**ENSF 462 Lab 01 Report Completed by: Dominic Choi**

**UCID: 30109955**

Q1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

|  |
| --- |
| HTTP |

Q2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. (If you want to display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

|  |
| --- |
| 0.081062000 seconds |

Q3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer that sent the HTTP GET message? Lab 1 Getting Started with Wireshark Lab and Socket Programming

|  |
| --- |
| Address of gaia.cs.umass.edu: 128.119.245.12  Address of my computer: 10.13.139.7 |

Q4. Expand the information on the HTTP message in the Wireshark “Details of selected packet” window so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the “User-Agent:” field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are using.]  
• Example: Firefox, Safari, Microsoft Internet Edge, Other

|  |
| --- |
| Firefox |

Q5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark “Details of selected packet” window so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following “Dest Port:” for the TCP segment containing the HTTP request) to which this HTTP request is being sent?

|  |
| --- |
| 80 |

Q6. If you enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-  
file1.html multiple times during Wireshark packet capture, are there any difference  
in the sent HTTP message and the received HTTP reply?

|  |
| --- |
| Only the time is different |

Part 2 output

