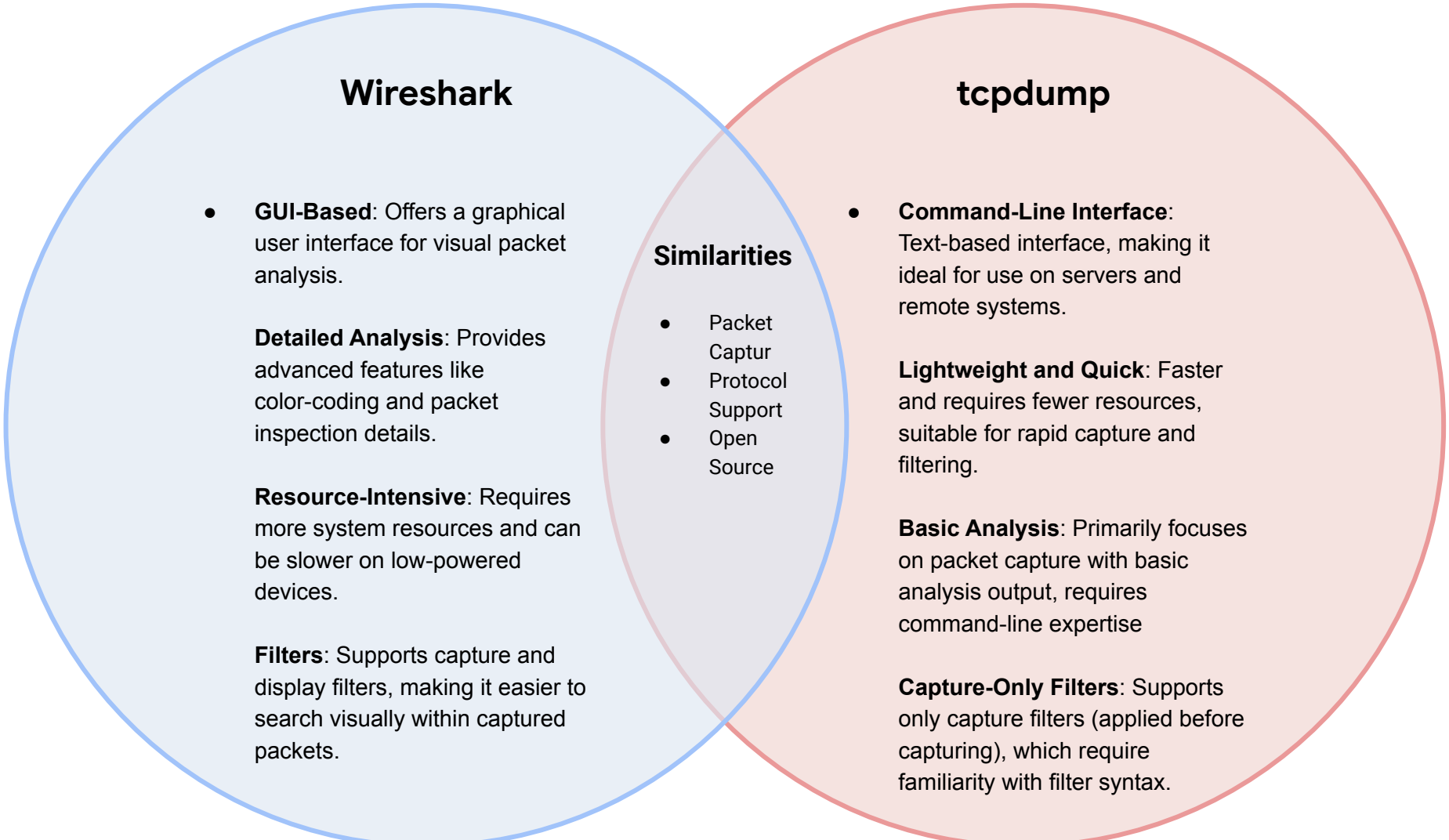
Wireshark
GUI-Based: Offers a graphical user interface for visual packet analysis.
Detailed Analysis: Provides advanced features like color-coding and packet inspection details.
Resource-Intensive: Requires more system resources and can be slower on low-powered devices.
Filters: Supports capture and display filters, making it easier to search visually within captured packets.
Similarities
Packet Captur
Protocol Support
Open Source
tcpdump
Command-Line Interface: Text-based interface, making it ideal for use on servers and remote systems.
Lightweight and Quick: Faster and requires fewer resources, suitable for rapid capture and filtering.
Basic Analysis: Primarily focuses on packet capture with basic analysis output, requires command-line expertise
Capture-Only Filters: Supports only capture filters (applied before capturing), which require familiarity with filter syntax.