



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

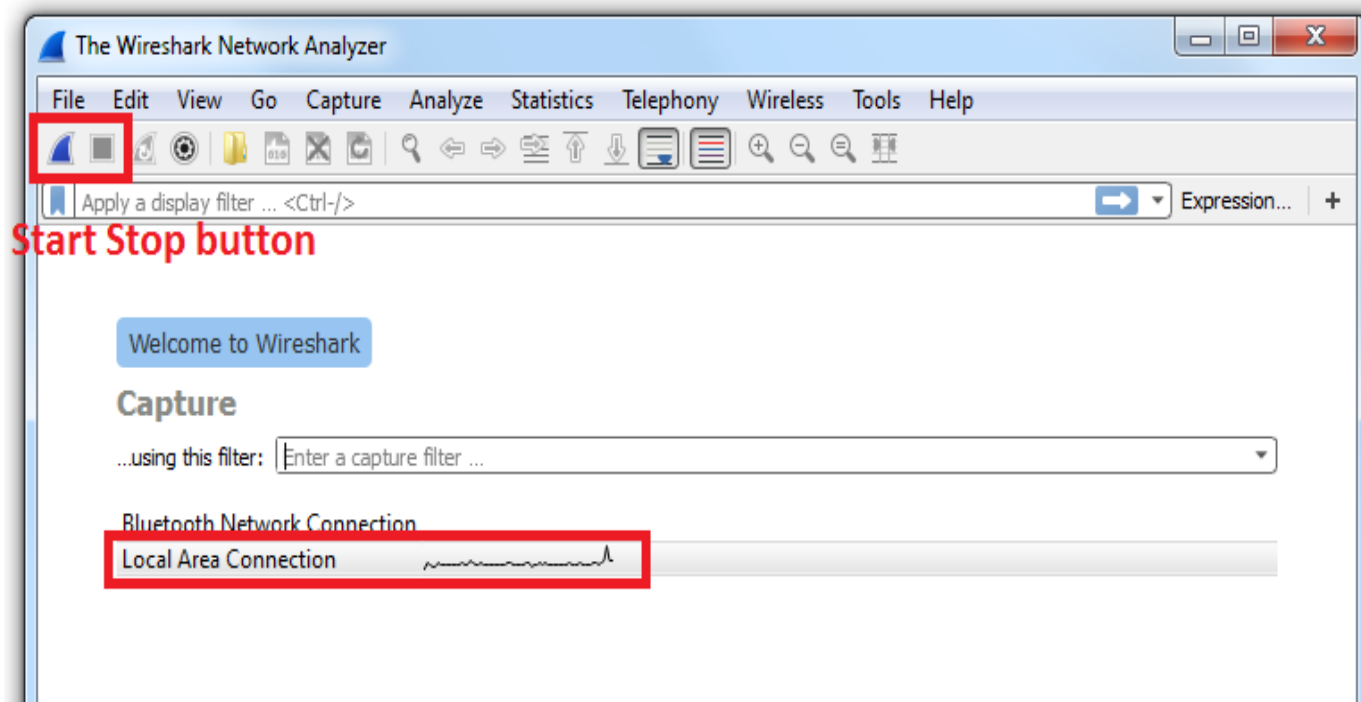

Bookmarks

- ▶ 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 - Capturing Packets with Wireshark


 Bookmark

Once your Wireshark program is set up as described on the previous page, to start packet capture click on the *Start* button in the upper left hand corner of the Wireshark window, as shown in Figure 1 below. All packets being sent from or received by your computer are now being captured by Wireshark! If you wish to stop capture, click on the *Stop* button next to it, however for now, leave packet capture running. You can also start/stop packet capture by selecting start/stop under the "Capture" menu.




▼ Topic 7: The Application Layer


7.1 Application Layer

Week 4 Quiz due Feb 15, 2016 at 15:30 UTC 


7.2 Hypertext Transfer Protocol (HTTP)

Week 4 Quiz due Feb 15, 2016 at 15:30 UTC 

7.3 Domain Name System (DNS)

Week 4 Quiz due Feb 15, 2016 at 15:30 UTC 

7.4 Lab 4 - Application Layer

Lab due Feb 15, 2016 at 15:30 UTC 

► Topic 8: Course Review

► MATLAB download and tutorials

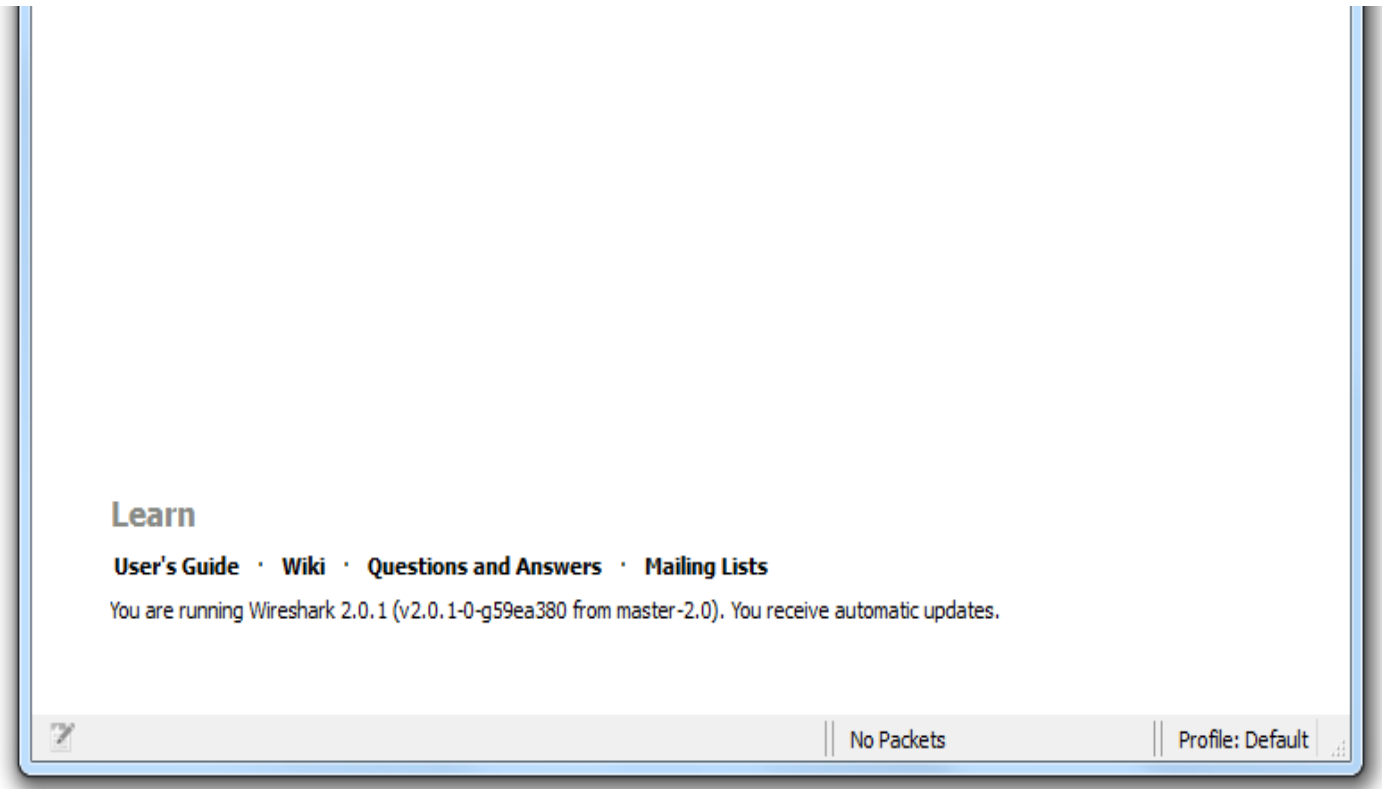


Figure 1: The Wireshark Start Screen.

The Wireshark graphical user interface window will look something like Figure 2 shown below.

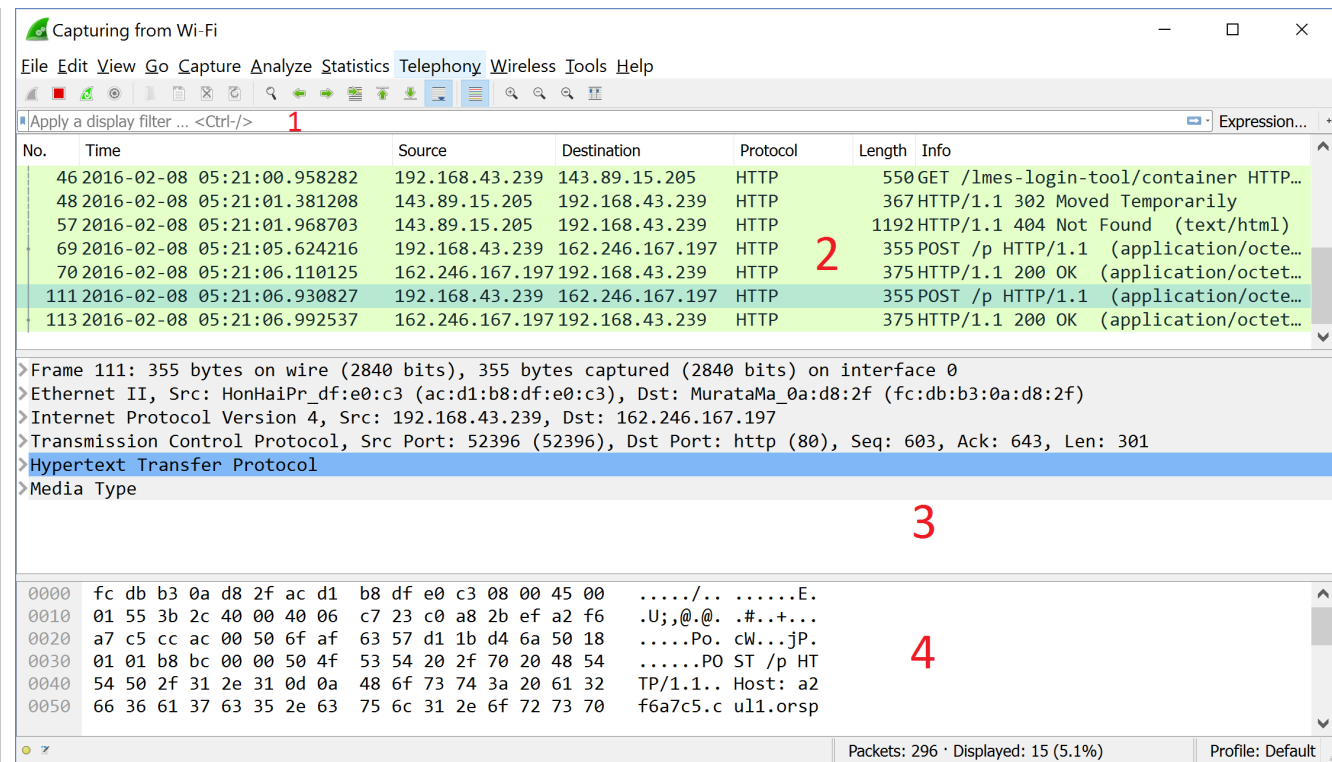


Figure 2: The Wireshark window during package capture.

Now, we will explain the four highlighted sub-windows in Figure 2.

1 : The packet display filter field allows users to enter a protocol name or other information in order to filter the information displayed in the packet-listing window. In this lab, we will use the packet-display filter field to have Wireshark hide packets except those that correspond to HTTP messages.

2 : The packet-listing window displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is not a packet number contained in any protocol header), the time at which the packet was captured, the packet source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.

3 : The packet-header details window provides details about the selected packet (highlighted) in the packet listing window. To select a packet in the packet listing window, place the cursor over the packet one-line summary in the packet listing window and click with the left mouse button. These details include information about the various link, network, transport and application layer protocols used to transmit the packet. The amount of detail about the packet at each layer can be expanded or minimized by clicking on the ">" icon on the left.

4 : The packet-contents window displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

© All Rights Reserved



© edX Inc. All rights reserved except where noted. EdX, Open edX and the edX and Open EdX logos are registered trademarks or trademarks of edX Inc.

POWERED BY
OPENedX

