

Wireshark Assignment 3 (Network Layer)

Objective

In this assignment, you will examine network traffic using Wireshark and exercise the basics of network layer protocols.

Instructions

1. Start up your favorite browser and Wireshark and start a packet capture.
2. Use traceroute to find a route to `www.twitch.tv` [**traceroute -I -q 1 <website/IP addr>**]
3. Send a single ping request with a size of 5000 bytes to `hbstann.com` [**ping -c 1 -s 5000 hbstann.com**]
4. Answer the questions below.

Tip: Before you start doing the exercises, it is highly recommended to close all programs that communicate over network to make the task easier for yourself.

Questions

1. How many ICMP echo requests did traceroute send? How does the TTL fields of these packets change?
2. What are the numbers and source IP addresses of TTL-exceeded responses (if any)? Compare them with the output of the traceroute command.
3. Can you explain how traceroute found out the route to destination? Is this route always the same assuming you run traceroute from same location/network? Explain briefly.
4. What is the IP header length and total packet length of the DNS query response with type A record for `hbstann.com`? (If no dns requests are made for `hbstann.com` please flush your dns cache and try again)
5. What is the value of Protocol field in IP header for UDP communication and for ICMP communication?
6. In the ping request you made to `hbstann.com`, has the IP datagram been fragmented? If so, how many fragments are used and why?

Deliverables

You are expected to submit your answers as a one-page-long softcopy solution to "Wireshark Turnitin Assignment 3: Network Layer - Report" section and your packet capture file (.pcap) to "Wireshark Assignment 3: Network Layer - PCAP Submission" section before the deadline. Please refer to course syllabus for late submission terms and follow Odtuclass system for further announcements.

Late delivery

Late delivery will be accepted for assignments. Your submission will be assessed out of 5 if it is delivered until the deadline. Late delivery will only be possible for two days after the deadlines. Your grade will be assessed

out of 4.5 points on the first day of late delivery and out of 4 points on the second day. Beyond two days, your submission will not be counted as a valid submission and the NA policy will be applied.

Cheating Policy

We have zero tolerance policy for cheating. People involved in cheating will be punished according to the university regulations.