**CS 6043/5143: Computer Networking**

**FALL 2019**

**PROJECT 2**

**Given: Oct. 8, 2019**

**Due: Oct. 21 (Monday), 2019 (NO LATER THAN 11:59PM)**

**Submission Instructions:**

1. Submit only on-line files on Blackboard before midnight. No hard copy will be accepted.

2. Wireshark files for this project can be found in the zip file “Project\_2\_Wireshark\_Traces.zip”.

**Total possible points: 10**

**Part I: UDP**

Open the file ‘UDP\_project\_2.pcapng’ in Wireshark and answer the following questions. Provide screenshots with necessary annotations in each case.

1. (0.5 pts) Find a UDP packet in the trace file and determine the name and length (in bytes) of each of the UDP header fields.
2. (0.5 pts) Using statistics feature of Wireshark, determine the percentage of IPv4 UDP packets in the capture.
3. (1 pts) The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.
4. (1 pts) What are the source port and length of the first UDP packet in the trace file? What is the largest possible source port number?
5. (1 pts) What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notations along with a screenshot of Wireshark showing those values.

**Part II: TCP**

Open the file ‘TCP\_project\_2.pcapng’ in Wireshark and answer the following questions. The trace file was captured while uploading ‘1600.txt’ file from a computer (10.63.7.192) to *gaia.cs.umass.edu* web server (128.119.245.12) using the HTTP POST method.

1. (1 pts) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and *gaia.cs.umass.edu*?
2. (1 pts) What are the sequence number and acknowledgement number of the first SYNACK packet sent from the server to the client computer? How were the values determined by the server? *(hint: relative seq and ack values displayed by Wireshark is fine, no need to show actual numbers)*
3. (1 pts) What are the minimum and maximum amount of available buffer spaces advertised at the receiver for the entire trace?
4. (1.5 pts) Are there any retransmitted segments in the trace file? What is the reasoning behind your answer?
5. (1.5 pts) What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.