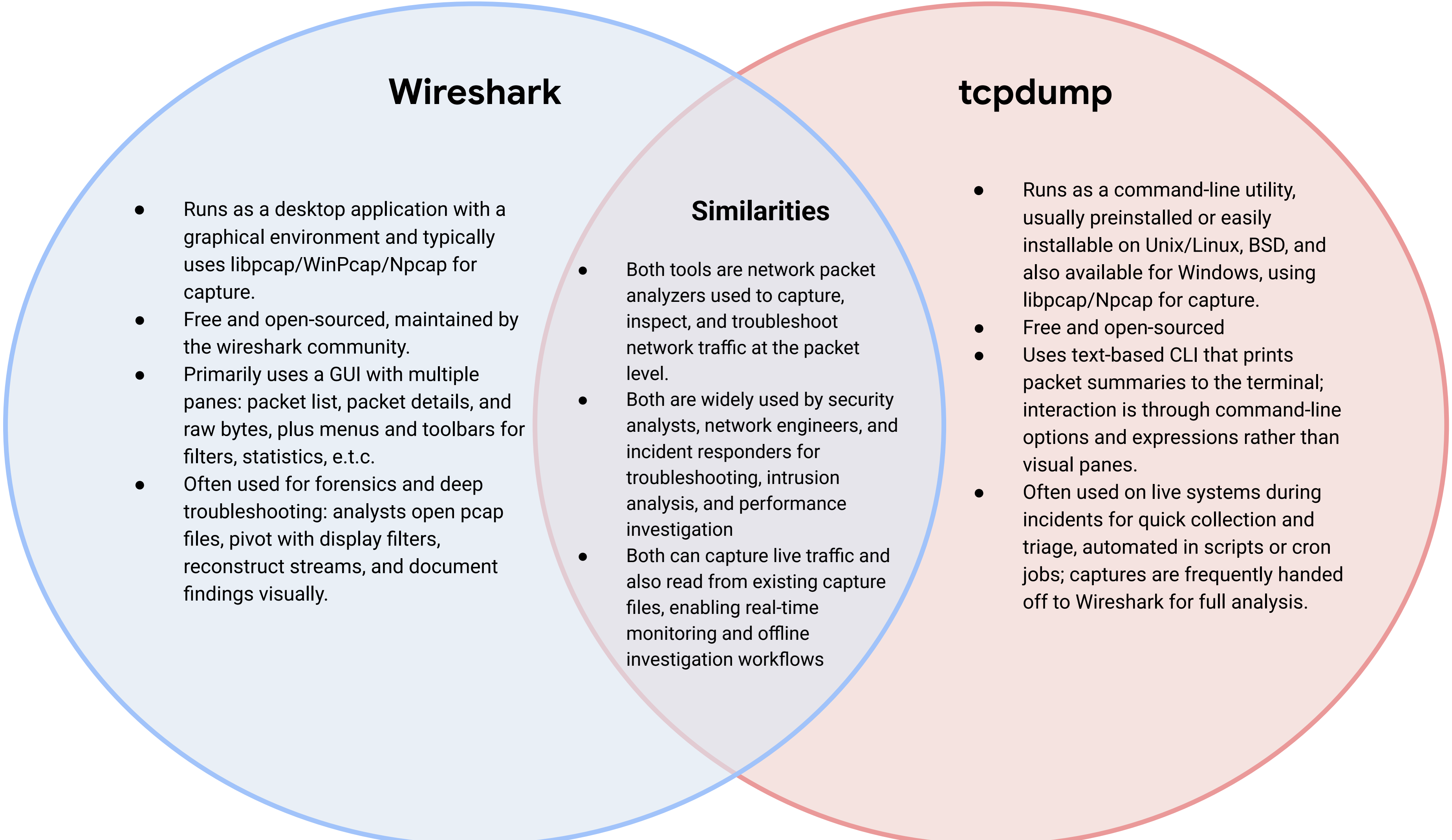

Wireshark

- Runs as a desktop application with a graphical environment and typically uses libpcap/WinPcap/Npcap for capture.
- Free and open-sourced, maintained by the wireshark community.
- Primarily uses a GUI with multiple panes: packet list, packet details, and raw bytes, plus menus and toolbars for filters, statistics, e.t.c.
- Often used for forensics and deep troubleshooting: analysts open pcap files, pivot with display filters, reconstruct streams, and document findings visually.

Similarities

- Both tools are network packet analyzers used to capture, inspect, and troubleshoot network traffic at the packet level.
- Both are widely used by security analysts, network engineers, and incident responders for troubleshooting, intrusion analysis, and performance investigation
- Both can capture live traffic and also read from existing capture files, enabling real-time monitoring and offline investigation workflows

tcpdump

- Runs as a command-line utility, usually preinstalled or easily installable on Unix/Linux, BSD, and also available for Windows, using libpcap/Npcap for capture.
- Free and open-sourced
- Uses text-based CLI that prints packet summaries to the terminal; interaction is through command-line options and expressions rather than visual panes.
- Often used on live systems during incidents for quick collection and triage, automated in scripts or cron jobs; captures are frequently handed off to Wireshark for full analysis.