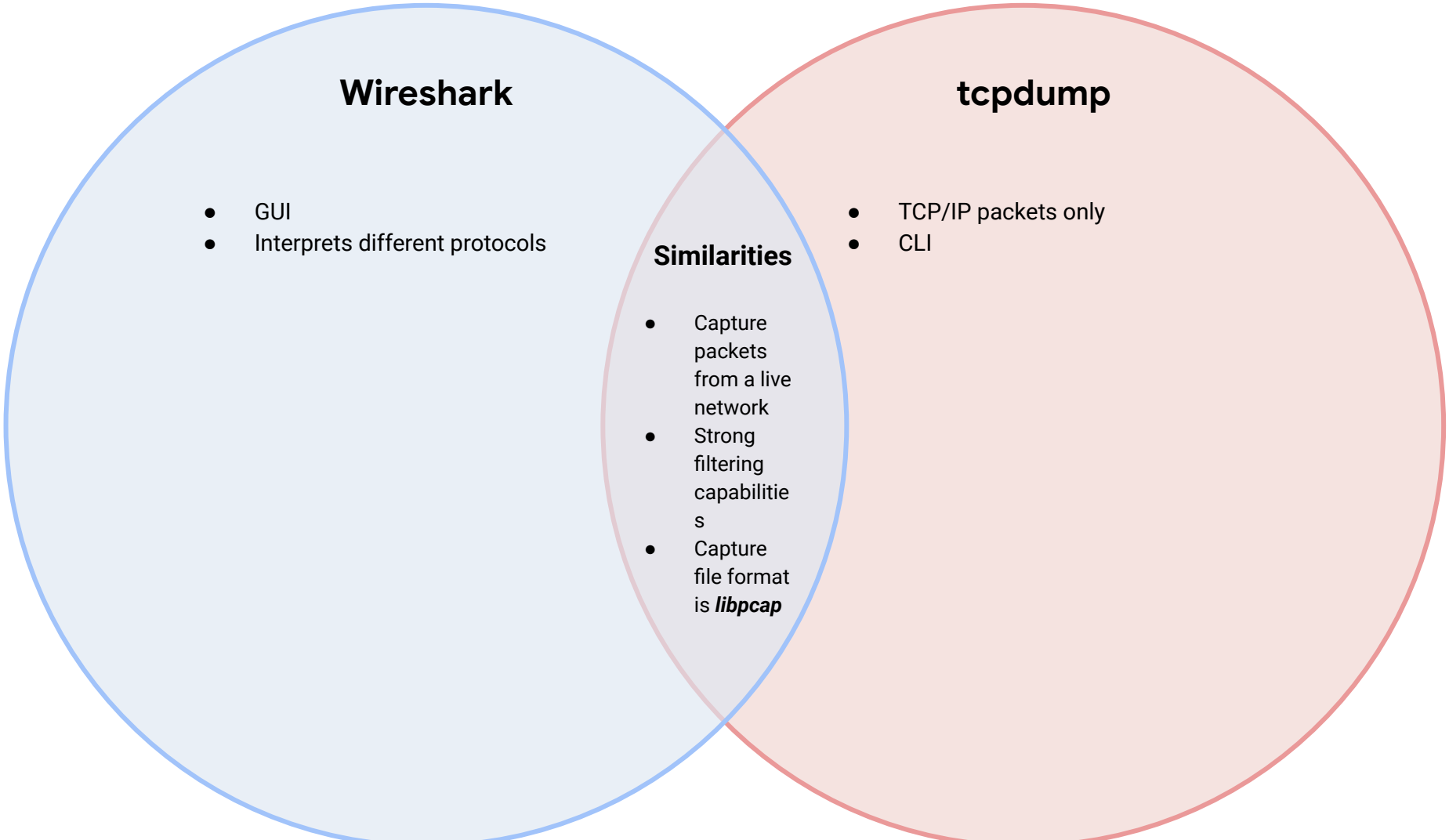
Wireshark
GUI
Interprets different protocols
Similarities
Capture packets from a live network
Strong filtering capabilities
Capture file format is libpcap
tcpdump
TCP/IP packets only
CLI