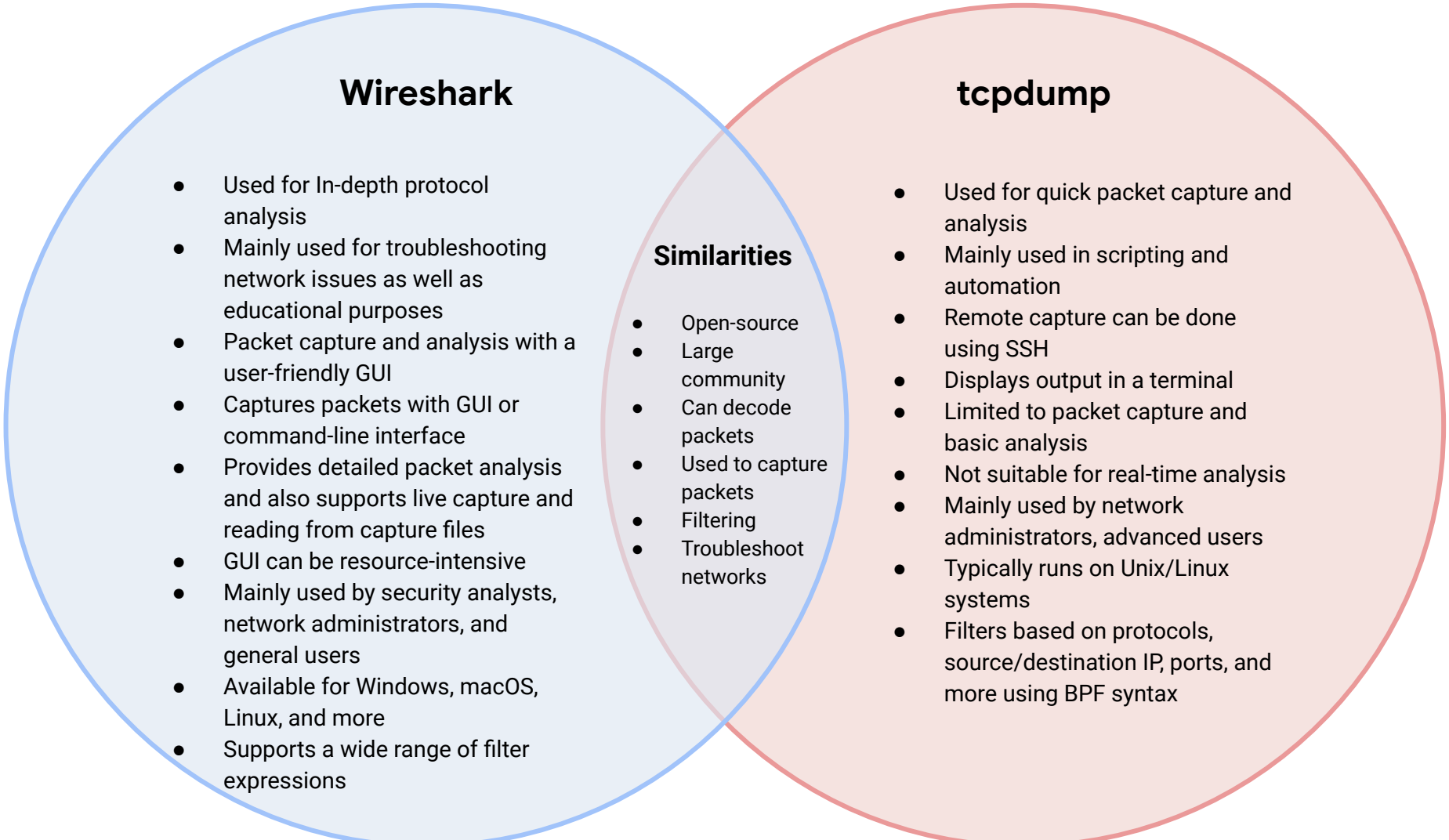
Wireshark
Used for In-depth protocol analysis
Mainly used for troubleshooting network issues as well as educational purposes
Packet capture and analysis with a user-friendly GUI
Captures packets with GUI or command-line interface
Provides detailed packet analysis and also supports live capture and reading from capture files
GUI can be resource-intensive
Mainly used by security analysts, network administrators, and general users
Available for Windows, macOS, Linux, and more
Supports a wide range of filter expressions
Similarities
Open-source
Large community
Can decode packets
Used to capture packets
Filtering
Troubleshoot networks
tcpdump
Used for quick packet capture and analysis
Mainly used in scripting and automation
Remote capture can be done using SSH
Displays output in a terminal
Limited to packet capture and basic analysis
Not suitable for real-time analysis
Mainly used by network administrators, advanced users
Typically runs on Unix/Linux systems
Filters based on protocols, source/destination IP, ports, and more using BPF syntax