

WireShark – a packet sniffer

Goal: The goal of this first lab was primarily to introduce you to Wireshark.

Steps:

1. Download and install the Wireshark software:

Go to <http://www.wireshark.org/download.html> and download and install the Wireshark binary for your computer.

2. Download the Wireshark user guide. Try it out. Refer to Wireshark Lab: Getting Started (Wireshark_INTRO_Sept_15_2009.pdf)
3. Answer the following questions, based on your Wireshark experimentation:
 - List the different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 of the Getting Started document.
 - How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
 - What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
 - From step 9 of the Getting Started document, how many bytes is each of the http header, TCP header, IP header and Ethernet header?

Note: Don't submit.