Hands-on with Networking Tools

Tools: tcpdump, netstat, wireshark, ping, mtr, and traceroute

Task-1: Capture traceroute traffic to/from one of four websites visited as part of Lab-1 using wireshark and answer the following a google doc. Feel free to include screenshots from terminal/wireshark to support your answers. [**7 Marks]**

1. What protocol is used to send probe packets? Identity key fields and comment on their values.
2.
3. Can you change the default protocol used to send probes? Demonstrate it.
4. What is the typical gap (delay) between probe packets?
5. What is contained in probe responses?
6. Which protocol has TTL field and comment on how the values of this field varied across probes and responses?
7. How long did it take to get the output of the traceroute session? Which is the bottleneck router?
8. Do you see any stars (*) in the output? Discuss the potential reasons behind the presence of these stars in the output.

Task-2: Answer Task-1 Q.3, Q.5 and Q.6 using tcpdump instead of wireshark to capture traffic to/from one of the remaining three websites visited as part of Lab-1. [**3 Marks]**

Task-3: Play with netstat or ss, ping and mtr and comment on what you see on wireshark and on terminal. [**5 Marks]**

Note on submission:

Your answers should be clear, very concise, and supported by evidence from the captured data and screenshots. Properly label and organize your Google Doc to ensure clarity and ease of evaluation.