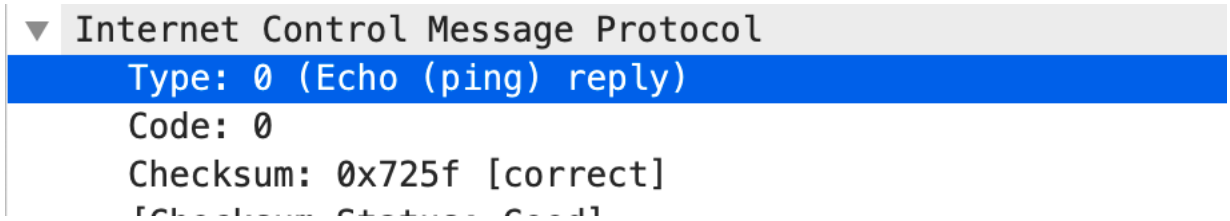
Step2.

1.What are the Type/Code values for an ICMP echo request and echo reply packet, respectively?

```
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▶ Internet Protocol Version 4, Src: 10.15.71.176 (10.15.71.176), Dst: 130.37.164.171 (130.37.164.171)
  ▼ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x6a7d [unverified] [in ICMP error packet]
```



2. How do the Identifier and Sequence Number compare for an echo request and the corresponding echo reply?

Identifier are same.
Sequence Number are same.

3. How do the Identifier and Sequence Number compare for successive echo request packets?

Identifier are same.
Sequence Number increase.

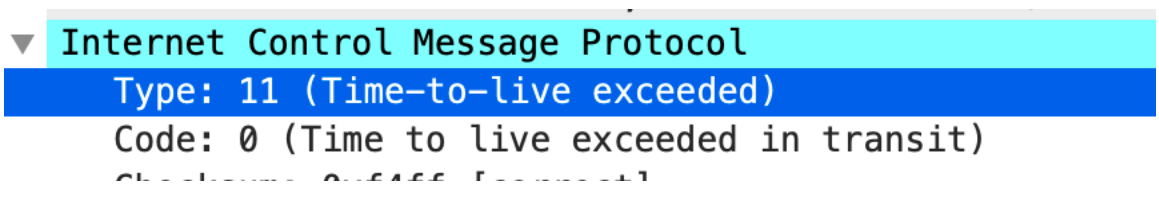
4. Is the data in the echo reply the same as in the echo request or different?

Same.

Turn-in: Hand in your answers to the above questions.

Step3.

1. What is the Type/Code value for an ICMP TTL Exceeded packet?



2. Say how the receiver can safely find and process all the ICMP fields if it does not know ahead of time what kind of ICMP message to expect. The potential issue, as you have probably noticed, is that different ICMP messages can have different formats. For instance, Echo has Sequence and Identifier fields while TTL Exceeded does not.

Each echo request and corresponding echo reply have the same Identifier value and the same Sequence Number value. The values are used to match the echo request to the right echo reply. Typically, the Identifier is kept the same and the Sequence Number is incremented. This ensures that as a pair, successive echo requests will have different Identifier/Sequence Number values so they (and their corresponding replies) can be distinguished.

3. How long is the ICMP header of a TTL Exceeded packet? Select different parts of the header in Wireshark to see how they correspond to the bytes in the packet.

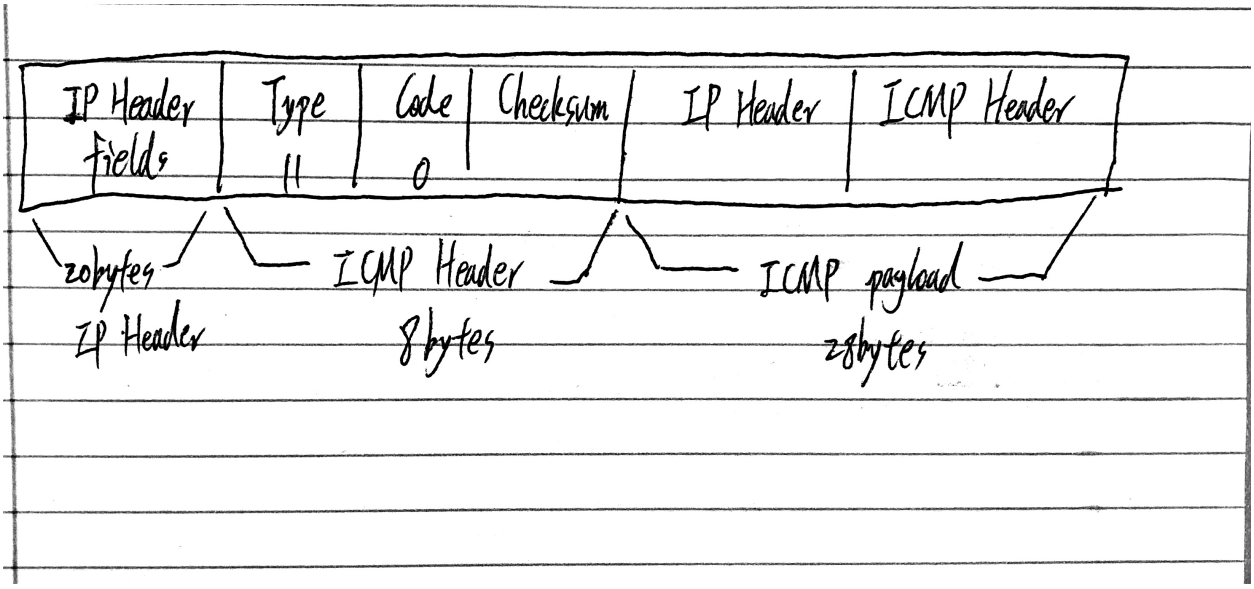
8bytes

4. The ICMP payload contains an IP header. What is the TTL value in this header? Explain why it has this value. Guess what it will be before you look!

1

The inner IP packet has TTL=1 in our case but depending on the router implementation it is possible that you will see TTL=0. It must be one of these values for the case of an ICMP TTL Exceeded message because the message is triggered when the TTL is decremented during processing and reaches 0, i.e., the TTL held a value of 1 when the packet arrived at the router

ICMP TTL Exceeded packet:



Turn-in: Hand in your drawing of an ICMP TTL Exceeded packet and the answers to the questions above.

Step4.

1. How does your computer (the source) learn the IP address of a router along the path from a TTL exceeded packet? Say where on this packet the IP address is found. You might proceed by looking at an echo packet to see the source and destination IP addresses. The routers along the path will have a different IP address, and this address will be present on the TTL Exceeded packet. If you are unsure, you can examine the traceroute text output to see the IP addresses of routers and look for these addresses on the TTL Exceeded packets.

The TTL Exceeded packets are coming from routers along the path back to your computer, triggered by the TTL field counting down to zero. The IP source address of the TTL Exceeded packet is the IP address of the router

2. How many times is each router along the path probed by traceroute? Look at the TTL Exceeded responses and see if you can discern a pattern.

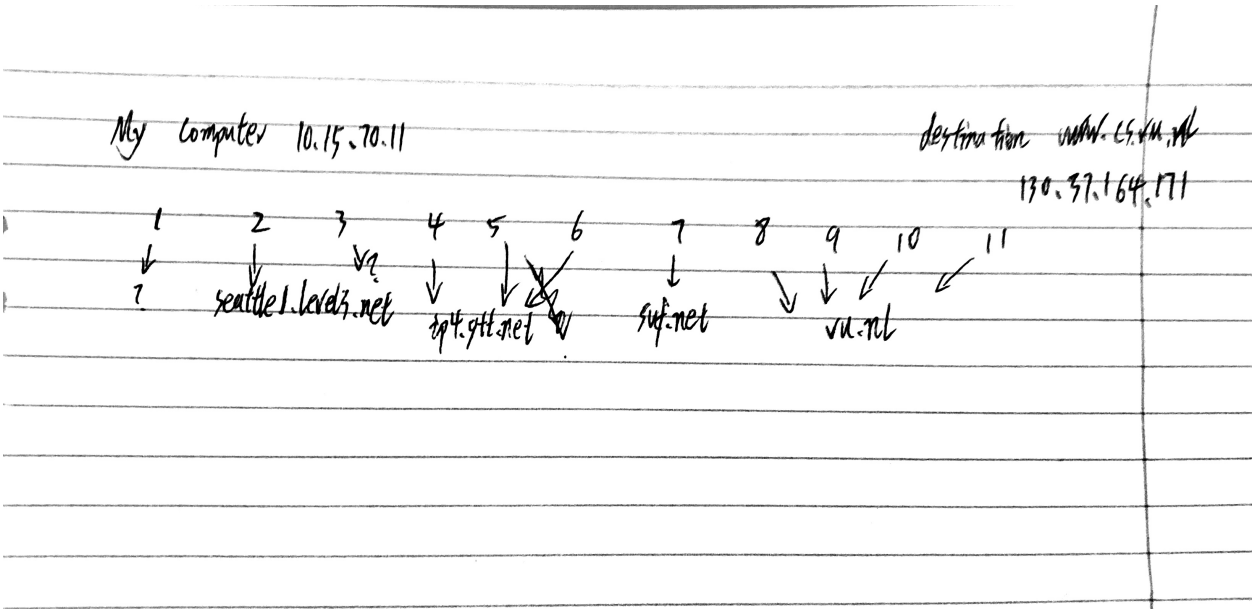
3 times.

Pattern: triples of echo / TTL exceeded from a given router

3. How does your computer (the source) craft an echo request packet to find (by eliciting a TTL Exceeded response) the router N hops along the path towards the destination? Describe the key attributes of the echo request packet. The echo request packets sent by traceroute are probing successively more distant routers along the path. You can look at these packets and see how they differ when they elicit responses from different routers.

The echo request packet should have an IP source of the computer doing the tracert command, an IP destination of the far end of the path, and a TTL value set to N. The last part is the key; routers will decrement the TTL and it will reach zero N hops away from the source towards the destination.

```
kenshin@Kenshins-MacBook-Pro ~ % ping www.cs.vu.nl
PING papac022.vu.nl (130.37.164.171): 56 data bytes
64 bytes from 130.37.164.171: icmp_seq=0 ttl=53 time=155.243 ms
64 bytes from 130.37.164.171: icmp_seq=1 ttl=53 time=162.688 ms
64 bytes from 130.37.164.171: icmp_seq=2 ttl=53 time=150.150 ms
^C
--- papac022.vu.nl ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 150.150/156.027/162.688/5.149 ms
kenshin@Kenshins-MacBook-Pro ~ % traceroute -I www.cs.vu.nl
traceroute to papac022.vu.nl (130.37.164.171), 64 hops max, 72 byte packets
 1  10.15.70.11 (10.15.70.11)  3.051 ms  2.565 ms  2.607 ms
 2  lag-3-199.ear2.seattle1.level3.net (4.53.158.129)  2269.088 ms  1594.870 ms  202.659 ms
 3  * * *
 4  ae17.cr4-sea2.ip4.gtt.net (173.205.57.37)  15.258 ms  4.209 ms  6.728 ms
 5  et-1-0-35.cr6-ams1.ip4.gtt.net (213.200.117.174)  148.594 ms  147.645 ms  149.197 ms
 6  surfnet-gw.ip4.gtt.net (77.67.72.110)  151.112 ms  155.919 ms  159.551 ms
 7  vu-router.customer.surf.net (145.145.20.58)  158.714 ms  158.140 ms  156.188 ms
 8  130.37.6.94 (130.37.6.94)  154.446 ms  156.030 ms  155.477 ms
 9  130.37.6.98 (130.37.6.98)  156.397 ms  162.263 ms  153.731 ms
10  130.37.250.126 (130.37.250.126)  154.218 ms  155.376 ms  160.312 ms
11  130.37.164.171 (130.37.164.171)  150.035 ms  151.273 ms  150.243 ms
kenshin@Kenshins-MacBook-Pro ~ %
```



Turn-in: Hand in your answers to the above questions and your drawing of the path, plus traceroute output if it was not supplied to you.

Grades:
98/100

Comments:
3.3 The ICMP header is 8 bytes. The type is one byte. The code is one byte. The checksum is 2 bytes. The options are 4 bytes.