CS331 Project 3 Problems – Ben Webb

1)

a. The application layer controls the connection between the client and the server. The first three packets are the three way handshake between the client and server (Syn, Syn/Ack, Ack). Then there is a GET/PSH request in packets 4-9. Packet 4 contains the GET, 5 is the server acknowledging it has received, 6 is the push, 7 is the HTTP status packet, and 8/9 are the client acknowledging it has received the packet. Packet 10 and 11 are closing the connection.
b. In packet 4 with the GET request, the client suggests using HTTP/1.1
c. The server responds in the PSH request with HTTP/1.0. The sever determines the HTTP version.
d. The client is using a GET request for the chklst.txt file from the server at path: 2001:470:1f11:2bc::1/chklist.txt
e. The server responds quickly (0.0007 s) with an ACK packet telling the client that it is processing the request. The server actually responds to the request with PSH, which takes 0.474 seconds.
f. The client application is a Macintosh running Safari, Mozilla/5.0, and Apple Web Kit. This is seen in packet 4 in the HTTP User Agent: section. What is interesting is that it appears all browsers 'support' Mozilla/5.0 because it was the first one and so it was fast to declare compatibility with a prior existing system.
g. DNT represents the user asking it not to be tracked. The idea is the server could provide personalized content but needs to track activity. This is apparently not supported on safari.
h. The client is requesting a keep alive connection which is persistent. That is the last part of the HTTP section of packet 4.
i. From packet 6, the server is not granting a persistent connection. It responds with a close connection. That means if the client wants to make another request, they must first reconnect with the server.
j. From packet 6, the server is a HTTP D. Which is Apache. It is a part of Hurricane Electric and is processing content for a user.
k. From packet 6, the server is in no-cache mode which means that caching is not directly supported. For anything to be cached it must also be sent to the origin server. This means that the cache will always be updated and vetted.
l. The server returns text as an html file. This is a list, like the client requested but instead of being returned as a file it is just text. This is transforming the file into a universally accepted version.
m. No this is not proper HTML format. It is probably just the text that can be transformed into an HTML format using MIME to go from a .txt file to direct text.
n. The first line in packet 7 is "Firmware Version: ver2.10Nab02 \n".
o. The server thinks that the wall time is the 0.46566 seconds but the, but packets think the time is 0.46436 seconds.

2) Chapter 2, P2: Short Message service (SMS) uses the GSM service which allows for 160 alphanumeric characters to be sent. Messages are sent to and stored in a short message

service center where the message is stored and forwards. iMessage runs on Apple Push Notification service (APN) where messages are stored on an apple server. This is a keep-alive connection that is continually pinged. WhatsApp relies on XMPP which is extended mail transfer protocol. They all receive an address at: [phonenumber]@s.whatsapp.net. The biggest difference between whatsapp and iMessage is that APN is built to just work with Apple devices whereas whatsapp works will all types of IP enabled devices. SMS is different from the first two because it relies entirely on the cellular network whereas the others use IP routing. SMS is then the simplest and broadly applicable because there is no simple proprietary service that provides the protocol, it is a simple one supported by all devices. (Source)

3) Message integrity is the desire to have the content of the message remain unchanged. Message confidentiality is the desire to only have who you want to read the message, read it. When broadcasting a message without encryption, one can almost be assured that there will be integrity without confidentiality. Confidentiality and Integrity are positively correlated. Confidentiality needs assertion of integrity between the confidants that they understand the message. Message integrity confirms message confidentiality, and thus confidentiality requires integrity.
4) MD5 is `2e0804f4765da4aa5cd024e4730686d0`. SHA-1 is `aa4e7f2d8a95ac232caf7ce38fa51ab46766358c`. Which I found with the command: `curl http://cs.colby.edu/courses/F19/cs331/projects/p2.html | openssl [sha1/md5]`
5) The first bytes describe the issuer of the certificate. USERTrust RSA Certification Authority" is the highest-level certificate provider. The first bytes of the key are "MIIBIjANBgkqhkiG9w" Which I found with the command: `openssl s_client -connect www.colby.edu:443 | openssl x509 -pubkey`