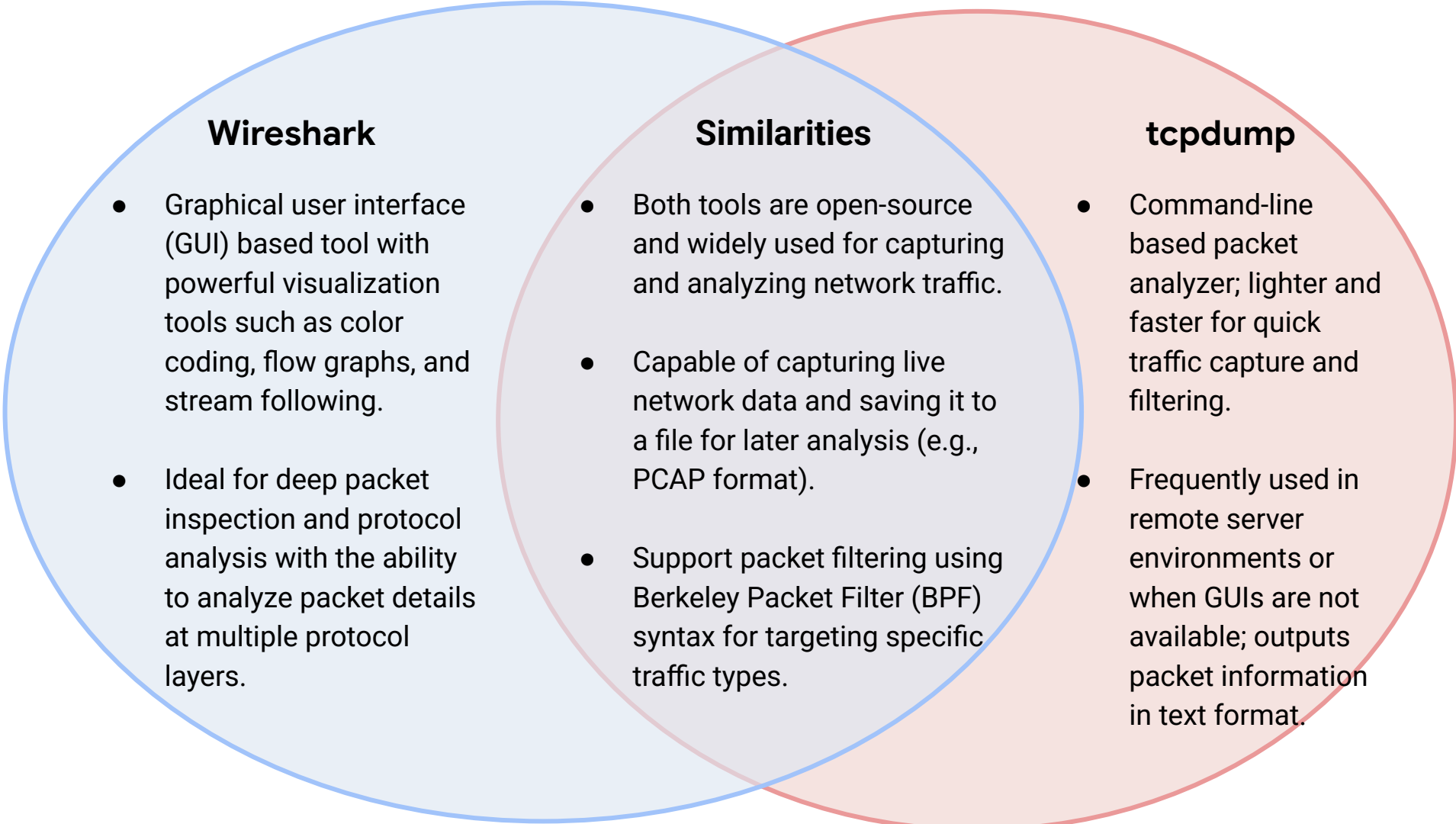
Wireshark
Graphical user interface (GUI) based tool with powerful visualization tools such as color coding, flow graphs, and stream following.
Ideal for deep packet inspection and protocol analysis with the ability to analyze packet details at multiple protocol layers.
Similarities
Both tools are open-source and widely used for capturing and analyzing network traffic.
Capable of capturing live network data and saving it to a file for later analysis (e.g., PCAP format).
Support packet filtering using Berkeley Packet Filter (BPF) syntax for targeting specific traffic types.
tcpdump
Command-line based packet analyzer; lighter and faster for quick traffic capture and filtering.
Frequently used in remote server environments or when GUIs are not available; outputs packet information in text format.