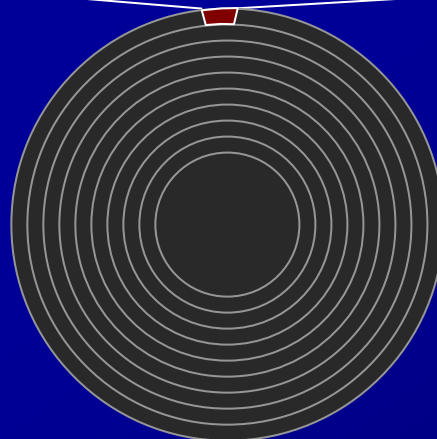
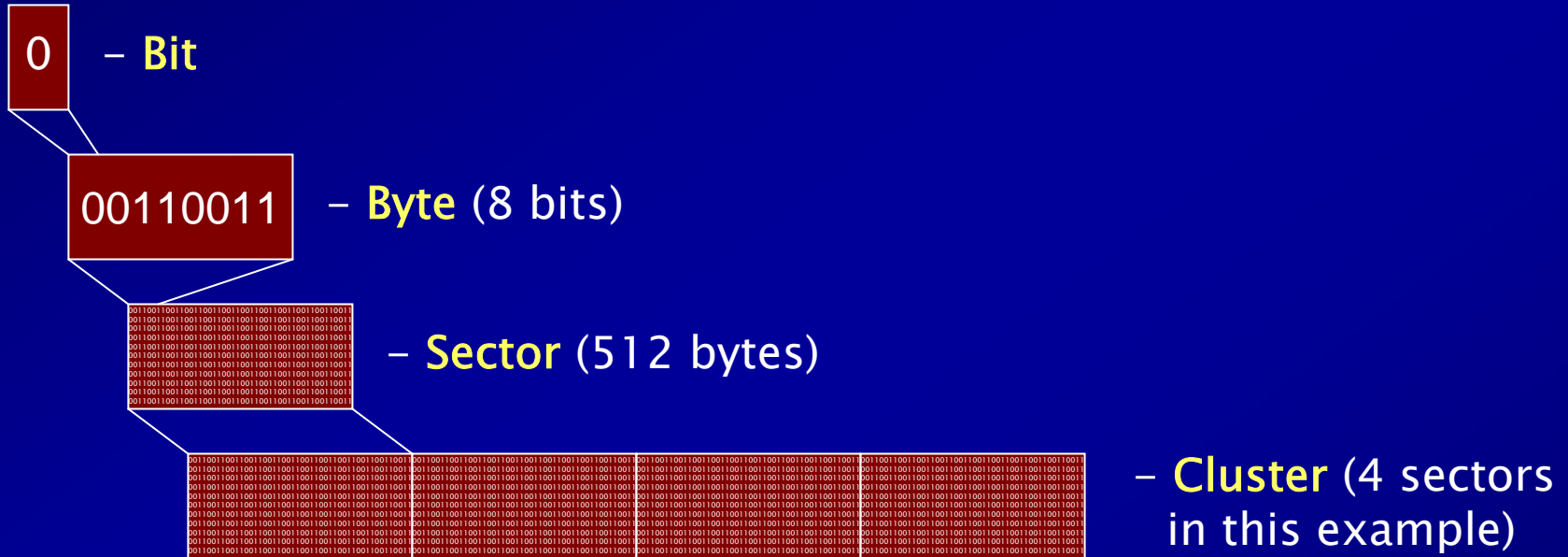


# Computer Data Expert

The following is from a presentation developed to support/explain a Data Forensics expert testimony.

Click to advance slides.

# Hard Drive Data Storage Basics

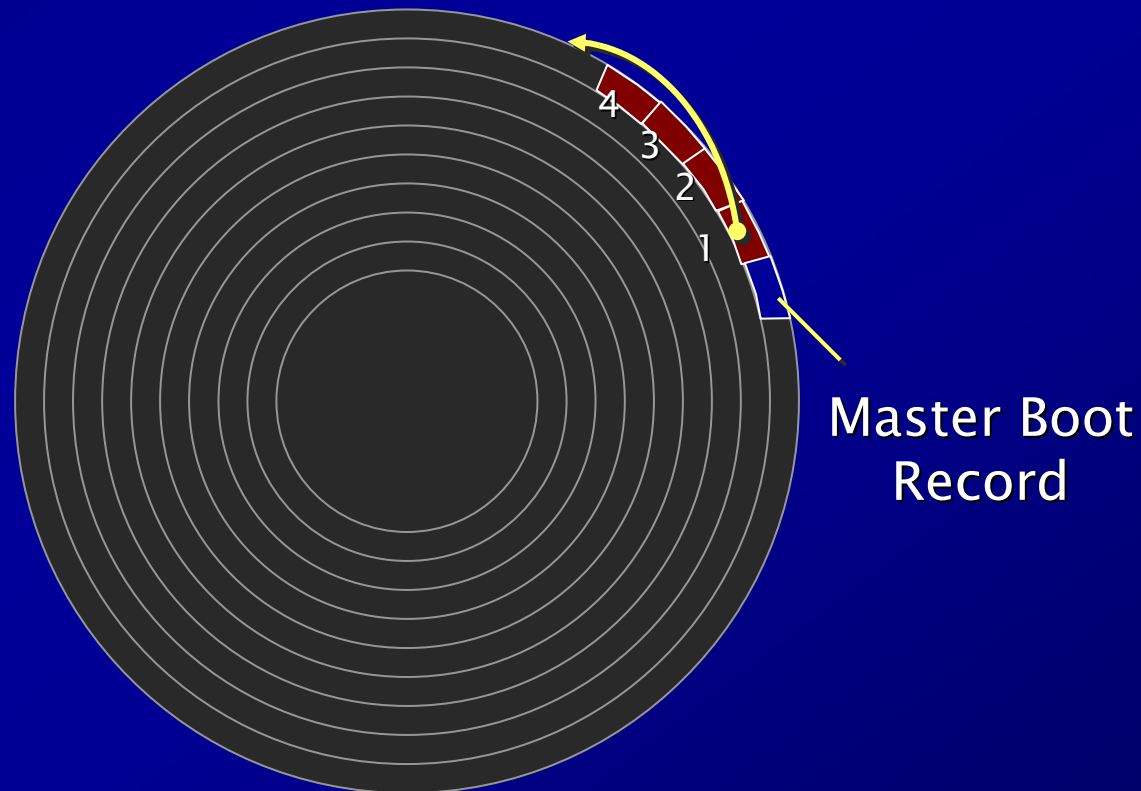


**Hard Drive** – as many clusters as drive geometry allows dependant on number of sectors in a cluster

# When you write a file...

---

- Starting at the “Master Boot Record”
  - Data is written to clusters around the hard disk into “unallocated” space.



# When you write a file...

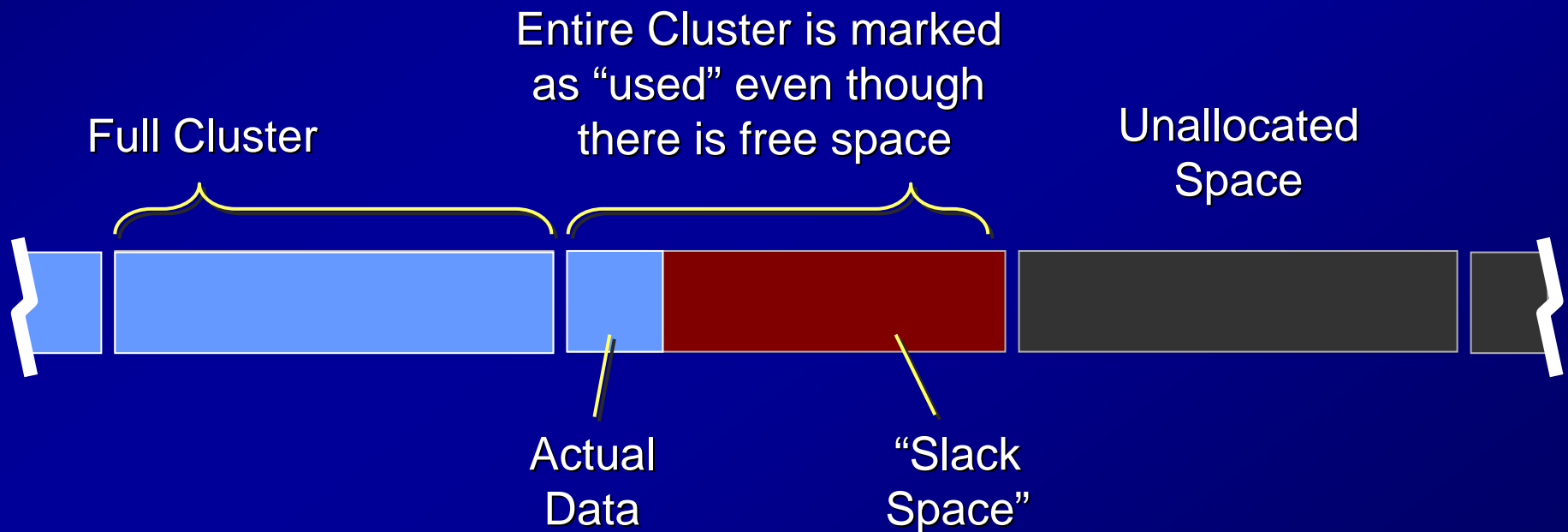
---

- Each time data is written to a cluster...
  - The entire cluster is marked “allocated” (occupied).



# When you write a file...

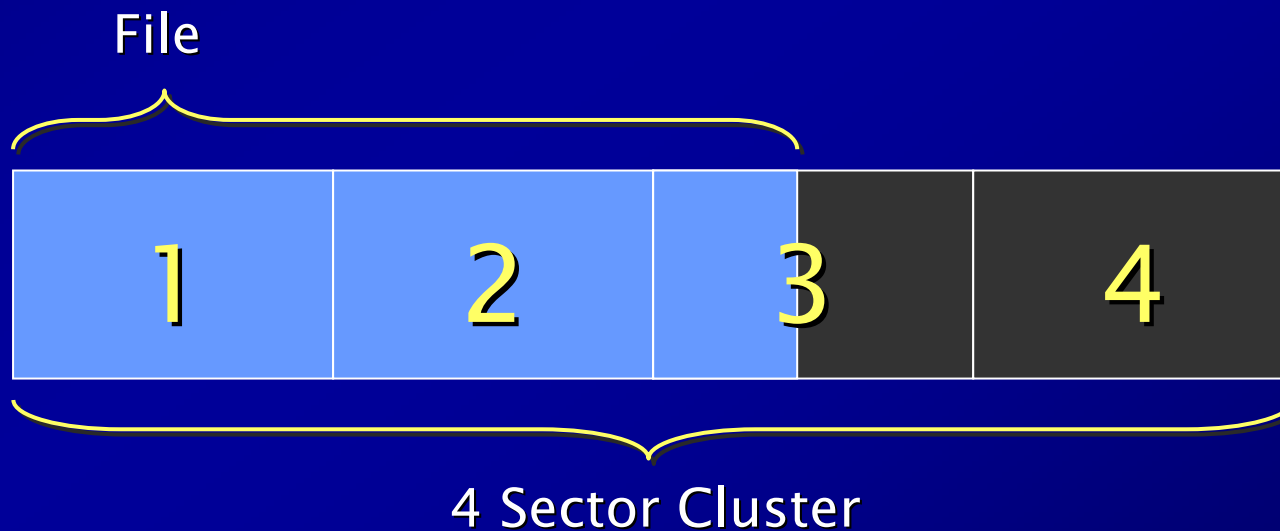
- Each time data is written to a cluster...
  - The entire cluster is marked “allocated” (occupied).
  - Even if only one byte of data is actually used.



# Slack Space

---

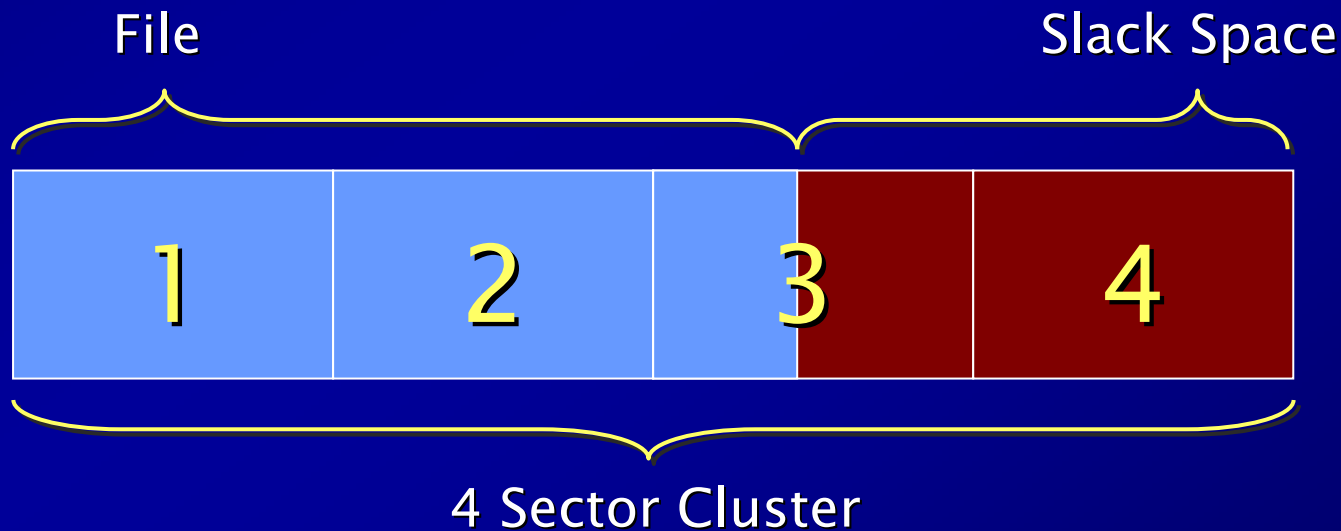
- This cluster is comprised of four 512-byte sectors, occupied by a file of approximately 2.5 sectors (1280 bytes) in length.



# Slack Space

---

- This cluster is comprised of four 512-byte sectors, occupied by a file of approximately 2.5 sectors (1280 bytes) in length.
- The Remainder of Sector 3 and all of Sector 4 is “Slack Space.” Similar to an audio tape recording.



# When you delete files...

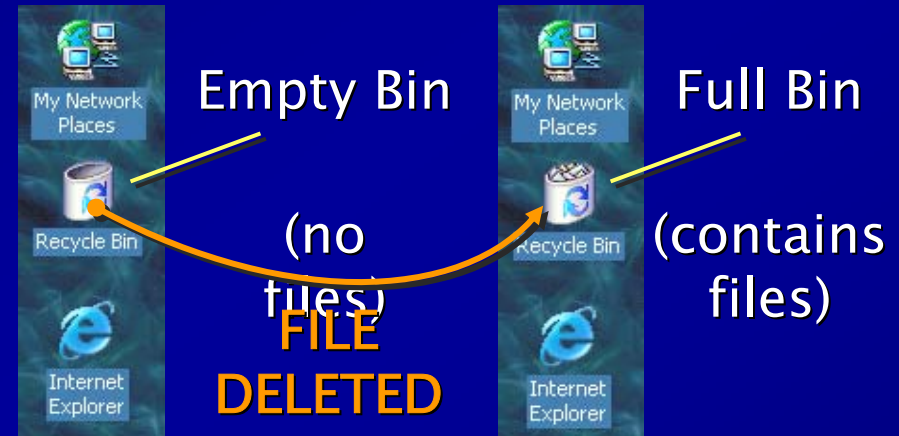
---

- Multiple-step process



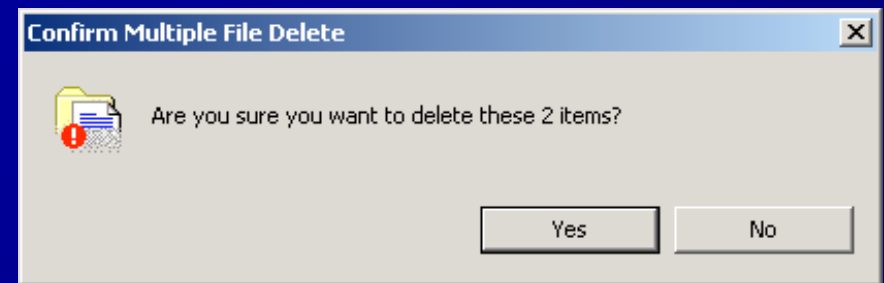
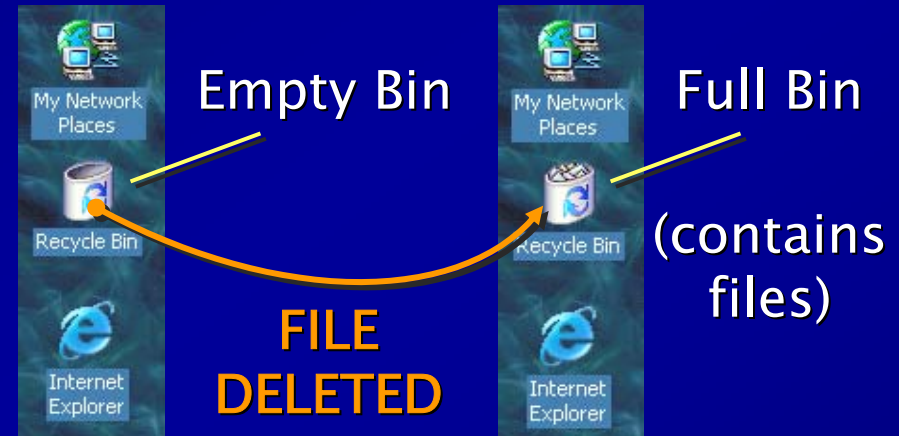
# When you delete files...

- Multiple-step process
  - Deleting moves files to the recycle bin



# When you delete files...

- Multiple-step process
  - Deleting moves files to the recycle bin
  - Recycle bin must be manually emptied, with a confirmation dialog, to actually “delete” the files

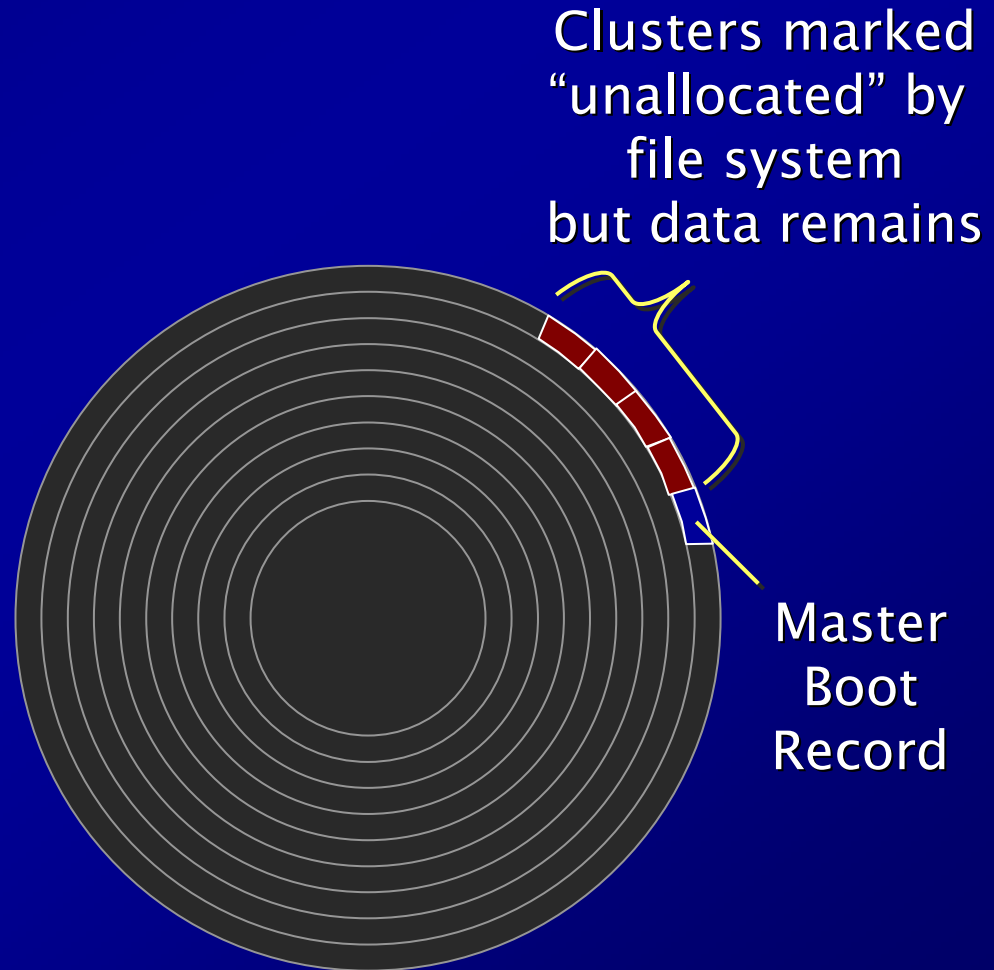


Delete Confirmation Dialog

# But are the files REALLY gone?

---

- No —
  - But the files (data) are now in “unallocated” (unoccupied) clusters, and are available to be written over.
  - Although the files disappear to most users, the data remains, and is recoverable.

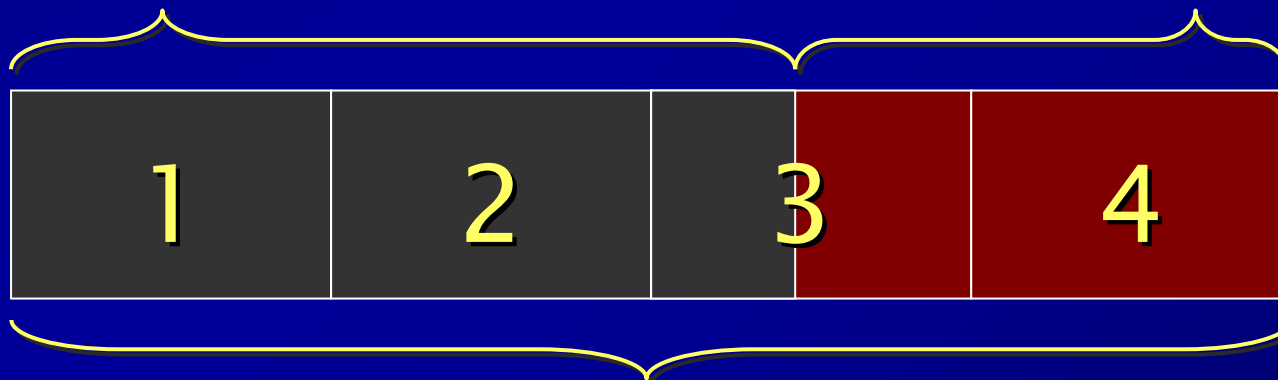


# How do you completely delete files?

- Files are not fully deleted unless they are overwritten or the disk is actually “wiped.”

Old File data  
Continues to exist  
until overwritten

Slack Space  
often includes portions  
of previous files



4 Sector Cluster

# What is file fragmentation?

---

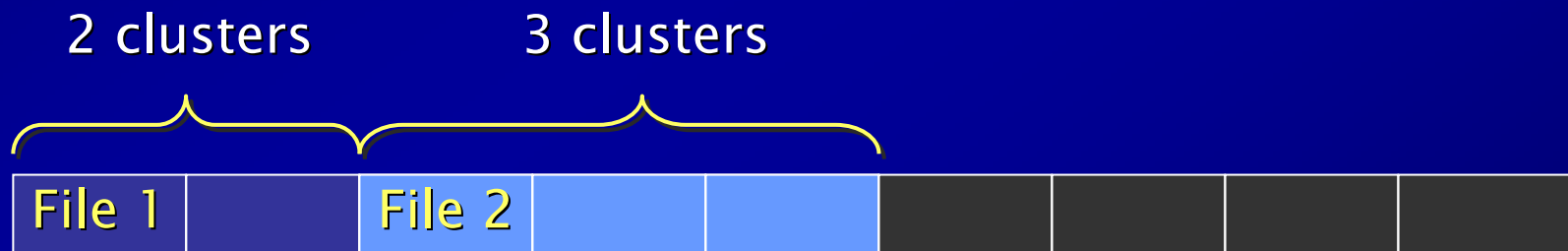
- A disk contains 2 files,
  - File 1 is 2 clusters



# What is file fragmentation?

---

- A disk contains 2 files,
  - File 1 is 2 clusters
  - File 2 in 3 clusters



# What is file fragmentation?

---

- A disk contains 2 files,
  - File 1 is 2 clusters
  - File 2 in 3 clusters
- File 1, a 2-cluster file, is deleted

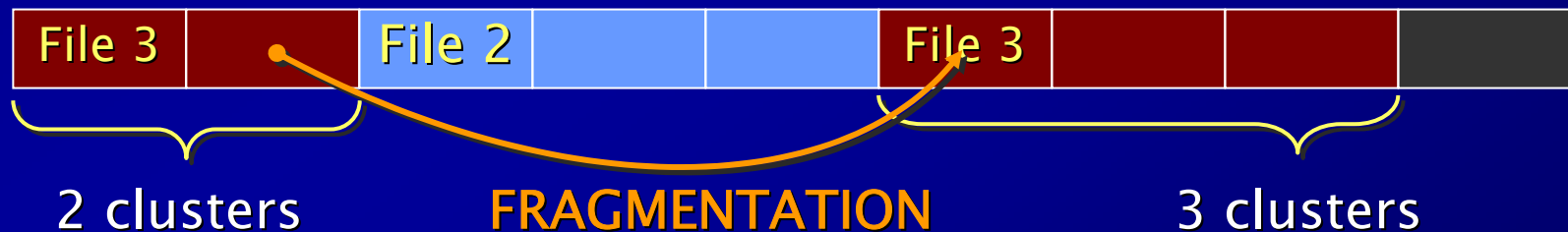


2 clusters become available

# What is file fragmentation?

---

- A disk contains 2 files,
  - File 1 is 2 clusters
  - File 2 in 3 clusters
- File 1, a 2-cluster file, is Deleted
- File 3, a **5-cluster** file, is Saved
  - File 3 now exists in two file fragments



# Writing a file to a fragmented HDD

- After use, fewer and fewer contiguous clusters remain. Most new files are saved with fragmentation, and disk fragmentation increases over time, while old file data remains in unallocated space.

New files are rarely in contiguous clusters as drive becomes fragmented.

 Old/Existing File Data

