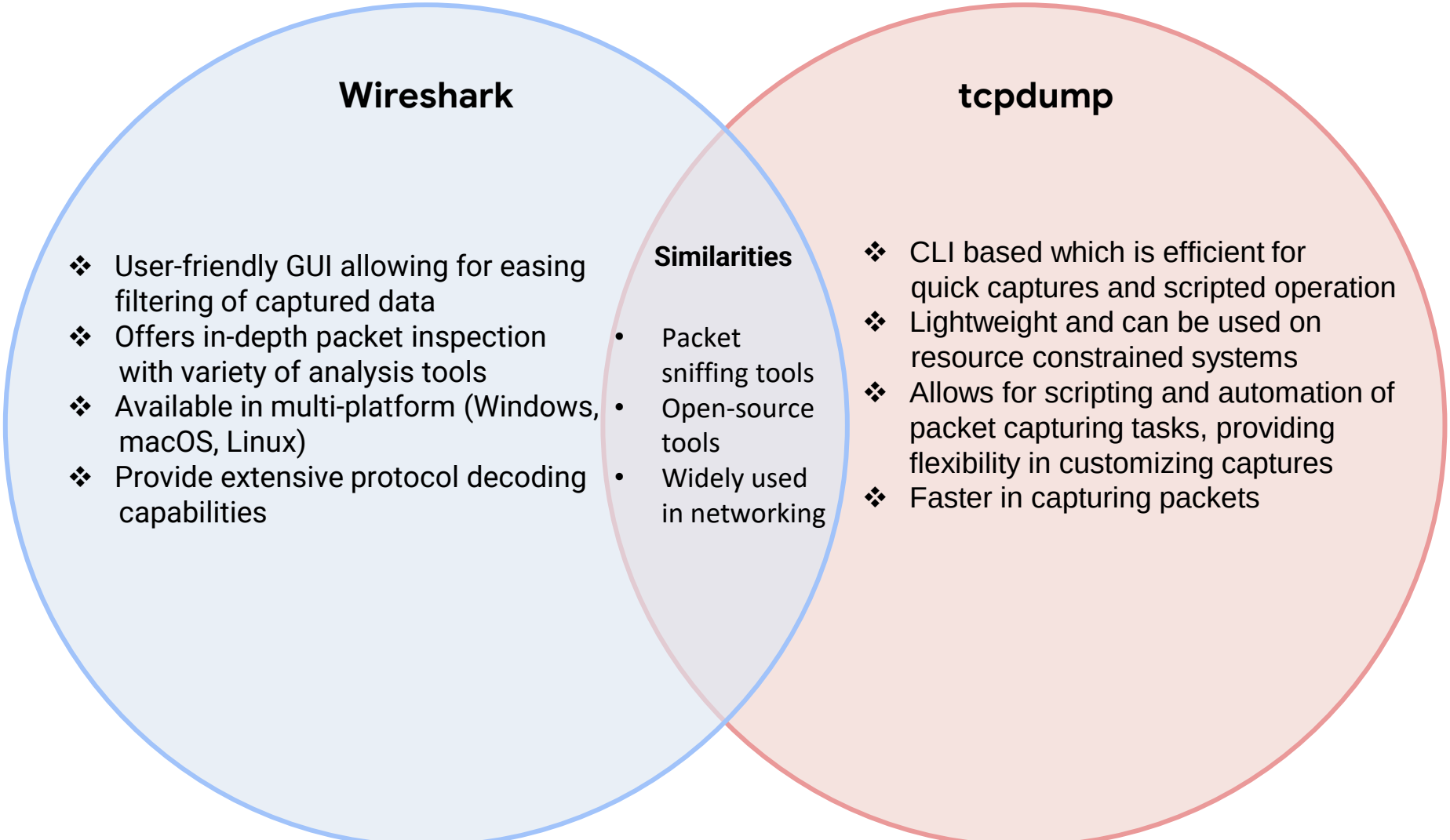
Wireshark
User-friendly GUI allowing for easing filtering of captured data
Offers in-depth packet inspection with variety of analysis tools
Available in multi-platform (Windows, macOS, Linux)
Provide extensive protocol decoding capabilities
Similarities
Packet sniffing tools
Open-source tools
Widely used in networking
tcpdump
CLI based which is efficient for quick captures and scripted operation
Lightweight and can be used on resource constrained systems
Allows for scripting and automation of packet capturing tasks, providing flexibility in customizing captures
Faster in capturing packets