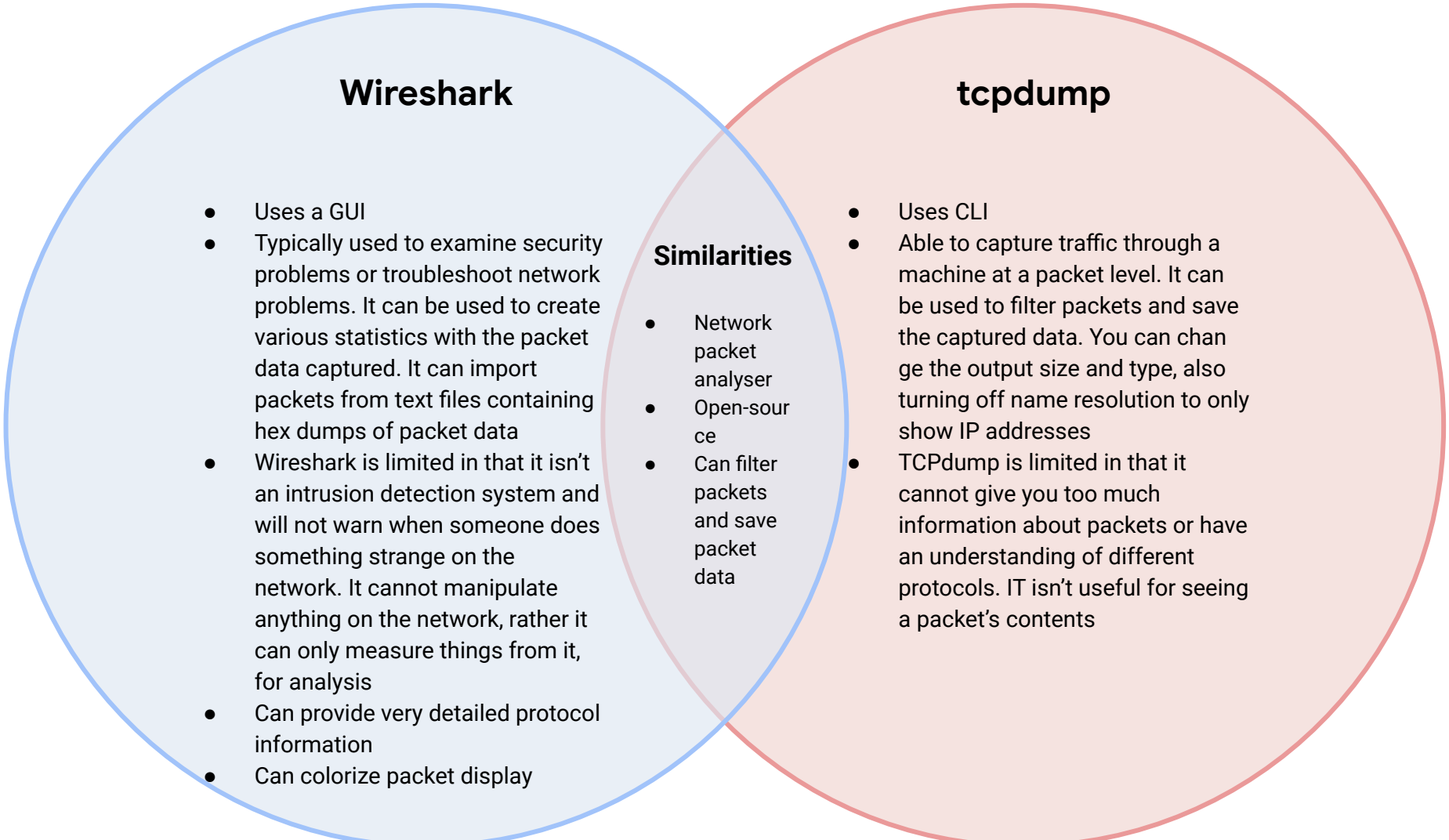
Wireshark
Uses a GUI
Typically used to examine security problems or troubleshoot network problems. It can be used to create various statistics with the packet data captured. It can import packets from text files containing hex dumps of packet data
Wireshark is limited in that it isn't an intrusion detection system and will not warn when someone does something strange on the network. It cannot manipulate anything on the network, rather it can only measure things from it, for analysis
Can provide very detailed protocol information
Can colorize packet display
Similarities
Network packet analyser
Open-source
Can filter packets and save packet data
tcpdump
Uses CLI
Able to capture traffic through a machine at a packet level. It can be used to filter packets and save the captured data. You can change the output size and type, also turning off name resolution to only show IP addresses
TCPdump is limited in that it cannot give you too much information about packets or have an understanding of different protocols. IT isn't useful for seeing a packet's contents