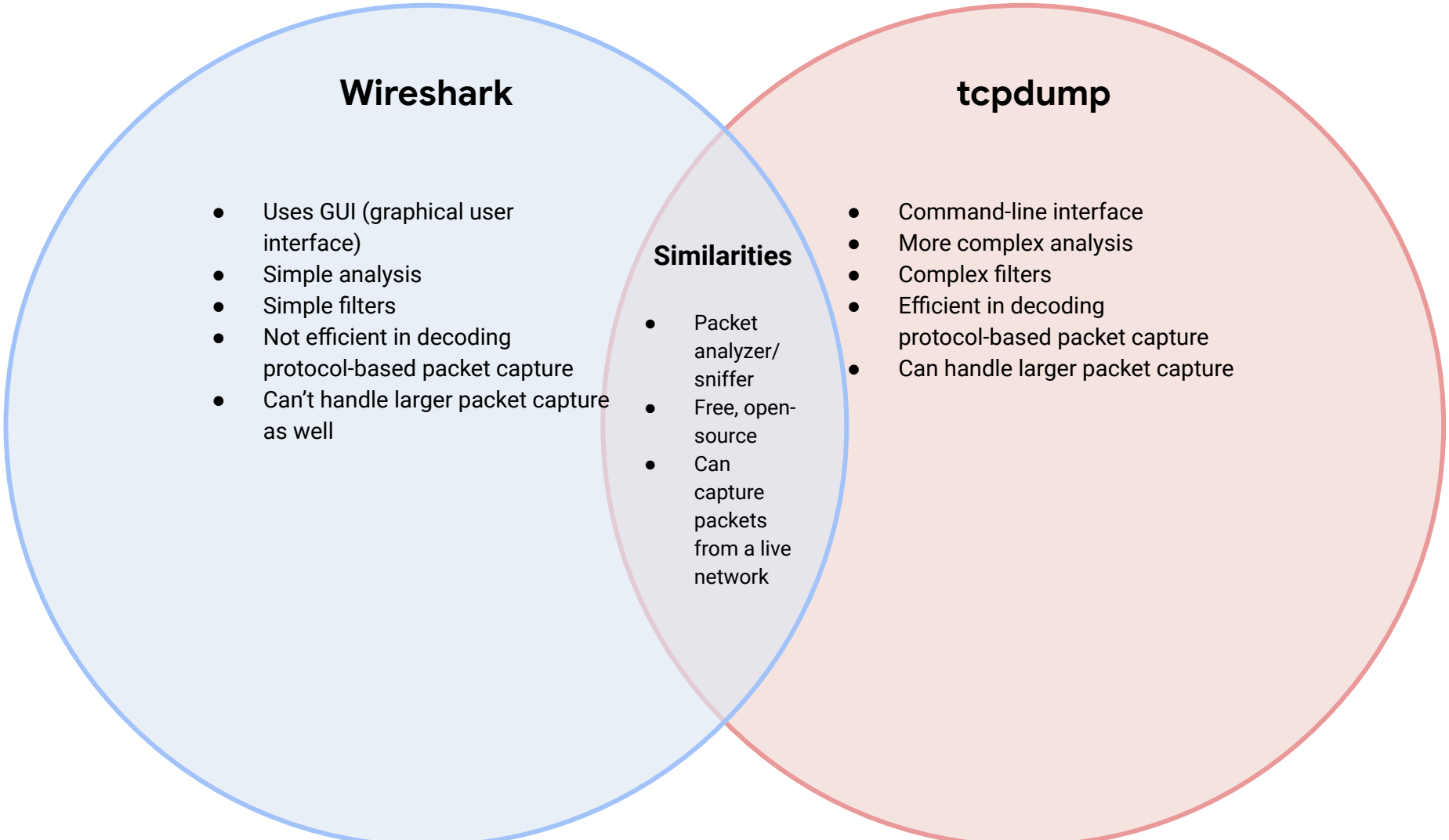
Wireshark
Uses GUI (graphical user interface)
Simple analysis
Simple filters
Not efficient in decoding protocol-based packet capture
Can't handle larger packet capture as well
Similarities
Packet analyzer/ sniffer
Free, open-source
Can capture packets from a live network
tcpdump
Command-line interface
More complex analysis
Complex filters
Efficient in decoding protocol-based packet capture
Can handle larger packet capture