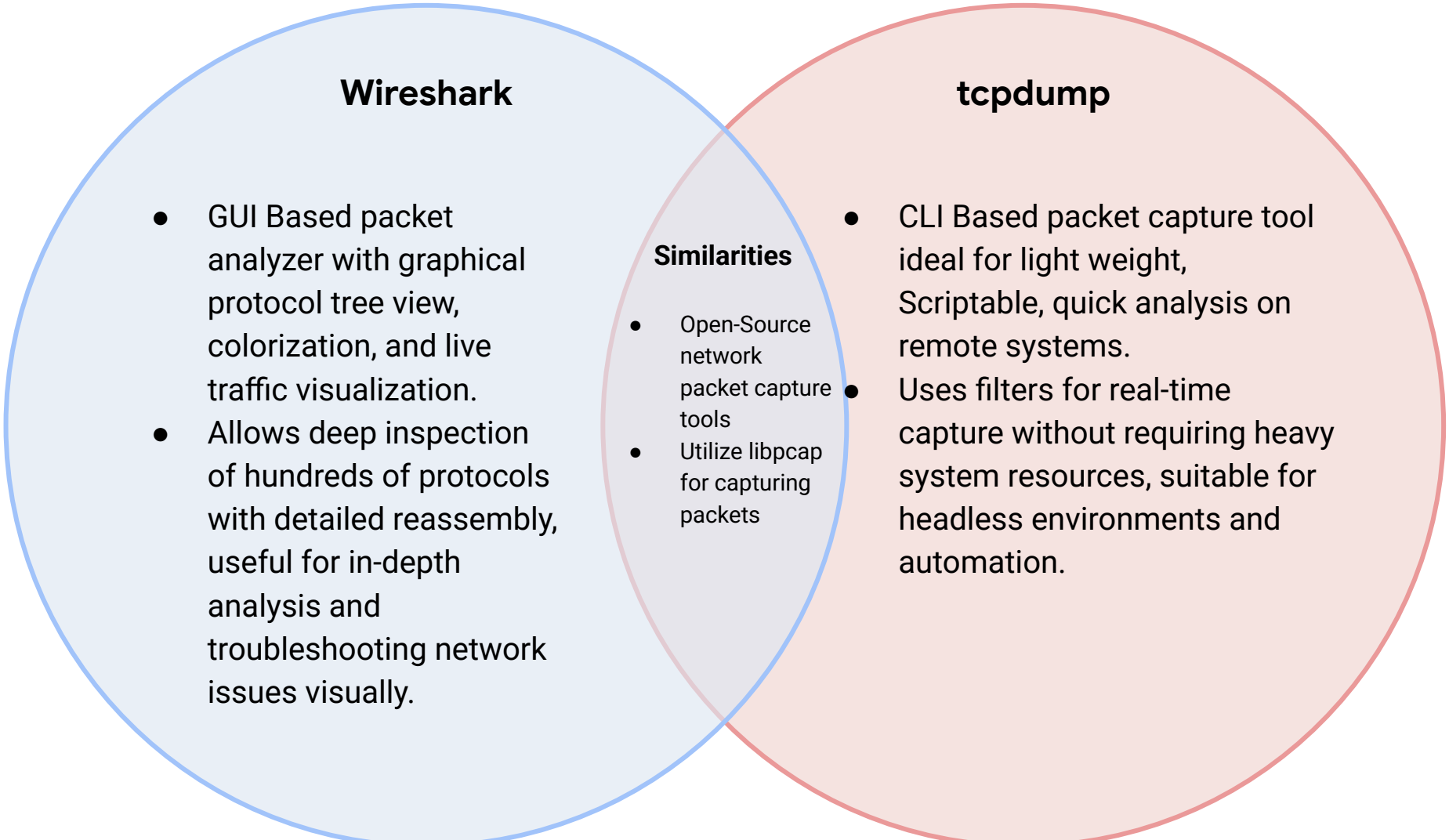
Wireshark
GUI Based packet analyzer with graphical protocol tree view, colorization, and live traffic visualization.
Allows deep inspection of hundreds of protocols with detailed reassembly, useful for in-depth analysis and troubleshooting network issues visually.
Similarities
Open-Source network packet capture tools
Utilize libpcap for capturing packets
tcpdump
CLI Based packet capture tool ideal for light weight, Scriptable, quick analysis on remote systems.
Uses filters for real-time capture without requiring heavy system resources, suitable for headless environments and automation.