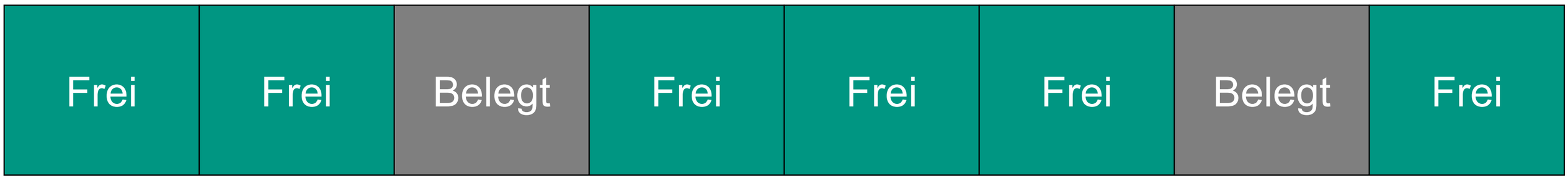
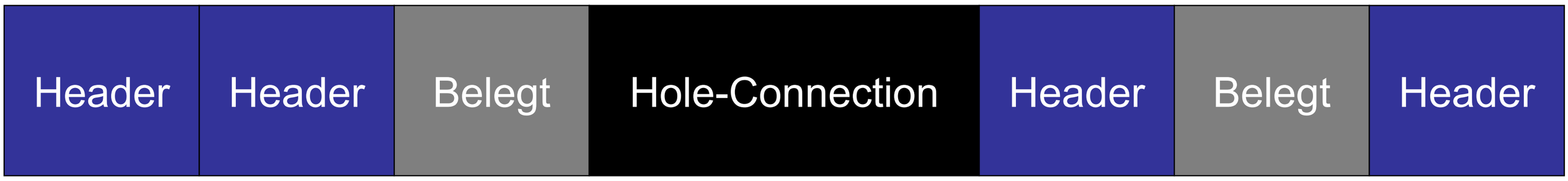


Schritt 0: Ausgangszustand des Hauptspeichers.

Schritt 1: Pool-Grooming führt zu Headerblöcken im Hauptspeicher.

Schritt 2: Die Hole-Connection belegt einen Bereich im Hauptspeicher.



Schritt 3: Zweites Pool-Grooming erstellt zusätzliche Headerblöcke.

Schritt 4: Abbruch der Hole-Connection führt zu freiem Speicherplatz.

Schritt 5: Ein Umgewandeltes Datenpaket wird im erzeugten freien Speicher abgelegt. Es folgt ein Buffer-Overflow in den anliegenden Header.