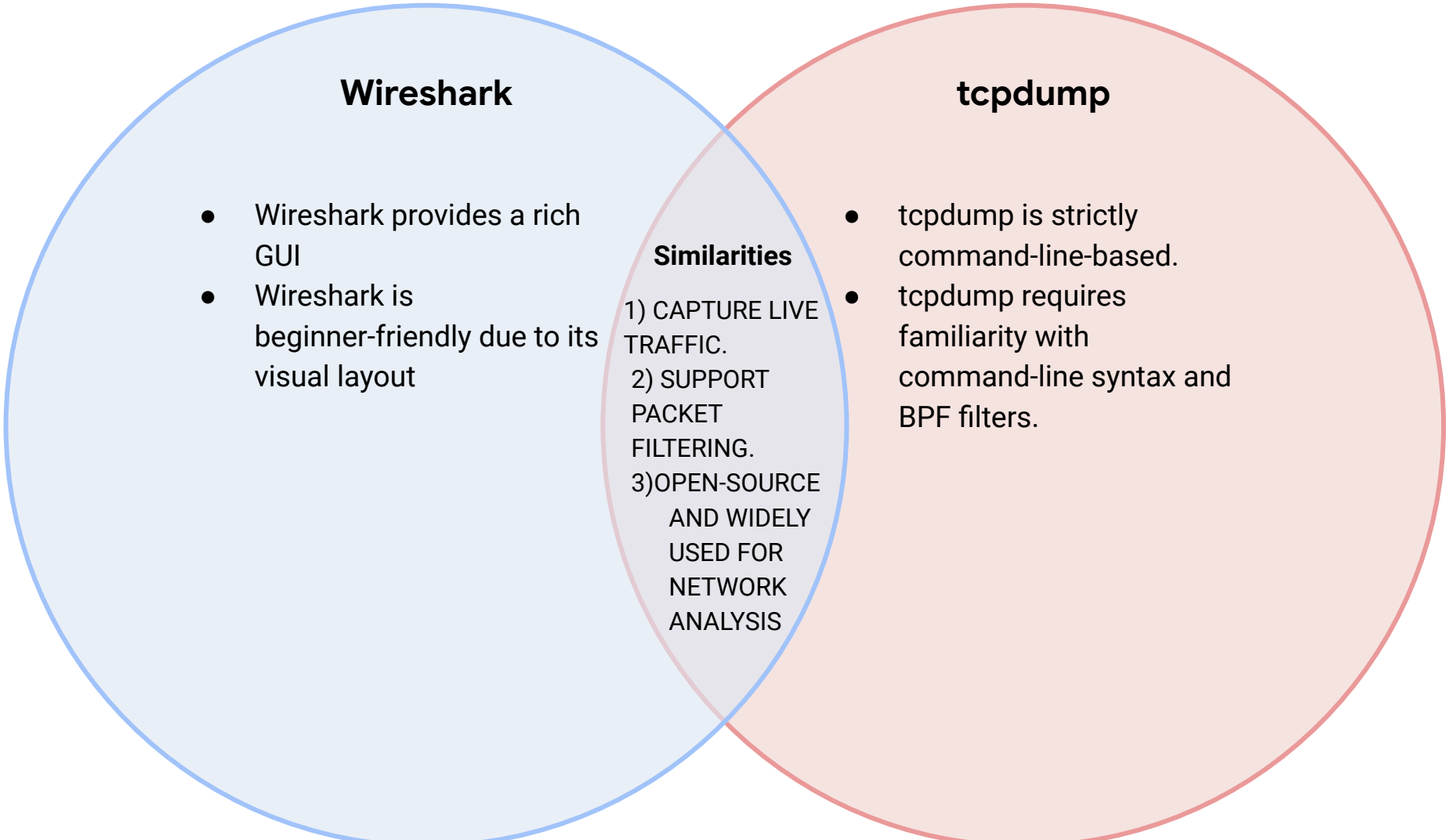
Wireshark
Wireshark provides a rich GUI
Wireshark is beginner-friendly due to its visual layout
Similarities
1) CAPTURE LIVE TRAFFIC.
2) SUPPORT PACKET FILTERING.
3)OPEN-SOURCE AND WIDELY USED FOR NETWORK ANALYSIS
tcpdump
tcpdump is strictly command-line-based.
tcpdump requires familiarity with command-line syntax and BPF filters.