Question 1

a) Packet 112 is sent by the client.

b) The server's IP is 216.75.194.220 and its port is 443 (https).

c) The next TCP sequence number will be 283. This is because the current sequence number is 79 and the message length is 204, $79 + 204 = 283$.

d) Packet 112 contains 3 SSL records.

e) Packet 112 contains an encrypted master secret: "Encrypted Handshake Message".

Question 2

In mobile IP, the mobile device must first forward to a base station which is then connected to the greater network. Mobile IP will also need to contend with channel utilization and conflicts more than wired does.

Question 3

a)

$$\begin{aligned} p &= 5 \\ q &= 11 \\ n = pq &= \mathbf{55} \\ z = (p-1)(q-1) &= 4 \cdot 10 = \mathbf{40} \end{aligned}$$

b) 3 is a good choice for e because it shares no common factors with z (40).

c) To find $x \mod 40 = 1$, there are only a couple of options that are less that 160: $1, 41, 81, 121$. The only number divisible by 3 is 81. Therefore d must be 27.

d)

$$\begin{aligned} c &= m^e \mod n \\ c &= 8^3 \mod 55 = \mathbf{17} \end{aligned}$$

Question 4

a) False

b) True

c) True

d) False

Question 5

a) The reciever will still be able to retrieve the original message even if one of the aggregate pulses was corrupted. This is because the 8 aggregate pulses are redundant and the average of the code will decode into the original signal.

b) Even if two of the eight pulses were corrupted, DS/CDMA would still be able to extract the original message.

c) The reciever will multiple each bit by the chipping sequence. Each of these These numbers are then averaged over the number of bits in the chipping sequence. Ideally, a "1" bit will result in the chipping sequence and a "-1" bit will result in an inverted chipping sequence. The reciever can determine which bit was the original by averaging the recieved data using the following formula:

$$\frac{\sum_{m=1}^{M} Z_{i,m}^{*} \cdot c_m}{M}$$

Where M is the length of the chipping sequence, Z_i is the current slot inside the stream and c is the chipping sequence. Note that M-bits inside the encoded stream will decode into a single bit.

Question 6

Topic: Active Networking

Great job outlining this topic. I wonder if hardware currently found in critical points of the internet could handle the increased processing required to implement active networking. Obviously, per-packet, the processing is quite basic, however, some routers need to handle an extremely high volume of packets so interpreting software instructions could prove to bog-down high traffic nodes.