Goal: To set the filter such that only packets from the local machine and to the local machine are captured on Windows.

1. Start->Run-> Type “cmd” and click on “OK”.
2. In the window that appears, type “ipconfig”
3. You will get information similar to what you see below:
   If you are connected on a wireless connection, then the heading will be “Ethernet adapter Wireless Connection:”

   Ethernet adapter Local Area Connection:
   
   - Connection-specific DNS Suffix : cpe.ku.ac.th
   - IP Address : 158.108.182.217
   - Subnet Mask : 255.255.252.0
   - Default Gateway : 158.108.180.1

   The above information tells you that the IP address of your local Windows machine is 158.108.182.217. Note that this will be a different value each time you connect to a network. Write down this IP address. We will use this to filter the output from Wireshark.

4. Start Wireshark and then Capture->Options.
5. In the Options window as shown below, select the appropriate interface:
   a. Gigabit Ethernet – if you are connected to the wired network
   b. 802.11a/b/g – if you are connected to the wireless network
6. Next, in the “Capture Filter” field enter the filter information in the following format:

   protocol direction value logical-operator protocol direction value ..... 

   protocol – leave empty if all protocols are needed, otherwise specify protocol name  
   direction – This must be “src” or “dst”  
   value – This must specify the value of “src” or “dst” i.e. the IP address  
   logical-operator – If you want to apply more than one filter, use “and”, “or”, “not” and so on.

   e.g.
   src 158.108.182.217 or dst 158.108.182.217

   In this example, I have omitted the protocol field as I would like to capture packets of various protocol types. “src 158.108.182.217” indicates that I want to capture all packets where the source host has the IP address 158.108.182.217. “dst 158.108.182.217” indicates that I want to capture all packets where the destination field has the IP address 158.108.182.217. The logical operator “or” is used to indicate that either one of the two expressions must be true to capture the packet.

   You must enter the information as shown in the example. However, you must use the IP address you obtained in step 3.