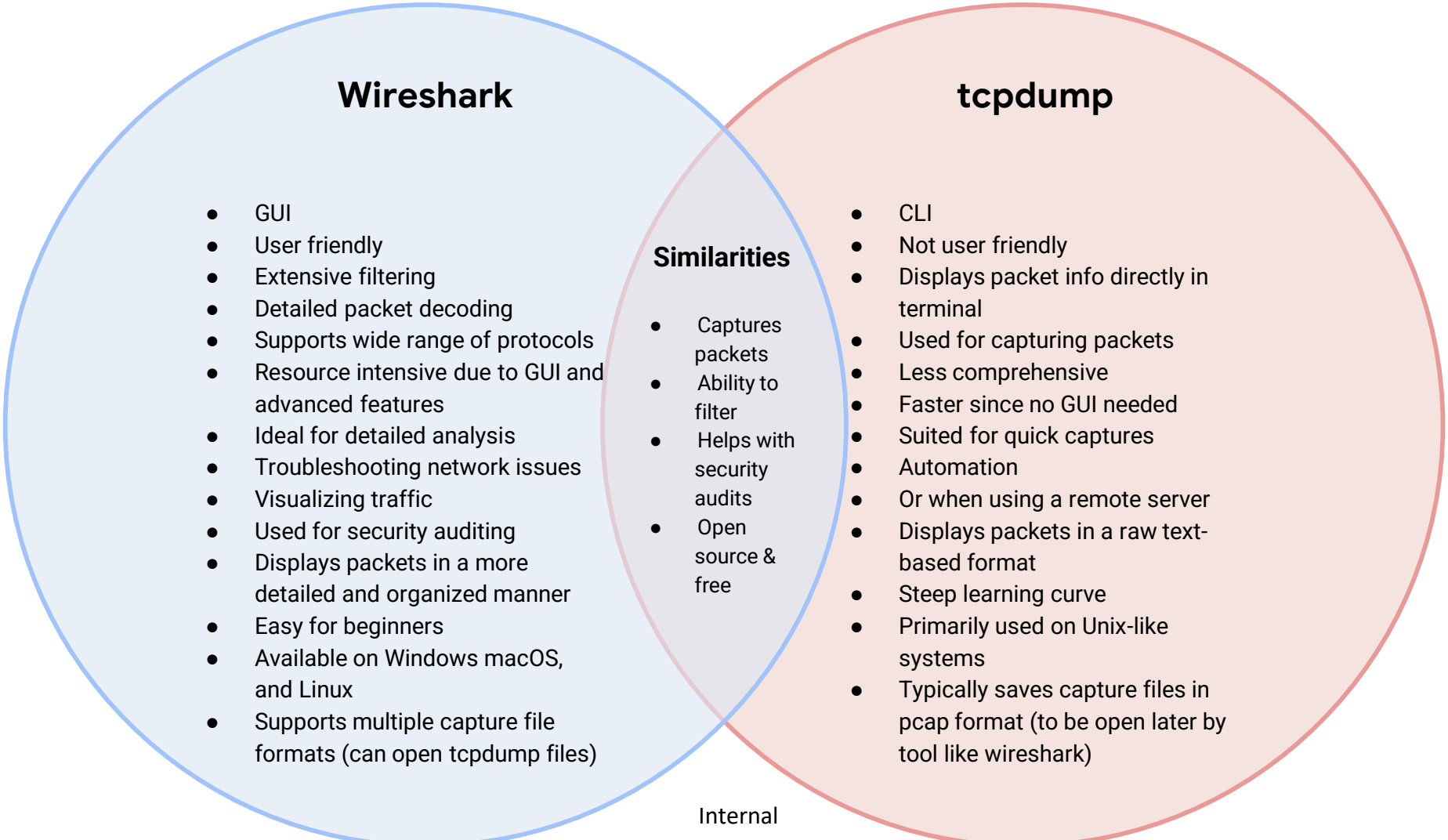
Wireshark
GUI
User friendly
Extensive filtering
Detailed packet decoding
Supports wide range of protocols
Resource intensive due to GUI and advanced features
Ideal for detailed analysis
Troubleshooting network issues
Visualizing traffic
Used for security auditing
Displays packets in a more detailed and organized manner
Easy for beginners
Available on Windows macOS, and Linux
Supports multiple capture file formats (can open tcpdump files)
Similarities
Captures packets
Ability to filter
Helps with security audits
Open source & free
tcpdump
CLI
Not user friendly
Displays packet info directly in terminal
Used for capturing packets
Less comprehensive
Faster since no GUI needed
Suited for quick captures
Automation
Or when using a remote server
Displays packets in a raw text-based format
Steep learning curve
Primarily used on Unix-like systems
Typically saves capture files in pcap format (to be open later by tool like wireshark)

Internal