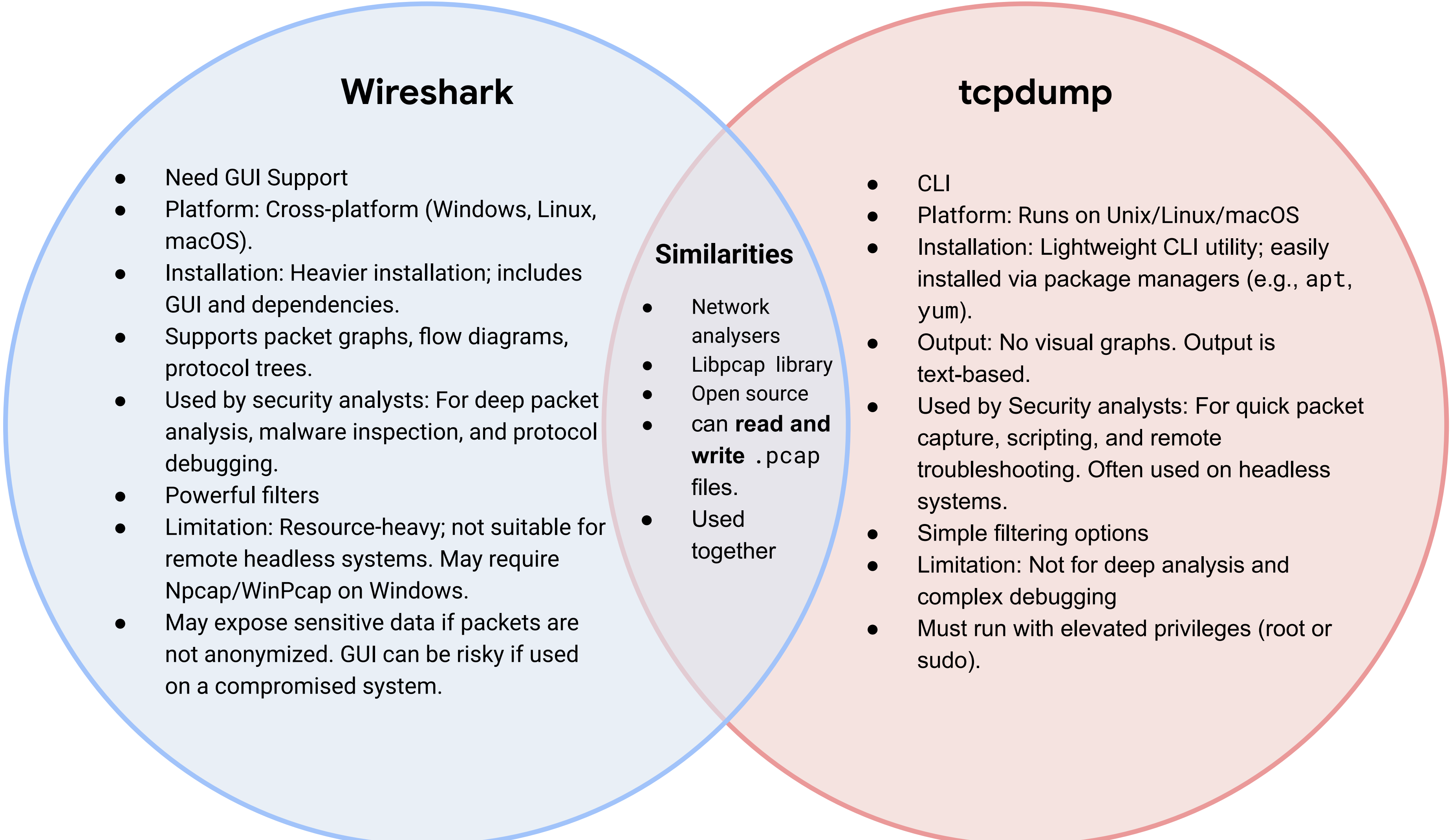

Wireshark

- Need GUI Support
- Platform: Cross-platform (Windows, Linux, macOS).
- Installation: Heavier installation; includes GUI and dependencies.
- Supports packet graphs, flow diagrams, protocol trees.
- Used by security analysts: For deep packet analysis, malware inspection, and protocol debugging.
- Powerful filters
- Limitation: Resource-heavy; not suitable for remote headless systems. May require Npcap/WinPcap on Windows.
- May expose sensitive data if packets are not anonymized. GUI can be risky if used on a compromised system.

Similarities

- Network analysers
- Libpcap library
- Open source
- can **read and write** `.pcap` files.
- Used together

tcpdump

- CLI
- Platform: Runs on Unix/Linux/macOS
- Installation: Lightweight CLI utility; easily installed via package managers (e.g., `apt`, `yum`).
- Output: No visual graphs. Output is text-based.
- Used by Security analysts: For quick packet capture, scripting, and remote troubleshooting. Often used on headless systems.
- Simple filtering options
- Limitation: Not for deep analysis and complex debugging
- Must run with elevated privileges (root or sudo).