Test Assignment

Disclaimer

This assignment assumes to take from half to full working day. The outcome of this assignment does not serve any practical purpose.

Objective

Implement linux command line utility which is capable to filter input file in "pcap" format as captured by tcpdump or wireshark software according to specified criteria. The output of the command should be saved in the result file in "pcap" format. All conditions specified in the requirements should be supported and they need to be combined in the "and" fashion. It may be assumed that the input file is Ethernet traffic recording.

Requirements

The utility should have following command line parameters:

filter [options] <input filename> <output filename>

The utility should support any combination of following options

-ip x.x.x.x – ip address of the packet, source or destination

-sip x.x.x.x – source ip address of the packet should match

-dip x.x.x.x – destination ip

-tcp x – packet should have tcp type and that port, source or destination

-stcp x - packet should have tcp type and that source port

-dtcp x - packet should have tcp type and that destination port

-udp x – packet should have udp type and that port, source or destination

-sudp x – packet should have udp type and that source port

-dudp x – packet should have udp type and that destination port

-vlan x – packet should have at least one vlan tag with that id

Delivery

Source code and build instructions should be delivered in dedicated github repository

Bonus points

- Design quality
- Code quality
- Error Handling
- Performance (with reasonable time investment)