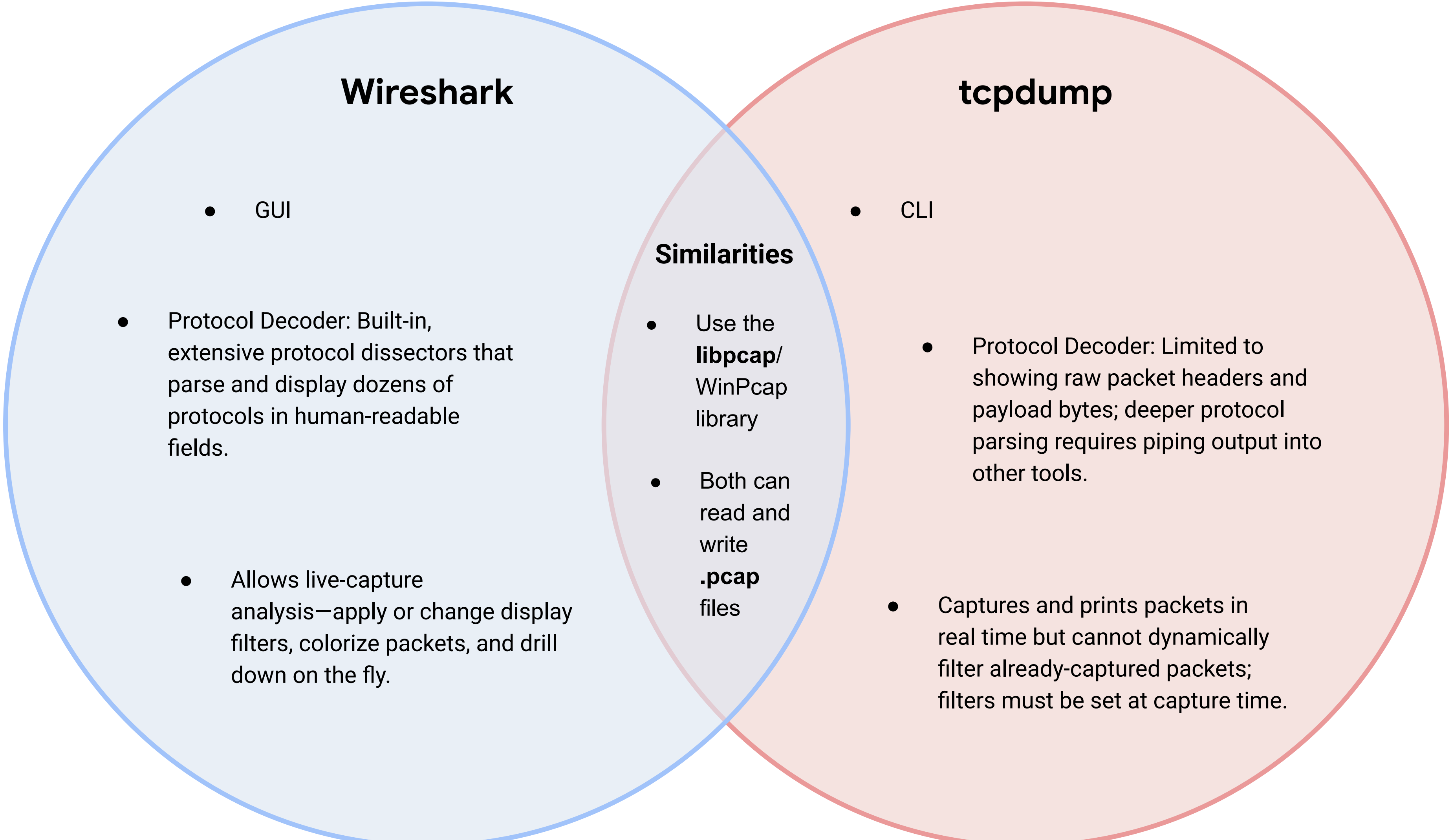

Wireshark

- GUI
- Protocol Decoder: Built-in, extensive protocol dissectors that parse and display dozens of protocols in human-readable fields.
- Allows live-capture analysis—apply or change display filters, colorize packets, and drill down on the fly.

Similarities

- Use the **libpcap**/ WinPcap library
- Both can read and write **.pcap** files

tcpdump

- CLI
- Protocol Decoder: Limited to showing raw packet headers and payload bytes; deeper protocol parsing requires piping output into other tools.
- Captures and prints packets in real time but cannot dynamically filter already-captured packets; filters must be set at capture time.