Introduction to Computer Network Project 3

TCP

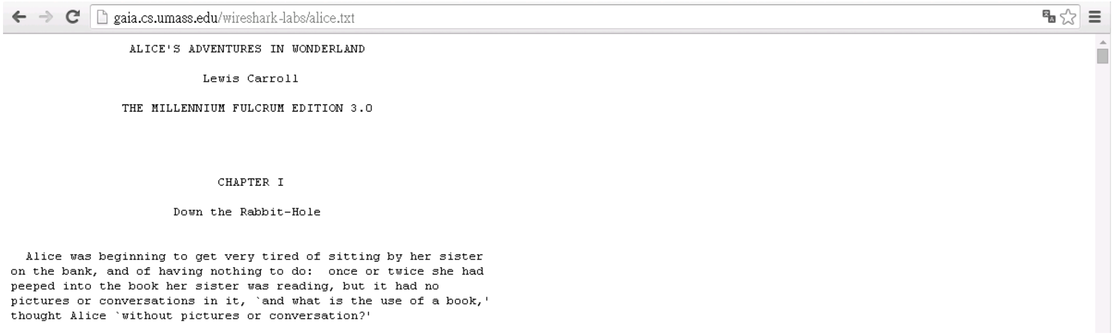
● Purpose

In this lab, we will go into the detail about how TCP works in practice. You need upload a file from the local to the designated server (website); Wireshark takes charge of capturing the round trip packets. Finally, you should analyze captured data and answer the questions.

● Introduction

Step 1:

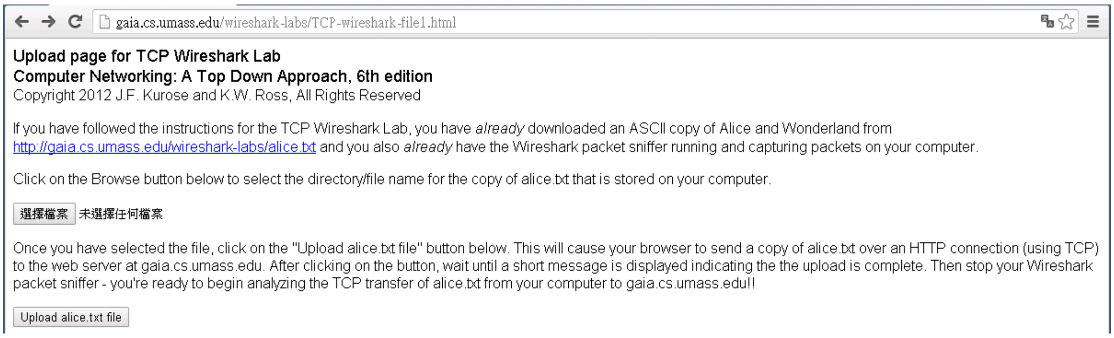
Go to http://gaia.cs.umass.edu/wireshark-labs/alice.txt and save the content as “alice.txt” to your computer. (Hint. Ctrl+S)



```
                ALICE'S ADVENTURES IN WONDERLAND

                          Lewis Carroll

               THE MILLENNIUM FULCRUM EDITION 3.0



                            CHAPTER I

                      Down the Rabbit-Hole


  Alice was beginning to get very tired of sitting by her sister
on the bank, and of having nothing to do:  once or twice she had
peeped into the book her sister was reading, but it had no
pictures or conversations in it, `and what is the use of a book,'
thought Alice `without pictures or conversation?'
```

Step 2:

Go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html and upload the file you just saved. (Hint. Before click “Upload alice.txt”, Wireshark MUST have started capturing.)



Upload page for TCP Wireshark Lab
Computer Networking: A Top Down Approach, 6th edition
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

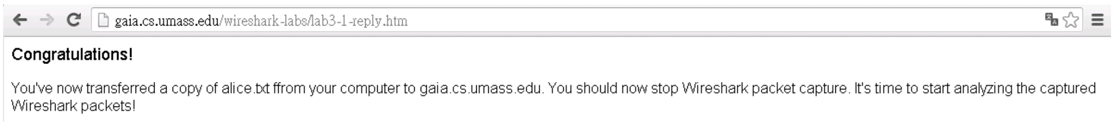
If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from http://gaia.cs.umass.edu/wireshark-labs/alice.txt and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to gaia.cs.umass.edu!!

Step 3:

While the website returns some phrases including “Congratulations!”, the transmission between the client and server is done. Stop capturing packets.



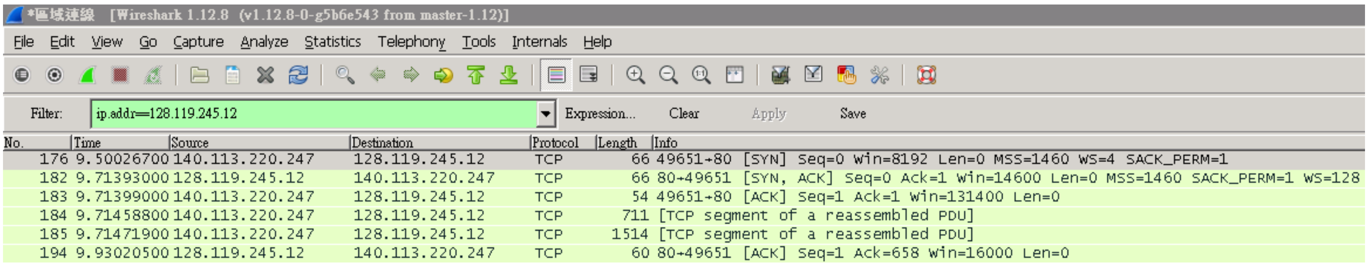
Congratulations!

You've now transferred a copy of alice.txt ffrom your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!

Tips:

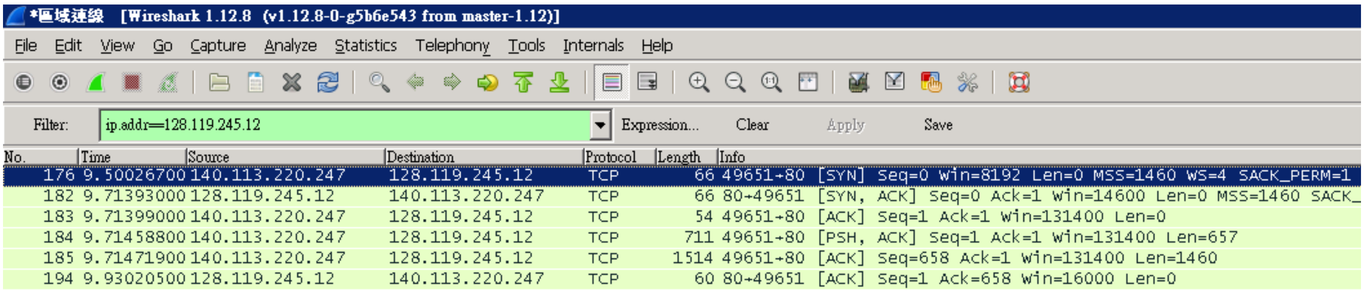
- Wireshark can export packet information as .pcapng file:
  1. File->Save (Need to stop capturing packet first)

- You can make Wireshark not to interpret the data as application layer data (e.g. HTTP). It's more convenient to observe the TCP header information.
  1. Analyze->Enabled protocols
  2. Uncheck "HTTP"
  3. Apply


*區域連線 [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.addr==128.119.245.12

```
No.   Time       Source          Destination     Protocol Length Info
  176 9.50026700 140.113.220.247 128.119.245.12  TCP        66 49651→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  182 9.71393000 128.119.245.12  140.113.220.247 TCP        66 80→49651 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
  183 9.71399000 140.113.220.247 128.119.245.12  TCP        54 49651→80 [ACK] Seq=1 Ack=1 Win=131400 Len=0
  184 9.71458800 140.113.220.247 128.119.245.12  TCP       711 [TCP segment of a reassembled PDU]
  185 9.71471900 140.113.220.247 128.119.245.12  TCP      1514 [TCP segment of a reassembled PDU]
  194 9.93020500 128.119.245.12  140.113.220.247 TCP        60 80→49651 [ACK] Seq=1 Ack=658 Win=16000 Len=0
```


*區域連線 [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.addr==128.119.245.12

```
No.   Time       Source          Destination     Protocol Length Info
  176 9.50026700 140.113.220.247 128.119.245.12  TCP        66 49651→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  182 9.71393000 128.119.245.12  140.113.220.247 TCP        66 80→49651 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_
  183 9.71399000 140.113.220.247 128.119.245.12  TCP        54 49651→80 [ACK] Seq=1 Ack=1 Win=131400 Len=0
  184 9.71458800 140.113.220.247 128.119.245.12  TCP       711 49651→80 [PSH, ACK] Seq=1 Ack=1 Win=131400 Len=657
  185 9.71471900 140.113.220.247 128.119.245.12  TCP      1514 49651→80 [ACK] Seq=658 Ack=1 Win=131400 Len=1460
  194 9.93020500 128.119.245.12  140.113.220.247 TCP        60 80→49651 [ACK] Seq=1 Ack=658 Win=16000 Len=0
```

- Question

(Notice: Wireshark uses relative sequence/ack number. You should check ASCII encode or change TCP setting for actual value.)

1. (For Client) What is the IP address and TCP port number used by the client computer that is transferring the file to gaia.cs.umass.edu?
2. (For Server) What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
3. 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?
4. What is the value of the ACK field in the SYN-ACK segment? What is it in the segment that identifies the segment as a SYN-ACK segment?
5. What is the sequence number of the TCP segment containing the HTTP POST command? (hint. http.request.method == POST)
6. What is the negotiated MSS (maximum segment size)?
7. What is the minimum amount of available buffer size (receive window) advertised by the client?
8. What is the throughput (bytes transferred per unit time) for the TCP connection (except 3-way handshake)? Explain how you calculated this value.

- Bonus

1. Why "TCP segment of a reassembled PDU" message appears in the Wireshark? How does hosts identify the TCP segments which belong to same application message? (10%)

- Requirement

1. Answer each question sequentially with the screenshots or exporting texts, and give some explanations. (10% of each)
2. Write down your thoughts or learnings during this lab. (20%)
3. Do not cheat, or you will get ZERO.
4. Upload your report (project3_studentID.pdf) to E3, and the deadline is 12/11 23:59.
5. Please upload only PDF files
6. If you have any question, contact TAs (icnta@win.cs.nctu.edu.tw) or come to EC638.