**Packet Capture Programming**

CSE351 Computer Networks (Fall 2016)

**Object:**

The goal of this project is to capture the packets of connected AP of your device using Pcap library of C language. For example, when we access to the Raspberry pi from the Mac using SSH, your program using the pcap library can capture packets between Raspberry pi and Mac if the Raspberry pi and Mac use the same AP.

**Program Specification:**

We give a code which has two empty part and you should fill the empty parts to complete the code for running the program successfully satisfying requirements in that empty part. This cord consist of two parts, main(), callback().

**main()** get the current device information, make a filter, and catch the packet. When packet passed through the defined filter then callback() is called.

**callback()** reads an information of passed packet and print out the selected information.

Code 1 in main():

* Open the device for sniffing using "pcap\_open\_live".
* Filtering the traffic using "pcap\_compile" and "pcap\_setfilter".
  + Your filtering rule is received by argument 2.
* Use "pcap\_loop" for callback function.
  + The number of packet capturing is received by argument 1.

Code 2 in callback():

* If the packet is IP packet and the source or destination address is same as the IP address of Raspberry Pi, print out the packet information.
* The packet information which you print out is version, header length, identification, time to live, source and destination address.

In order to fill the code, it is very helpful to refer the http://www.tcpdump.org/pcap.html.

File name:

pcap.c

Compile:

gcc –o pcap pcap.c -lpcap

Usage:

./pcap <the number of packet capturing> <filtering rule>

Example:

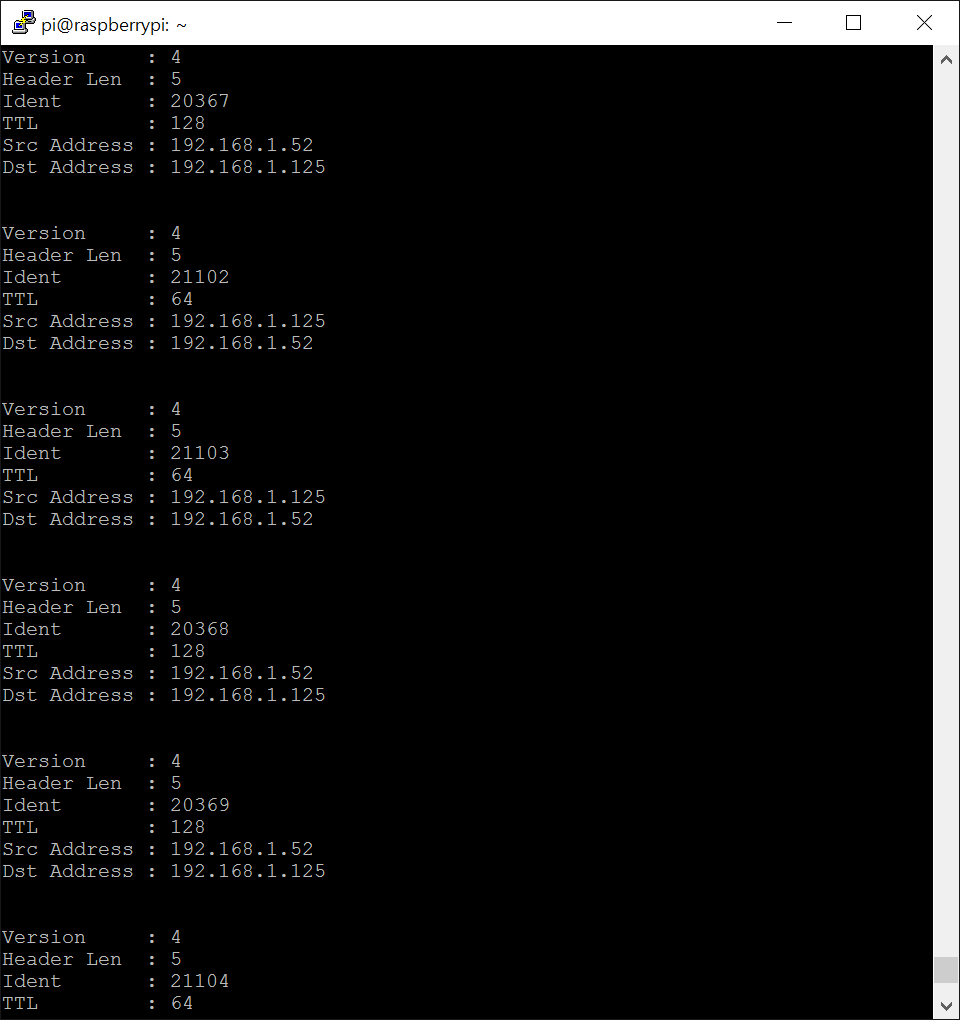
./pcap -1 “port 22”

It means packet through port 22 is captured infinitely.

**Output Specification:**

Running the program in MAC and access the Raspberry Pi using the SSH port 22(if you run the program filtering the “port 22” like the above example). And then if you type some command then you can see the below screen and capture the screen in your MAC.

Captured example output:



**Submission:**

* Submit your codes and your captured file of browser through email: [ujjeong@unist.ac.kr](mailto:ujjeong@unist.ac.kr)
* The email should have the title in the format of “[CSE351] pcap\_<name>\_<student id>”
  + You can submit only one file (in \*.zip or \*.tar.gz only)
  + Make the directory name “pcap\_<student id>”