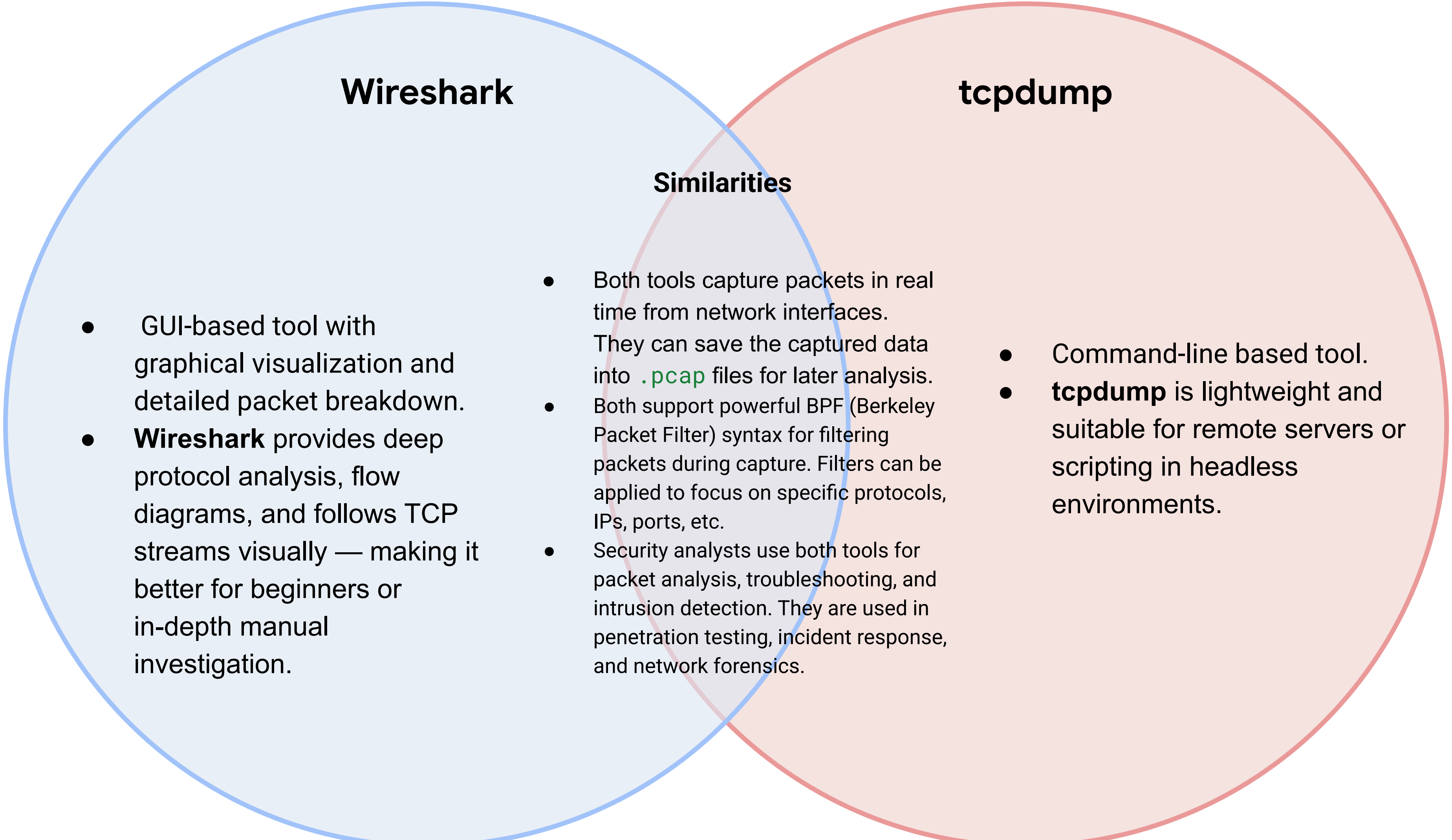

Wireshark

- GUI-based tool with graphical visualization and detailed packet breakdown.
- **Wireshark** provides deep protocol analysis, flow diagrams, and follows TCP streams visually — making it better for beginners or in-depth manual investigation.

Similarities

- Both tools capture packets in real time from network interfaces. They can save the captured data into `.pcap` files for later analysis.
- Both support powerful BPF (Berkeley Packet Filter) syntax for filtering packets during capture. Filters can be applied to focus on specific protocols, IPs, ports, etc.
- Security analysts use both tools for packet analysis, troubleshooting, and intrusion detection. They are used in penetration testing, incident response, and network forensics.

tcpdump

- Command-line based tool.
- **tcpdump** is lightweight and suitable for remote servers or scripting in headless environments.