Susana Noto
PS1

Report

For the assignment, I used the link http://www.northeastern.edu/. I also used wireshark to help capture all of the information when and after I clicked on the link.

First, there is a DNS query to find out the information about the Northeastern webpage. It uses UDP to do this. You can find this wireshark snippet under DNS in proof-log. Then, a query response is sent that includes the CNAME and IP address for the web page. (This is under DNS_ANSWER in the proof-log.)

Next, a TCP SYN packet is sent to the Northeastern webpage. Then, Northeastern sends an SYN-ACK back. Lastly, the browser sends ACK back to the webpage. This is the process of the three-way TCP handshake. (These are under the photos TCP_SYN, TCP_SYN_ACK, and TCP_ACK.)

Lastly, data is pushed to the computer through TCP. Usually, this would be seen as a GET request through HTTP, but this website uses encrypted HTTPs so it can be seen in PSH and ACK packets in wireshark. (This is under PSH in proof-log.)

In summary, there are a lot of steps a browser goes through when a user presses on a link. First, it does a DNS query to find the correct CNAME and IP address for the web page. Next, it goes through a three step TCP handshake with the server. Lastly, data is loaded onto the page through a series of packets.