Instruction

In this Mini-Project, we are going to learn to use Wireshark to investigate the behavior of the celebrated **TCP protocol** in detail. We will do so by analyzing a pcap file (see "Pcap File" on the project page) recording multiple network connections. However, for some simple tasks to begin with, you may also need to create your own trace. This assignment aims to enhance your practical skills in network traffic analysis and improve your understanding of the TCP protocol.

Requirement (for all questions): When answering a question, if possible, you should show a **screenshot** of your window or the **printout** of packets, then explain your answer shortly. **Screenshots without explanation will only receive half credit**. Make sure all the screenshots are neither too big nor small and font size set properly.

Submission: Compile your report in a single pdf file **no more than 10 pages** and submit to `https://send2me.cn/_5SOll8F/TcOgtjqQAWi-nw`. Lengthy report will only harm your grades – Don't nei-juan! Spend your time wisely, preferably on more valuable things!

Task List

1. Wireshark Basics (10%)

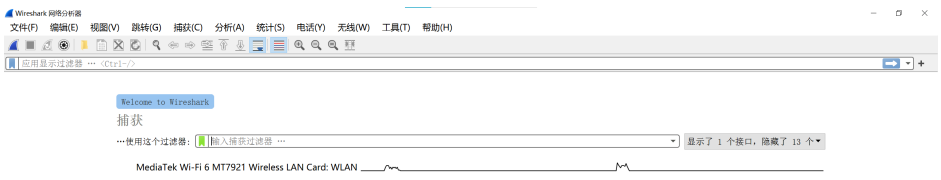
Before we dive into exploring TCP, let us first familiarize ourselves with the tool for all these tasks, i.e., **Wireshark**. It is a powerful (free!) network protocol analyzer, which you can perform various operations on. You will need it for most tasks in this mini-project.

Download: Wireshark.

Installation: Choose the correct version for your device and follow the installing instructions will do. (Any version on any operating system is okay as long as you can finish these tasks. For troubleshooting, please search the web.)

Now we shall begin.

Open Wireshark, and you'll see the window similar to figure shown below (details may vary from different versions, here's only an example.):



To use Wireshark, you may need to configure it first. Right at the bottom of the window

listed several links to help you with it. You are also recommended to search the web for some detailed instructions.

After configuration, do the following:

(1) Begin packet capture(*Capture* → *Start*)

(2) Launch your browser and go to sse.tongji.edu.cn

(Before this step, you are recommended to close other browser pages first.)

(3) Wait for a few seconds, go back to Wireshark and stop capturing.

Tip 1. It's quite normal that you see a large number of records in the window. But you can select the useful ones by *filtering* it! (Use the input bar under the tab to filter what you want, search the web for help if you do not know how to write a filter properly.)

Tip 2. To print a packet, click *File* → *Print*, choose *Selected packet only*, choose *Packet summary line*. In either way, you're encouraged to show as less packets as you can to support your answer (by filtering or other ways).

Now answer questions 1.1 - 1.2

Q 1.1(**5%**): What is the IP address used by your own computer, and the IP address of sse.tongji.edu.cn? (You're required to show the **timestamp** in the form of (**yyyy/mm/dd exact time**) in your screenshot/printout, change of default setting may be needed.)

Q 1.2 (**5%**): Now try launching some other applications on your computer (e.g., QQ, Wechat ...) that can **access the Internet**. Start capturing again while leaving the website you just accessed **open**, wait for a few seconds then stop.

What can you see from the packet trace? Use *filter* to show the **two** (There may be more connections on your laptop, but you only need to show two of them for this) connections respectively, including the filter statement you used.

2. TCP Basics

We'll be exploring TCP protocol in this section. What you just did in part 1 is still useful and we'll start from this. Consider about the connection between your laptop and sse.tongji.edu.cn for questions **2.1 - 2.3**

Q 2.1 (**5%**):

a. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the source and destination?

b. What in the segment identifies the segment as a SYN segment?

Q 2.2 (**10%**):

a. What is the sequence number of the SYNACK segment sent by destination to the source in reply to the SYN?

b. What is the value of the Acknowledgement field in the SYNACK segment?

c. How did the destination determine the value in acknowledgement field?

d. What is it in the segment that identifies the segment as a SYNACK segment?

Q 2.3(**5%**): Now you may know about the "three-way handshake" better! Is it possible to establish a TCP connection with less "handshakes" ? Give your reasons.

Now it's time for more challenging tasks! Open **Multiconnections2023.pcapng** using Wireshark. As you can read from its name, there were several connections in this file. **Please read the requirements carefully.**

Q 2.4(**15%**): Pick **one** segment in the TCP connection you chose.

a. At what time was it sent?

b. When was the ACK for this segment received?

c. What is the length of the segment?

d. Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for this segment? Show your process and a plot for the segment you chose.

   Hint: Select a TCP segment in the"listing of captured packets" window that is being sent from the source to the destination. Then select: *Statistics* → *TCP Stream Graph* → *Round Trip Time Graph.*

Q 2.5(**25%**): Similar as mentioned above, open **Time Sequence(tcptrace)** and other useful plots to answer following questions. (For this question, analyze the connection between **100.75.250.48** and **120.233.43.93)**

a. You may notice that for a TCP connection, plot of **tcptrace** differs from directions of transmission. There's a relating concept about it. Find out the concept, explain it and give another example.

b. Analyze the plot(s). Does the lack of receiver buffer space ever throttle the sender? How did you identify it?

c. Maybe you've found out that the connection isn't very "smooth". Were there any congestion during the whole process and can you evaluate their severity? (you don't need to give a specific quantitative indicator, qualitative ones will do. There's no standard answer to this, logic is all you need.)

d. What actions did TCP connection take when retransmission is needed?(e.g. scale of window size, changes of sequence number) Make some reasonable assumptions on potential causes of transmission failure and try to give your ideas on how to prevent them(Same as Q 2.5.c, logic is all you need.).

Q 2.6(**10%**):How to calculate throughput (bytes transferred per unit time) for chosen TCP connection? You only need to explain how to do this.

Q 2.7(**10%**): Find out when the TCP connection is terminated, analyze and explain the "four-way handshake" process).

Illustrate your understanding with **visualization**(figures are needed for this. Any tools used in plotting is okay as long as you can make it clear.)

Q 2.8(**5%**): About the termination process, is it possible to end a TCP connection with less "handshakes" ? Give your reasons.

Feedback (5%)

Please also write down your ideas about this mini-project and how long it took you to finish it. This assignment is being posted for the first time this year and your feedback is greatly needed! Thank you!

Any kind of comment will not have an impact on your grades of this mini-project, except you write nothing.

Grading Rubrics

Completeness, Correctness, Simplicity, Format.