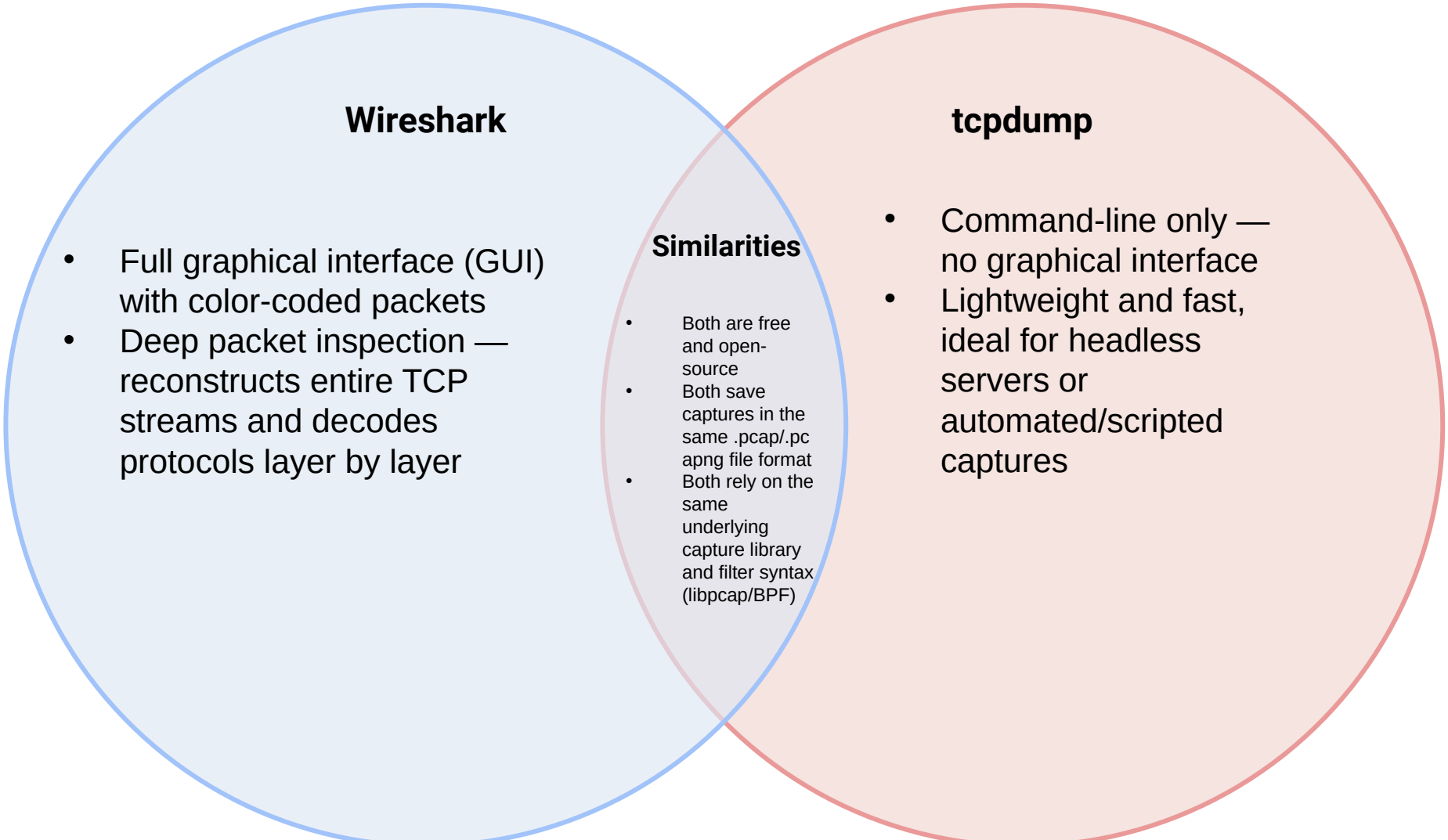

Wireshark
Full graphical interface (GUI) with color-coded packets
Deep packet inspection — reconstructs entire TCP streams and decodes protocols layer by layer
Similarities
Both are free and open-source
Both save captures in the same .pcap/.pcapng file format
Both rely on the same underlying capture library and filter syntax (libpcap/BPF)
tcpdump
Command-line only — no graphical interface
Lightweight and fast, ideal for headless servers or automated/scripted captures