

18-345 Introduction to Telecom Networks

Project 5: Using Wireshark

Out: November 21, 2008

Due: December 5, 2008

Project Goal

This project will give you some hands-on experience with Wireshark¹, a tool that allows you to collect and analyze network traffic. You will investigate basic network flows and gain a better understanding of the TCP/IP protocol stack.

Setup: Downloading & Using Wireshark

Go to <http://www.wireshark.org/download.html> to download the Wireshark software. When installing at a machine running Windows, you would need to have administrative privileges to install WinPcap, which is the library that comes with the Wireshark package and gives Wireshark its ability to capture packets. You can also install Wireshark without the WinPcap library, but in that case you will only be able to view and analyze previously collected packet traces. To account for this, we will be providing upon request previously collected packet traces to those who do not have access to a machine with administrative privileges. Please also note that the former version of Wireshark is installed on the Linux machines at the universities clusters, where it can be also used to view and analyze previously collected packet traces.

Wireshark captures all of the packets that traverse your network connection. After starting Wireshark, begin capturing packets by selecting “Capture => Start” on the menu bar.

A window should pop up called “Wireshark: Capture Options”. This will show you a variety of settings to configure the Wireshark software.

In case you have many NICs, the most important setting is the interface that you want to use. A good way to determine which interface to use is to see which has an IP address; if an interface has an IP address, it means that that interface is connected to the internet! Select the interface from the “Interface:” drop-down menu that has an IP address from listed in the “IP Address:” section right below the menu.

Another good option to check before capturing packets on this page (“Capture Options”) is “Update list of packets in real-time”. This tells Wireshark to show you the packets it receives as it gets them.

Clicking “OK” at this point will start capturing packets.

Before, during, or after capturing packets you can filter packets by typing a protocol name (e.g., ip, tcp, udp, icmp) or host names (e.g., host 128.1.12.12) at the Filter field then press Apply. To check for more examples of filtering commands select “Capture => Capture Filters...”.

¹. Previous versions of Wireshark were known as Ethereal.

Assignment 1

While Wireshark is capturing packets, use a browser to retrieve the webpage: <http://www.cmu.edu>. Click a few links that lead to images, etc. Use Wireshark to do the following:

- a) Identify the IP address and port of the server machine involved in this exchange.
- b) Identify the messages involved in the TCP setup process and describe the role they play in creating the connection.
- c) How do the TCP sequence numbers evolve over time? How can one packet's sequence number be used to predict the subsequent message's TCP number?

Assignment 2

While Wireshark is capturing packets, telnet to red.ece.cmu.edu. Login using any ID you would like to use, but use a fake password (e.g., Andrew). After the system rejects your login, examine the contents of your Wireshark log to answer the following:

- a) Right click on one of the packets involved in this transmission, and select "Follow TCP Stream".

You will see that the login and password are transmitted differently. By examining the packets transmitted during this procedure, explain how the telnet login process works.

- b) Why might this process be dangerous to use?
- c) Telnet unix.andrew.cmu.edu. What response do you get? Why do you get this response?

Assignment 3

While Wireshark is capturing packets, tracert www.gmail.com if you are using Windows and traceroute www.gmail.com if you are using Linux. Examine the Wireshark log to answer the following:

- a) What is the protocol that is used in sending the requests, and the one used in sending the replies?
- b) Compare between the TTL field value in every group of 3 requests, what do you notice?
- c) Are the replies coming from the source? If not, why is that?
- d) How are the 3 printed times for each source calculated?

Please include the tracert/traceroute output in your submission.

Important Note from the Computing Services about Sniffing Network Traffic

The following is taken from CMU's computing services documents.

Network Traffic: Network traffic should be considered private. Because of this, any "packet sniffing", or other deliberate attempts to read network information which is not intended for your use will be grounds for loss of network privileges for a period of not less than one full semester. In some cases, the loss of privileges may be permanent. Note that it is permissible to run a packet sniffer explicitly configured in nonpromiscuous mode (you may sniff packets going to or from your machine). This allows users to explore aspects of networking while protecting the privacy of others.

Hand in Instructions

Submission will take place over blackboard. Please submit a Word document (.doc) or a text file (.txt) with your answers to the questions in assignments 1, 2, and 3, along with snapshots of the packet traces. Pack all of your files into a single compressed file and name it p5ANDREWID.zip, where "p5" stands for project 5 and "ANDREWID" is your Andrew ID.

Note: Since packet trace logs can reach large sizes, please use filters or specify packet ranges while saving the logs to reduce the file sizes. Please note that it is OK that the submitted logs include packets that are not part of the assignment.

Evaluation

The following scheme of partial credit will be used for grading.

	Points
Assignment 1	30
Assignment 2	30
Assignment 3	40
Total	100

Note: There will be no demo for this project.