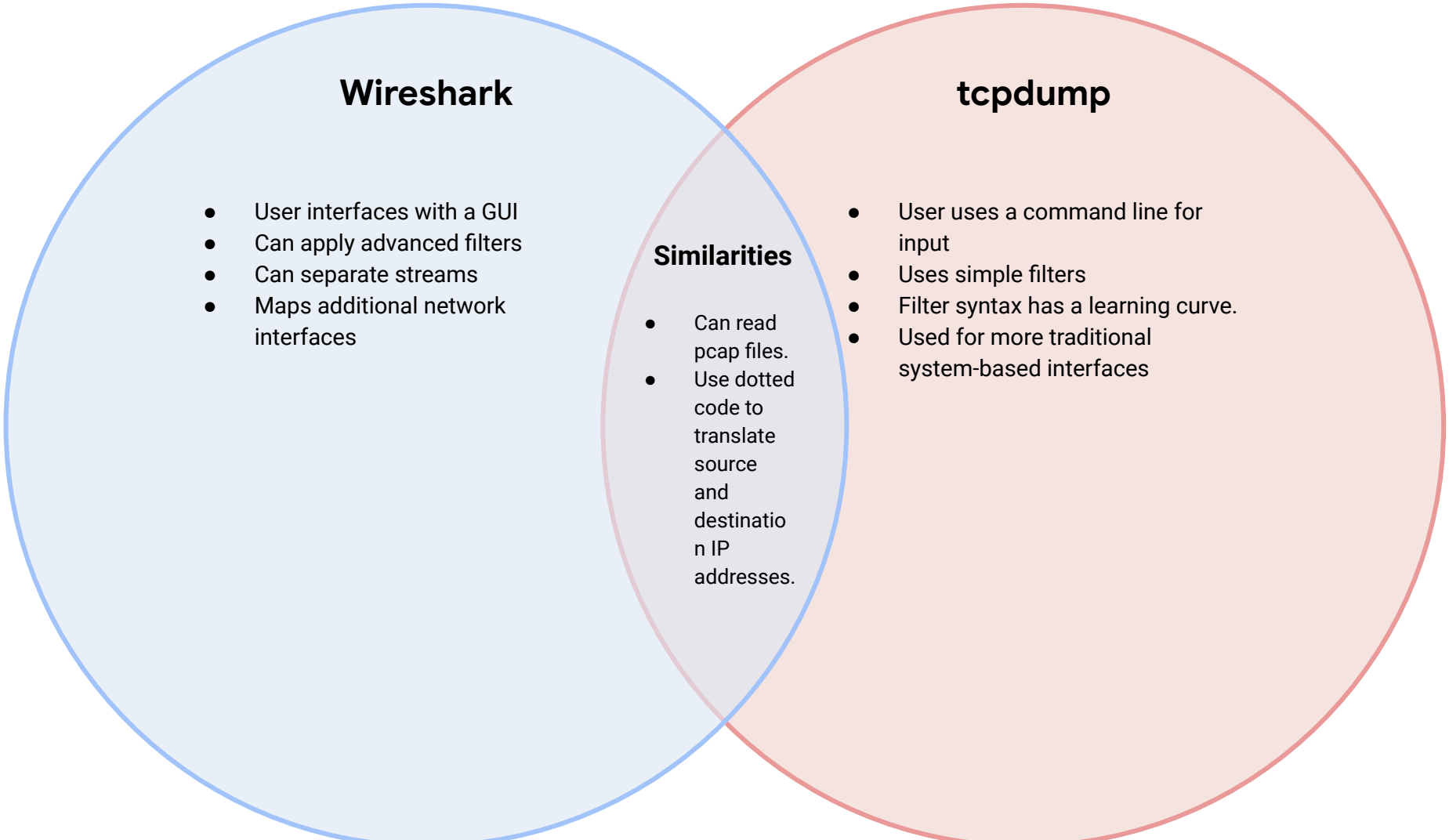
Wireshark
User interfaces with a GUI
Can apply advanced filters
Can separate streams
Maps additional network interfaces
Similarities
Can read pcap files.
Use dotted code to translate source and destination IP addresses.
tcpdump
User uses a command line for input
Uses simple filters
Filter syntax has a learning curve.
Used for more traditional system-based interfaces