Virginia Tech ECE 5484: Fundamentals of Computer Systems Summer 2020

Project 4 Assignment

Preface

Before starting this project, please be sure that you have completed all of the following activities.

- View the lectures for Modules 10-12 and read the associated sections of the textbook to gain an understanding of TCP/IP protocol suite and of the data link and physical layers.
- Review the course syllabus and be sure that you understand grading and submission policies.
- Review the course schedule to understand the due dates for this and other assignments.
- Review the Graduate Honor System at https://graduateschool.vt.edu/academics/expectations/graduate-honor-system.html.
- Review the Graduate Honor System Constitution, especially Articles I (Sections 1, 2, and 3), V, VI, VII, VIII, and IX.
- You are welcome to discuss high-level aspects of the project with others and you are encouraged to the Project discussion area on the class website for this. Any questions concerning specific results must be directed to the instructor or graduate teaching assistant.
- You will need to use the Wireshark network protocol analyzer that you should have installed in Project 3.

1. Introduction

The objective of this project is to reinforce your understanding of the TCP/IP protocol suite. In particular, you will use the Wireshark network protocol analyzer to examine details of TCP, UDP, and IP protocols from the TCP/IP protocol suite. You must:

i) capture and analyze TCP segments;
ii) capture and analyze UDP datagrams;
iii) capture and analyze IP datagrams; and
iv) write and submit a brief written report. The written report is to provide answers to the questions posed in Sections 2, 3, and 4 below.

This project assumes you installed and gained familiarity with Wireshark in Project 3.

2. TCP Capture and Analysis

For this part of the project, you will generate HTTP traffic, which is carried using TCP, and examine the resulting trace. Follow the steps below.[1]

1. Start Wireshark and set the interface to use to capture packets.
2. Click on "Capture Options." Be sure that the "Use promiscuous mode" is turned off (unchecked). Be sure that "Capture Filter" is blank (no capture filter should be set). This can also be done from the main Wireshark window using the "Capture:Interfaces" and the "Capture:Options" menus.
3. Open your web browser and clear the cache.
4. Begin packet capture by clicking the "Start" button. Or, from the main Wireshark window, choose the "Capture:Start" menu.
5. Enter the URL http://www.ieee.org in your web browser. Wait long enough that the browser receives a response from the web server and then stop the capture using the "Capture:Stop" menu or using the stop button on the toolbar. NOTE: be sure to enter **http://www.ieee.org**, not https://www.ieee.org.

[1] Avoid running over a virtual private network (VPN) connection for the tests in Sections 2, 3, and 4.

6. Use the display filter to select the packets to be displayed in Wireshark by entering the IP address of the **www.ieee.org** web server, which in my capture is 23.0.16.220 , as "ip.host==23.0.16.220" (lowercase, no quotes) into the display filter specification window near the top of the Wireshark window. The IP address for **www.ieee.org** may be different for you. So you'll need to look for which IP address you got. This will change for each person. You might have the same IP as I did, but you may have another one. In my experience the server starts with 23 so you can try looking for that.
7. Find the HTTP packet from your client to the host IP you found (www.ieee.org) that contains the first GET request ("GET / HTTP/1.1").[2]
8. Right click on the packet, select "Conversation Filter:TCP" as shown in Figure 1.

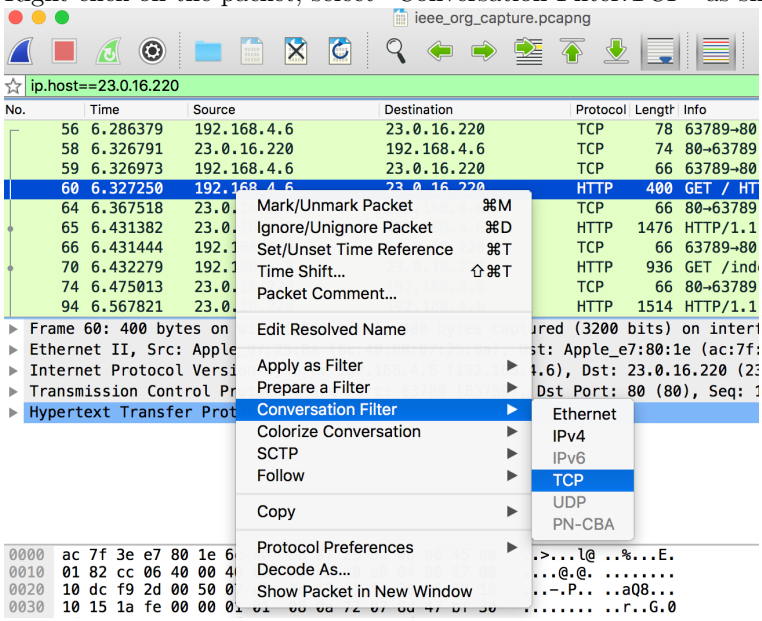

Figure 1. Selecting the TCP conversation.

First, consider the basics of the communication between your computer (the client) and www.ieee.org (the server) that is responding to the request. Answer the following questions in your report in Section 2.1.

Q 1.What is the IP address of the client?

Q 2.What is the port number used on the client for the TCP session with the server?

Q 3.What is the IP address of the server?

Q 4.What is the port number used by the server for the TCP session with the client?

Next, consider TCP's three-way handshake and use of acknowledgment numbers. Answer the following questions in your report in Section 2.1. Note that, by default, Wireshark specifies *relative* TCP sequence numbers. This is fine for this assignment, but do keep in mind that the actual initial sequence number is a more random number.[3]

Q 5.What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and the server?

Q 6.What field and value in that field in the TCP segment identifies the segment as a SYN segment?

[2]Contemporary browsers may initiate multiple HTTP requests using different TCP sessions to simultaneously retrieve multiple page elements. Consider just a single TCP session, identified by the source and destination port numbers, when answering the questions in this section. This should be the first TCP session initiated by your browser, i.e., the one that includes the initial HTTP GET request.

[3]Wireshark can display absolute sequence numbers. Go to the "Edit:Preferences" menu. Then, chose "Protocols" and "TCP" in the left-hand pane. Then, uncheck "Relative sequence numbers."

Q 7.What is the sequence number of the SYN/ACK segment sent by the server to the client in reply to the SYN from the client?

Q 8.What is the value of the acknowledgement number in the SYN/ACK segment sent by the server to the client?

Q 9.What does this acknowledgment number indicate?

Q 10.What field in the TCP segment and value in that field identifies the segment as a SYN/ACK segment?

Q 11.Locate the first GET message sent to the server. What is the sequence number of this message?

Q 12.What is the total length of the HTTP request containing the GET? Note that this message is the data field for TCP.

Q 13.Locate the TCP segment from the server that acknowledges the GET message. Does the acknowledgment number agree with what you would expect? Briefly explain why or why not. **Provide a screen shot of the Wireshark window displaying the information you use to answer this question.**

3. UDP Capture and Analysis

For this part of the project, you will use the "nslookup" command, which uses DNS, to generate some UDP traffic. DNS traffic is carried as UDP datagrams.

1. Start Wireshark, if not already running, and clear the capture filter and the display filter.
2. Begin packet capture by choosing "Capture:Interfaces" and then selecting "Start" for the appropriate network interface from which you wish to capture packets.
3. From a command prompt[4] on your computer, enter "nslookup www.ece.vt.edu" which will use DNS to find the IP address associated with the host name www.ece.vt.edu. Wait for the response from the web server and then stop the capture in Wireshark.
4. Use the display filter to select the packets to be displayed in Wireshark by entering "udp" (lowercase, no quotes) into the display filter specification window near the top of the Wireshark window.

Consider the fields in a UDP header. Answer the following questions in Section 2.2 of your report

Q 14.Select one UDP datagram to or from your computer that is part of the DNS transaction. Double click on the packet in the main Wireshark window to create a new window displaying the packet. From this datagram, list each field in the header and indicate the length of the field and its value for this datagram. **Provide a screen shot of the window displaying the information you use to answer questions Q14-Q17.**

Q 15.The value in the Length field is the length of what? Verify your answer with the captured UDP datagram considered in the previous question.

Q 16.What is the maximum number of bytes that can be included in a UDP payload?

Q 17.What is the protocol number associated with UDP? Express the answer in decimal.

Q 18.Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

4. IP Analysis

For this part of the project, you will consider IP and routing in the Internet. You will generate traffic using a traceroute program. Traceroute allows you to trace the route from your host to any other host on the Internet, taking advantage of ICMP or ICMPv6[5] messages. Traceroute programs include "tracert" accessible

[4]With the Windows operating system, a command prompt is available in the "Accessories" folder under "All Programs" in the Start menu.

[5]IPv6 is used in some networks. The host www.google.com supports both IPv4 and IPv6. Virginia Tech's IP traffic to www.google.com is carried using IPv6. In this case, ICMPv6 is used instead of ICMP. If ICMPv6 is used, then the associated IP addresses will be IPv6 addresses. If you wish, you may configure your client to use only IPv4.

from a command prompt in Windows, pingplotter[6] or similar program that runs as a Windows application, and "*traceroute -I*" on Linux systems. Follow these steps.

1. Familiarize yourself with a traceroute program and trace the route to an IP address selected by you. (You need not include any output from this first step in your project report.)
2. Start Wireshark and begin packet capture by choosing "Capture:Interfaces" and then selecting "Start" for the appropriate network interface from which you wish to capture packets.
3. Perform a traceroute to host www.google.com. After the traceroute completes, stop the Wireshark capture.
4. Use the display filter to select the packets to be displayed in Wireshark by entering "icmp" if using IPv4 or "icmpv6" if using IPv6 (lowercase, no quotes) into the display filter specification window near the top of the Wireshark window.

In the Wireshark trace, locate *the first* or earliest ICMP or ICMPv6 echo reply message. Use this message to answer the following questions in Section 2.3 of your report.

Q 19.Did your traceroute operation use ICMP or ICMPv6? **Provide a screen shot of the Wireshark window displaying the information you use to answer question Q19-25.**

Q 20.What is the IP address of the host that generated the first TTL exceeded?

Q 21.Does this address match the destination address in the echo request messages?

Q 22.What is the content of the Protocol field of the datagram containing the echo reply? (Next Header if IPv6)

Q 23.What is the purpose of this Protocol field? (Next Header if IPv6)

Q 24.How many bytes are in the IP header?

Q 25.How many bytes are in the payload of the IP datagram? Briefly explain how you determine this value?

5. Submission

5.1. Report

You must document your work on this project in a brief written report. Your report should contain the following items.

- At the top of the first page of your report, include: your name (as recorded by the university); your email address; and the assignment name (e.g., "ECE 5484, Project 4"). Do *not* include your Virginia Tech ID number or your social security number.
- The body of the report must contain the following sections. Use section numbers and headings to organize your report.

Section 1 – Objectives: Provide a very brief summary of the project objectives.

Section 2 – Questions: Answer the 25 questions specified in Sections 2, 3, and 4. Clearly indicate the question numbers associated with your answer. **Include the three associated screen shots.** Divide Section 2 into three subsections: 2.1. TCP, 2.2. UDP, and 2.3. IP.

Section 3 – Conclusions: Briefly discuss outcomes, including any significant observations, successes, or failures not discussed previously. Indicate the approximate number of hours you spent on this assignment. (The number of hours is just for the instructor to assess the suitability of this project assignment.)

Your writing should be well-organized, concise, and technical in nature. Your report should use complete, grammatically correct English sentences. Use section headings within the report that match the section names listed above. Every figure and table should have a caption and should be introduced in the body of the report.

[6]See http://www.pingplotter.com.

5.2. Submission

Carefully follow these instructions when submitting your project.

- Create a single PDF file for your report. Name the PDF file *lastname_firstname*_P4.pdf, where *lastname* is your last or family name and *firstname* is your first or given name.
- Submit your assignment as the single PDF file in the Assignments area of the class website. You must submit your assignment by 11:55 p.m. on the due date.

6. Grading

The project will be evaluated based on the following criteria.

- Presentation (15 points)
  - Complete, clear, and well organized report
  - Mechanics (spelling, grammar, etc.)
- Objectives (5 points)
  - Brief description of project objectives
- Protocol analysis (75 points with 25 points each for TCP, UDP, and IP)
  - Correct answers to the questions
  - Screen shots provided as specified
- Conclusions (5 points)
  - Brief summary of outcomes, including any significant observations, successes, or failures not discussed previously

7. Seeking Assistance

This is *not* a team project. Your project should be completely your work. You are welcome to discuss high-level aspects of the project use of Wireshark with others, and you are encouraged to use the Ca course website for this purpose. Any questions concerning deta answers must be directed to the instructor. Please refer to the Honor Code statement in the syllabus.