**EE 499 – Lab 11**

Question 1) The captured protocols are TCP and HTTP.

Question 2) It is written: GET / HTTP/1.1

The message is plain-text because my machine is requesting to get the “http” version of google from Google’s server. Furthermore, it is plain-text because I can read the message. If it were ciphered, I would only see a lot of random bytes.

Question 3) It is written: HTTP/1.1 200 OK (text/html)

The message is plain-text because Google’s server is sending the “http” version. Furthermore, it is plain-text because I can read the message. If it were ciphered, I would only see a lot of random bytes.

Question 4) The three common fields present in every TLS Record Layer entry are: Content Type, Version, and Length.

Question 5) Handshake (22)

Question 6) Application Data (23)

Question 7) On the client side, the nonce is 0. On the server side, the nonce is 32.

Question 8) 15 cipher suites are supported by the client.

Question 9) The cipher suite accepted by the server that will be used in the data flow is: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)

Question 10) There are 3 certificates included.

1. For the first certificate, the algorithm used is sha256WithRSAEncryption.
2. For the second certificate, the algorithm used is sha256WithRSAEncryption.
3. For the third certificate, the algorithm used is sha1WithRSAEncryption.

Question 11) Ecrypted PreMaster Length: 256 bytes.

Question 12) Ecrypted PreMaster Length: 256 bytes.