Wireshark Lab 3

Trevor Bramwell
CS372 - Introduction to Computer Networks
Wireshark Lab 3: TCP

February 9, 2012

2 A first look at the capture trace

2.1

See 2.3

2.2

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

Answer
The IP address of gaia.cs.umass.edu is *128.119.245.12*. It is sending and recieveing on port *80*.

```
No.     Time        Source                Destination           Protocol Length Info
    159 12.491446   10.0.1.25             128.119.245.12        HTTP     347    POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)

Frame 159: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits)
Ethernet II, Src: Azurewav_66:dd:8f (00:25:d3:66:dd:8f), Dst: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.25 (10.0.1.25), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 43535 (43535), Dst Port: http (80), Seq: 152685, Ack: 1, Len: 281
[107 Reassembled TCP Segments (152965 bytes): #14(644), #15(1448), #16(1448), #17(1448),
    #19(1448), #21(1448), #22(1448), #23(1448), #25(1448), #26(1448), #27(1448), #29(1448), #30(1448),
    #31(1448), #33(1448), #34(1448), #35(1448), #37(1448)]
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryNfqNLZXx7ZLACwjF"
```

2.3

Question
What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

Answer
The IP address of my client computer is *10.0.1.25* The TCP port is *43535*

3 TCP Basics

3.4

Question
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?

Answer
The sequence number is 0. The flags are set to 0x02 [0000 0000 0010].

```
No.     Time        Source                Destination           Protocol Length Info
     10 11.916542   10.0.1.25             128.119.245.12        TCP      74     43535 > http [SYN] Seq=0 Win=14600 Len=0
        MSS=1460 SACK_PERM=1 TSval=256195 TSecr=0 WS=16

Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Azurewav_66:dd:8f (00:25:d3:66:dd:8f), Dst: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
Internet Protocol Version 4, Src: 10.0.1.25 (10.0.1.25), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 43535 (43535), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 43535 (43535)
    Destination port: http (80)
    [Stream index: 3]
    Sequence number: 0    (relative sequence number)
    Header length: 40 bytes
    Flags: 0x02 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgement: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
    Window size value: 14600
    [Calculated window size: 14600]
    Checksum: 0x80cb [validation disabled]
    Options: (20 bytes)
```

3.5

Question

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

Answer

The sequence number of the SYNACK segment is 0. The ACKnowledgement field is
set to 1. gaia.cs.umass.edu determined that value from it recieving a packet. The flags 0x12 identify the segment as a SYNACK segment.

```
No.     Time        Source                Destination           Protocol Length Info
     12 12.018131   128.119.245.12        10.0.1.25             TCP      74     http > 43535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
        MSS=1460 SACK_PERM=1 TSval=1267473327 TSecr=256195 WS=128

Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: Azurewav_66:dd:8f (00:25:d3:66:dd:8f)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.0.1.25 (10.0.1.25)
Transmission Control Protocol, Src Port: http (80), Dst Port: 43535 (43535), Seq: 0, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 43535 (43535)
    [Stream index: 3]
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 40 bytes
    Flags: 0x12 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgement: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
    Window size value: 5792
    [Calculated window size: 5792]
    Checksum: 0xf8ae [validation disabled]
    Options: (20 bytes)
    [SEQ/ACK analysis]
```

3.6

What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, youll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a POST within its DATA field.

3.7

Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see page 249 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 249 for all subsequent segments. 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.

3.8

What is the length of each of the first six TCP segments?

3.9

What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

3.10

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

3.11

How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 257 in the text).

3.12

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

4 TCP congestion control in action

4.13

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. Can you identify where TCPs slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that weve studied in the text.

4.14

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