Przemek Gardias

Wireshark Lab 3

1. The IP address of my host is 10.0.1.36. The IP address of the destination host is 103.235.46.39.
2. ICMP packets do not have source and destination port numbers because they do not communicate between application layers but instead communicate between network layers. They instead use a combination of type and code to identify the message which is being sent.
3. The referenced packet information is saved in the .zip as **packet1.pdf**. The ICMP type is 8, and the code is 0. The other fields of the ICMP packet contain the checksum, identifier, sequence num, and data. The size of these fields (except for data) is two bytes each.
4. For the reply packet, the ICMP type is 0, and the code is 0. The other fields are the same as the previous ping packet, and the size of the corresponding fields is the same as before, two bytes each.
5. The IP address of my host is 10.0.1.36. The IP address of the destination host is 128.93.162.84.
6. No. If ICMP sent UDP packets, the IP number would be 0x11.
7. It is not different from the ICMP ping query packets from the first half of the lab.
8. The referenced ICMP error packet information is saved in the .zip as **packet2.pdf**. The ICMP error packet has extra fields which contain the IP header and the original ICMP packet that the error is for.
9. The last three ICMP packets received by the source hosts are message type 0. They are different because the datagrams made it before the TTL expired, so type 11 messages were not required.
10. As can be seen on the attached screenshot of the tracert, there is a very large delay between step 11 and 12, during which the delay jumps from 16 ms at step 11 to 98 ms at step 12. In the command prompt, this link is from New York (JFK) to what is most likely somewhere in Europe, but I unable to tell by just the provided address: renater-gw-ix1.gtt.net