

# Traffic measurement in practice

## Lab exercises

### 1. The basic features of Wireshark

1.1 Open Wireshark in start packet capturing. Is there any traffic? What is the reason?

1.2 Start a browser and open an arbitrary webpage. Filter the packets that correspond to its download. What filter did you use?

1.3 Close any application that generates significant traffic on TCP port 443. Open Google Chrome and open a sufficiently large webpage. Filter traffic corresponding to its download. Set Wireshark to decrypt encrypted data (see General information). What kind of problems can the usage of https cause in the analysis of network traffic?

### 2. Filtering and analyzing Youtube traffic

2.1 Open a sufficiently long video on Youtube and start it. Filter traffic corresponding to the download of the video and save their information to a csv file. Calculate the average and the coefficient of variation of the packets lengths. Interpret the results.

2.2 Examine the interarrival times (not the same as arrival times!) of packet arrivals. Calculate the basics statistics of the interarrival times (average, coefficient of variation) and interpret the results. Examine and interpret the distribution of interarrival times (e.g. using a histogram).

### 3. Filtering and analyzing VoIP traffic – pair work (optional)

3.1 Open an arbitrary VoIP application, start a voice call and examine the related traffic. (Interarrival time and packet length statistics). What differences can be seen compared to previous traffic?

3.2 Start a call using Discord and examine the related traffic. Compare it with previous results.

## 4. Passive traffic measurement

4.1 Download the capture file given by the instructor and analyze it. Extract the following information (more in the General information document):

- Aggregated throughput (in Bps/KBps/MBps) using 1 second scale
- Distribution of packet lengths
- Protocol distribution
- Statistics of most popular ports
- Distribution of traffic according to hosts. What percentage of traffic are generated by the most popular hosts?
- Flow statistics. What is the distribution of flow lengths? And the distribution of flow sizes?