HKUSTx: ELEC1200.3x A System View of Communications: From Signals to Packets (Part 3)

Bookmarks

- Pre-course Materials
- Topic 1: Course Overview
- Topic 2: The Link Layer
- Topic 3: The Network Layer
- Topic 4: Routing
- Topic 5: The Transport Layer
- Topic 6: Reliable Transfer Protocols

Topic 7: The Application Layer > 7.4 Lab 4 - Application Layer > Lab 4 - Download and Setup Wireshark

Bookmark

Download Wireshark

We will use the Wireshark network protocol analyzer (a packet sniffer) to analyze some specific application protocols. Please **download** Wireshark here: https://www.wireshark.org/download.html and install it.

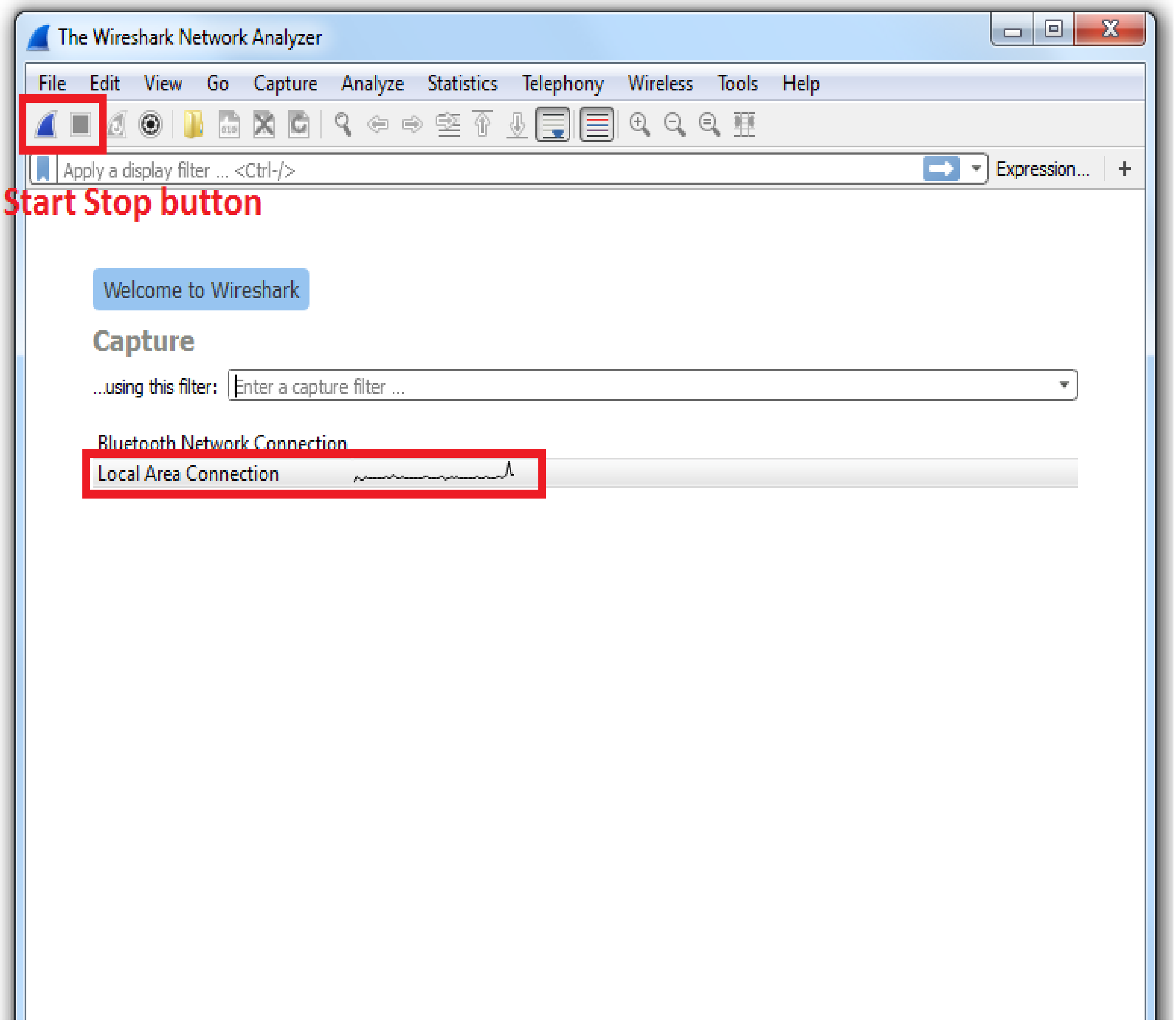
If you use Linux, Wireshark packages are available for most platforms and you can use them without installing Wireshark from source code. For example, in Ubuntu you can install Wireshark 1.6.7 using the command:

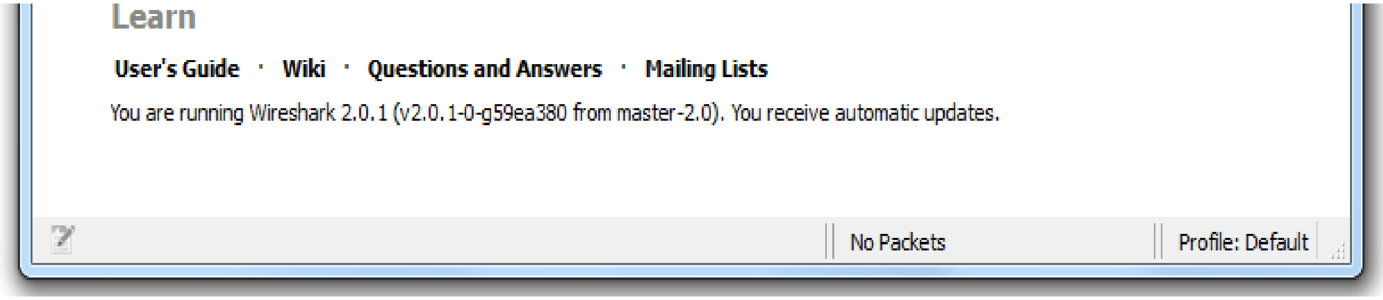
```
sudo apt-get install wireshark
```

Setup Wireshark (Windows)

In this section, we describe the setup of Wireshark for these labs assuming that you are using Windows. Setup for other operating systems is similar. We provide some notes on the setup under Linux in the next section.

When you start Wireshark, you should see the window shown below as Figure 1. The area highlighted by the lower red box shows the link layer connections available on your computer. This may differ according to your computer setup. For example, your computer may show a "Wi-Fi" interface. Select the connection you are using to access the internet by clicking on it. In the example shown here, we have selected the "Local Area Connection" shown in Figure 1.

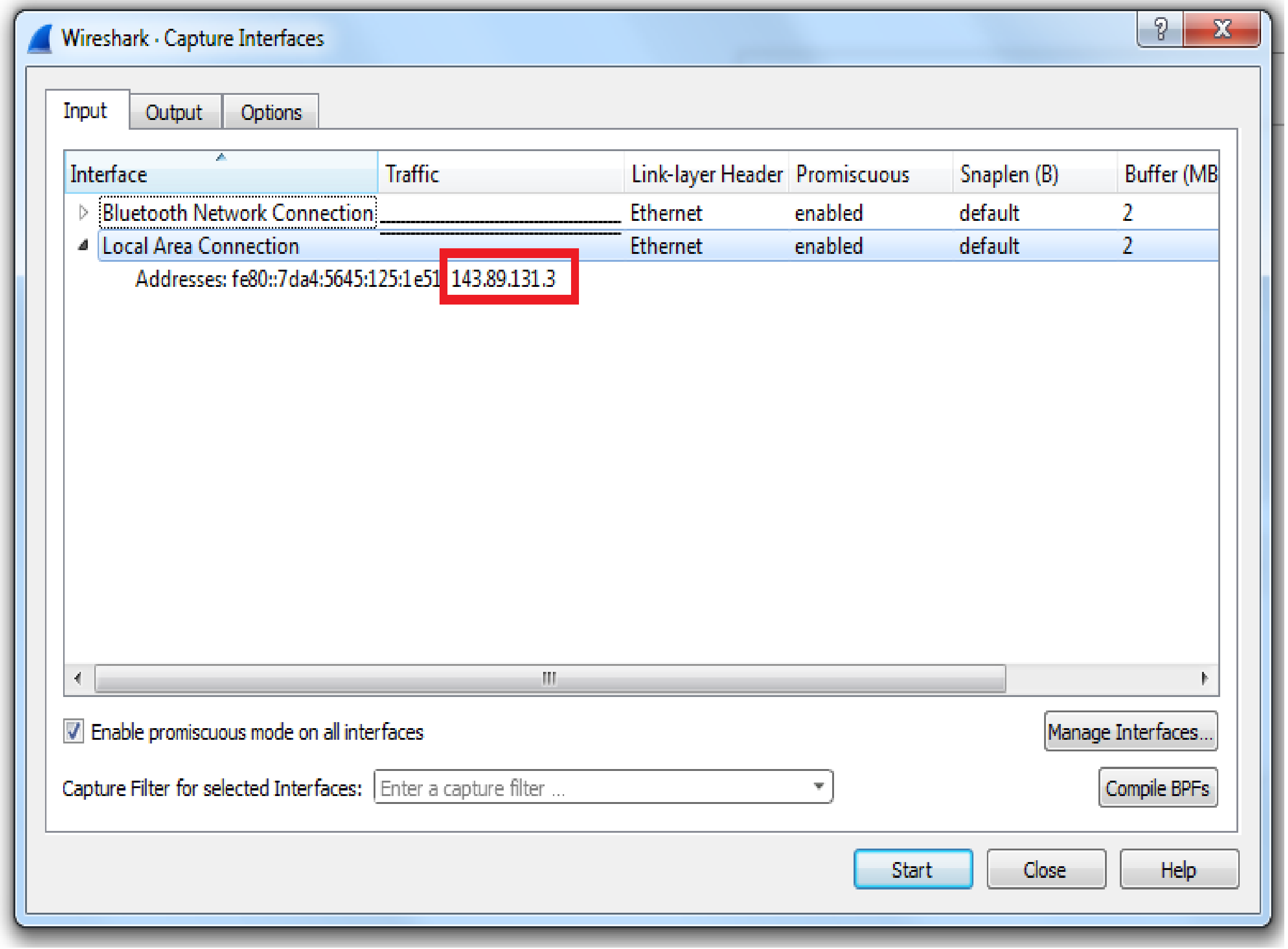

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Start Stop button
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Bluetooth Network Connection
Local Area Connection



You are running Wireshark 2.0.1 (v2.0.1-0-g59ea380 from master-2.0). You receive automatic updates.

Figure 1: Wireshark Window.

From the menu, select Capture => *Options.* A window similar to that shown in Figure 2 below will appear. Click on the button next to the link layer interface you are using to expand the information about that link. As illustrated in Figure 2, you will be able to see the IP address of the link you are using on your computer.



Wireshark · Capture Interfaces

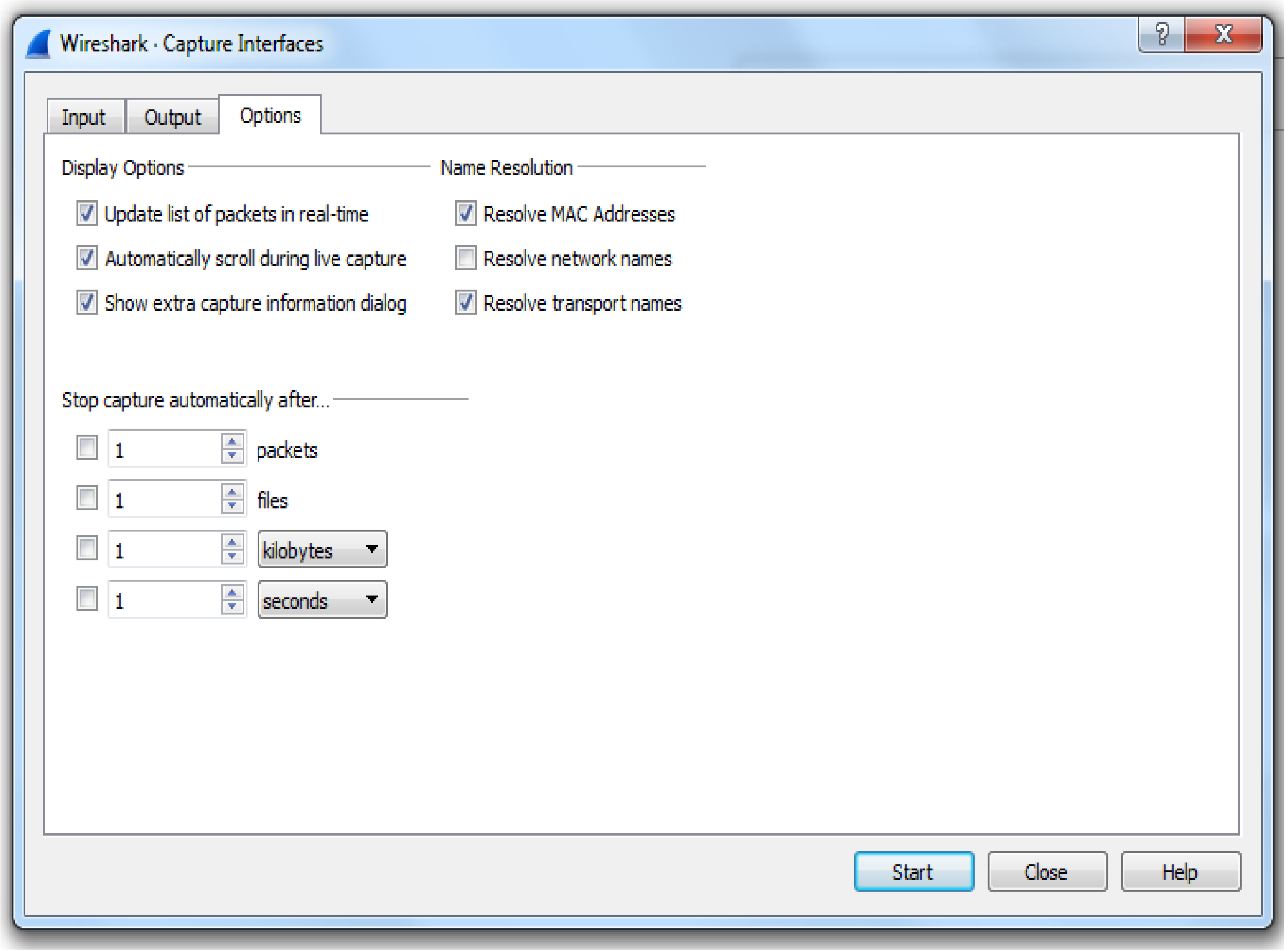
Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB
Bluetooth Network Connection		Ethernet	enabled	default	2
Local Area Connection		Ethernet	enabled	default	2
Addresses: fe80::7da4:5645:125:1e51 143.89.131.3					

☑ Enable promiscuous mode on all interfaces

Capture Filter for selected Interfaces: Enter a capture filter ...

Figure 2: Wireshark Capture Options Window

Tick the following options under "Options" pane of the window as shown in Figure 3. After that close the window, by clicking on "Close" in the lower right corner.



Display Options

☑ Update list of packets in real-time

☑ Automatically scroll during live capture

☑ Show extra capture information dialog

Name Resolution

☑ Resolve MAC Addresses

□ Resolve network names

☑ Resolve transport names

Stop capture automatically after...

□ 1 packets

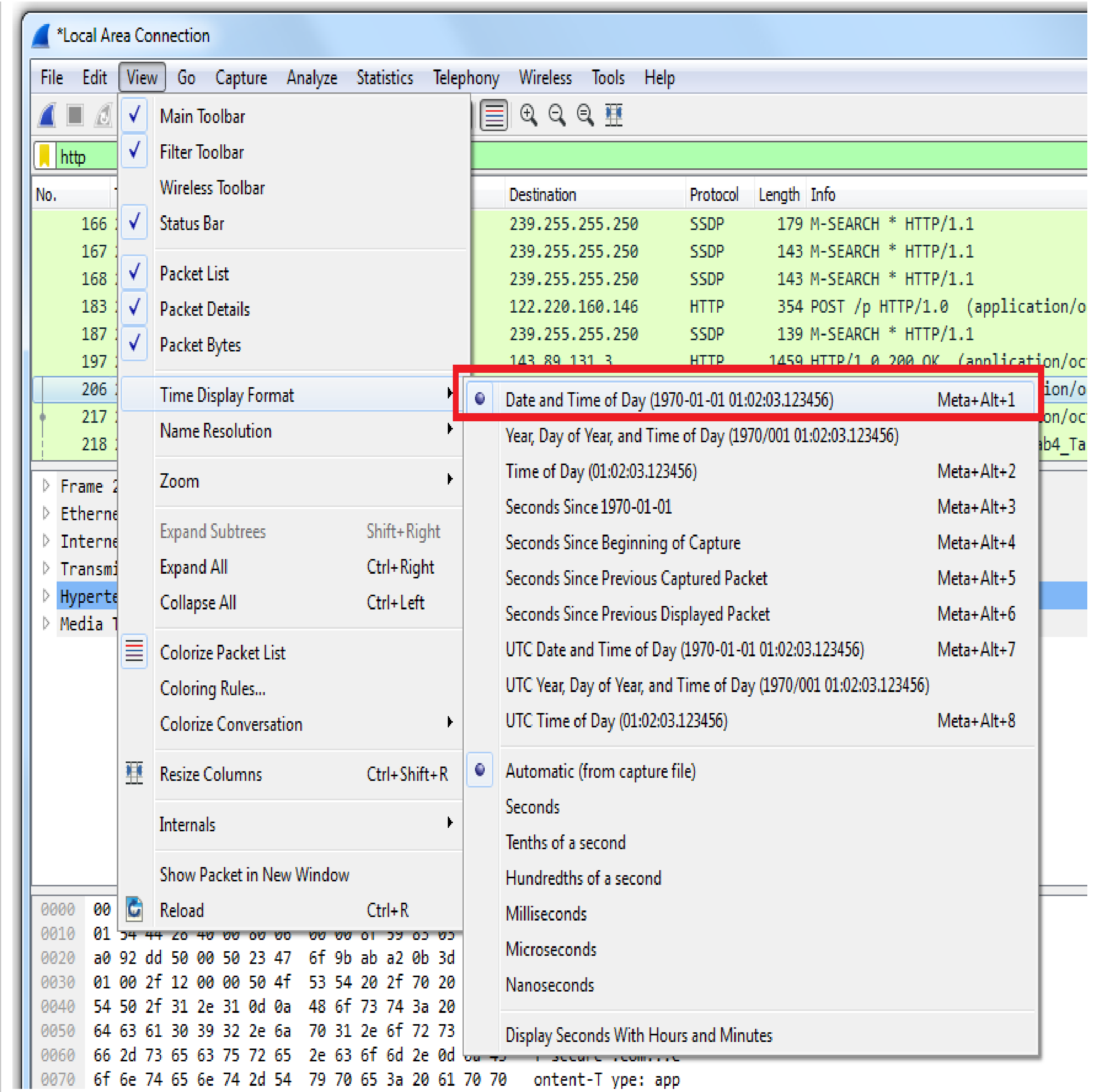
□ 1 files

□ 1 kilobytes

□ 1 seconds

Figure 3: Wireshark Capture Options Window.

Next, setup the time display format by selecting "View=>Time Display Format" as shown in Figure 4.


*Local Area Connection
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
http
✓ Main Toolbar
✓ Filter Toolbar
Wireless Toolbar
✓ Status Bar
✓ Packet List
✓ Packet Details
✓ Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload Ctrl+R
● Date and Time of Day (1970-01-01 01:02:03.123456) Meta+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Meta+Alt+2
Seconds Since 1970-01-01 Meta+Alt+3
Seconds Since Beginning of Capture Meta+Alt+4
Seconds Since Previous Captured Packet Meta+Alt+5
Seconds Since Previous Displayed Packet Meta+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Meta+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Meta+Alt+8
● Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes

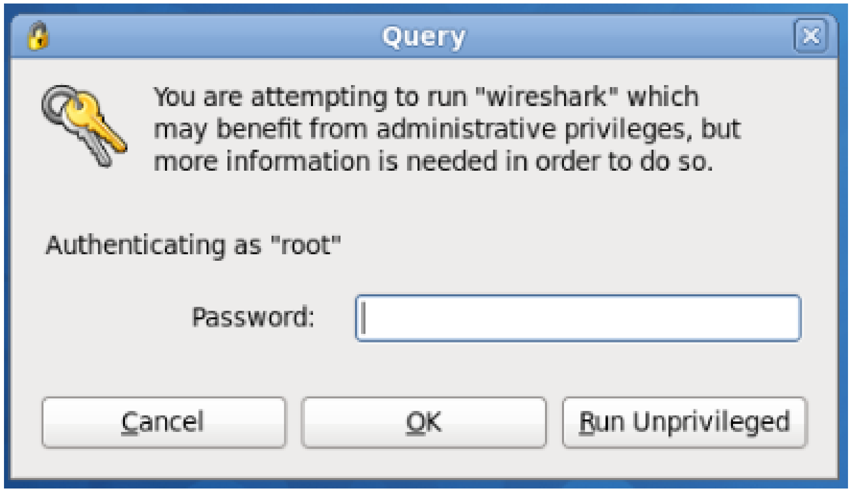
```
No.    Destination       Protocol  Length Info
166    239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
167    239.255.255.250   SSDP      143 M-SEARCH * HTTP/1.1
168    239.255.255.250   SSDP      143 M-SEARCH * HTTP/1.1
183    122.220.160.146   HTTP      354 POST /p HTTP/1.0  (application/o
187    239.255.255.250   SSDP      139 M-SEARCH * HTTP/1.1
197    143.89.131.3      HTTP     1459 HTTP/1.0 200 OK  (application/oc
206                                                          ion/o
217                                                          on/oc
218                                                          ab4_Ta

Frame 2
Etherne
Interne
Transmi
Hyperte
Media T

0000  00
0010  01 34 44 28 40 00 80 06  00 00 8f 59 83 03
0020  a0 92 dd 50 00 50 23 47  6f 9b ab a2 0b 3d
0030  01 00 2f 12 00 00 50 4f  53 54 20 2f 70 20
0040  54 50 2f 31 2e 31 0d 0a  48 6f 73 74 3a 20
0050  64 63 61 30 39 32 2e 6a  70 31 2e 6f 72 73
0060  66 2d 73 65 63 75 72 65  2e 63 6f 6d 2e 0d 0a 43
0070  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 61 70 70   ontent-T ype: app
```

Figure 4: Wireshark View Window

Setup Wireshark (Linux)

If you are using the Linux operation system, select *Applications* => *Internet* => *Wireshark Network Analyzer*.

Then you need to enter password for "root".



Query

You are attempting to run "wireshark" which may benefit from administrative privileges, but more information is needed in order to do so.

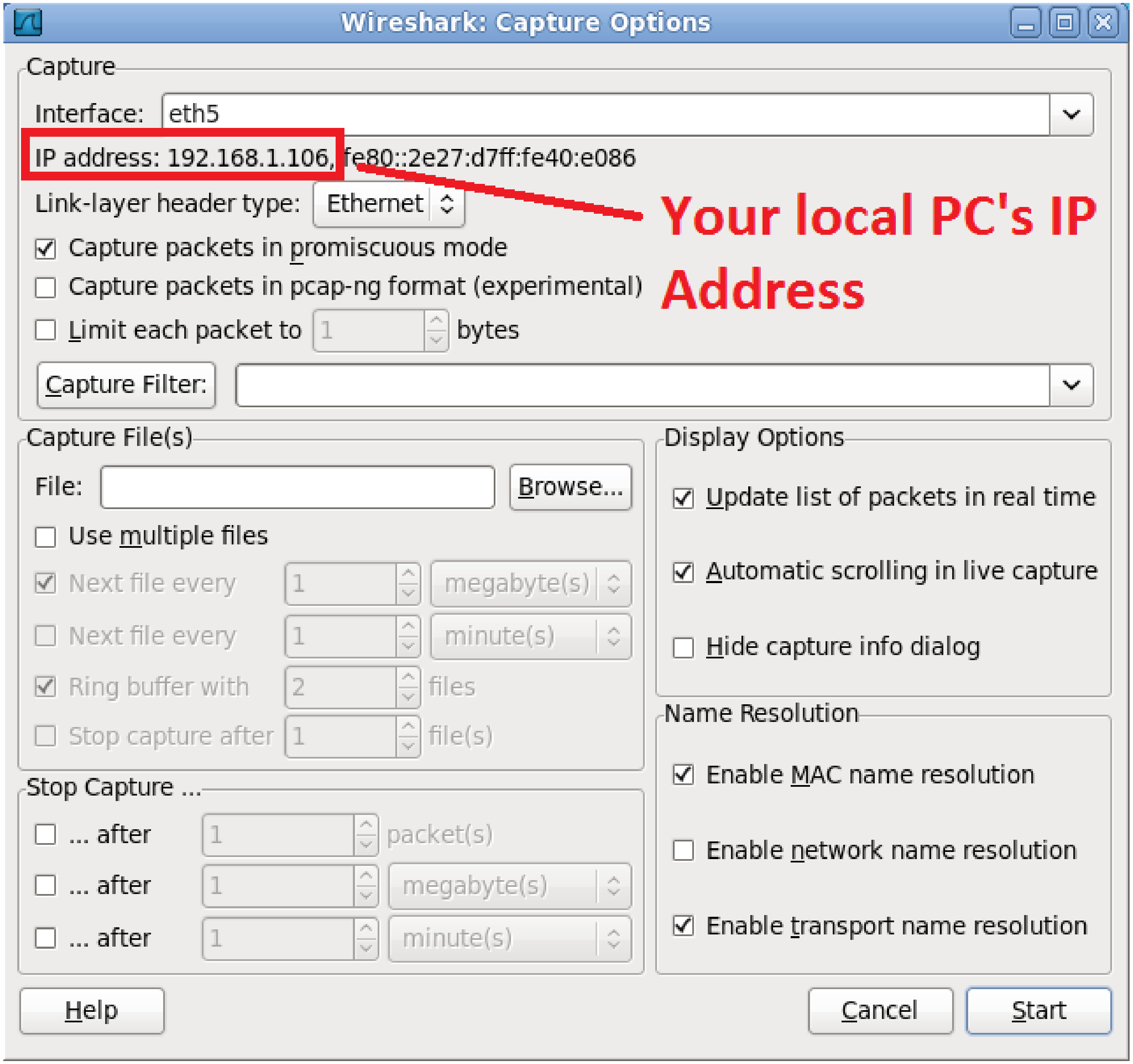
Authenticating as "root"

Password:

If you need to ask someone else to grant permission for you, you could click on “*Run Unprivileged*” in the pop-up dialog box, and then enter the following line in the terminal after login as "root":

```
setcap 'CAP_NET_RAW+eip CAP_NET_ADMIN+eip' /usr/sbin/dumpcap
```

When you select "Capture Options", the Capture Options window will be displayed as shown in Figure 5. Choose the link layer interface you are using from the drop down box at the top. The IP address of this link will be shown below. Click on the options so that they match those shown in Figure 5. In this example, the computer is connected to the Internet via a wired Ethernet interface. The computer is using "eth5" network interface, which is the wired connection. If you use a wireless connection, instead of "eth*x*", the interface name will be something like "wlan*x”.*



Wireshark: Capture Options

Capture

Interface: eth5

IP address: 192.168.1.106, fe80::2e27:d7ff:fe40:e086

Your local PC's IP Address

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to 1 bytes

Capture Filter:

Capture File(s)

File:

Browse...

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☐ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Figure 5: Wireshark Capture Options Window (Linux).

POWERED BY OPENedX

Download on the App Store

ANDROID APP ON Google play