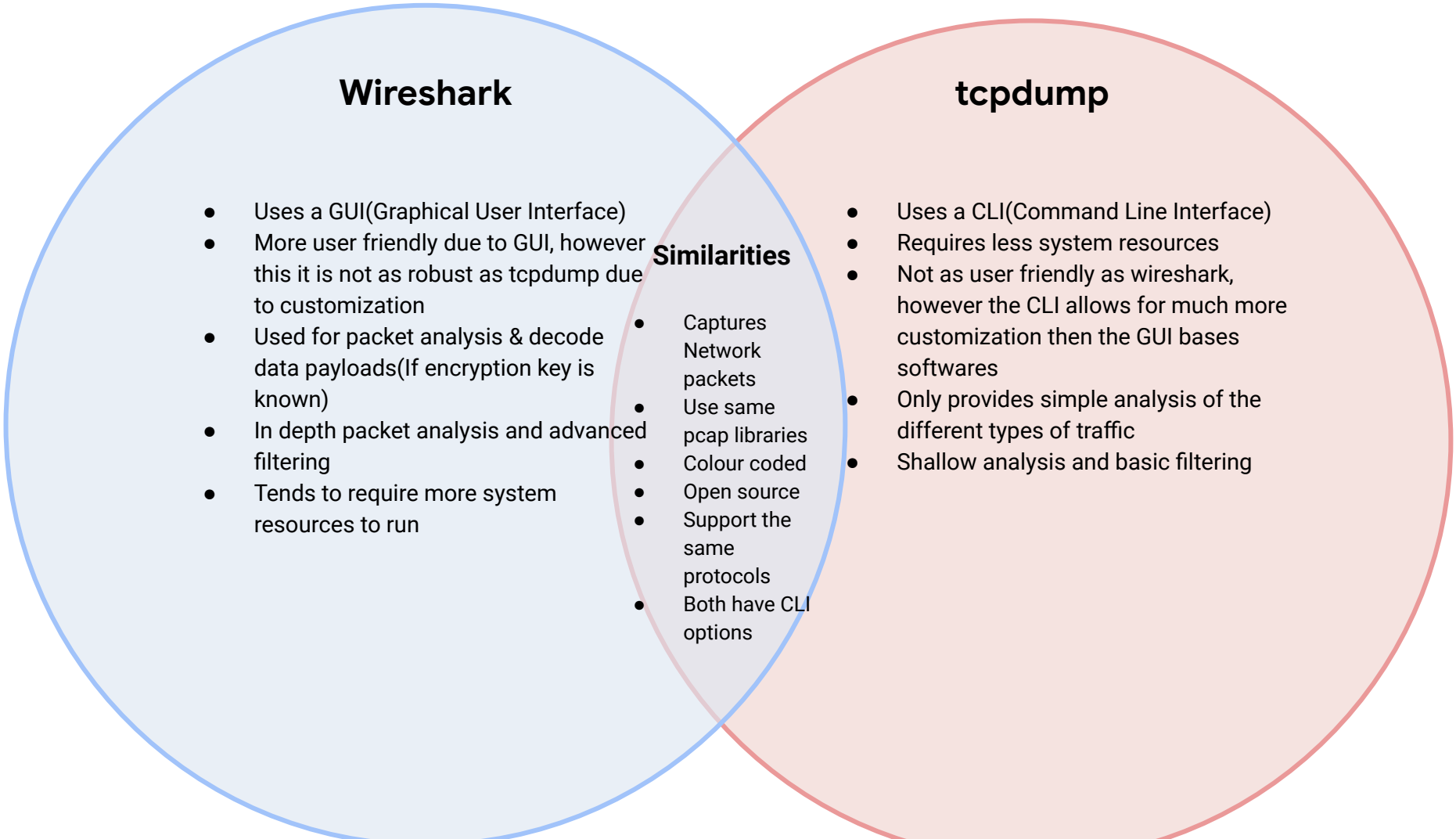
Wireshark
Uses a GUI(Graphical User Interface)
More user friendly due to GUI, however this it is not as robust as tcpdump due to customization
Used for packet analysis & decode data payloads(If encryption key is known)
In depth packet analysis and advanced filtering
Tends to require more system resources to run
Similarities
Captures Network packets
Use same pcap libraries
Colour coded
Open source
Support the same protocols
Both have CLI options
tcpdump
Uses a CLI(Command Line Interface)
Requires less system resources
Not as user friendly as wireshark, however the CLI allows for much more customization then the GUI bases softwares
Only provides simple analysis of the different types of traffic
Shallow analysis and basic filtering