The Roux Institute
at Northeastern University

CS5700 Fundamentals of Computer Networks
Spring 2023

Homework Assignment 02 **Assigned:** Tue 14 MAR 2023
Wireshark **Due:** Sun 26 MAR 2023

Instructions:

- The assignment is to be uploaded to the course repository (GitHub) by the due date, which is scheduled for 11:59pm ET that day since solutions will be distributed soon after.
- We expect that you will study with friends and often work out problem solutions together, but *you must write up your own solutions, in your own words*. **Cheating will not be tolerated.** Professors and TAs will be available to answer questions but will not do your homework for you. One of our course goals is to teach you how to think on your own and solve your own problems using your resources.
- We require that all homework submissions be neat and organized. **There will be point deductions if the submission is not neat** (is disordered, difficult to read, etc.).

Wireshark Reference Blog: https://www.varonis.com/blog/how-to-use-wireshark

What is Wireshark? Wireshark is an open-source network protocol analysis software program widely considered the industry standard. A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods. Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. One way to best learn and visualize low-level networking involves inspecting the traffic under the Wireshark microscope.

How does Wireshark work? Wireshark is a packet sniffer and analysis tool. It captures network traffic from Ethernet, Bluetooth, wireless (IEEE.802.11), and other network technologies, and stores that data for offline analysis.

Wireshark allows you to filter the log before the capture starts or during analysis so you can narrow down and zero in on what you're looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses, or you can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it has become the standard tool for packet analysis.

To begin this assignment, download and install Wireshark. It is simple and supports all operating systems. To begin, go to the official Wireshark download page for the operating system you need. The basic version of Wireshark is free. The URL is: https://www.wireshark.org/download.html

Wireshark for Windows

Wireshark comes in two options for Windows: 32-bit and 64-bit. Pick the correct version for your OS; the current release is 4.0.4 as of this writing.

Wireshark for Mac

Wireshark is available on Mac as a Homebrew install.

To install Homebrew, you need to run this command at your Terminal prompt:

```
/usr/bin/ruby -e "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/master/install)”
```

Once you have the Homebrew system in place, you can access several open-source projects for your Mac. To install Wireshark, run this command from the Terminal:

```
brew install wireshark
```

Homebrew will download and install Wireshark and any dependencies needed to function correctly.

Wireshark for Linux

Installing Wireshark on Linux can be a little different depending on the Linux distribution. If you aren’t running one of the following distros, please double-check the commands.

Ubuntu

From a Terminal prompt, run these commands:

```
sudo apt-get install wireshark
sudo dpkg-reconfigure wireshark-common
sudo adduser $USER wireshark
```

Those commands download and update the package and add user privileges to run Wireshark.

Red Hat Fedora

From a Terminal prompt, run these commands:

```
sudo dnf install wireshark-qt
sudo usermod -a -G wireshark username
```

The first command installs the GUI and CLI version of Wireshark, and the second adds permissions to use Wireshark.

Kali Linux

Wireshark is probably already installed because it’s part of the basic package. Check your menu under the option “Sniffing & Spoofing” to verify.

Wireshark installation will likely require a reboot as new network drivers are installed at the operating system level.

Launch Wireshark and become familiar with how to use the protocol analyzer. Some tutorials can be found at the varonis.com blog listed above as well as on the wireshark.org website. Once you are familiar with the tool, begin the assignments below.

Preparatory Steps:

Download the capture file. This file will be google1.pcapng. Open the capture file in your Wireshark version.

Problem 1 [100 points]: Wireshark Utilization Questions

1. What is the duration of the capture file in seconds? What about the start and end time of the capture expressed in hh:mm:ss?

2. How many protocols do you see in the protocol window? List the names of some of these protocols. You can find information about the protocols from the "protocol" field. You can sort on this field or any other field in the review window. You can also add or delete fields from the list.

3. How many IPv4 conversations do you have in your capture? You can get these if you investigate Statistics -> Conversations.

4. What is the IP address of the DNS server you are connecting to? To minimize the search time, you should search for a specific string, in this case "google" since we ended up typing www.google.com in the web browser and it is what the system needs to resolve with DNS to get to the appropriate IP address of the Google server servicing your search request. To find a string within a packet, click on Edit > Find Packet. Under "Find By:" select "string" and enter your search string in the text entry box.

5. What is the IP address of the Google server? Once you locate DNS query within all captured packets, you will be able to easily find this address as well.

6. Type udp.port in Apply a Display Filter … <Ctrl-/>? field and click Enter. List the protocols in the "Protocol" field that you see.

7. What is the Checksum field in the UDP header used for and can it be used for reliable data delivery?

8. What is the TOS field in the IP header used for and can it be used for reliable data delivery?

9. What is the Sequence Number field in the TCP header used for?

10. What is the timestamp field in the UDP header used for?

11. Elaborate how the router uses TCP acknowledgment for reliable packet delivery?

Grading

This assignment will be graded according to the point scale associated with each subproblem.

Submission

Please summarize your answers to the questions above in an Adobe PDF document that is to be submitted to Canvas for HW2.