# Wireshark Lab #3 - TCP

**수업코드 12175**

**2018079116 정진성**

**1. What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt 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).**

IP address: 192.168.0.2

TCP port number: 61855

**2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?**

IP address: 128.119.245.12

Port number: 80

**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? (Note: this is the "raw" sequence number carried in the TCP segment itself; it is NOT the packet # in the "No." column in the Wireshark window. Remember there is no such thing as a "packet number" in TCP or UDP; as you know, there are sequence numbers in TCP and that's what we're after here. Also note that this is not the relative sequence number with respect to the starting sequence number of this TCP session.). What is it in this TCP segment that identifies the segment as a SYN segment? Will the TCP receiver in this session be able to use Selective Acknowledgments (allowing TCP to function a bit more like a "selective repeat" receiver, see section 3.4.5 in the text)?**

TCP SYN segment sequence number: 1829903733 (relative sequence number: 0)

SYN flag의 bit가 1로 set 되었음으로 인해 SYN segment임을 식별할 수 있다.

TCP option에서 SACK permitted를 확인할 수 있기 때문에 SACK을 사용할 수 있다.

**4. 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 it in the segment that identifies the segment as a SYNACK segment? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?**

Sequence number: 1926806039 (relative sequence number: 0)

Flag 의 Acknowledgment bit 가 1 로 set 되고, SYN flag bit 가 1 로 set 되었으므로 SYNACK 임을 알 수 있다.

Acknowledgment field 의 값은 1 이고, 초기 SYN segment 의 sequence number + 1 이다.

**5. What is the sequence number of the TCP segment containing the header of the HTTP POST command? Note that in order to find the POST message header, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text "POST" within its DATA field 4,5. How many bytes of data are contained in the payload (data) field of this TCP segment? Did all of the data in the transferred file alice.txt fit into this single segment?**

Sequence number: 2842354685 (relative sequence number: 1)

TCP payload: 728bytes

Single segment로 모든 데이터를 전송하지 못했다. Alice.txt는 149kb이기 때문이다.

**6. Consider the TCP segment containing the HTTP "POST" as the first segment in the data transfer part of the TCP connection.**

**• At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent?** Dec 4, 2023 12:53:17.931184000 대한민국 표준시

**• At what time was the ACK for this first data-containing segment received?** Dec 4, 2023 12:53:18.156007000 대한민국 표준시

**• What is the RTT for this first data-containing segment?** 12:53:18.156007000 - 12:53:17.931184000 = 0.224823

**• What is the RTT value the second data-carrying TCP segment and its ACK?** 12:53:18.156007000 - 12:53:17.931184000 = 0.224823

**• What is the EstimatedRTT value (see Section 3.5.3, in the text) after the ACK for the second data-carrying segment is received? Assume that in making this calculation after the received of the ACK for the second segment, that the initial value of EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242, and a value of α = 0.125.**

**Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph- >Round Trip Time Graph.**

EstimatedRTT: (0.875) * 0.224823 + (0.125) * 0.224823 = 0.224823

**7. What is the length (header plus payload) of each of the first four data-carrying TCP segments?**

Segment1: 728 bytes

Segment2: 1460 bytes

Segment3: 5840 bytes

Segment4: 5840 bytes

**8. What is the minimum amount of available buffer space advertised to the client by gaia.cs.umass.edu among these first four data-carrying TCP segments? Does the lack of receiver buffer space ever throttle the sender for these first four data-carrying segments?**

Minimum: 513

Window size가 240에서 263, 354, 445로 늘어난 것으로 보아 receiver는 충분한 buffer space를 가지고 있었기 때문에 throttle하지 않았을 것이다.

**9. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?**

재전송된 segments들은 없다. 이는 wireshark의 time-sequencenumber 그래프에서 모든 sequence number가 단조롭게 증가하는 것으로 알 수 있다. 재전송되었다면 같은 sequence number가 발견되었을 것이다.

**10. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to gaia.cs.umass.edu? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 in the text) among these first ten data-carrying segments?**

Segment1: 728 bytes, Segment2: 1460 bytes, Segment3: 5840 bytes, Segment4: 5840 bytes, Segment5: 1460 bytes, Segment6: 23360 bytes, Segement7: 2920 bytes, Segment8: 1460 bytes, Segment9: 20440 bytes, Segment10: 17520 bytes

Segment3과 4가 동일한 5840 bytes를 전달하기 때문에 case where the receiver is ACKing every other received segment를 찾을 수 있다.

**11. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.**

Alice.txt의 크기가 152,138 bytes이고, 이 크기를 마지막 ack 패킷의 전송시간과 처음 패킷의 전송시간을 뺀 걸린 시간으로 나누어 throughput을 구할 수 있다.

Throughput: 152138(bytes) / 1.041704(sec) = 146,047.2456667153 (bytes/sec)

**12. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Consider the "fleets" of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase. Figure 6 shows a slightly different view of this data.**

t=0.025, 0.053일때는 slow start phase인것으로 보인다. Seq number가 지수적으로 급격히 증가하는 양상을 띠기 때문이다. t=0.1일 때에는 seq number의 증가 속도가 줄어, 지수함수적 모양이 아닌 점진적으로 증가하는 양상을 때기 때문에 congestion avoidance phase 인 것으로 판단된다.

**13. These "fleets" of segments appear to have some periodicity. What can you say about the period?**

발견할 수 있는 periodicity는 네트워크의 대역폭이나, 혼잡제어 메커니즘에 의해 나타날 수 있다.

**14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu**

내 plot을 관찰해보면 크기가 작아 많은 sequence number가 발생하지 않아서 확실하게 판단하기는 어렵지만, seq num이 지수적으로 끝까지 증가하는 것으로 확인된다. 따라서 혼잡제어가 발생하지 않은 slow start phase에서 파일의 전송이 끝난 것으로 판단할 수 있다.