

For this assignment, we'd like to use Wireshark to explore some of the data transmitted when browsing the web. Download and install Wireshark from Wireshark.org and begin a capture using the gear icon at the top. As your laptop will, likely, have more than one interface, make sure to choose the one that actually shows traffic.

You will see a lot of, non-relevant, traffic going across when you have everything set correctly. Trying to find one packet in 20,000 is going to be very difficult without a filter. On the screen when you choose the interface, you will notice a field titled "Capture filter for selected interfaces." Here you can enter restrictions on information you'd like to see. Try restricting this to only HTTP traffic by entering "port XX" where XX is the TCP port number for HTTP traffic (you may want to look this up). Although most traffic on the web is using HTTPS (which works on a different port and is encrypted), you can still find some HTTP website left out there.

Now try restricting your view to only DNS traffic. Remember how DNS works, so you will only see your communication to the local DNS server. The local DNS server will be doing all the work of contacting the root DNS servers for you, so you will not see this on Wireshark.

For this assignment, we'd like you to submit one .TRACE (or .PCAP) file which shows both a DNS query AND HTTP GET request. This must be one file, so you will have to modify your capture filter to include both types of data.