

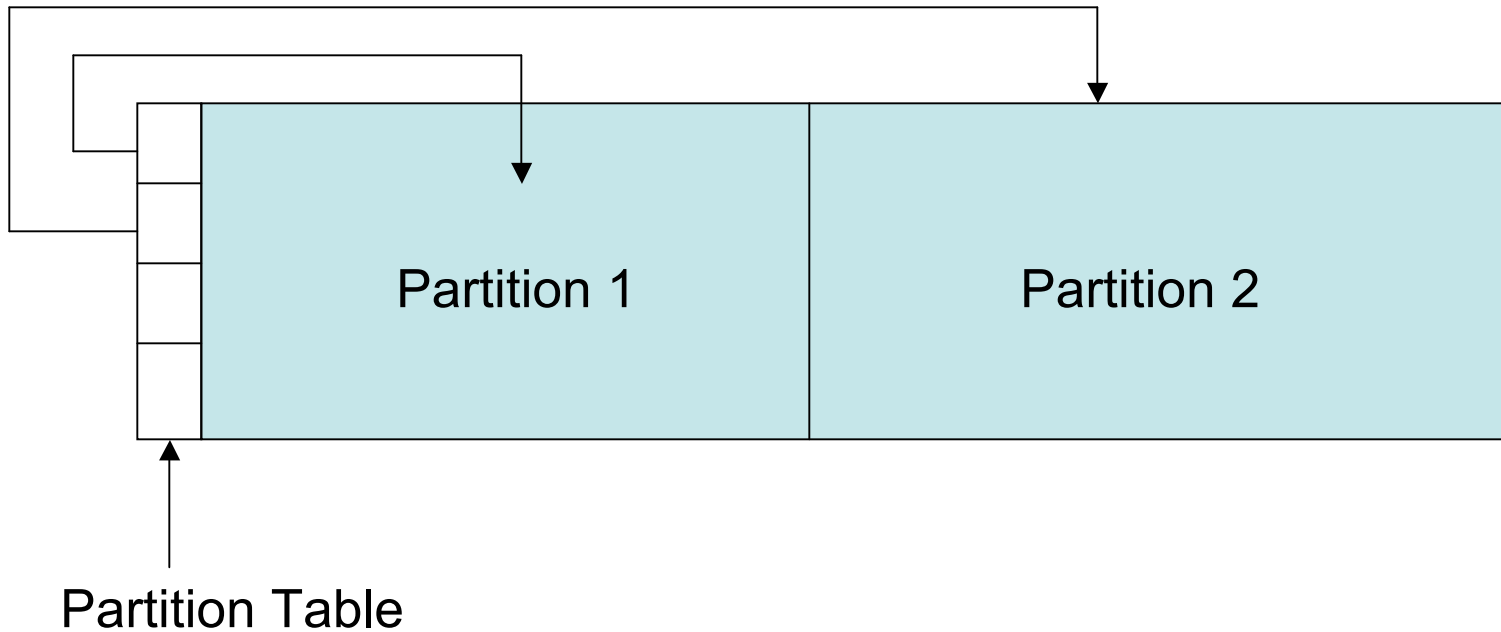
PC-Based Partitions

Priscilla Oppenheimer

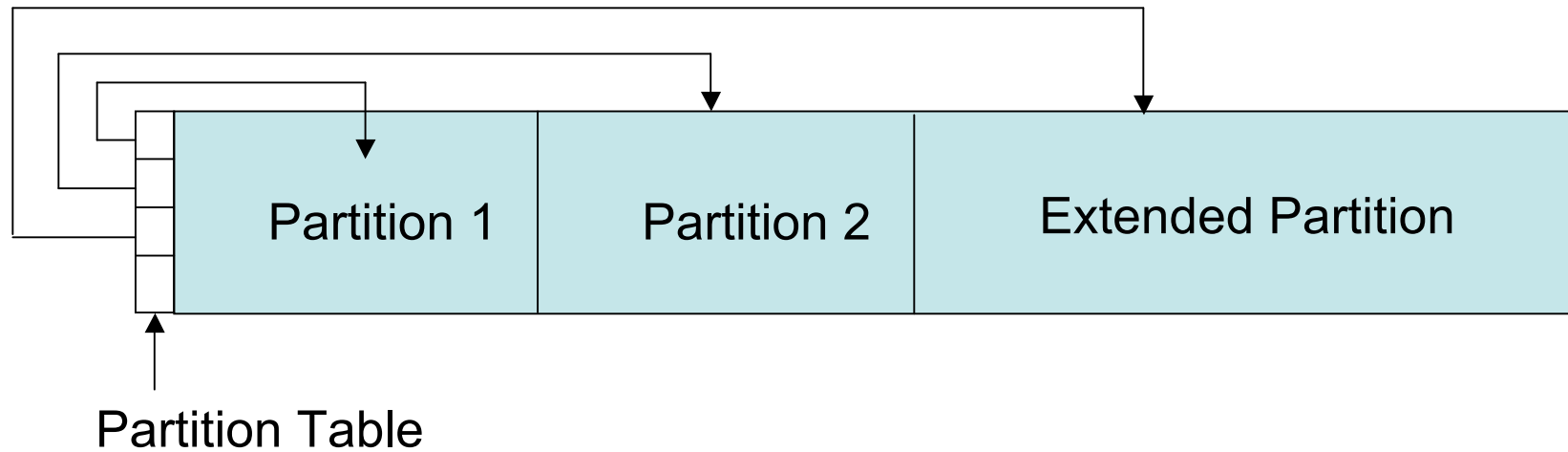
DOS Partitions

- MBR in first 512-byte sector
 - Boot code (Bytes 0-445)
 - Partition table (bytes 446-509)
 - Signature (bytes 510-511, value = 0xAA55)
- Partition table has four entries

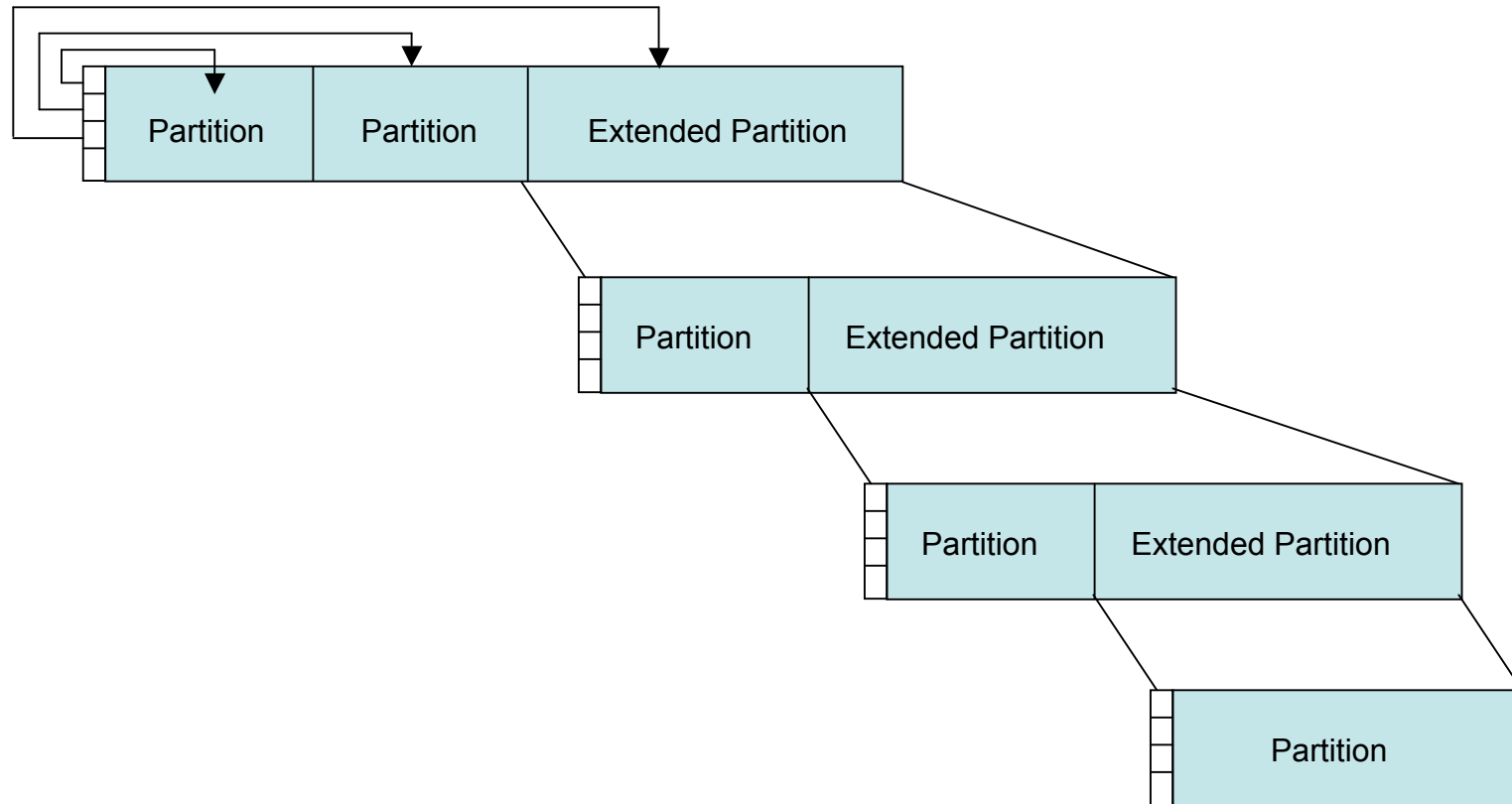
DOS Disk



Extended Partitions



Extended Partitions



Partition Table

- Four 16-byte Entries
- Each entry describes a partition
 - Bootable flag (0x80 means bootable)
 - Starting CHS address
 - Partition type
 - Ending CHS address
 - Starting LBA address
 - Size (number of sectors in partition)

Decoding Partition Tables Gotchas

- Decimal or Hex?
- Little Endian or Big Endian?
- Output to text? How do you get the text back to the “lab” for analysis?
- Output to file? Where will you put it?
Don't write to suspect's HD!

Use Unix/Linux dd Utility to View Partition Table

- `dd if=/dev/hda count=1 | xxd`
- Partition table starts at 446 decimal

```
0000000: eb48 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0  .H.....
{skip}
00001b0: 0000 0000 0000 0000 786b 786b 0000 8001  .....xkxk....
00001c0: 0100 0cfe fffe 3f00 0000 82c8 7302 0000  .....?.....s...
00001d0: 8101 82fe bf40 c1c8 7302 40b0 0f00 0000  .....@..s.@.....
00001e0: 8141 83fe ff00 0179 8302 c018 2502 0000  .A.....y....%...
00001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  .....U.
```

Partition Table Entries

Try Decoding It By Hand...

#	Flag	Type	Starting LBA Address	Size
1				
2				
3				
4				

Partition Table Entries

#	Flag	Type	Starting LBA Address	Size
1	0x80	0x0C	0x0000003F	0x0273C882
2	0x00	0x82	0x0273C8C1	0x000FB040
3	0x00	0x83	0x02837901	0x022518C0
4	0x00	0x00	0x00000000	0x00000000

Partition Table in English

- Partition 1
 - Bootable (0x80 at byte 0)
 - Type is Fat32, LBA (0x0C at byte 4)
 - It starts at sector 3F (63 in decimal)
 - Its size is 0x0273C882 sectors
 - About 41 million sectors in decimal
 - 41M x 512 bytes = 20,992,000,000 = ~21 GB

Partition Table in English (cont.)

- Partition 2
 - Not bootable (0x00 at byte 0)
 - Type is Linux Swap (0x82 at byte 4)
 - It starts at sector 41,142,465 in decimal
 - Its size is 0x000FB040 sectors
 - About 1 million sectors in decimal
 - 1M x 512 bytes = 512,000,000 = ~.5 GB

Partition Table in English (cont.)

- Partition 3
 - Not bootable (0x00 in byte 0)
 - Type is Linux (0x83 at byte 4)
 - It starts at sector 42170625 in decimal
 - Its size is 0x022518C0 sectors
 - About 36 million sectors in decimal
 - $36\text{M} \times 512 \text{ bytes} = 18,432,000,000 = \sim 18.5 \text{ GB}$

Use fdisk to View Table

```
root@tty0[knoppix]# fdisk /dev/hda
```

```
Command (m for help): p
```

```
Disk /dev/hda: 255 heads, 63 sectors, 4865  
cylinders
```

Nr	AF	Hd	Sec	Cyl	Hd	Sec	Cyl	Start	Size	ID
1	80	1	1	0	254	63	1022	63	41142402	0c
2	00	0	1	513	254	63	576	41142465	1028160	82
3	00	0	1	577	254	63	768	42170625	35985600	83
4	00	0	0	0	0	0	0	0	0	00

A Word About Non-Intel Macs...

- No MBR
 - Firmware has code to process partition map
- Partition map starts in the second sector
- Several 512-byte data structures, one for each partition
- Data structure includes
 - Signature value = 0x504D
 - Starting sector
 - Size
 - Type
 - Volume name

Mac Example

```
Priscillas-Computer:~ Priscilla$ sudo dd  
if=/dev/disk0 skip=1 count=4lxxd
```

```
0000000: 504d 0000 0000 0004 0000 0001 0000 003f PM.....?  
0000010: 4170 706c 6500 0000 0000 0000 0000 0000 Apple.....  
0000020: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000030: 4170 706c 655f 7061 7274 6974 696f 6e5f Apple_partition_  
0000040: 6d61 7000 0000 0000 0000 0000 0000 0000 map.....  
0000050: 0000 0000 0000 003f 0000 0003 0000 0000 .....?.....  
{skip}  
0000200: 504d 0000 0000 0004 0000 0040 0004 0000 PM.....@....  
0000210: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000220: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000230: 4170 706c 655f 4672 6565 0000 0000 0000 Apple_Free.....  
{skip}  
0000400: 504d 0000 0000 0004 0004 0040 037a 3df6 PM.....@.z=.  
0000410: 556e 7469 746c 6564 0000 0000 0000 0000 Untitled.....  
0000420: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000430: 4170 706c 655f 4846 5300 0000 0000 0000 Apple_HFS.....  
0000440: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000450: 0000 0000 037a 3df6 4000 0033 0000 0000 .....z=@..3....  
{skip}  
0000600: 504d 0000 0000 0004 037e 3e36 0000 000a PM.....~>6....  
0000610: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000620: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
0000630: 4170 706c 655f 4672 6565 0000 0000 0000 Apple_Free.....
```

Use pdisk to View Table

```
Priscillas-Computer:~ Priscilla$ sudo pdisk /dev/disk0  
Command (? for help): p
```

```
Partition map (with 512 byte blocks) on '/dev/disk0'
```

#:	type	name	length	base	(size)
1:	Apple_partition_map	Apple	63	@ 1	
2:	Apple_Free		262144	@ 64	(128.0M)
3:	Apple_HFS	Untitled	58342902	@ 262208	(27.8G)
4:	Apple_Free		10	@ 58605110	