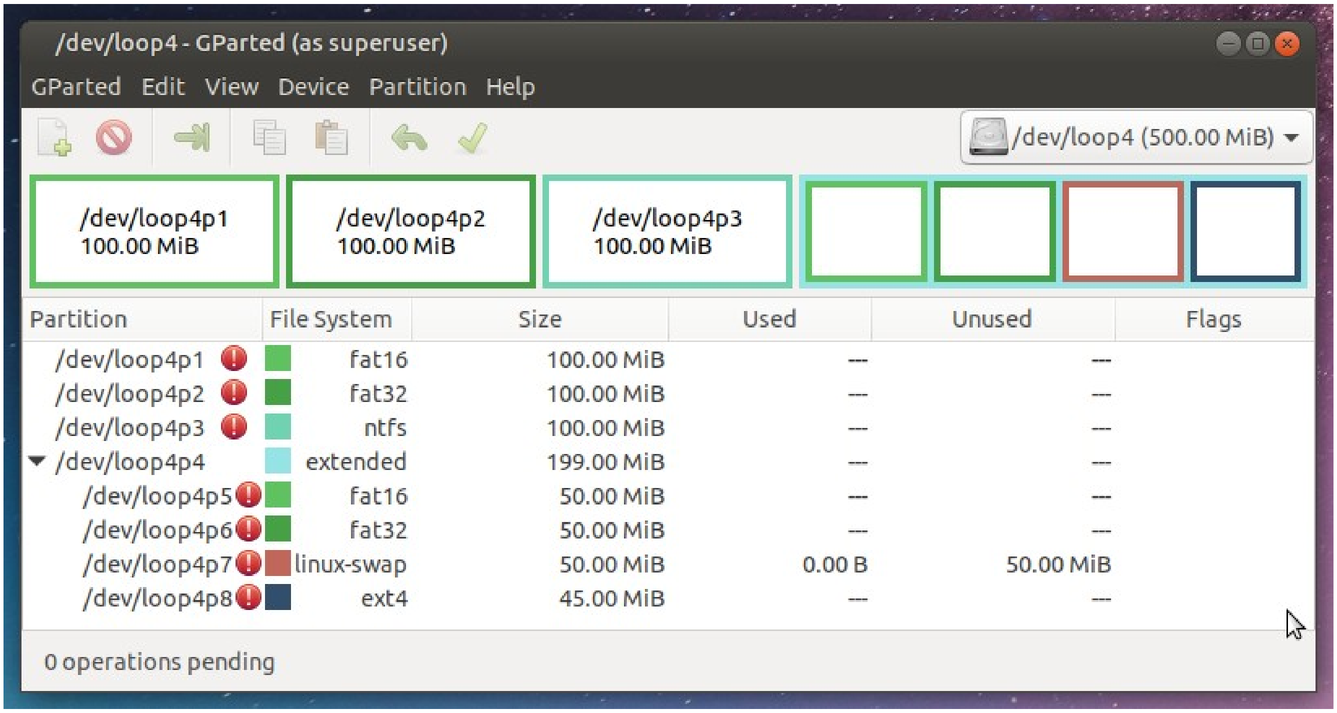
Analyzing EBR partitions manually

Use image1 for manual analysis

DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

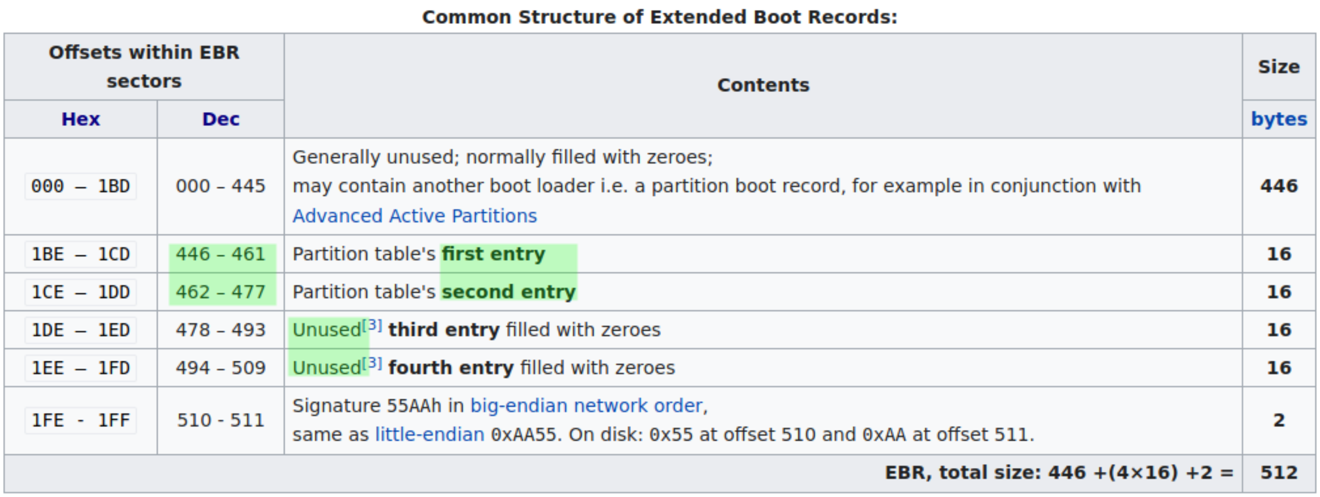


Partition	File System	Size	Used	Unused	Flags
/dev/loop4p1	fat16	100.00 MiB	---	---	
/dev/loop4p2	fat32	100.00 MiB	---	---	
/dev/loop4p3	ntfs	100.00 MiB	---	---	
/dev/loop4p4	extended	199.00 MiB	---	---	
/dev/loop4p5	fat16	50.00 MiB	---	---	
/dev/loop4p6	fat32	50.00 MiB	---	---	
/dev/loop4p7	linux-swap	50.00 MiB	0.00 B	50.00 MiB	
/dev/loop4p8	ext4	45.00 MiB	---	---	

0 operations pending

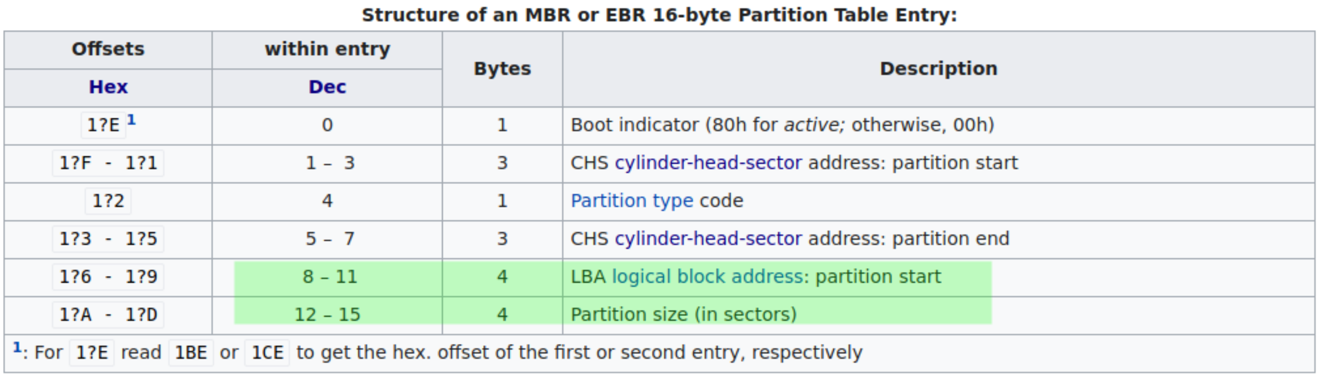
Part	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-------	0000000000	0000002047	0000002048	Unallocated
002:	000:000	0000002048	0000206847	0000204800	DOS FAT16 (0x06)
003:	000:001	0000206848	0000411647	0000204800	Win95 FAT32 (0x0b)
004:	000:002	0000411648	0000616447	0000204800	NTFS / exFAT (0x07)
005:	Meta	0000616448	0001023999	0000407552	DOS Extended (0x05)
006:	Meta	0000616448	0000616448	0000000001	Extended Table (#1)
007:	-------	0000616448	0000618495	0000002048	Unallocated
ET1	PE1	616448+2048(S1)=618496		L1=102400	
008:	001:000	0000618496	0000720895	0000102400	DOS FAT16 (0x06)
009:	-------	0000720896	0000722943	0000002048	Unallocated
ET1	PE2	616448+106222(S2)=72267		L2=102674	(S2,L2) points Next DOS Extended

Part	Slot	Start	End	Length	Description
		0			
010:	Meta	0000722670	0000825343	0000102674	DOS Extended (0x05)
011:	Meta	0000722670	0000722670	0000000001	Extended Table (#2)
ET2	PE1	722670+274(S1)=722944		L1=102400	
012:	002:000	0000722944	0000825343	0000102400	Win95 FAT32 (0x0b)
013:	-------	0000825344	0000827391	0000002048	Unallocated
ET2	PE2	616448+210772(S2)=827220		L2=102572	(S2,L2) points Next DOS Extended
014:	Meta	0000827220	0000929791	0000102572	DOS Extended (0x05)
015:	Meta	0000827220	0000827220	0000000001	Extended Table (#3)
ET3	PE1	827220+172(S1)=827392		L1=102400	
016:	003:000	0000827392	0000929791	0000102400	Linux Swap / Solaris x86 (0x82)
017:	-------	0000929792	0000931839	0000002048	Unallocated
ET3	PE2	616448+315322(S2)=931770		L2=92230	(S2,L2) points Next DOS Extended
018:	Meta	0000931770	0001023999	0000092230	DOS Extended (0x05)
019:	Meta	0000931770	0000931770	0000000001	Extended Table (#4)
ET4	PE1	931770+70(S1)=931840		L1=92160	
020:	004:000	0000931840	0001023999	0000092160	Linux (0x83)
ET4	PE2	S2=0		L2=0	PE2=0 or (S2,L2)=(0,0) means the end of the EBR list.



Common Structure of Extended Boot Records:

Offsets within EBR sectors		Contents	Size
Hex	Dec		bytes
000 – 1BD	000 – 445	Generally unused; normally filled with zeroes; may contain another boot loader i.e. a partition boot record, for example in conjunction with Advanced Active Partitions	446
1BE – 1CD	446 – 461	Partition table's **first entry**	16
1CE – 1DD	462 – 477	Partition table's **second entry**	16
1DE – 1ED	478 – 493	Unused[3] **third entry** filled with zeroes	16
1EE – 1FD	494 – 509	Unused[3] **fourth entry** filled with zeroes	16
1FE - 1FF	510 - 511	Signature 55AAh in big-endian network order, same as little-endian 0xAA55. On disk: 0x55 at offset 510 and 0xAA at offset 511.	2
		EBR, total size: 446 +(4×16) +2 =	**512**

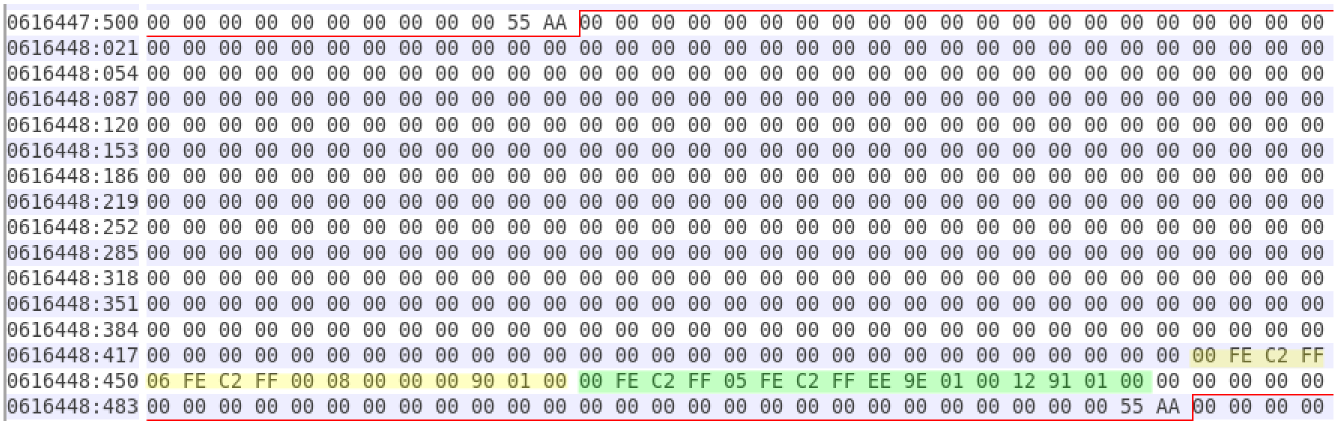


Structure of an MBR or EBR 16-byte Partition Table Entry:

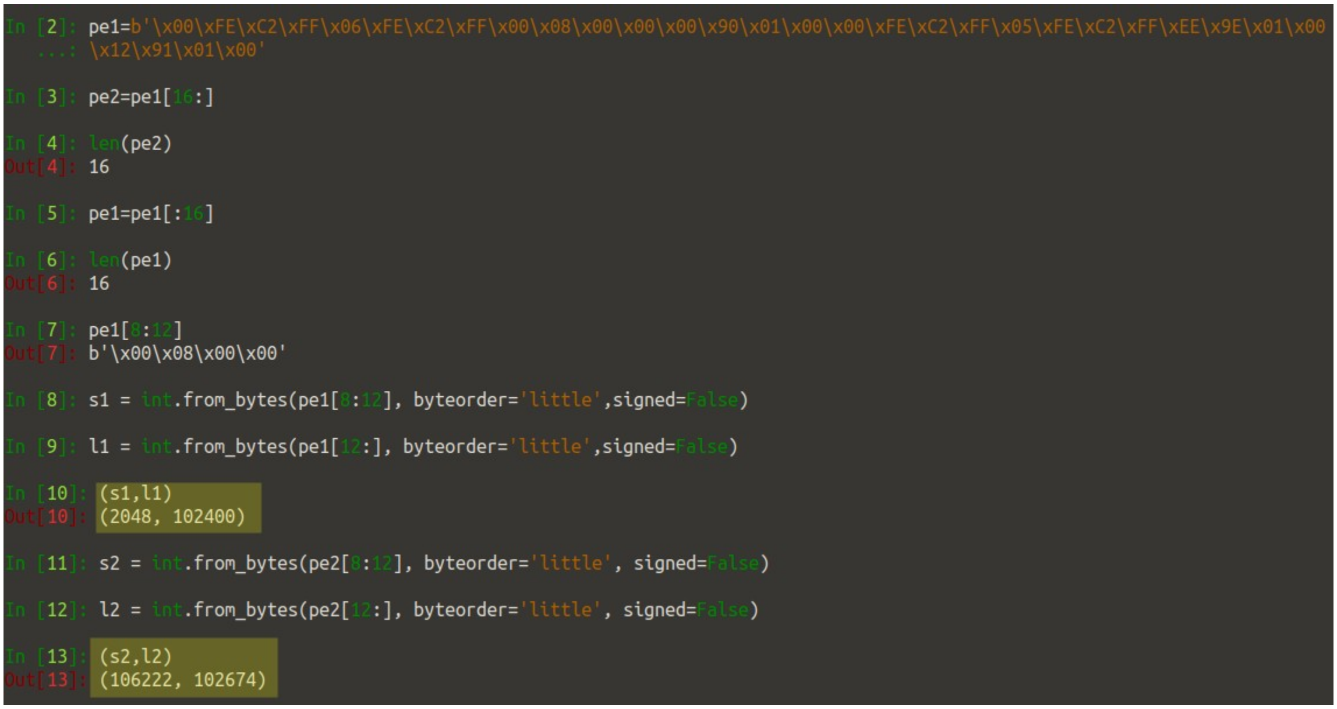
Offsets	within entry	Bytes	Description
Hex	Dec		
1?E [1]	0	1	Boot indicator (80h for *active;* otherwise, 00h)
1?F - 1?1	1 – 3	3	CHS cylinder-head-sector address: partition start
1?2	4	1	Partition type code
1?3 - 1?5	5 – 7	3	CHS cylinder-head-sector address: partition end
1?6 - 1?9	8 – 11	4	LBA logical block address: partition start
1?A - 1?D	12 – 15	4	Partition size (in sectors)

[1]: For 1?E read 1BE or 1CE to get the hex. offset of the first or second entry, respectively

```
005:    Meta        0000616448   0001023999  0000407552     DOS Extended (0x05)
006:    Meta        0000616448   0000616448  0000000001     Extended Table (#1)
```

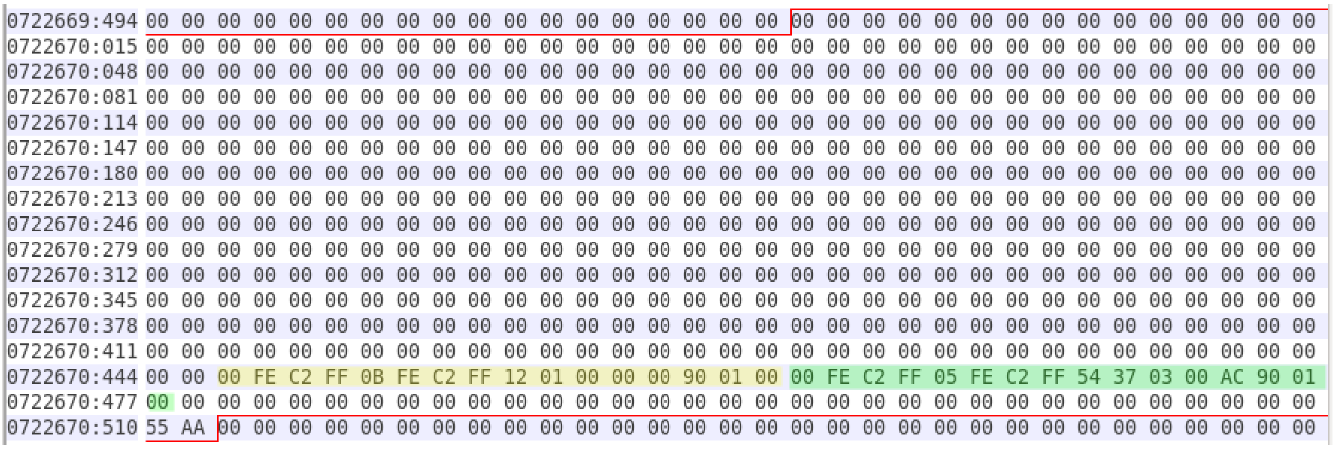


```
0616447:500 00 00 00 00 00 00 00 00 00 00 55 AA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:021 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:054 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:087 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:153 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:186 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:219 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:252 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:285 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:318 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:351 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:384 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0616448:417 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE C2 FF
0616448:450 06 FE C2 FF 00 08 00 00 00 90 01 00 00 FE C2 FF 05 FE C2 FF EE 9E 01 00 12 91 01 00 00 00 00 00 00
0616448:483 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA 00 00 00 00
```

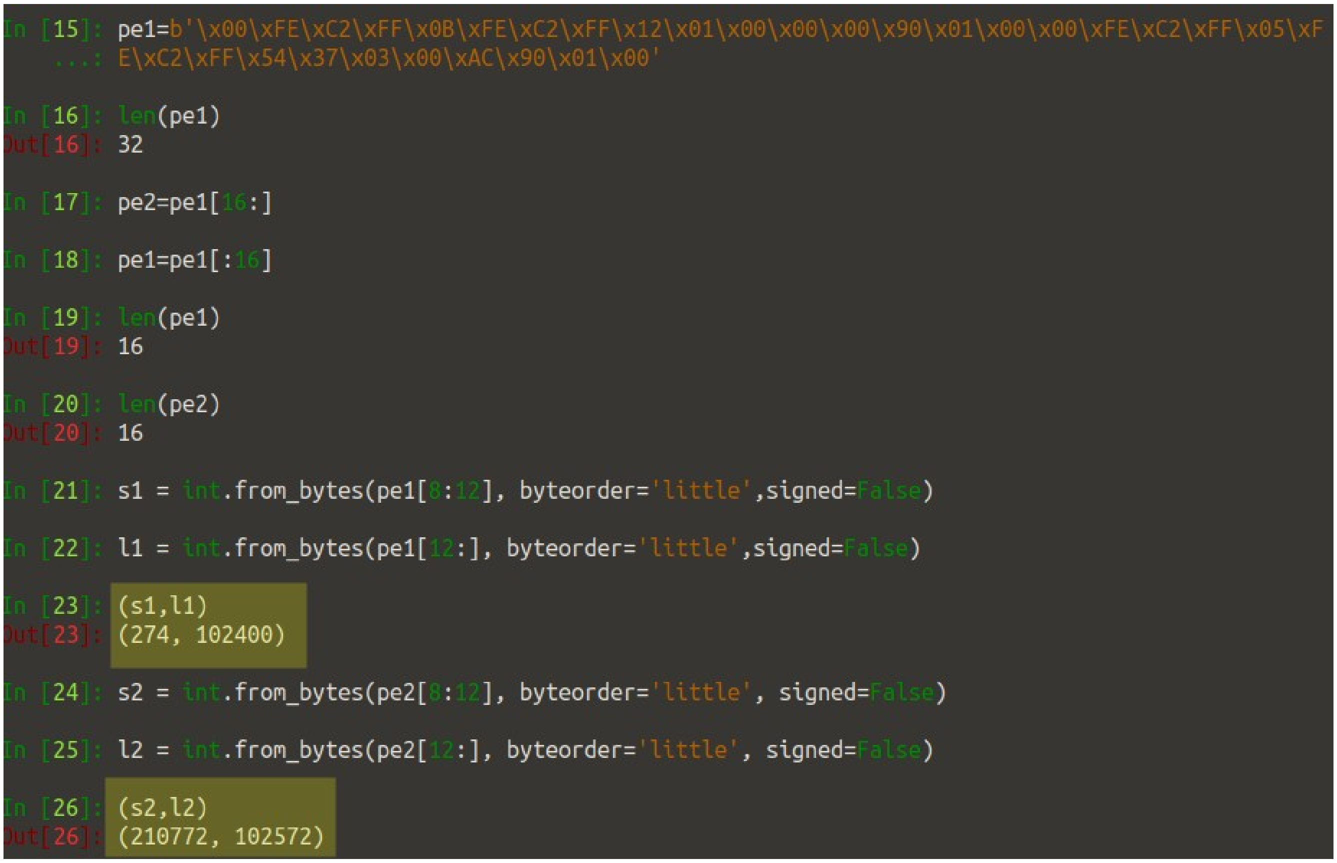


```
In [2]: pe1=b'\x00\xFE\xC2\xFF\x06\xFE\xC2\xFF\x00\x08\x00\x00\x00\x90\x01\x00\x00\xFE\xC2\xFF\x05\xFE\xC2\xFF\xEE\x9E\x01\x00
   ...: \x12\x91\x01\x00'

In [3]: pe2=pe1[16:]

In [4]: len(pe2)
Out[4]: 16

In [5]: pe1=pe1[:16]

In [6]: len(pe1)
Out[6]: 16

In [7]: pe1[8:12]
Out[7]: b'\x00\x08\x00\x00'

In [8]: s1 = int.from_bytes(pe1[8:12], byteorder='little',signed=False)

In [9]: l1 = int.from_bytes(pe1[12:], byteorder='little',signed=False)

In [10]: (s1,l1)
Out[10]: (2048, 102400)

In [11]: s2 = int.from_bytes(pe2[8:12], byteorder='little', signed=False)

In [12]: l2 = int.from_bytes(pe2[12:], byteorder='little', signed=False)

In [13]: (s2,l2)
Out[13]: (106222, 102674)
```

010:	Meta	0000722670	0000825343	0000102674	DOS Extended (0x05)
011:	Meta	0000722670	0000722670	0000000001	Extended Table (#2)

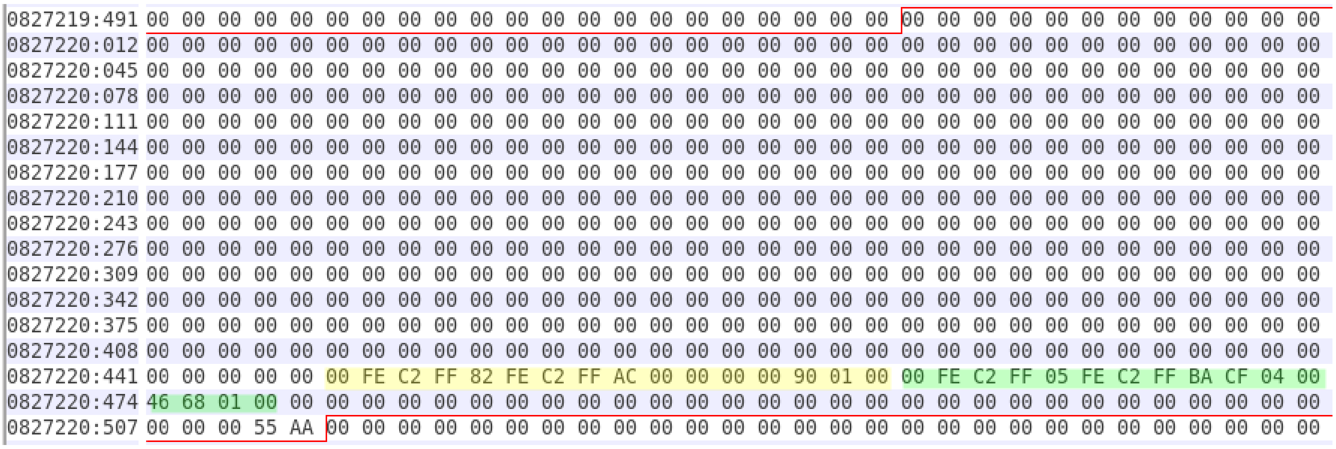


```
0722669:494 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:015 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:081 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:114 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:147 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:213 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:246 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:279 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:312 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:345 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:378 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:411 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:444 00 00 00 FE C2 FF 0B FE C2 FF 12 01 00 00 00 90 01 00 00 FE C2 FF 05 FE C2 FF 54 37 03 00 AC 90 01
0722670:477 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0722670:510 55 AA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

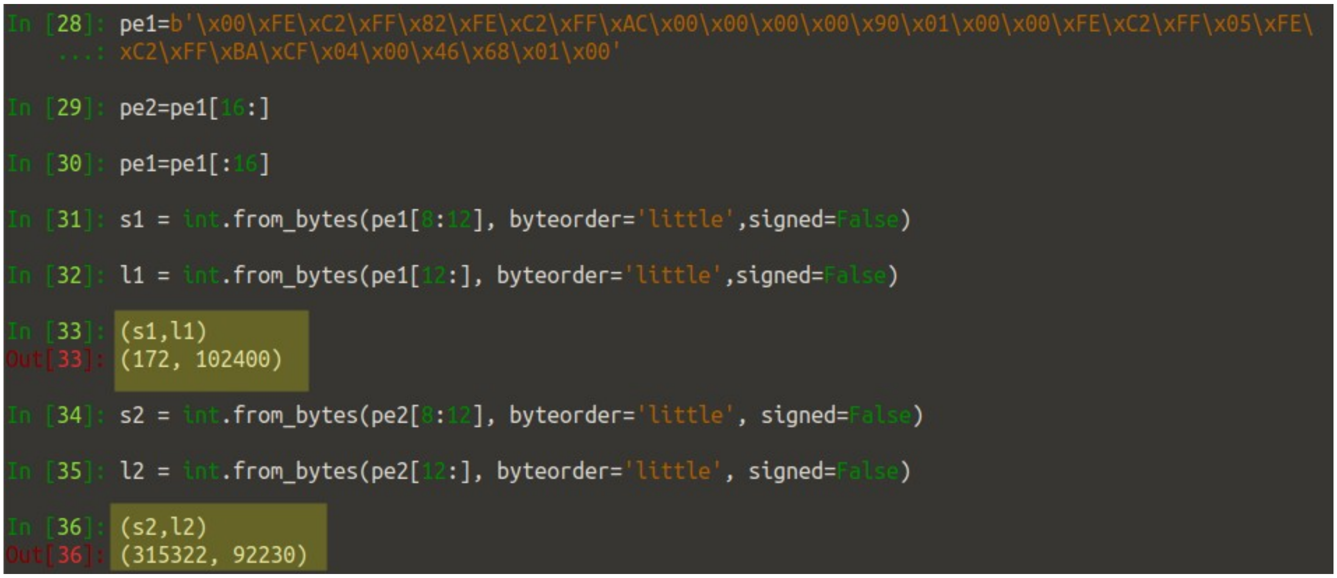


```
In [15]: pe1=b'\x00\xFE\xC2\xFF\x0B\xFE\xC2\xFF\x12\x01\x00\x00\x00\x90\x01\x00\x00\xFE\xC2\xFF\x05\xF
    ...: E\xC2\xFF\x54\x37\x03\x00\xAC\x90\x01\x00'

In [16]: len(pe1)
Out[16]: 32

In [17]: pe2=pe1[16:]

In [18]: pe1=pe1[:16]

In [19]: len(pe1)
Out[19]: 16

In [20]: len(pe2)
Out[20]: 16

In [21]: s1 = int.from_bytes(pe1[8:12], byteorder='little',signed=False)

In [22]: l1 = int.from_bytes(pe1[12:], byteorder='little',signed=False)

In [23]: (s1,l1)
Out[23]: (274, 102400)

In [24]: s2 = int.from_bytes(pe2[8:12], byteorder='little', signed=False)

In [25]: l2 = int.from_bytes(pe2[12:], byteorder='little', signed=False)

In [26]: (s2,l2)
Out[26]: (210772, 102572)
```

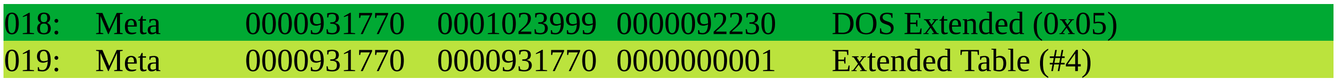
014:	Meta	0000827220	0000929791	0000102572	DOS Extended (0x05)
015:	Meta	0000827220	0000827220	0000000001	Extended Table (#3)



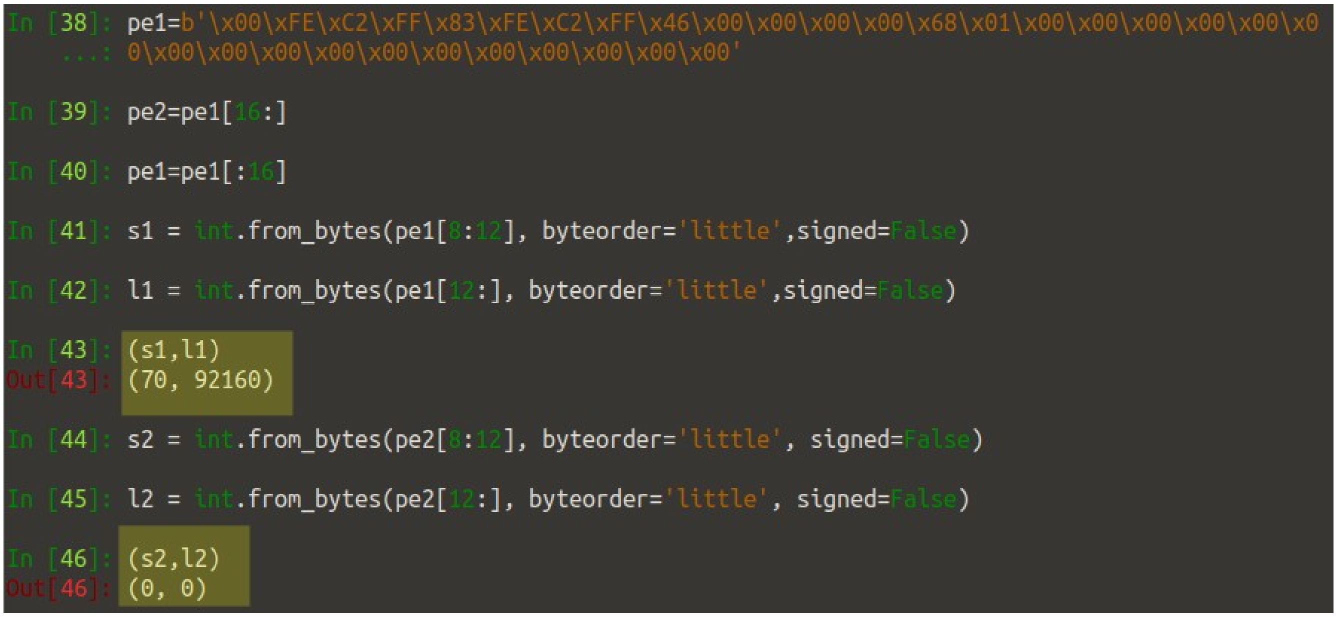
```
0827219:491 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:012 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:045 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:078 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:111 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:177 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:243 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:276 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:309 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:342 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:375 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:408 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:441 00 00 00 00 00 00 FE C2 FF 82 FE C2 FF AC 00 00 00 00 90 01 00 00 FE C2 FF 05 FE C2 FF BA CF 04 00
0827220:474 46 68 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0827220:507 00 00 00 55 AA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
In [28]: pe1=b'\x00\xFE\xC2\xFF\x82\xFE\xC2\xFF\xAC\x00\x00\x00\x00\x90\x01\x00\x00\xFE\xC2\xFF\x05\xFE\
    ...: xC2\xFF\xBA\xCF\x04\x00\x46\x68\x01\x00'

In [29]: pe2=pe1[16:]

In [30]: pe1=pe1[:16]

In [31]: s1 = int.from_bytes(pe1[8:12], byteorder='little',signed=False)

In [32]: l1 = int.from_bytes(pe1[12:], byteorder='little',signed=False)

In [33]: (s1,l1)
Out[33]: (172, 102400)

In [34]: s2 = int.from_bytes(pe2[8:12], byteorder='little', signed=False)

In [35]: l2 = int.from_bytes(pe2[12:], byteorder='little', signed=False)

In [36]: (s2,l2)
Out[36]: (315322, 92230)
```



018:	Meta	0000931770	0001023999	0000092230	DOS Extended (0x05)
019:	Meta	0000931770	0000931770	0000000001	Extended Table (#4)



```
In [38]: pe1=b'\x00\xFE\xC2\xFF\x83\xFE\xC2\xFF\x46\x00\x00\x00\x00\x68\x01\x00\x00\x00\x00\x00\x0
    ...: 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

In [39]: pe2=pe1[16:]

In [40]: pe1=pe1[:16]

In [41]: s1 = int.from_bytes(pe1[8:12], byteorder='little',signed=False)

In [42]: l1 = int.from_bytes(pe1[12:], byteorder='little',signed=False)

In [43]: (s1,l1)
Out[43]: (70, 92160)

In [44]: s2 = int.from_bytes(pe2[8:12], byteorder='little', signed=False)

In [45]: l2 = int.from_bytes(pe2[12:], byteorder='little', signed=False)

In [46]: (s2,l2)
Out[46]: (0, 0)
```