CIS427 Fall 2022 Programming Assignment 2

Instructor: Zheng Song

Due Thursday, Dec 8, 2022

1. Introduction

This programming assignment is designed to let you familiar with using Wireshark to analyze network protocols. This assignment weights 10% of your final grade.

In this assignment, you will install and use Wireshark to analyze TCP/IP/Ethernet Protocols. You will be given pre-captured network traffic traces that can be imported to Wireshark. To answer the questions in each section, you need to follow the steps given in each section, to retrieve the required information from the trace by using Wireshark. Whenever possible, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

2. The Assignment

1) Introduction to Wireshark:

Install and become familiar with Wireshark by completing the “Getting started” Wireshark laboratory exercise available at http://www-net.cs.umass.edu/wireshark-labs/Wireshark_Intro_v8.0.pdf. You do not need to submit anything for Part 2.1 of this project.

Note that when using Wireshark or other packet capture device or software, you should monitor only traffic sent by or to your own computer. In all work for this course, you must respect the privacy of all users.

2) Analyzing TCP:

In this part of this project, you will analyze TCP traffic using Wireshark. Answer the following questions, by opening the Wireshark captured packet trace file *tcp-ethereal-trace-1* in canvas (that is download the trace and open that trace in Wireshark). This packet trace file was captured while following the steps in the “TCP” Wireshark laboratory exercise available at the textbook’s companion web site. (A copy of this laboratory is also available in this assignment’s page in canvas.) Read the “TCP” Wireshark laboratory description to understand how this trace file is obtained and provide answers for the following questions based on the trace file.

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to

select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows). What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

3. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

4. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

3) Analyzing IP

In this part of the project, we'll investigate the IP protocol, focusing on the IP datagram. We'll do so by analyzing a trace of IP datagrams sent and received by an execution of the `traceroute` program on a computer. We'll investigate the various fields in the IP datagram, and study IP fragmentation in detail. Answer the following questions, by opening the Wireshark captured packet trace file *ip-ethereal-trace-1* in Canvas (that is download the trace and open that trace in Wireshark). This packet trace file was captured while following the steps in the "IP" Wireshark laboratory exercise available at the textbook's companion web site. (A copy of this laboratory is also available from Canvas.) Read the "IP" Wireshark laboratory description to understand how this trace file is obtained and provide answers for the following questions based on the trace file.

5. What is the IP address of the computer running traceroute?

6. Select the first ICMP Echo Request message, and expand the Internet Protocol part of the packet in the packet details window. Within the IP packet header, what is the value in the upper layer protocol field?

7. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.

8. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

4) Analyzing Ethernet Frames

In this part of the project, we'll investigate the Ethernet protocol. We will analyze a trace *ethernet-ethereal-trace-1* generated by browsing the webpage http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html. The trace can be downloaded from Canvas. This packet trace file was captured while following the steps in the "Ethernet" Wireshark laboratory exercise available at the textbook's companion web site. (A copy of this laboratory is also available from Canvas.) Read the "Ethernet" Wireshark laboratory description to understand how this trace file is obtained and provide answers for the following questions based on the trace file. Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message.

9. What is the 48-bit Ethernet address of the host that browses the webpage http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html?

10. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

Requirements

- You only need to submit a lab report to answer all the questions given above. Provide responses in your written submission in the order given in the assignment.
- Create your written submission using a word/latex processor and submit your written solution as a single PDF file. **No hand-written report will be accepted.**
- Tip: Pressing the Print Screen key captures a screenshot of the entire desktop area, and places it in the clipboard. Pressing the combination of Alt-Print Screen captures only the current active window.