ELEX 4340 : Data Communications
2015 Fall Session

Introduction to the Wireshark Protocol Analyzer

Introduction

In this lab you will use the Wireshark Protocol Analyzer to capture, filter and examine IP frames.

You will follow the procedure described in two of the twelve Wireshark labs prepared by J.F. Kurose and K.W. Ross, authors of the book "Computer Networking."

If you prepare by reading the lab descriptions before coming to the lab you should be able to complete the two labs during your lab session.

Although we will not have time to study all of the IP protocols in detail, these labs should help you become familiar with this useful tool.

Pre-Lab

The Wireshark labs are available from:
`http://www-net.cs.umass.edu/wireshark-labs`

The two labs to be done are:

- Getting Started, and
- IP

For the IP lab you may want to have access to the IP RFC 791 - IP and RFC 792 - ICMP.

Submit a short report to the dropbox on the course web site with your name, ID, lab number and answers to the following questions:

- what protocol layer is shown in the 'Protocol' column in the top window?
- what is the purpose of the filter?
- how do you get Wireshark show you more or less detail about a particular protocol layer?
- which window shows the contents of the frame in hex format?

Lab Procedure

Wireshark has been installed on the lab computers. Go through the instructions in the two lab writeups to practice using Wireshark.

Skip the Fragmentation section of the IP lab (questions starting at 10) since fragmentation is almost never required by modern networking equipment.

Since you are not checking for fragmentation you do not need to use Pingplotter. Instead, follow the instructions for Linux/Unix/MacOS but use the standard Windows `tracert` program in a command prompt window. Use `tracert` without the second (numeric) argument.

Shut down the browser when doing the IP lab to minimize the number of unrelated packets captured.

To answer questions 5 and 6 consider the purpose of each field and decide whether that field *should* change or not. Then examine the captured packets to verify your answer. Don't just blindly compare all of the fields in all of the packets.

Note that the ICMP echo response (the response to a 'ping') and the ICMP TTL exceeded response frames contain a copy of the IP frame that triggered this response, including the header. Don't confuse the response packet's header with the embedded header.

When asked to print your results, use the Wireshark print menu option to print to a text file. Include the text in your report using a monospaced font and single spacing. You can change the background color and add callout boxes to annotate your results. Use landscape mode or small fonts to minized line breaks.

Report

Submit a report in PDF format containing:

- The lab number, your name, BCIT ID and date.
- The answers to questions 1 through 4 in the Introduction lab. For question 4, use a screen shot rather than printing the packet.
- The answers to questions 1 through 9 in Section 2 of the IP lab.