Virginia Tech ECE 5484: Fundamentals of Computer Systems Summer 2020

Project 3 Assignment

Preface

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

Read Chapter 12 through Section 12.5 of the textbook and view the associated online lectures to gain an understanding of TCP/IP protocol suite.

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.

Download and install the Wireshark network protocol analyzer. It is available at no charge at https://www.wireshark.org/. This assignment provides an introduction to Wireshark. Additional information is available at the Wireshark website. Wireshark will be used again in Project 4.

1. Introduction

The objective of this project is to reinforce your understanding of network protocols and the TCP/IP protocol suite. You will use the Wireshark network protocol analyzer. You must:

i) install and become familiar with the basic operation of Wireshark;
ii) capture and analyze a simple HTTP transaction; and
iii) document your work in a short report.

2. Getting Started with Wireshark

Wireshark is a network protocol analyzer that is available under the GNU General Public License. Wireshark allows you to capture network packets that are seen on an interface of your computer (in some cases, even if they are not destined for your computer) and to inspect and analyze captured or stored sets of packets. The tool includes built-in protocol decoders that allow you to inspect protocol-specific fields and flows. This section is intended to get you into the water and swimming with Wireshark.

2.1. Installing Wireshark

Download Wireshark from https://www.wireshark.org/. Run the installation file and follow the instructions to install Wireshark. The default installation is assumed for the project. Note that the Wireshark website includes an FAQ list, a help Wiki, and extensive documentation.

As part of the Wireshark installation, for Windows machines you should also install Npcap. It is recommended that this be done as part of the Wireshark installation. During the installation of Npcap, you can choose to have it started automatically when the system starts.

You are to report on installation in Section 2 of your project report.

2.2. Quick Introduction to Wireshark

Wireshark has three basic functions:

i) capturing packets,

ii) displaying the captured packets; and
iii) analyzing packet flows.

You can capture all traffic on an interface or you can create a *capture filter* to capture only packets with specific characteristics. After the packets have been captured, you can display all packets or, using a *display filter*, you can display only packets that have certain characteristics. You can also analyze sets of packets, such as the packets that are part of a TCP session.

As an introduction to some basic functions in Wireshark and to ensure that you can capture packets, carefully follow the steps below. These steps will guide you through the process of capturing, displaying, and analyzing packets from a HTTP (web) session.

Start Wireshark. You should see an opening window similar to the one shown in Figure 1. Select the network interface you are using to connect to the Internet and then click "Capture Options."

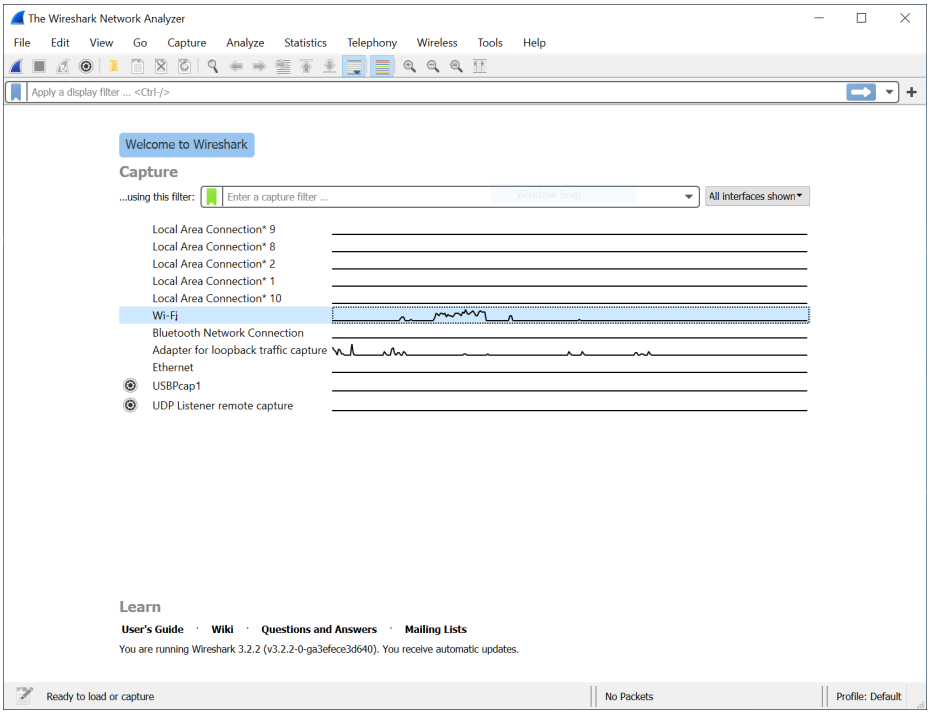

Figure 1. Select the network interface and, then, click "Capture Options" in the opening window.

In the capture options window (see Figure 2), disable (uncheck) the "Use promiscuous mode on all interfaces" option. This will limit packet capture to only those packets originating from or destined for your host. This is required for many wireless LAN adapters and is good etiquette for all types of adapters. Also, be sure that "Update list of packets in real time" is selected (checked). This causes Wireshark to display packets as they are captured. [1]

In the same capture options window (See Figure 2), enter "tcp port http" or "tcp port 80" as the capture filter. This will set up a capture filter to capture only TCP traffic going to or coming from the default HTTP port, which is port 80. The capture filter will cause Wireshark to save only TCP packets with the value 80 in the port field in the TCP segment header. So, only traffic to or from a web server (or, at least, to or from the default port for HTTP) will be captured. Click on "Start" to start capturing packets.[2]

[1] You can set preferences on a more permanent basis by selecting the "Edit:Preferences..." menu item (or clicking the associated toolbar icon) from the regular Wireshark window. Select "Capture" in the pane on the left to set capture preferences.

[2] You can change capture options by selecting the "Capture:Options..." menu item (or clicking the associated toolbar icon) from the regular Wireshark window.

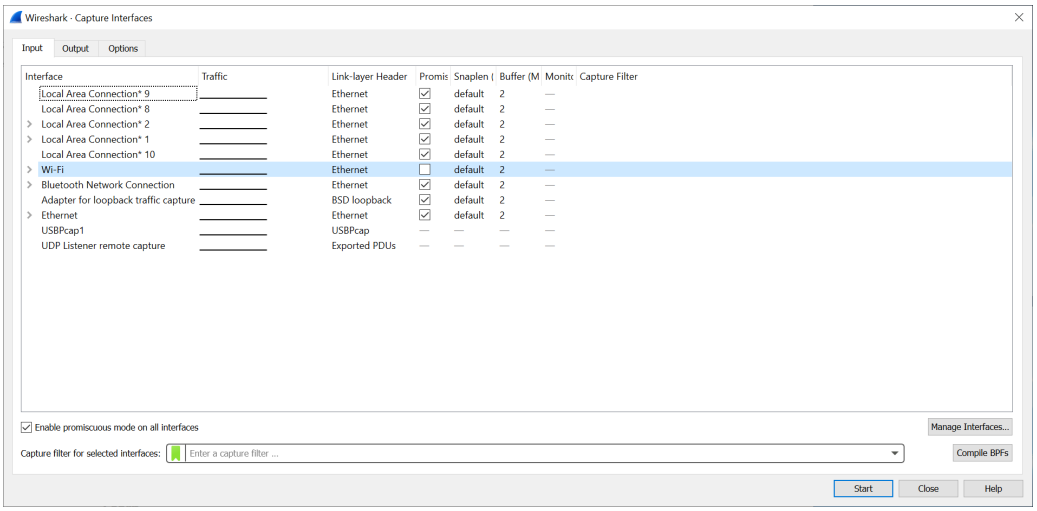

Figure 2. Turn off promiscuous mode and set capture filter in the capture options window.

Depending on what is happening elsewhere on your host, you may or may not see any packets being displayed. If you do not see any activity, then open a web browser and go to your favorite website, such as http://www.vt.edu/. This will create a flow of packets that should be captured and displayed by Wireshark. After you see some packets, such as in Figure 3, you can stop the capture by selecting the "Capture:Stop" menu item (or by clicking the associated toolbar icon).

Select a particular packet in the top pane of the display. (Note that Packet 88 is selected in Figure 3.) You can then see details of the various protocols used in the middle pane, such as Ethernet, IP, TCP, and, perhaps, HTTP. The bottom pane shows packet contents in hexadecimal. You may need to expand the Wireshark window and/or expand panes in the window to see all parts of all three panes. You can also double click on the packet to create a new window in which to inspect the packet.

Enter a display filter in the "Filter:" box above the packet display. You can directly enter an expression or click on "Expression. . . " to see a long list of options organized as a hierarchy. Enter "tcp.srcport == 80" in the filter input or use the "Expression. . . " feature to select this filter, as shown in Figure 4. Then click "Apply" to see just those packets with the source as port 80, i.e., just those packets sent from the web server. Click "Clear" to remove the display filter.

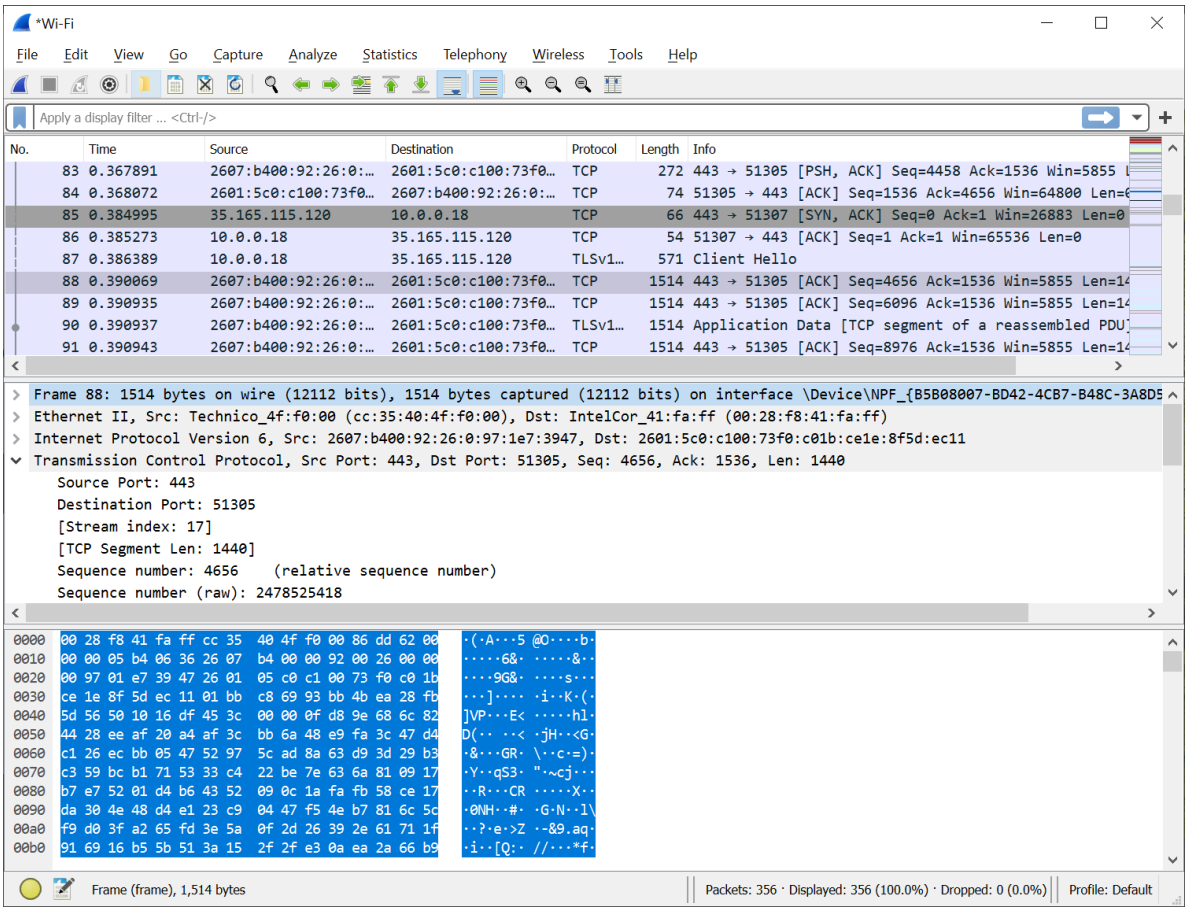

Figure 3. Example of captured packets.

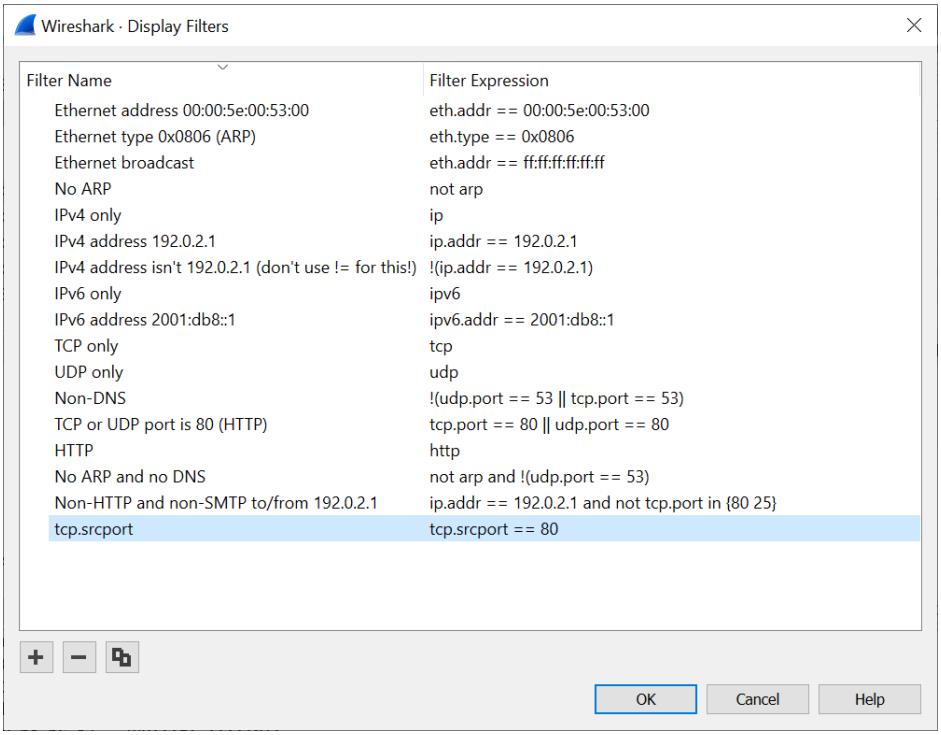

Figure 4. Example of selecting a display filter expression.

Right click a TCP or HTTP packet, select "Conversation Filter," and then select "TCP" to display only those packets associated with the packet's TCP session. Click "Clear" to remove this display filter.

Select the "File:Save" menu item to save a file of the captured packets. Select the "File:Close" menu item to close the captured packets file. Then select the "File:Open menu" item to reopen the file. Verify that it is the same set of captured packets as observed earlier.

You will provide a screen shot of the captured packets, similar to Figure **3** above, in Section 3 of your project report.

You should now have installed Wireshark and you should be able to use it for basic packet capture tasks. Review the Wireshark Users' Guide (select the "Help:Contents" menu item or see the Wireshark website) and other documents at the Wireshark web site for further information.

3. Packet Analysis with Wireshark

Follow the steps below to analyze an HTTP transfer using Wireshark. You will provide a screen shot and answer the questions given below in Section 4 of your project report

Open with Wireshark the "pcap file for "Packet Analysis with Wireshark" found on the Project 3 Canvas page. This is a pcap capture of http://www.orionsarrow.com/egg.txt (before the website moved to https).

From the Wireshark menu, select Statistics → Flow Graph. From the trace obtained, calculate the **HTTP response time**. The HTTP response time is the time taken for the web server to respond to the HTTP request for egg.txt. This value can be determined by noting the time at which the HTTP request was sent to the server and at the time at which the browser received the first fragment of the HTTP response. Note that the server may respond with a TCP acknowledgment before it responds with the actual HTTP response. Include a screenshot of the flow graph to support your calculation.

From the Wireshark menu, select Statistics → Protocol Hierarchy.

1. What percentage of the captured packets are using TCP?
2. From your captured packets, what is an example Application Layer protocol that uses TCP?

Include a screenshot of the protocol hierarchy to support your calculation.

Find the packet from your host to www.orionsarrow.com that contains the HTTP GET request. By selecting different fields in Wireshark's middle pane, you can answer the following questions:

1. How many bytes are in the IP header?
2. How many bytes are in the TCP header?
3. How many bytes are in the HTTP message?

4. Submission

4.1. 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 3"). 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 – Wireshark Installation: Briefly describe the outcome of your installation of Wireshark. Indicate if Wireshark was successfully installed and include a brief discussion of any problems encountered.

Section 3 – Familiarization: Provide a screen shot of the captured packets from your running the "Quick Introduction to Wireshark" exercise. This should be similar to Figure 3 above.

Section 4 – Protocol Analysis: Provide a screen shot of the packet capture from the HTTP transaction with host www.orionsarrow.com that is similar to what is shown in Figure 3 above. Be sure that the packet with HTTP request from your computer to host www.orionsarrow.com is selected and shown in the screen shot. Also include screenshots of the Protocol Hierarchy and Flow Graph. Finally, answer the following questions, as described above in the section on "Packet Analysis with Wireshark."

1. What is the measured HTTP response time?
2. What percentage of the captured packets are using TCP?
3. From your captured packets, what is an example Application Layer protocol that uses TCP?
4. How many IP header bytes are in the packet containing the GET request?
5. How many TCP header bytes are in the packet containing the GET request?
6. How many bytes are in the HTTP message for the GET request?
7. What is the total length, in bytes, of the IP datagram carrying the IP header, the TCP header, and the HTTP message for the GET request?

Section 5 – Conclusions: Briefly discuss outcomes, including any significant observations, successes, or failures not discussed previously. (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.

4.2. Submission

Carefully follow these instructions when submitting your project.

Create a single PDF file for your report. Name the PDF file *lastname_firstname*_P3.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 Assignment area at the class website. You must submit your assignment by 11:55 p.m. on the due date.

5. Grading

The project will be evaluated based on the following criteria.

- Presentation (20 points)
  - Complete, clear, and well organized report
  - Mechanics (spelling, grammar, etc.)
- Objectives (5 points)
  - Brief description of project objectives
- Installation (10 points)
  - Discussion of installation outcome and any problems
- Familiarization exercise (10 points)
  - Screen shot from the familiarization exercise
  - Discussion of any problems
- Protocol analysis (50 points)
  - Screen shots from the HTTP transaction
  - Correct answers to the questions
- Conclusions (5 points)

– Brief conclusions, including any significant observations, successes, or failures not previously discussed

6. Seeking Assistance

This is not a team project. Your project should be completely your own work. You are welcome to discuss high-level aspects of the project and use of Wireshark with others, and you are encouraged to use the Projects discussion area at the class website for this purpose. Any questions concerning detailed answers must be directed to the instructor or teaching assistant. Please refer to the Honor Code statement in the syllabus.

Appendix: Possibly Helpful Hints

Here are some hints and pointers that may be useful in completing this project. Be sure to check the Projects discussion area on the class website for more questions and answers.

- When you start Wireshark, you may get the following message: "The NPF driver isn't running. You may have trouble capturing or listing interfaces." If so, then you need to:

  i) stop Wireshark;
  ii) start the WinPcap driver as shown in Figure 1 above; and
  iii) restart Wireshark.

- You can set preferences using the Edit:Preferences menu in the main Wireshark window.
- You can control packet capture using the Capture menu in the main Wireshark window.
- If you capture packets and see the HTTP message "304 Not Modified," it means the requested content is in the browser's cache. For the purposes of this project, you should:

  i) clear your browsers cache,
  ii) restart the packet capture in Wireshark; and
  iii) try the access again.

- By default, the Time values in Wireshark's display are expressed in seconds.