CSED353: Computer Networks

Assignment #5: Internet Traffic analysis using Wireshark

Submission Due Date: 11:59 pm, May 5th (Sun.), 2019

In this assignment, you will analyze captured Internet traffic using wireshark to understand what packets are transmitted in computer networks.

This assignment should be done individually and is worth a total **5%** of the final mark. You can refer to wireshark tutorial in the course web page (http://dpnm.postech.ac.kr/cs353/2019/src/Wireshark_Tutorial.pdf). Please download a captured network traffic file that size is 320MB from the course web page (http://dpnm.postech.ac.kr/cs353/2019/src/trace.pcap) for analysis.

1. Capturing packets using wireshark

Using wireshark, capture packets at least 30 seconds. While capturing packets, try to generate more than three different application traffic.

2. Traffic analysis using wireshark

Analyze captured network traffic in terms of following categories:

- Number of total packets and total bytes
- The time difference between the first and the last packet
- The number of packet and total bytes of TCP, UDP and ICMP traffic
- The number of packet and total bytes of each end host
- The number of packet and total bytes of FTP, SSH, DNS, and HTTP
- Select two applications other than the aforementioned applications, and print out the number of packets and the bytes of the traffic which allocates well-known port number (TCP/UDP 1 - 1024)
- Enumerate the average packet size, average packet inter-arrival time

Analyze traffic traces using wireshark and attach each analysis result with screen capture.

3. Submission

The final submission files are a traffic file that is captured using wireshark and a report that includes screen capture about your analysis result. The report should also include the detailed description of your analysis. The report should be formatted as ".PDF".

Have fun!