

FAT Concepts

Priscilla Oppenheimer

File Allocation Table (FAT) File Systems

- Simple and common
- Primary file system for DOS and Windows 9x
- Can be used with Windows NT, 2000, and XP
 - New Technologies File System (NTFS) is default for NT, 2000, and XP
- Supported by all Windows and UNIX varieties
- Used in flash cards and USB thumb drives

The FAT Family

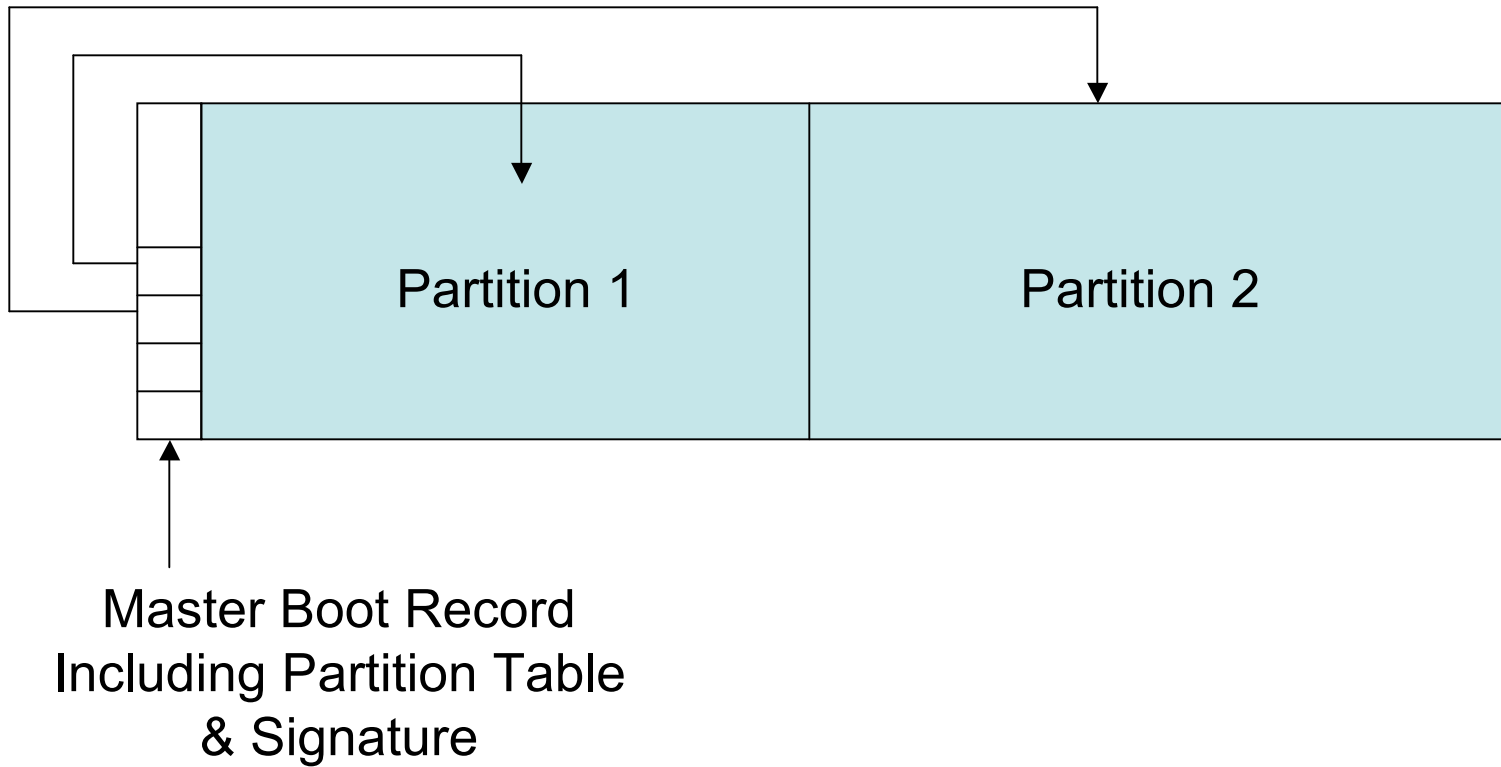
- FAT12, FAT16, FAT32
 - The number refers to the quantity of bits used in the FAT to refer to clusters



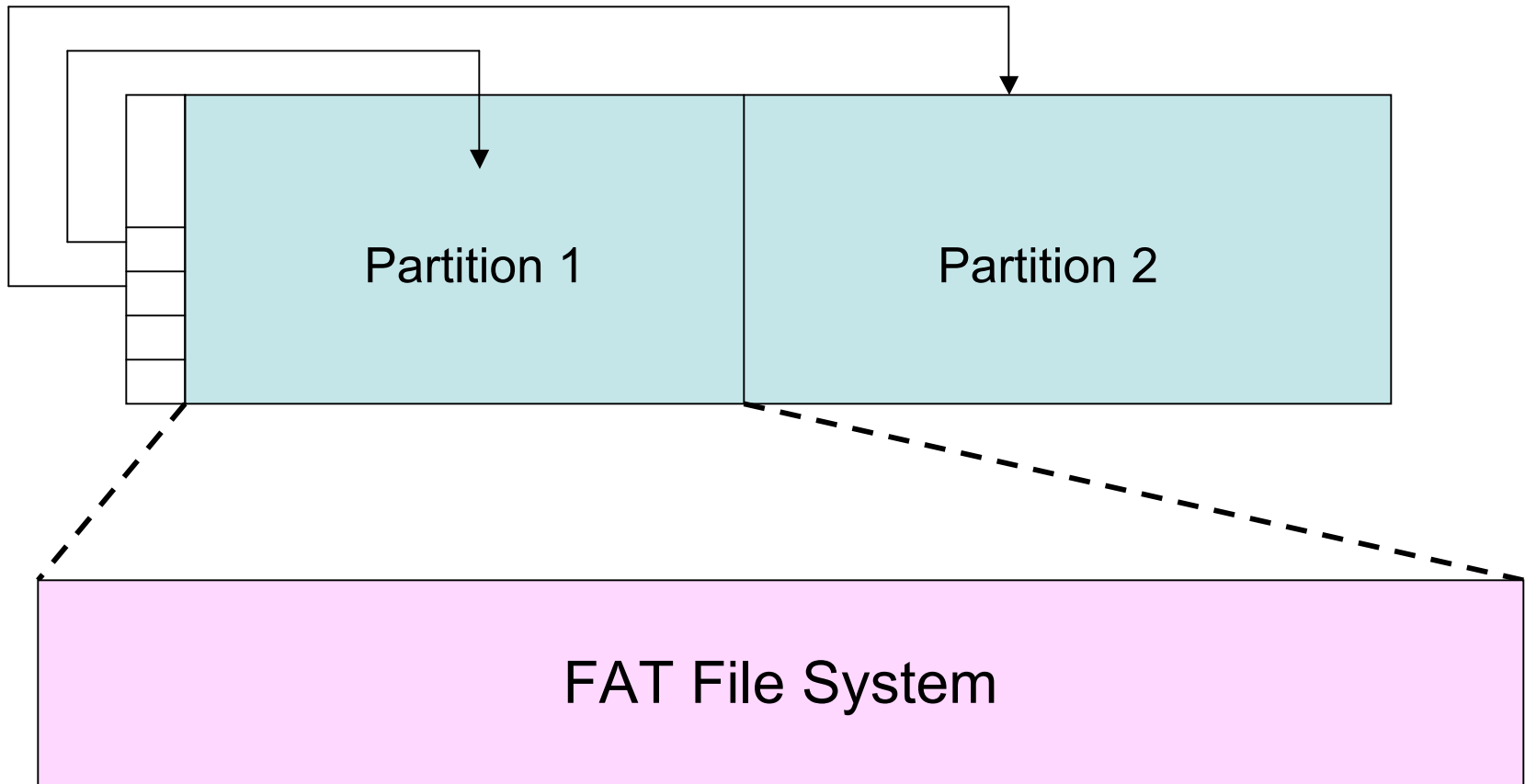
DOS Partitions Review

- 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
 - Disk has four primary partitions
 - A primary partition may hold extended partitions

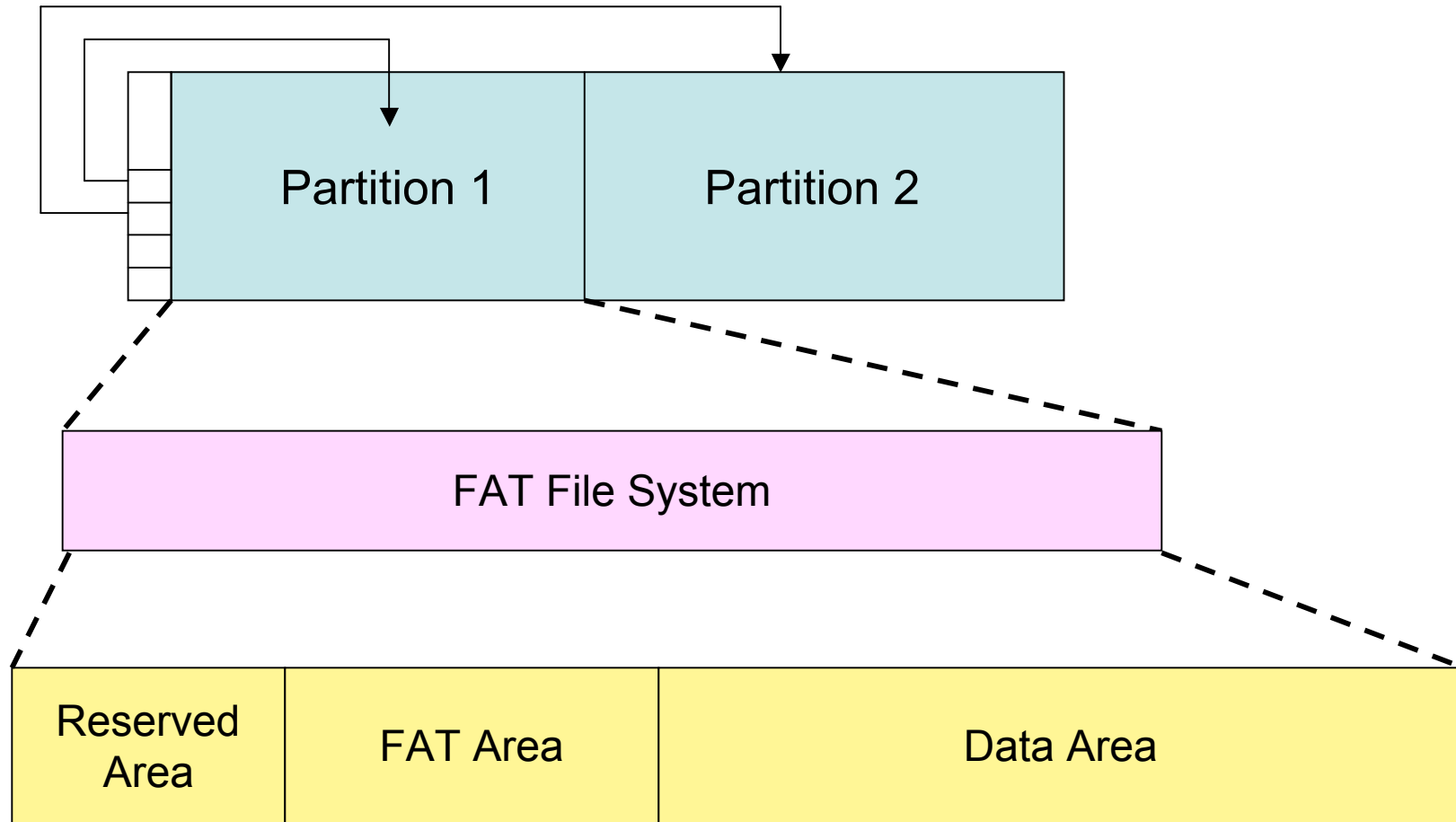
DOS Disk



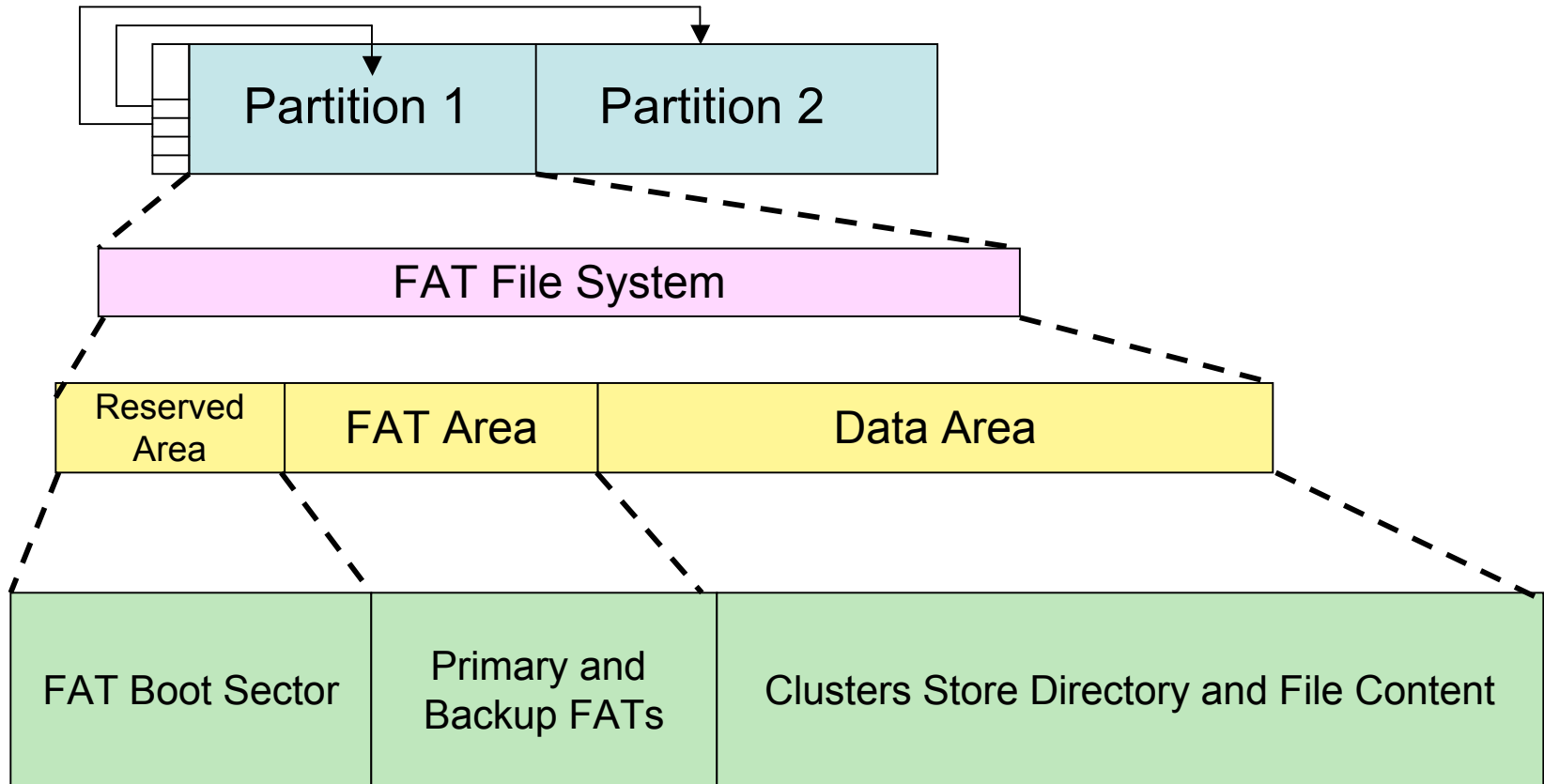
Partition Holds a File System from the FAT Family



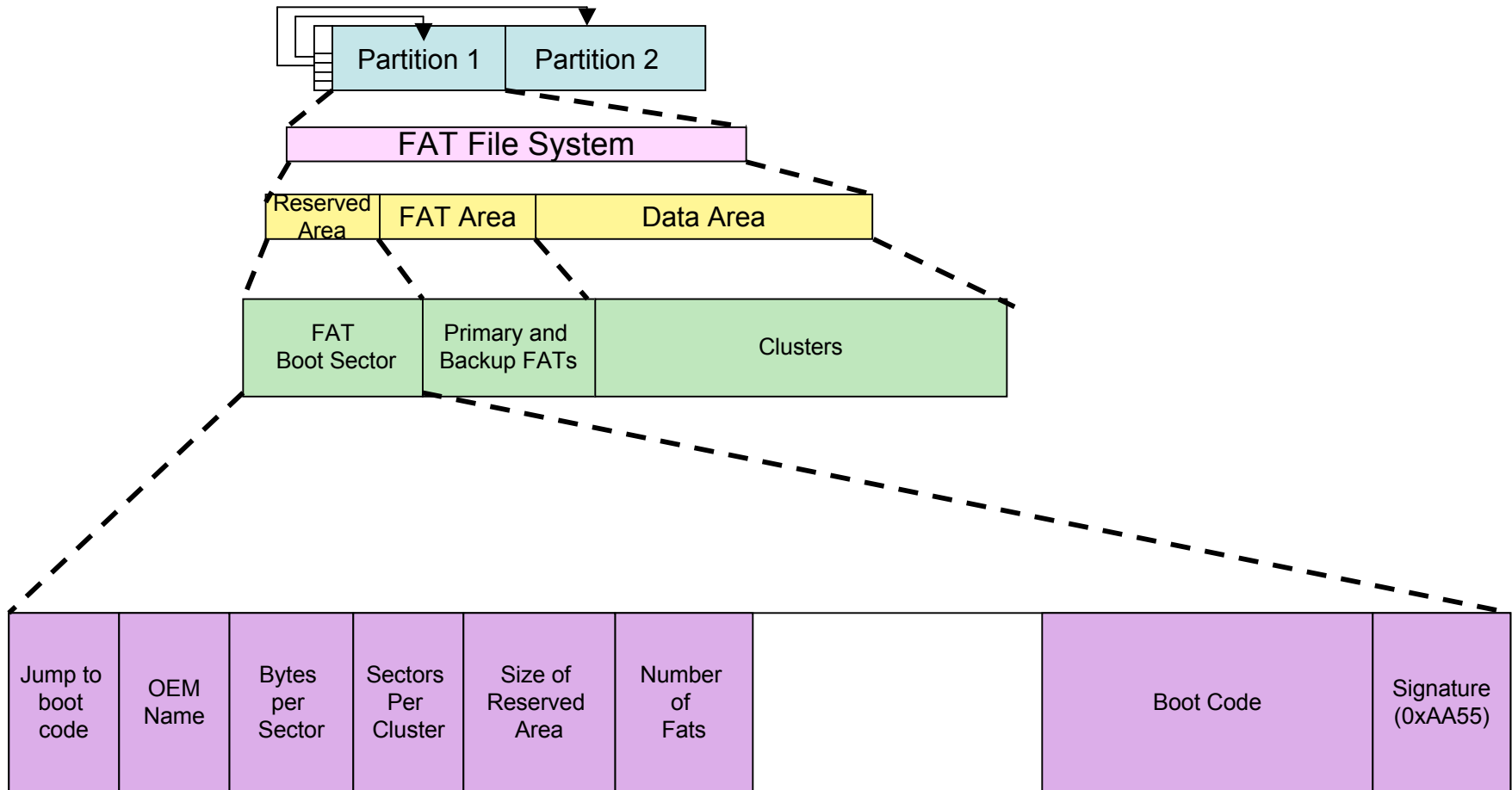
FAT Family File System



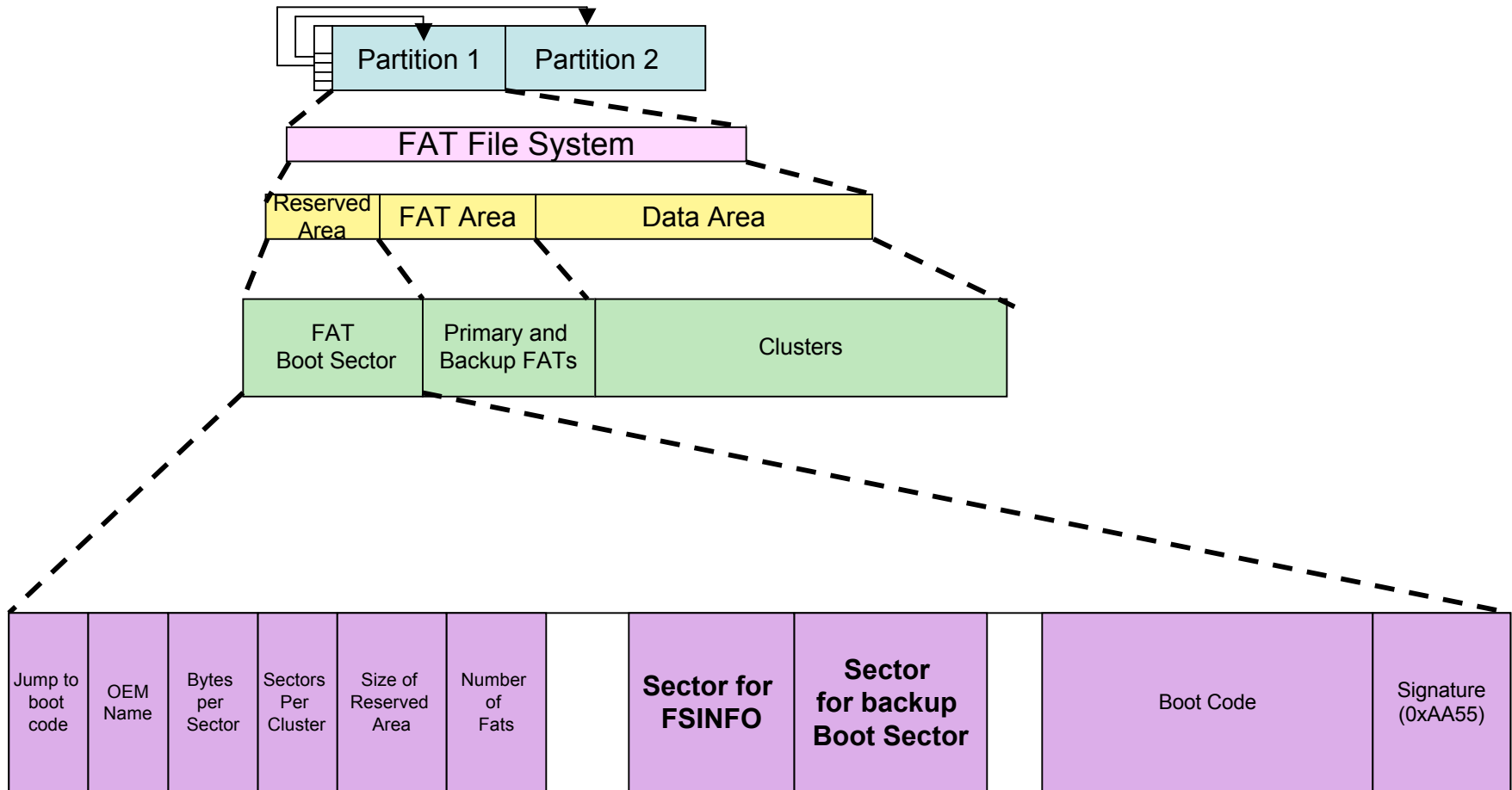
FAT File System Layout



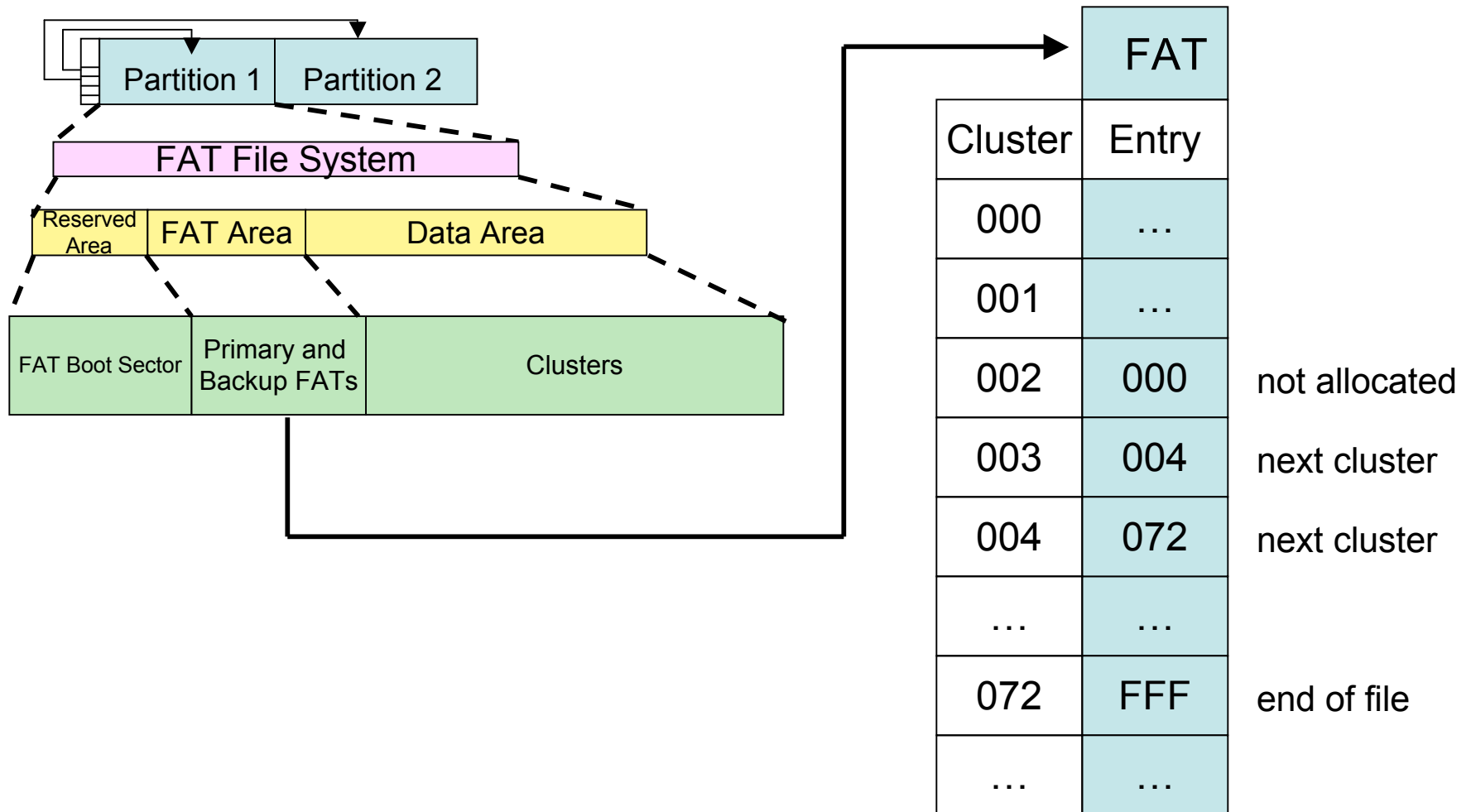
FAT File System Boot Sector



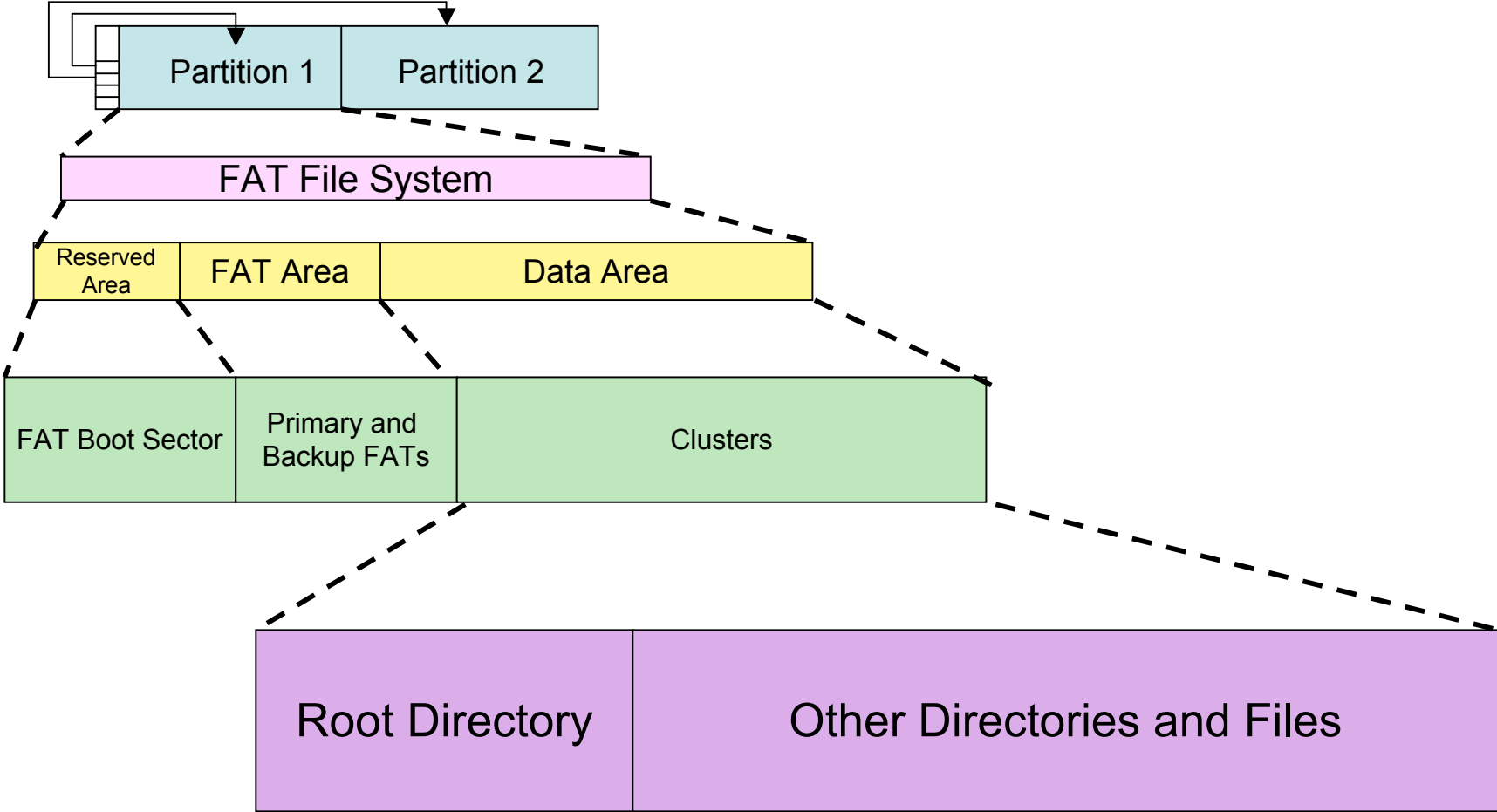
FAT32 Boot Sector



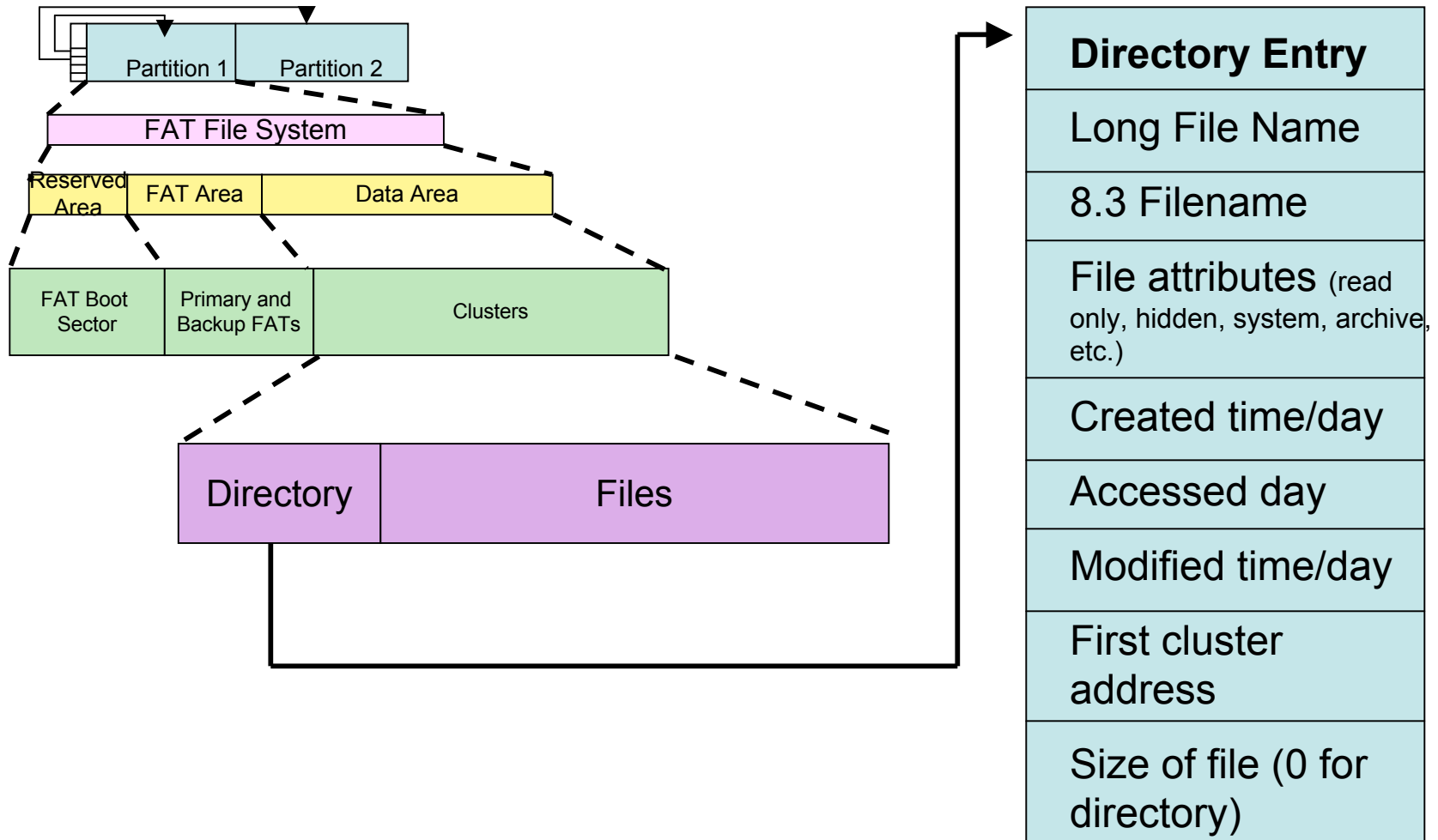
File Allocation Table Concepts



Data Area Concepts

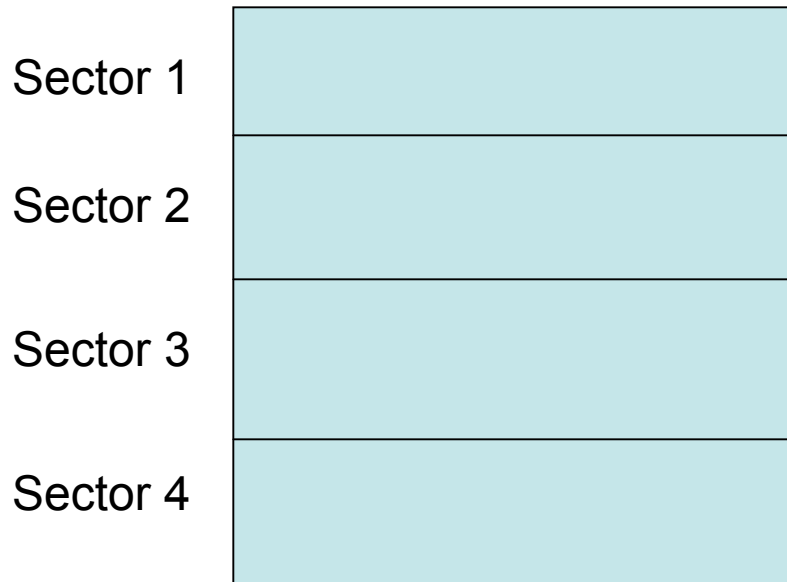


FAT Directories

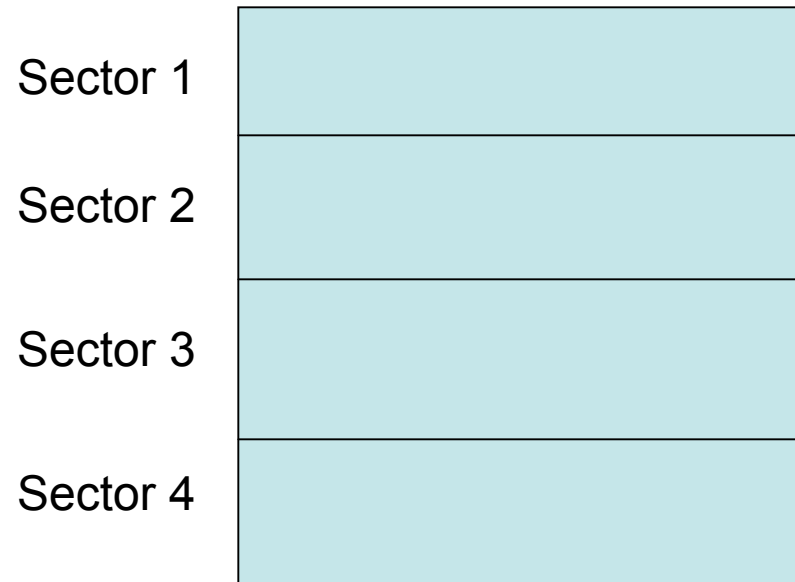


Clusters

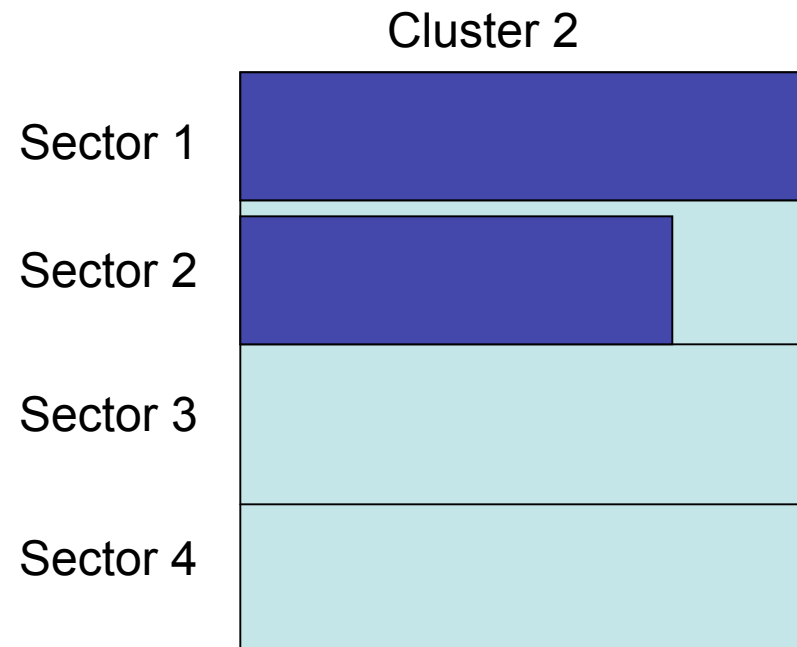
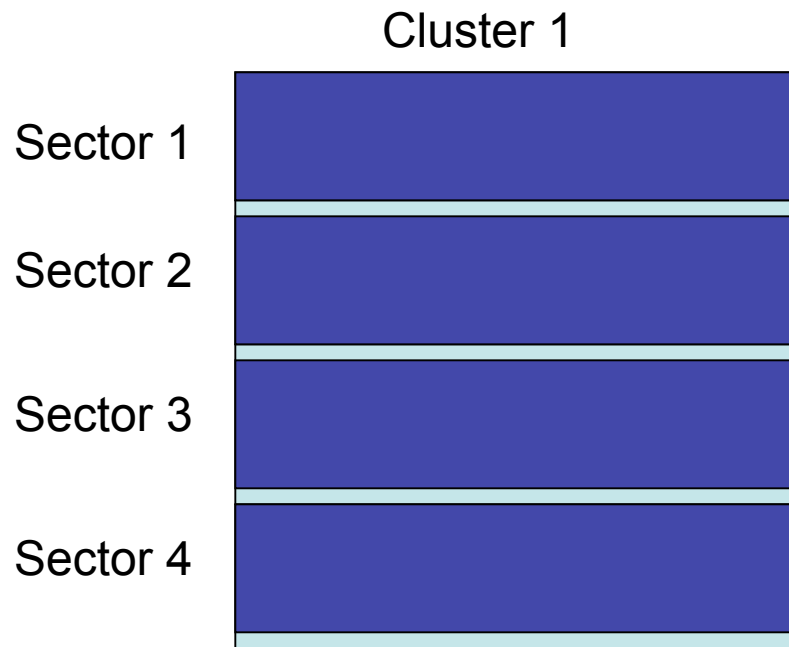
Cluster 1



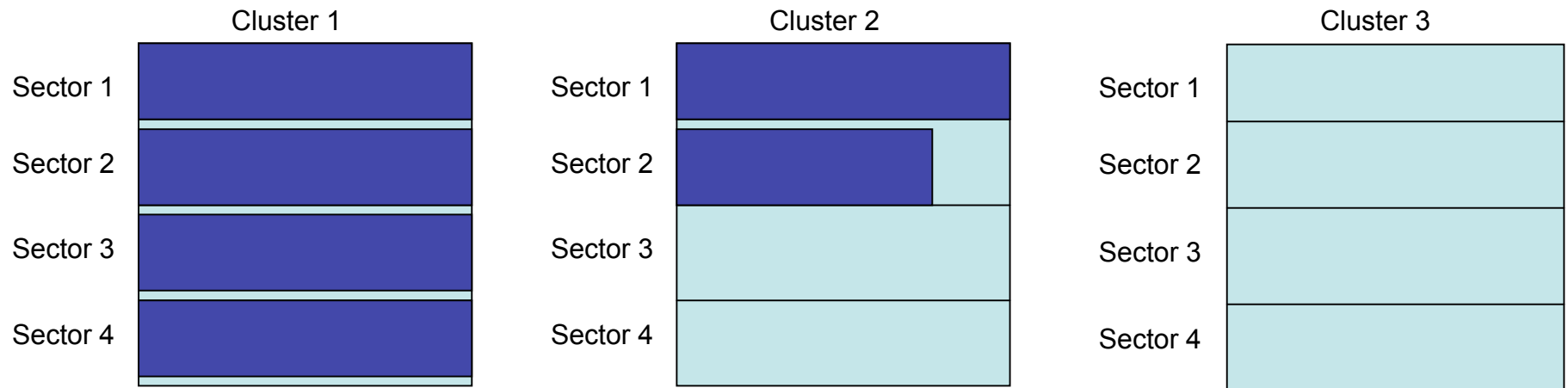
Cluster 2



File Data (Example 1)



File Data (Example 2)



Slack

- Slack is the space allocated to a file, but unused
 - Space at the end of a sector that remains unused by the file
 - Sectors allocated to the file that the file hasn't yet used
- Slack space often contains useful evidence
 - Unused bytes in an allocated sector are less useful
 - Unused sectors in an allocated cluster retain their original contents and are very useful

Unallocated Clusters

- Many clusters on a modern hard drive are unallocated
- Unallocated clusters may have been allocated earlier though
 - These clusters retain their data until they are reallocated to a new file
 - Deleted files are still recoverable!



Deleting a FAT File

Deleting dir1\file1.txt

1. Read Fat Boot Sector (sector 0 of the volume) to understand structure and location of Reserved, FAT, and Data areas
2. Locate dir1 in Root Directory; determine its starting cluster
3. Go to dir1 cluster; determine starting cluster for file1.txt
4. Set FAT entries for file1.txt to 0
5. Change filename to σile1.txt in dir1 directory
 - First character becomes 0xE5

Directory and FAT

Directory

First cluster used by file



file1.txt	02C
file2	
file3	
file4	

FAT

000	...		
001	...		
002	...		
	...		
02C	0	2	D
02D	0	2	E
02E	F	F	F
	...		

Directory and FAT

Deleted file

Directory

First cluster used by file



file1.txt	02C
file2	
file3	
file4	

FAT

000	...
001	...
002	...
	...
02C	0 0 0
02D	0 0 0
02E	0 0 0
	...

Cluster Allocation Algorithms

- First available
 - Always start at the beginning of the file system
 - Fragmented files common
 - Recovery of deleted content better at end of file system

Cluster Allocation Algorithms

- Best fit
 - Search for consecutive clusters that fit the size of file
 - Only works for files that don't grow
- Next available
 - Start search with the cluster that was most recently allocated
 - More balanced for data recovery
 - Used by Windows 98 and XP

FAT32 FSINFO

Hints about where the OS can find free clusters

Byte Range	Description
0-3	Signature (0x41615252)
4-483	Not Used
484-487	Signature (0x61417272)
488-491	Number of free clusters
492-495	Next free cluster
496-507	Not Used
508-511	Signature (0xAA550000)