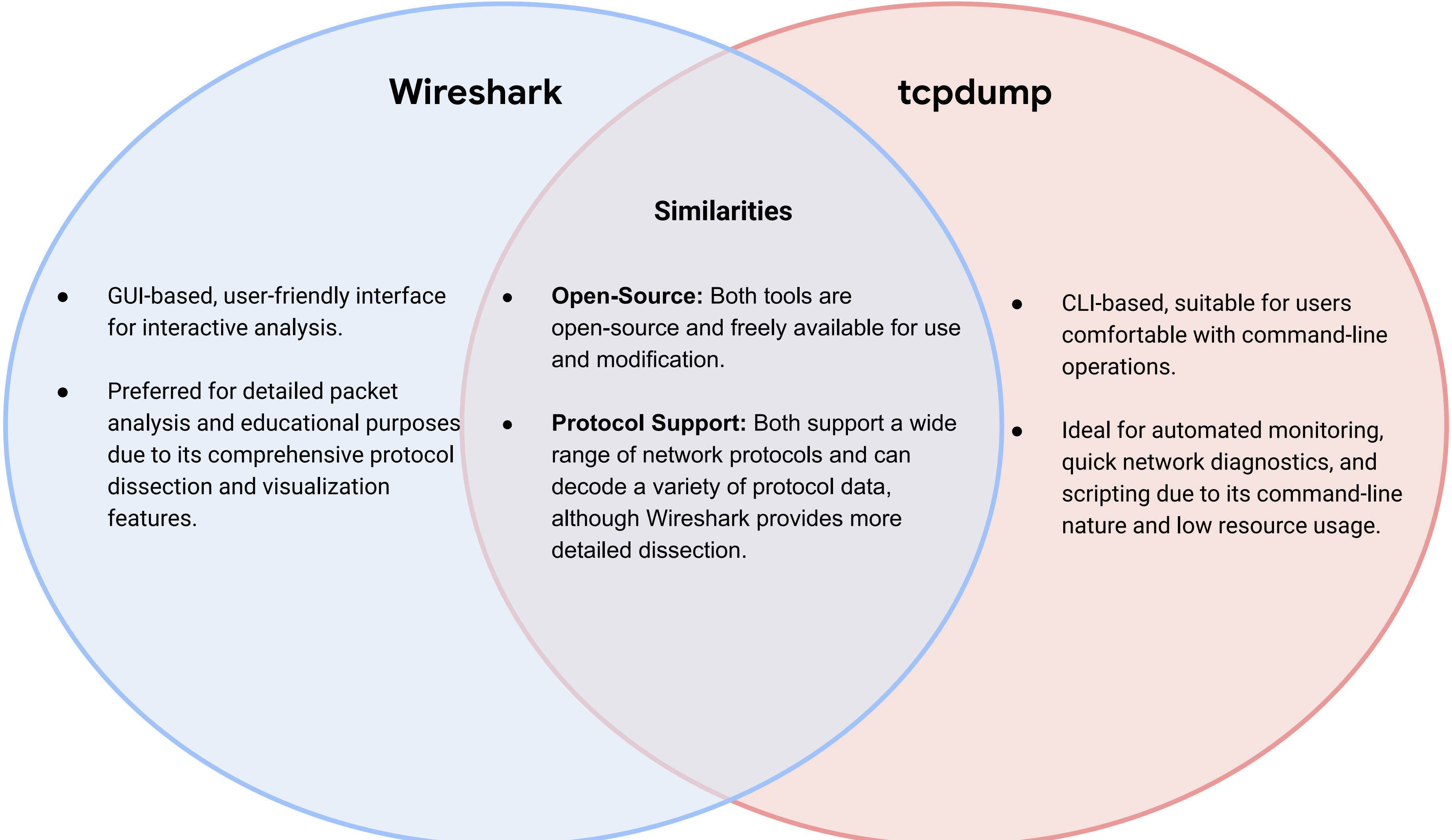

Wireshark

- GUI-based, user-friendly interface for interactive analysis.
- Preferred for detailed packet analysis and educational purposes due to its comprehensive protocol dissection and visualization features.

Similarities

- **Open-Source:** Both tools are open-source and freely available for use and modification.
- **Protocol Support:** Both support a wide range of network protocols and can decode a variety of protocol data, although Wireshark provides more detailed dissection.

tcpdump

- CLI-based, suitable for users comfortable with command-line operations.
- Ideal for automated monitoring, quick network diagnostics, and scripting due to its command-line nature and low resource usage.