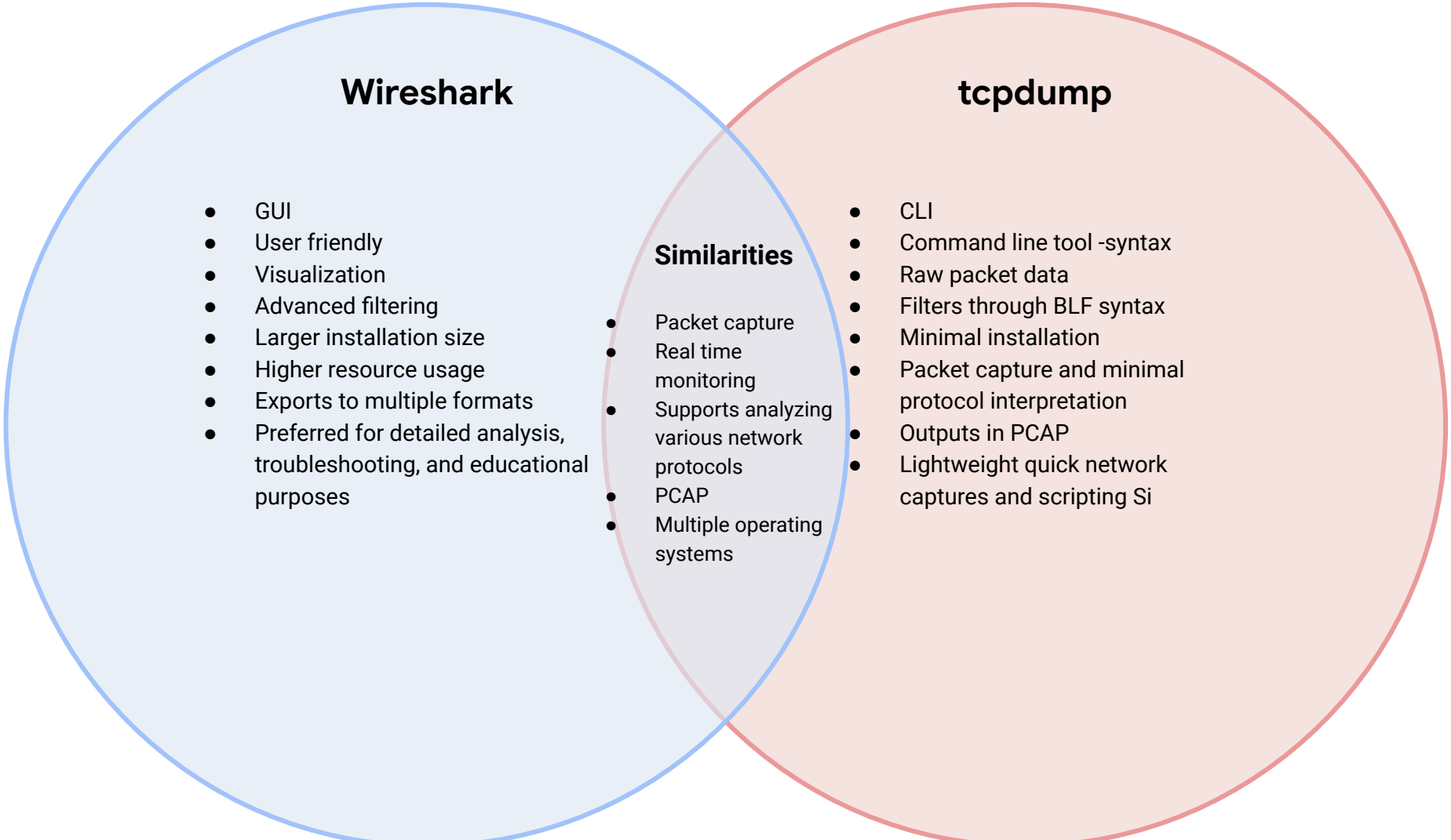
Wireshark
GUI
User friendly
Visualization
Advanced filtering
Larger installation size
Higher resource usage
Exports to multiple formats
Preferred for detailed analysis, troubleshooting, and educational purposes
Similarities
Packet capture
Real time monitoring
Supports analyzing various network protocols
PCAP
Multiple operating systems
tcpdump
CLI
Command line tool -syntax
Raw packet data
Filters through BLF syntax
Minimal installation
Packet capture and minimal protocol interpretation
Outputs in PCAP
Lightweight quick network captures and scripting Si