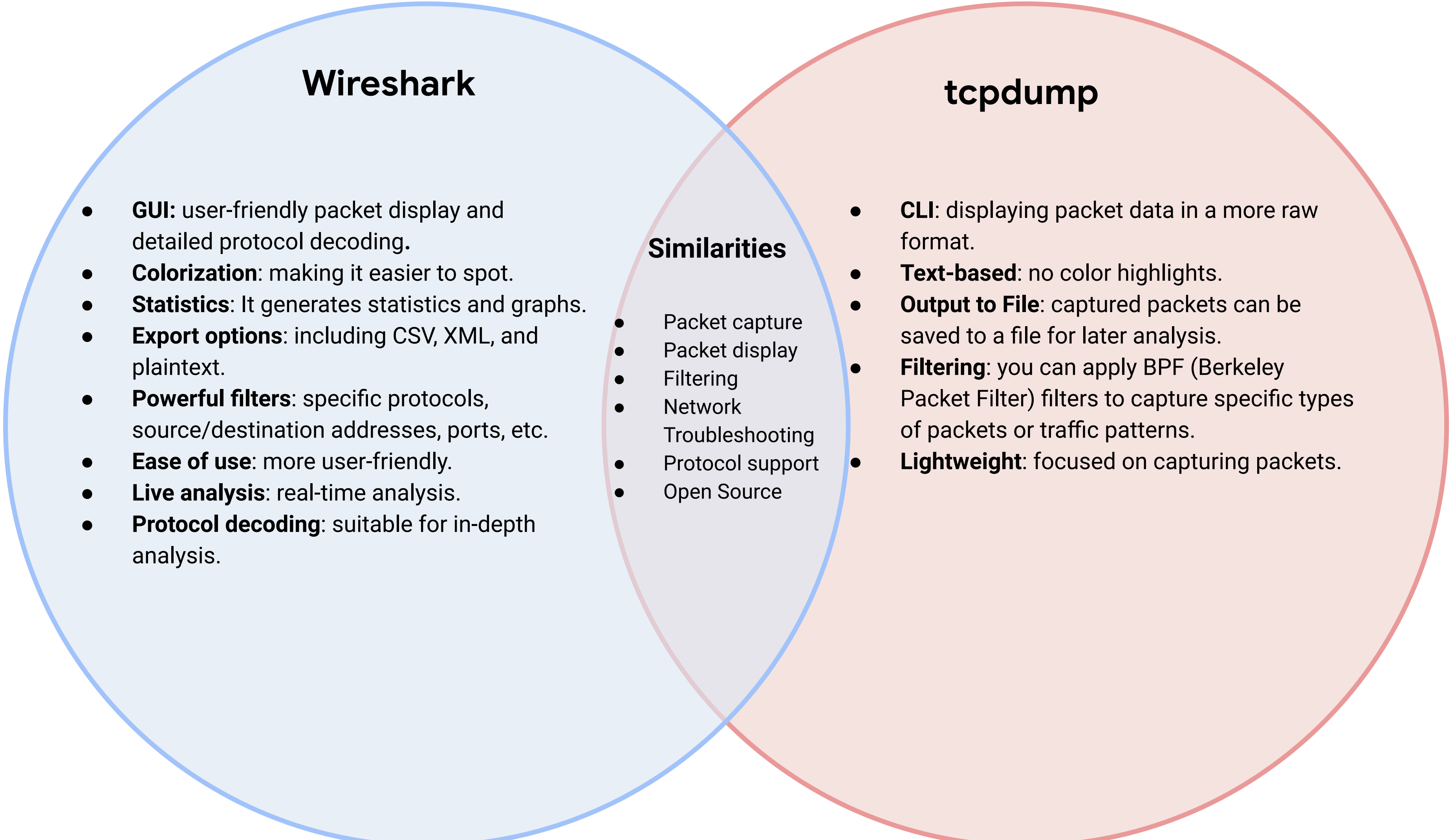

Wireshark

- **GUI:** user-friendly packet display and detailed protocol decoding.
- **Colorization**: making it easier to spot.
- **Statistics**: It generates statistics and graphs.
- **Export options**: including CSV, XML, and plaintext.
- **Powerful filters**: specific protocols, source/destination addresses, ports, etc.
- **Ease of use**: more user-friendly.
- **Live analysis**: real-time analysis.
- **Protocol decoding**: suitable for in-depth analysis.

Similarities

- Packet capture
- Packet display
- Filtering
- Network Troubleshooting
- Protocol support
- Open Source

tcpdump

- **CLI**: displaying packet data in a more raw format.
- **Text-based**: no color highlights.
- **Output to File**: captured packets can be saved to a file for later analysis.
- **Filtering**: you can apply BPF (Berkeley Packet Filter) filters to capture specific types of packets or traffic patterns.
- **Lightweight**: focused on capturing packets.