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

1. Login into Ubuntu.
2. Open a terminal and type “ifconfig” at the prompt.
3. You will get information similar to what you see below:

```
chidanan@chidanan-deSKTOP:~$ ifconfig
eth0   Link encap:Ethernet  HWaddr 00:0C:29:87:B4:3A
       inet addr:192.168.44.128  Bcast:192.168.44.255  Mask:255.255.255.0
       inet6 addr: fe80::20c:29ff:fe87:b43a/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:172 errors:0 dropped:0 overruns:0 frame:0
       TX packets:212 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:19950 (19.4 KB) TX bytes:23810 (23.2 KB)
       Interrupt:16 Base address:0x1424

lo    Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:16436  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

The above information tells you that the IP address of your local Ubuntu machine is 192.168.44.128. 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 by typing “sudo wireshark” at the prompt and then Capture->Options.
5. In the Options window as shown below, select the appropriate interface: eth0
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 192.168.44.128 or dst 192.168.44.128
```
In this example, I have omitted the protocol field as I would like to capture packets of various protocol types. “src 192.168.44.128” indicates that I want to capture all packets where the source host has the IP address 192.168.44.128. “dst 192.168.44.128” indicates that I want to capture all packets where the destination field has the IP address 192.168.44.128. 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.