Intro to Deep Packet Inspection

When inspecting packets in a packet capture there can be a lot of traffic displayed that you do not want or need to see. To narrow down which packets are displayed at any given time, you can apply filters. Filters can apply to destination addresses, source addresses, protocols, etc.

Three Real World Use-Cases

1. Monitoring your company’s web traffic specifically
2. Monitoring a specific host’s http traffic
3. Blocking a specific IP address’ traffic from displaying

Step By Step Guides

How to filter DNS traffic in Wireshark

1. In Wireshark, click on the search bar near the top of the screen
2. Type “dns” into the search bar
3. Click the arrow to the right of the search bar

How to filter FTP Traffic and analyze user logins

1. In Wireshark, click on the search bar near the top of the screen
2. Type “ftp” into the search bar
3. Use a “|” to separate the ftp filter from the next one
4. Type “string matches “login” to filter any packets with the word login in their content

How to inspect ICMP messages

1. Type “icmp” into the search bar
2. Click on a packet
3. View its details in the packet details window

Screenshots



