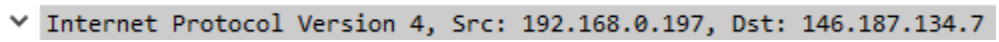
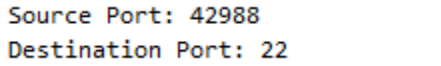
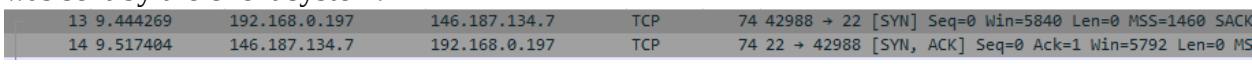
Lab 4 – Wireshark TCP

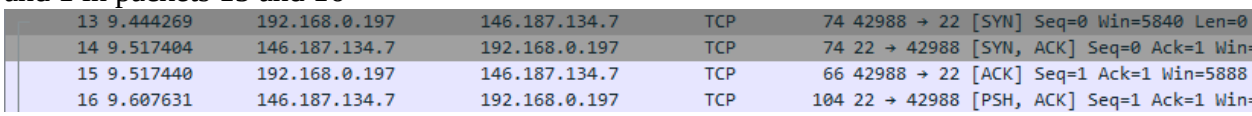
CSCD 330
Ian Kaiserman

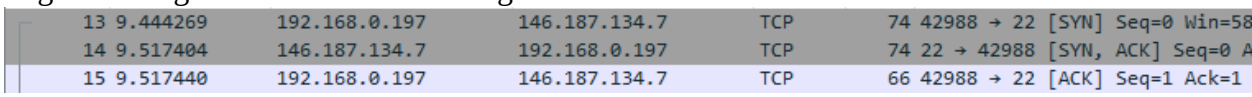
Questions

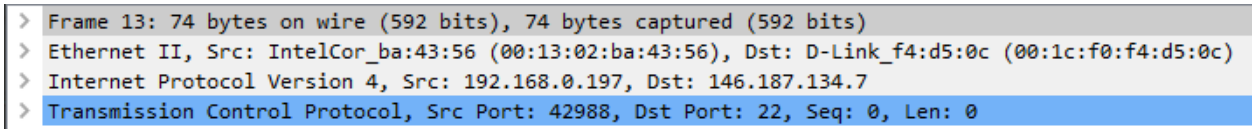
1. What is the IP address of the client and what is the IP address of the remote machine in this trace?
    a. Client IP: 192.168.0.197 (local network address)
    b. Remote machine IP: 146.187.134.7
    c. 

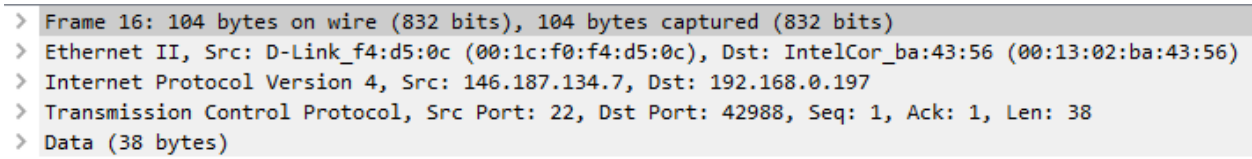
2. What port numbers are being used for the client and remote machine?
    a. 22, 42988 (switching back and forth depending on if it's a sent packet or an ACK)
    b. 

3. What packet numbers are involved in the initiation of the TCP ssh session? How can you tell TCP is starting a new session?
    a. Packet numbers 13 and 14 indicate a successful initiation of the ssh session, since packet 13 is the only packet that is not an ACK, and the packet right after, with the same sequence number of 0, is an acknowledgment of that information that was sent by the client system.
    b. 

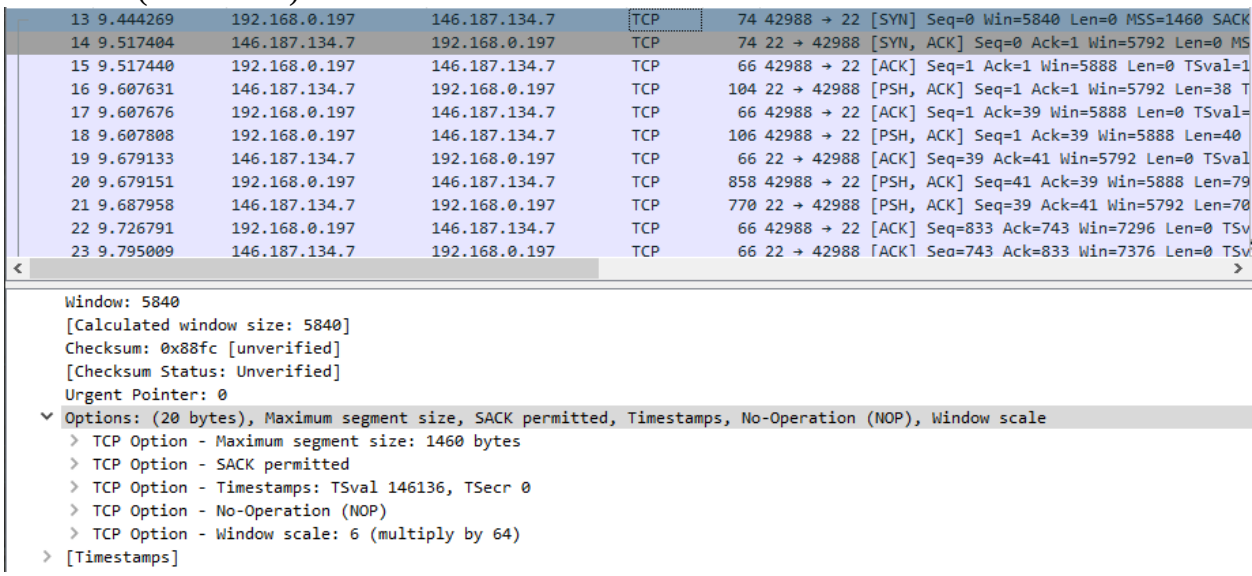
4. What are the sequence numbers of the client and remote machine in the beginning?
    a. Sequence numbers of the first transmissions of data are 0 in packets 13 and 14 and 1 in packets 15 and 16
    b. 

5. Is any data being sent during TCP initiation? How can you tell?
    a. No, as there is no Data header in the first three packets (13-15), as well as no PSH flag indicating that information is being sent.
    

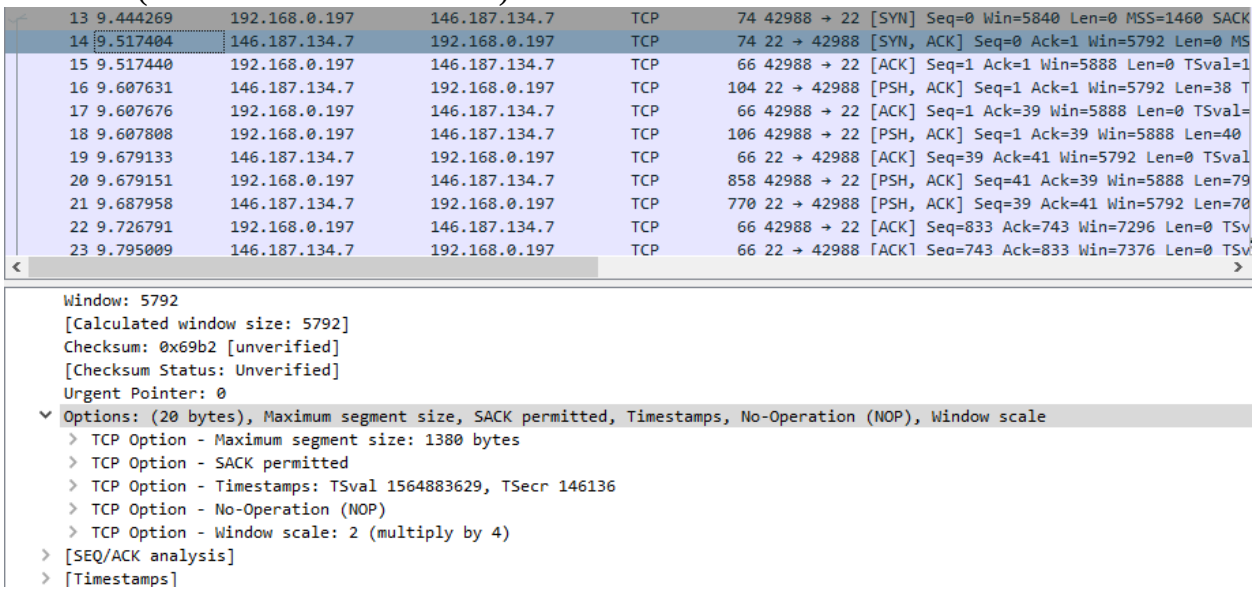
    Packet 13
    

    Packet 16
    

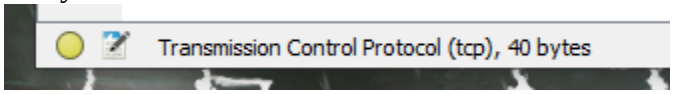
6. What is the Maximum Segment Size on both machines (MSS)? What is the meaning of the MSS?
    a 1460 bytes on the client, 1380 on the remote machine.
    b The two MSS values essentially determine the maximum segment size that is going to be supported during the transactions which is going to be the smaller of the two, in this case 1380 bytes.
    c Packet 13 (from client)



    d Packet 14 (ACK from remote machine)



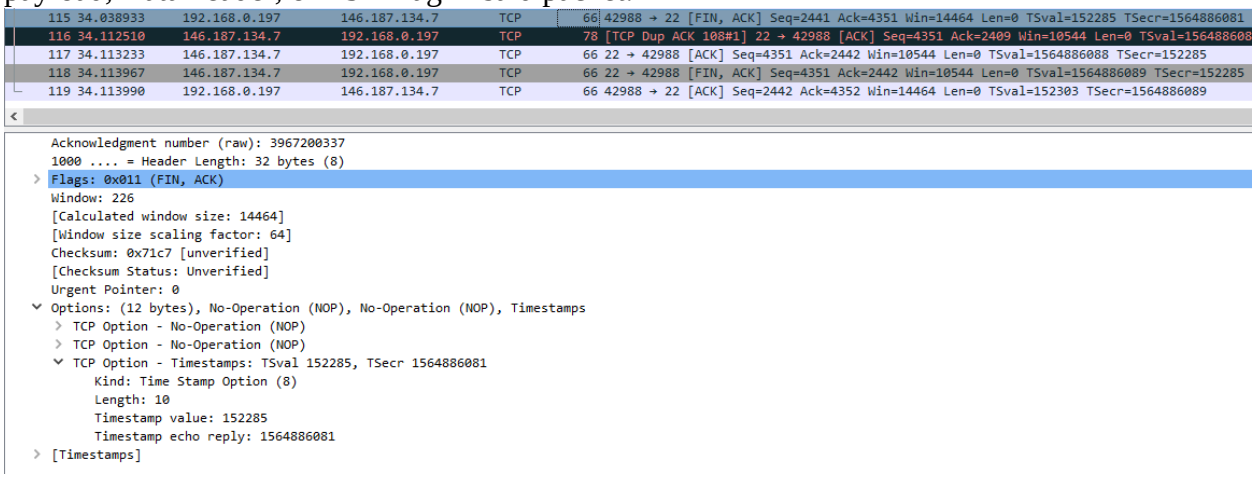
7. How many bytes are in the TCP header?
    a 40 bytes in total



8. What is the smallest window size during this entire connection? What is the meaning of the win field?

a. The smallest window size in the connection is 92 with a scaling factor of 64. The window field shows how much information the receiving side is willing to receive at that moment.

9. In this trace, packet 16 and on up has the PSH flag set. What does this flag mean? Why do you think it is set in this trace?
    a. The PSH flag indicates that data, or a payload, is being sent from the source to the destination. The fact that it was set in various moments in this trace likely means that data was being transferred between client/remote machine or vise versa over SSH in those moments.
10. Can you see the ASCII (American Standard Code for Information Interchange) commands typed in this ssh session and the data returned? Why or why not?
    a. There were several earlier packets where discernable phrases were seen in the payload, things like “Diffie-hellman-group-exchange”, but nothing seemed to be apparent “commands”, so from my perspective I would say no. I believe that’s because the commands themselves wouldn’t be things that are sent over SSH, because SSH itself would be doing the heavy-lifting for those commands, and give much more precise commands to the remote machine on what to do and what to send back to the client.
11. View the last few packets of this trace file. Which side sent the first FIN packet? Does the FIN packet seem to be counted as data? How can you tell?
    a. The client sent the first FIN packet. It is not counted as data, since there is no payload, Data header, or PSH flag in said packet.



A Different Look

Now, we can view some overall statistics for this trace. Click on Statistics, then Flow Graph. In the Flow Graph window, find the “Flow type:” pull down menu at the bottom; select TCP flow. This graph displays the flow of data and the sequence and acknowledgement numbers. Answer the next two questions from this graph.

12. From the first SYN packet until the last ACK of the final FIN packets, how long did this session last?

a. Assuming the time numbers are in seconds, the whole session lasted around 24.67 seconds.

13. How much data was sent from the remote machine?
    a.

Finally, let us look at some other way to graph the TCP flow. Back in the main Wireshark window, click on Statistic and then TCP Stream Graph. Choose Round Trip Time Graph. Answer the question below.

14. Does it appear that the packets are being sent at a constant rate? What is the average RTT?
    a. Not at all. The graph is extremely sporadic and shows no constant rate.