**Assignment 7**

**Wireshark and TCP**

due: Thursday, April 12

60 points

**description**

In this assignment, you'll examine pre-captured packets with Wireshark. The purpose of the assignment is to see real protocols in action.

**installing Wireshark**

Wireshark is already installed on the Linux partitions on the lab computers. You'd need to have administrative privileges in order to capture packets, but this isn't necessary for this assignment.

If you'd prefer, you may work on this assignment at home. Wireshark and instructions for installing it on your operating system of choice may be found on the [Wireshark website](http://www.wireshark.org/).

To answer the questions, download the following [packet capture file](https://cis.temple.edu/~jfiore/2016/fall/3329/assignments/09/sb.pcap) and open it in Wireshark.

**questions**

1. In which packet can you find an HTTP GET?
2. What web page was visited?
3. What browser was used?
4. What version of HTTP was used?
5. Was persistent or non-persistent HTTP used? How can you tell?
6. In the client's request, what other information about the browser and client OS were sent to the web server?
7. In the HTTP server's response, what information was sent about the server, e.g., what server software was used?
8. If we look at the content of the HTTP data, (click on one of the early segments in a TCP session on then go Tools, then Follow TCP Stream), why is it that we can't read the content of the files? (Hint: what does the server header Content-encoding: gzip mean?
9. In which packets do you see a [TCP three-way handshake](http://en.wikipedia.org/wiki/Transmission_Control_Protocol#Connection_establishment)?
10. What does Wireshark say the client's initial sequence number is? In my version of Wireshark, it says relative sequence number. What does this mean?
11. What is ACK number sent by the server during the second leg of the three-way handshake?
12. What sequence number is sent by the server during the second leg of the three-way handshake?
13. What is the ACK number sent by the client during the third leg of the three-way handshake?
14. In the first leg of the three-way handshake, how large is the TCP header? Is this larger than TCP's minimum header?
15. Is any data sent during the third leg of the three-way handshake? If so, what is it?
16. During the three-way handshake, what is the client's TCP advertised receive window? How does this value relate to the maximum possible?
17. What are the source and destination ports of the segments traveling from the client to the server?
18. What are the source and destination IP addresses of the datagrams traveling from the client to the server?
19. What are the source and destination ports of the segments traveling from the server to the client?
20. What are the source and destination IP addresses of the datagrams traveling from the server to the client?
21. In which segments do you find a [TCP connection close](http://en.wikipedia.org/wiki/Transmission_Control_Protocol#Connection_termination)? How can you tell?
22. In the packet containing the first leg of the three-way handshake, what is the value of the protocol (i.e., upper-layer-protocol) field in the IP header?

23 In this same packet's IP header, what is the value of the Identification field? What is the purpose of the Identification field? In what case would we expect to find the same Identification value in other packets?