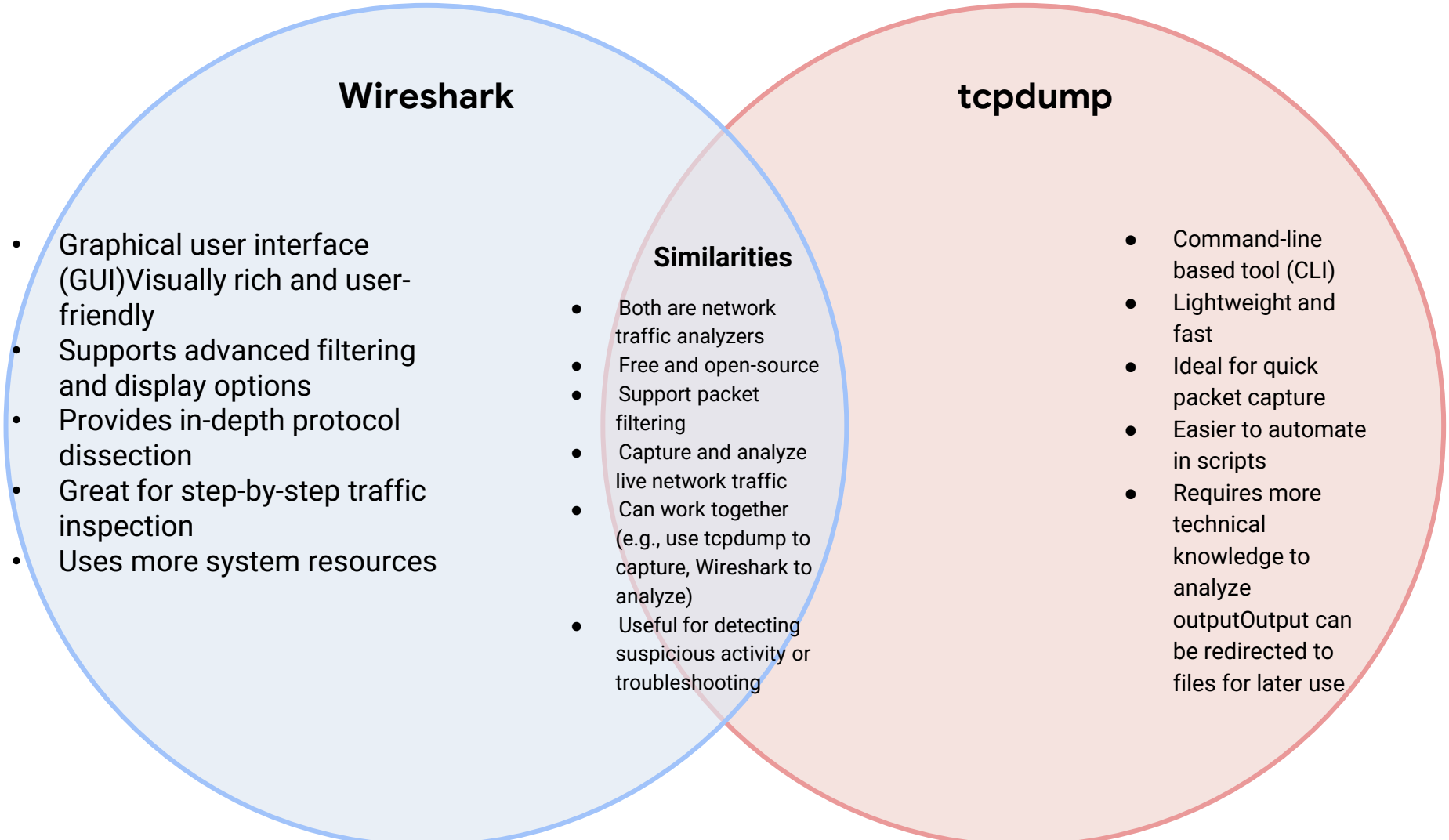
Wireshark
Graphical user interface (GUI)Visually rich and user-friendly
Supports advanced filtering and display options
Provides in-depth protocol dissection
Great for step-by-step traffic inspection
Uses more system resources
Similarities
Both are network traffic analyzers
Free and open-source
Support packet filtering
Capture and analyze live network traffic
Can work together (e.g., use tcpdump to capture, Wireshark to analyze)
Useful for detecting suspicious activity or troubleshooting
tcpdump
Command-line based tool (CLI)
Lightweight and fast
Ideal for quick packet capture
Easier to automate in scripts
Requires more technical knowledge to analyze outputOutput can be redirected to files for later use