Richard Moot
CS372
May 24, 2016

Lab 4

1. 192.168.29.215
2. ICMP (1)
3. There are 20 bytes in the IP header. The payload is 528 bytes, which you can see by expanding out the Internet Control Message Protocol and eventually expanding that same field again below that to see it highlights 520 bytes for the actual payload.[1]
4. No it has not, the fragmentation offset is set to 0.
5. Identification, Header Checksum, Time to Live, Source, & Destination Port.
6. The Source and Destination fields stay constant. These fields must stay constant in order to properly trace the route from the source to the destination, while the Identification, Header Checksum and Time to Live fields change in order to measure the times and routes that are taken.
7. It is decrementing by 1 as you go down the list.
8. 0x0000e958 (59736) is the identification, and the TTL field is 64.
9. The TTL stays at 64 since it is the first hop and would always have the same TTL on a TTL-exceeded reply.
10. Yes, this IP datagram has been fragmented into 2 pieces. This is indicated by their showing 2 IPv4 Fragments (1980) bytes.
11. First, the fragmentation offset is higher than 0, which indicates that it is fragmented. Also, the flags are set 0x00, which means that this piece arrived last and not first since the other higher numbered but smaller fragment had different flags. This is not the first fragment, since the offset is not 0.[1]
12. This packet appears to be the first datagram fragment, since its offset is 0. After this fragment, there was one more since this one was 1500 and the next was 520. Also, the flags indicate there is more by being set as 0x01.[1]
13. The header checksum changed and the length.
14. There were 3 fragments created from the original.[1]
15. Total Length, Flags, and Header Checksum.

[1]See additional attached for printed packet from WireShark