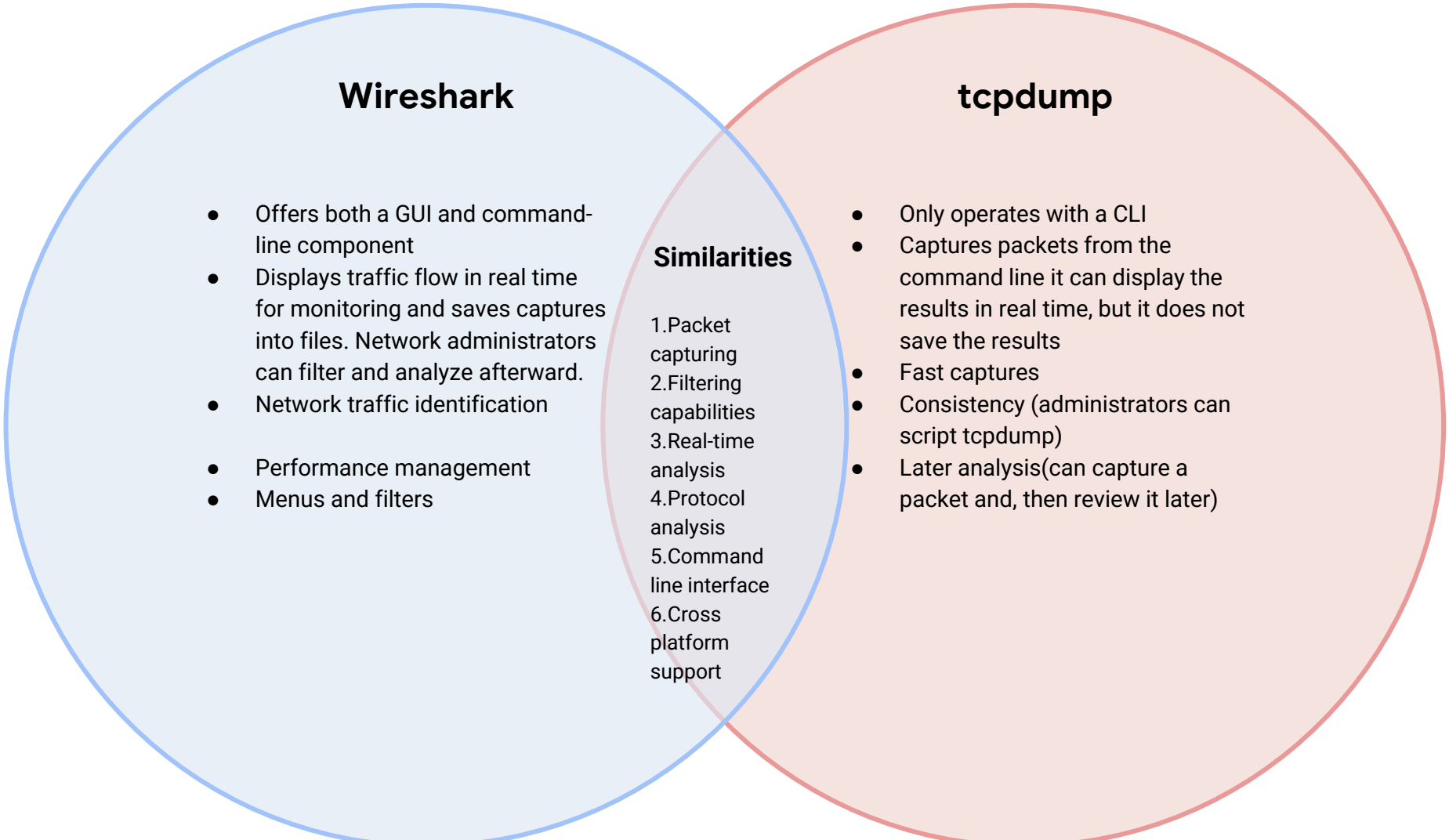
Wireshark
Offers both a GUI and command-line component
Displays traffic flow in real time for monitoring and saves captures into files. Network administrators can filter and analyze afterward.
Network traffic identification
Performance management
Menus and filters
Similarities
1.Packet capturing
2.Filtering capabilities
3.Real-time analysis
4.Protocol analysis
5.Command line interface
6.Cross platform support
tcpdump
Only operates with a CLI
Captures packets from the command line it can display the results in real time, but it does not save the results
Fast captures
Consistency (administrators can script tcpdump)
Later analysis(can capture a packet and, then review it later)