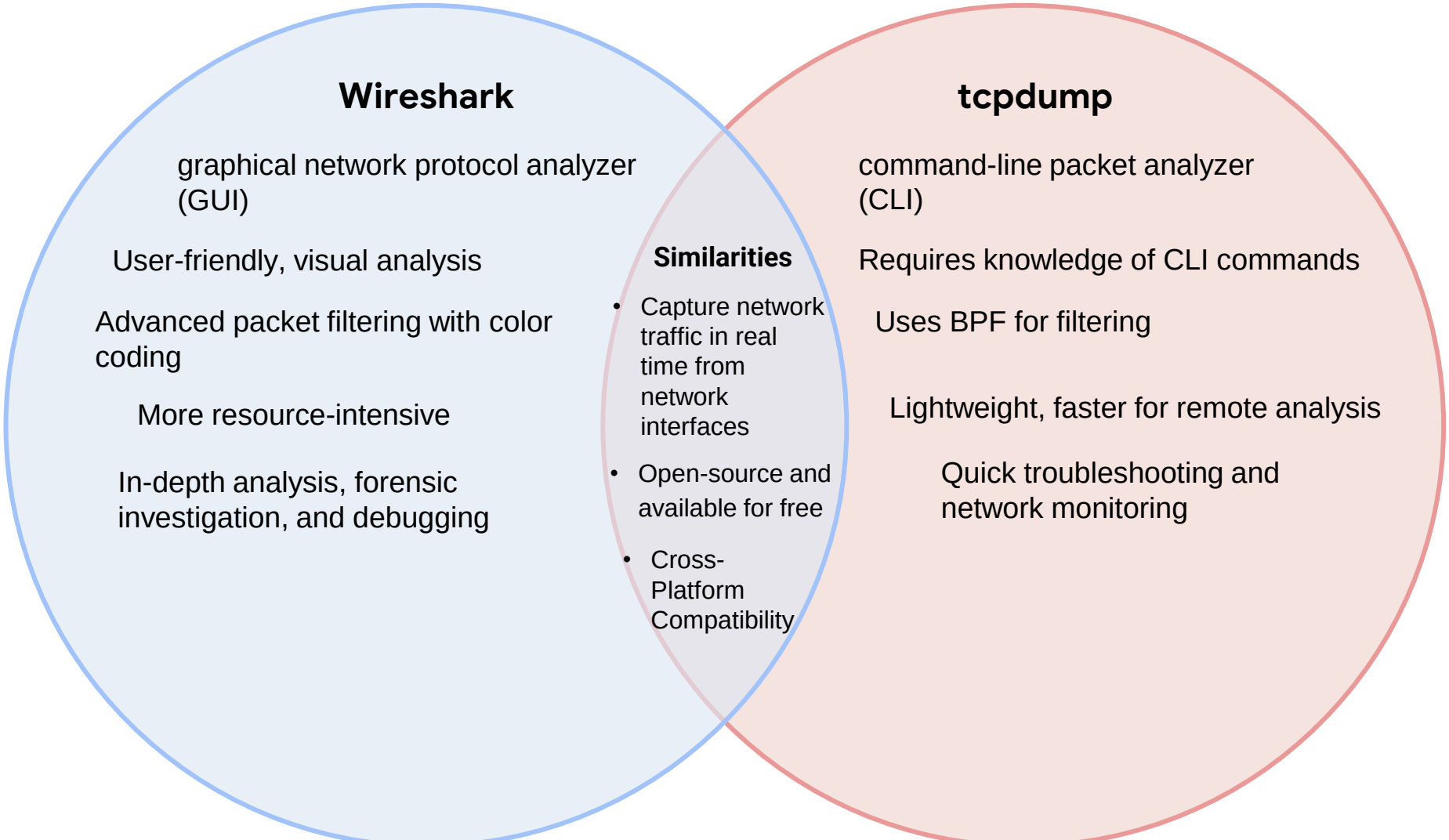
Wireshark
graphical network protocol analyzer (GUI)
User-friendly, visual analysis
Advanced packet filtering with color coding
More resource-intensive
In-depth analysis, forensic investigation, and debugging
Similarities
Capture network traffic in real time from network interfaces
Open-source and available for free
Cross-Platform Compatibility
tcpdump
command-line packet analyzer (CLI)
Requires knowledge of CLI commands
Uses BPF for filtering
Lightweight, faster for remote analysis
Quick troubleshooting and network monitoring