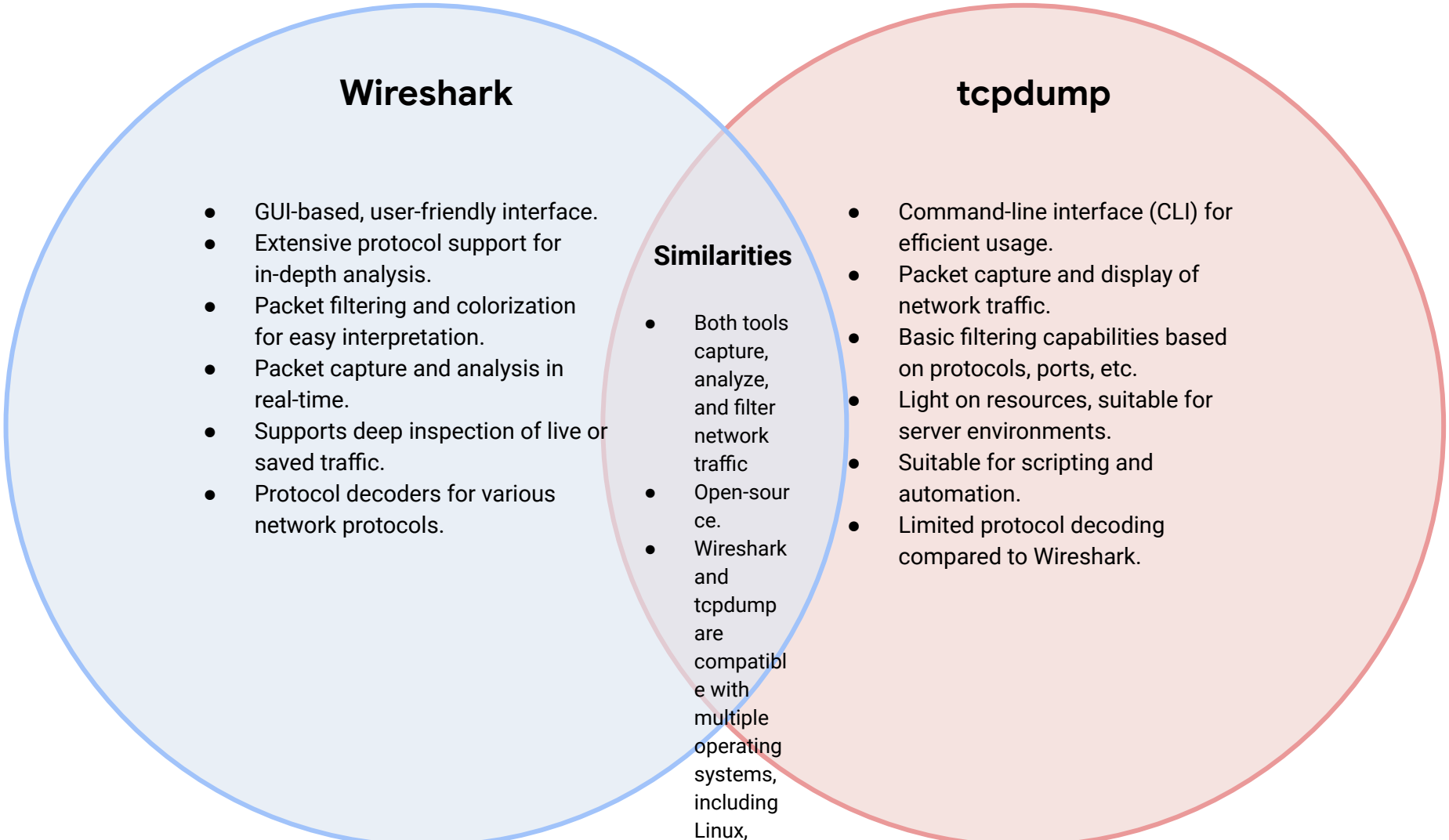
Wireshark
GUI-based, user-friendly interface.
Extensive protocol support for in-depth analysis.
Packet filtering and colorization for easy interpretation.
Packet capture and analysis in real-time.
Supports deep inspection of live or saved traffic.
Protocol decoders for various network protocols.
Similarities
Both tools capture, analyze, and filter network traffic
Open-source.
Wireshark and tcpdump are compatible with multiple operating systems, including Linux,
tcpdump
Command-line interface (CLI) for efficient usage.
Packet capture and display of network traffic.
Basic filtering capabilities based on protocols, ports, etc.
Light on resources, suitable for server environments.
Suitable for scripting and automation.
Limited protocol decoding compared to Wireshark.