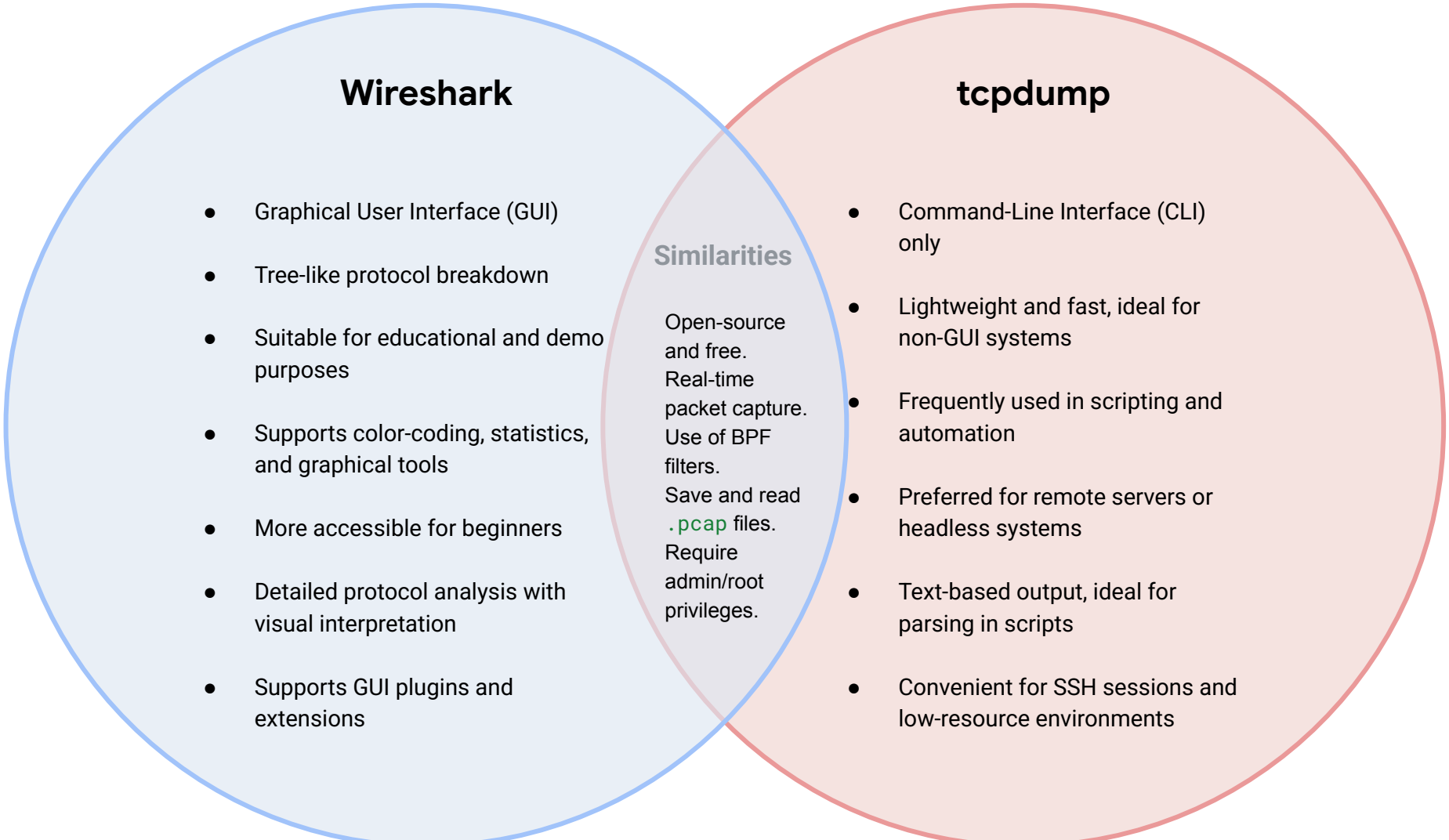
Wireshark
Graphical User Interface (GUI)
Tree-like protocol breakdown
Suitable for educational and demo purposes
Supports color-coding, statistics, and graphical tools
More accessible for beginners
Detailed protocol analysis with visual interpretation
Supports GUI plugins and extensions
Similarities
Open-source and free.
Real-time packet capture.
Use of BPF filters.
Save and read .pcap files.
Require admin/root privileges.
tcpdump
Command-Line Interface (CLI) only
Lightweight and fast, ideal for non-GUI systems
Frequently used in scripting and automation
Preferred for remote servers or headless systems
Text-based output, ideal for parsing in scripts
Convenient for SSH sessions and low-resource environments