CSED702D: Internet Traffic Monitoring and Analysis

# Programming Assignment: Programming using Libpcap

Submission Due Date: 11:59 pm, Sept. 28th (Mon.), 2015

In this programming assignment, you will develop three simple programs using libpcap to learn how to use it and to understand the Ethernet packet structure.

This assignment should be finished individually and is worth a total 5% of the final mark. The source code should be written in C or C++ using libpcap library. The use of any supplemental library is prohibited and all programming logic and details should be implemented by yourself. Plagiarism is not tolerated.

**Remark**

- Before you start programming, please construct the libpcap executable environment. Any Linux distribution will be fine, but I highly recommend using Ubuntu or CentOS distribution.
- Make sure that you have read the presentation material on libpcap provided during the class.
- You can freely define any functions or classes using C or C++ language (do not use other languages such as Python, Java), but do not use any external libraries except standard I/O library.

## 1. Capturing packets using libpcap

Write a program that captures packets on your NIC. The program needs to capture TCP, UDP and ICMP traffic only. (Using **pcap_setfilter** API)

Using the program, capture packets more than one minute. While capturing packets, generate more than five different application traffic which use well-known port number (TCP/UDP 1-1024) (e.g., HTTP(S), SSH, FTP)

## 2. Packet analysis using libpcap (Part 1)

Write a traffic analysis program which analyzes traffic traces 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 that you captured in the previous part using your analysis program and attach the analysis result.

## 3. Packet analysis using libpcap (Part 2)

IP packets can be encapsulated in other IP packets, tunneling for example. In the mobile network, GTP (GPRS Tunneling Protocol) is used to establish a tunnel through the network and transmit packets.

Write a program that decapsulates given GTP packets and analyzes given traffic traces same as previous part.

Trace file: http://dpnm.postech.ac.kr/cs702/src/internet_trace.pcap

## 4. Submission

The final submission files should include all source files and report which describes how to compile and execute your program. The report should also include the detailed description of your program. The report should be formatted as ".PDF" and written in English.

Send the final submission files, except traffic traces, to (**noraki@postech.ac.kr**) through e-mail.

Upload the captured traffic traces to the designated FTP server using following information. You

can only upload the file. (Downloading, renaming, deleting actions are prohibited.)

| Server Information | |
|---|---|
| **FTP Server Domain** | **lab.noraki.net** |
| **Port** | **2121** |
| **ID** | **cs702** |
| **Password** | **csed702** |
| **Submission File Name** | **[Your Student ID].pcap** |

If you have a question, please mail me (**noraki@postech.ac.kr**).

Have fun!