Gasser Ahmed
gasser18@vt.edu
ECE 5484, Project 3

Section 1 – Objectives:

Reinforce the understanding of network protocols and the TCP/IP protocol suite by using Wireshark network protocol analyzer.

By following the steps below:

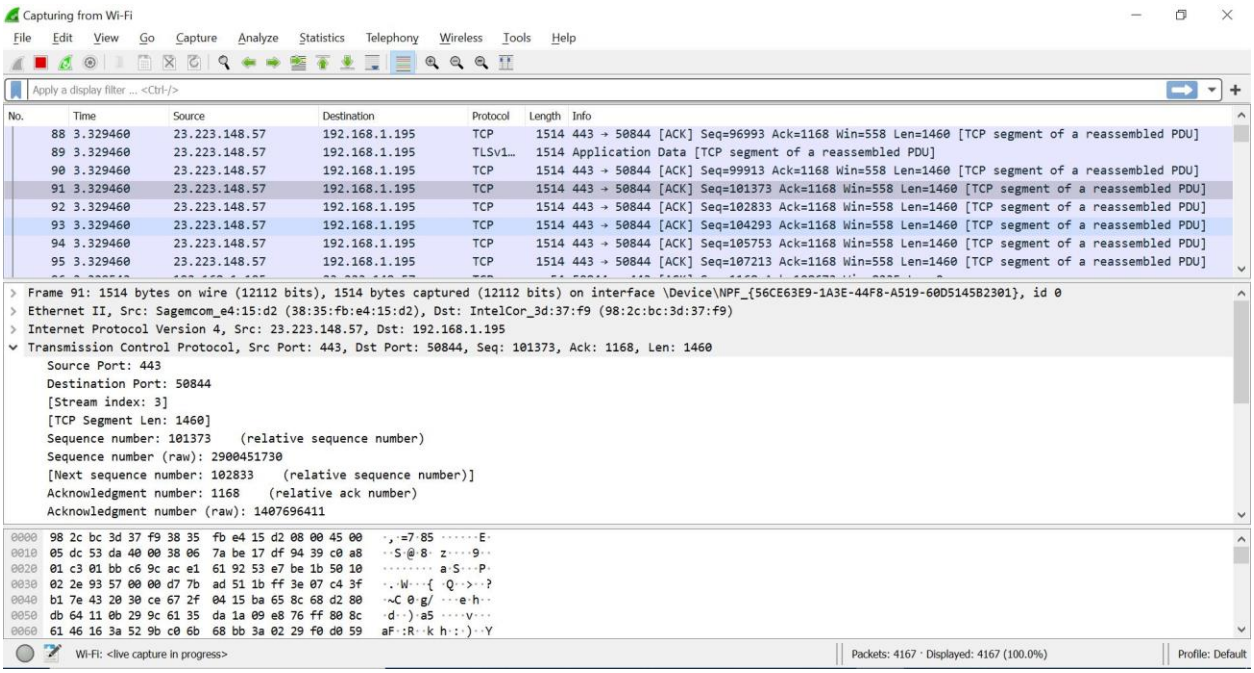
1. Install and become familiar with the basic operation of Wireshark.
2. Capture and analyze a simple HTTP transaction.

Section 2 – Wireshark Installation:

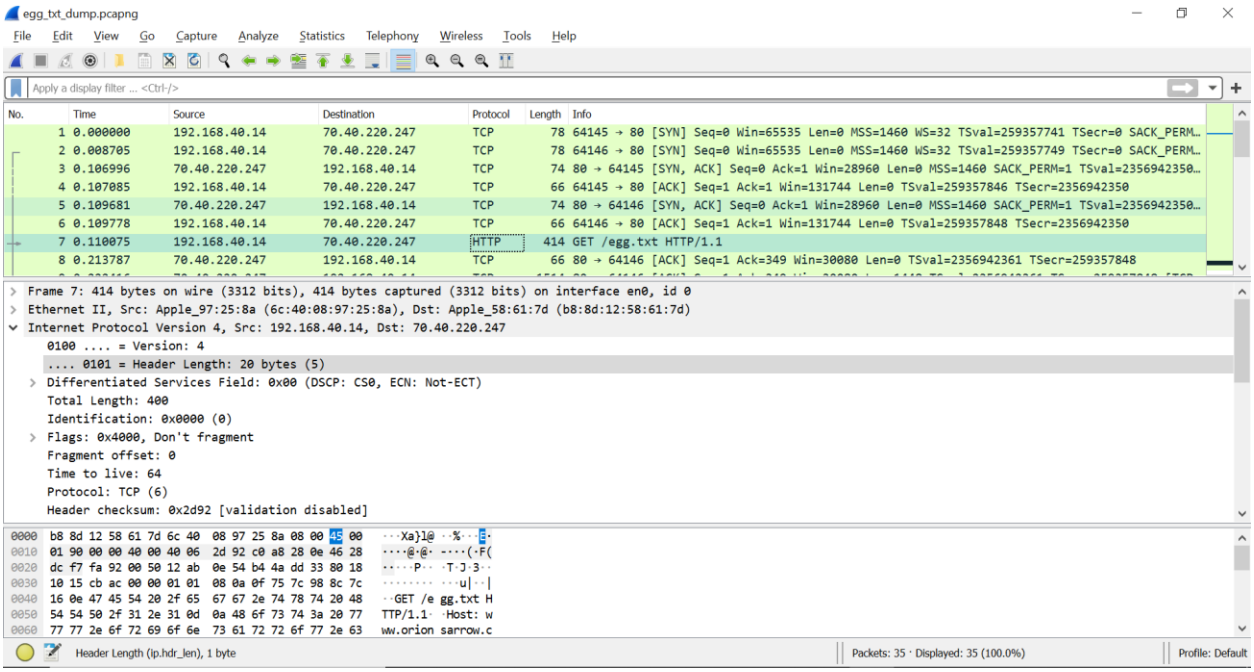
I was able to install Wireshark successfully. The installation process was very straight forward, and I did not face any problems or issues. Having Npcap waiting for my input to move forward with the setup while I was on the main Wireshark setup window was probably the trickiest part of the setup.

Section 3 – Familiarization:

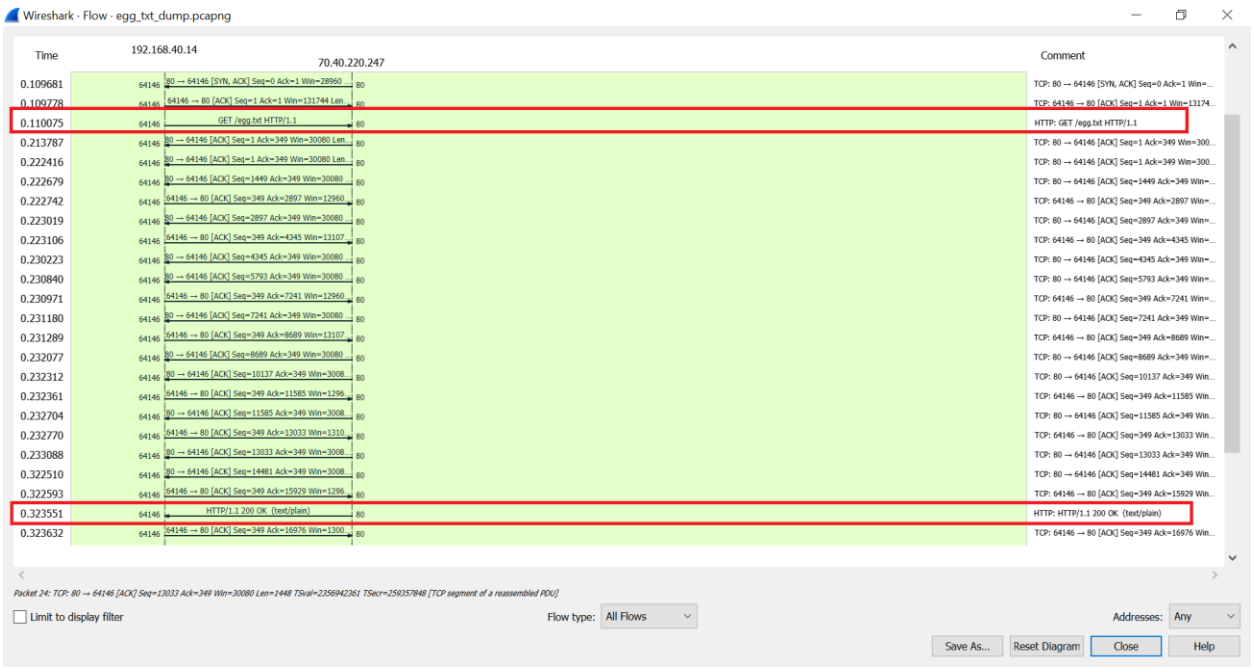
The familiarization process was straightforward and I didn't have any problems encountered during that phase.



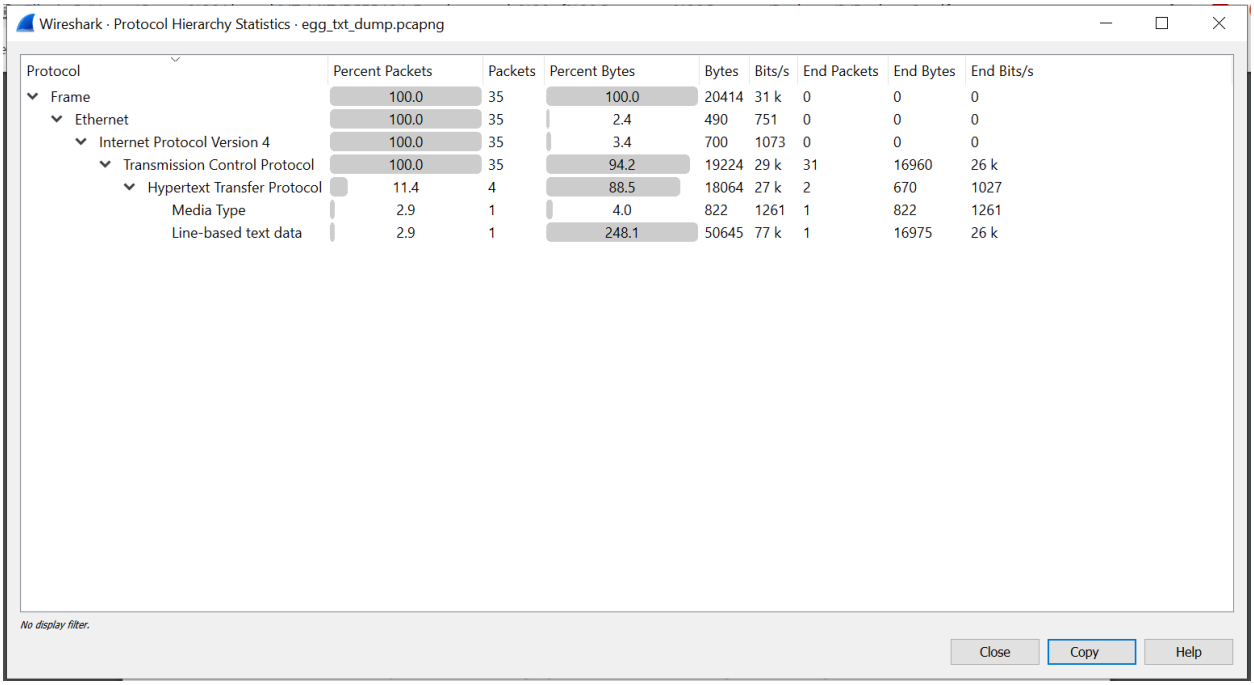
Section 4 – Protocol Analysis (Screenshots and Answers):



1. HTTP Response time for egg.txt: 0.323551 – 0.110075 = 0.213476 s

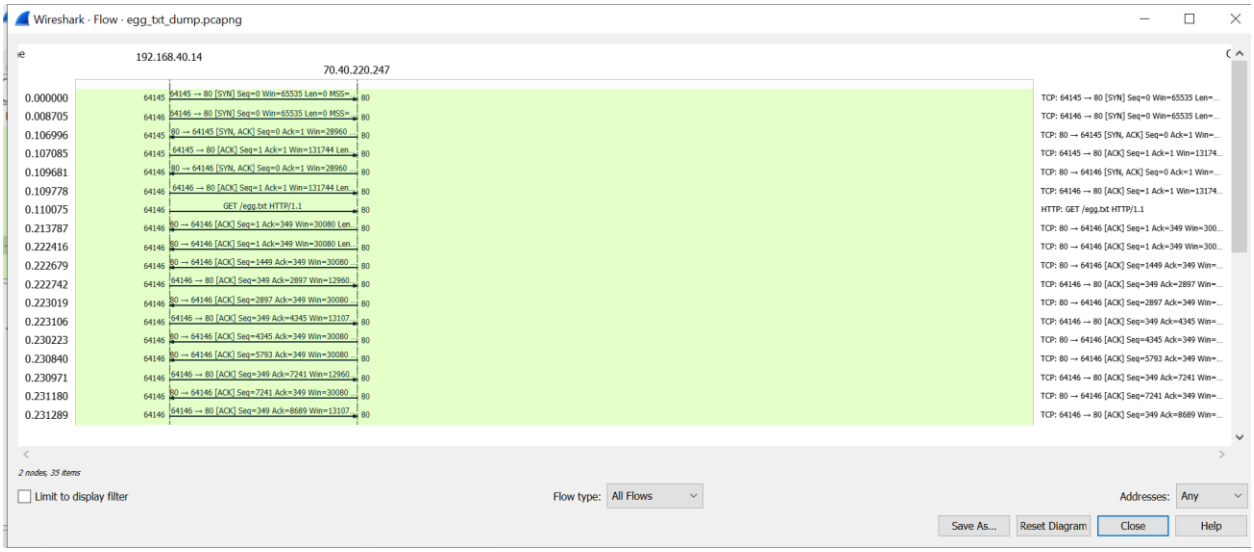


Protocol Hierarchy:



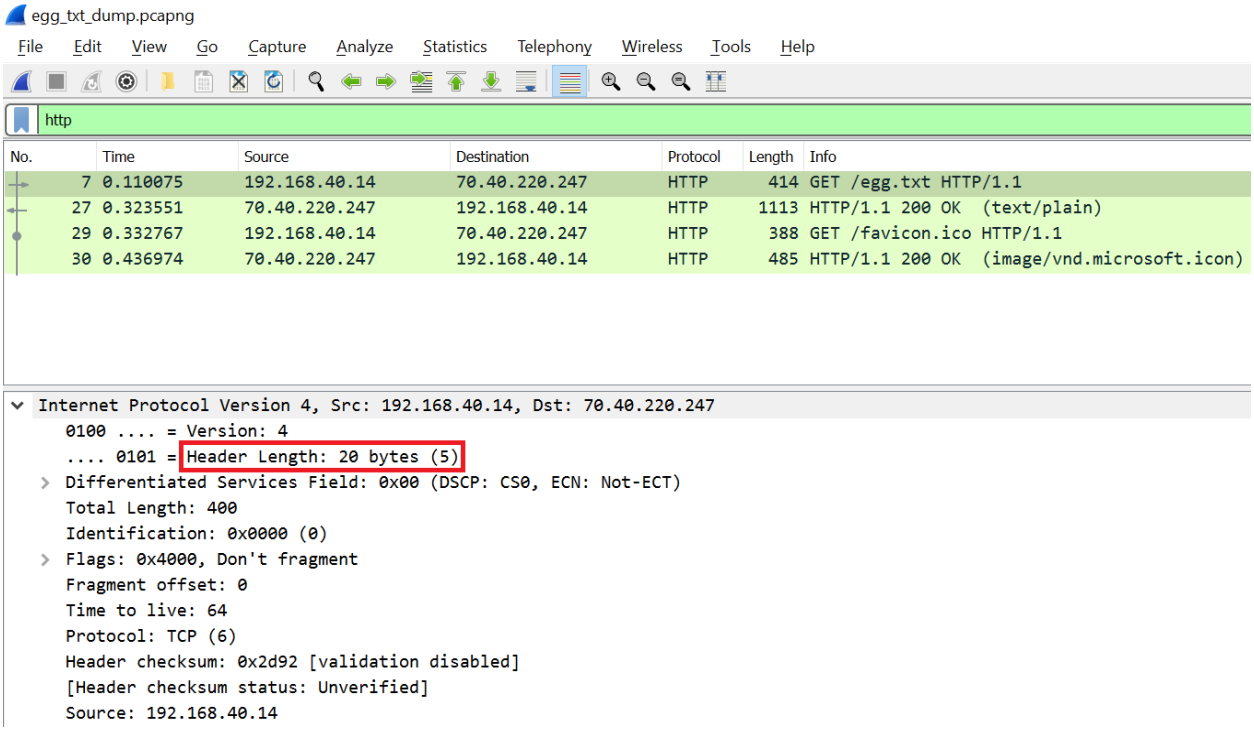
2. Percentage of the captured packets are using TCP: 100%
3. From the captured packets, an example Application Layer protocol that uses TCP: Hypertext Transfer Protocol (HTTP)

Flow Graph:

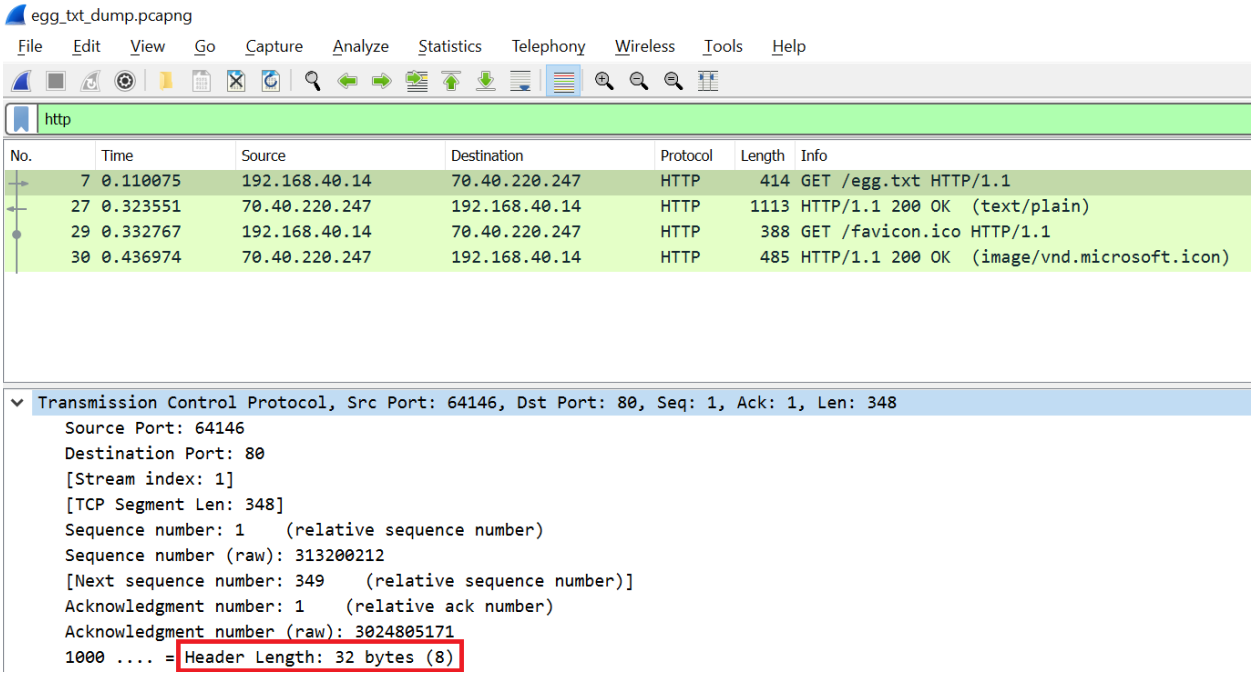


HTTP GET request Questions:

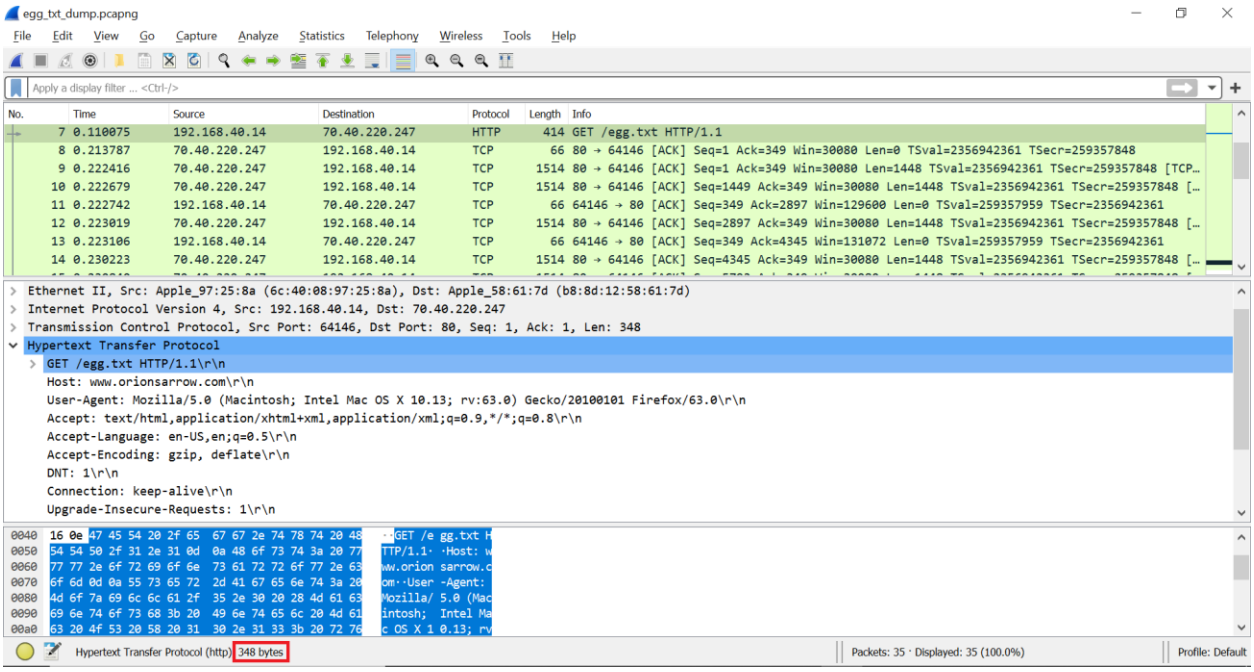
4. How many bytes are in the IP header? 20 bytes



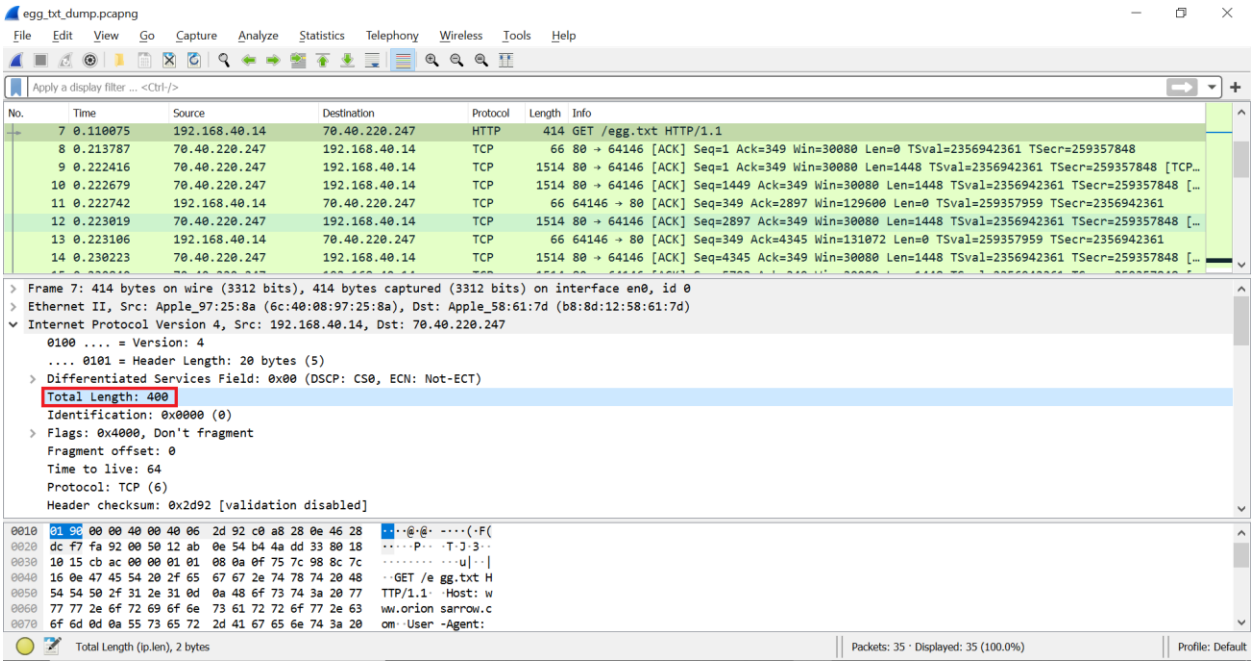
5. How many bytes are in the TCP header? 32 bytes



6. How many bytes are in the HTTP message? 348 bytes



7. What is the total length, in bytes, of the IP datagram carrying the IP header, the TCP header, and the HTTP message for the GET request? 400 bytes
(either by summing results of steps 4, 5, and 6 or by directly getting that number from Total Length under “Internet Protocol Version 4”)



Section 5 – Conclusions:

After going through the installation, familiarization, and protocol analysis phases, I was able to become more familiar with Wireshark and have a better understanding of what it does and how it works. However, the protocol analysis part was the trickiest part especially with questions 6 and 7 as it took me a long time to figure out how to get the number of bytes in the HTTP message and total length of the IP datagram.

In general, the project was very helpful in understanding Wireshark and having a deeper look into how network protocols work. Lastly, the approximate number of hours I devoted to the project was about 5-8 hours.