Course: CISC 856: Upper Layer Protocols
Bo Lu Email: lubo@udel.edu
Document: TLS Homework
Due Date: 10/30/2012

1. What is cipher suite in TLS?

2. Why is FINISHED TLS record PDU necessary?

3. What are the 3 security services TLS provide? Please give the definition.

4. A TLS record PDU looks as follows (in hexadecimal notation):
16 03 01 00 41 01 00 00 3d 03 01 49 47 77 14 b9 02 5d e6 35 ff 49 d0 65 cb 89 93 7d 68 9b 55 e7 b6 49 e6 93 e9 e9 48 c0 b7 d2 13 00 00 16 00 04 00 05 00 0a 00 09 00 64 00 62 00 03 00 06 00 13 00 12 00 63 01 00

TLS record format

Type	Protocol
20	ChangeCipherSpec protocol
21	Alert protocol
22	Handshake protocol
23	Application data protocol

Please answer the following questions based on the PDU and the format of TLS record (You may need to refer to the format of the upper layer protocol).

1. Which upper layer protocol is used?
2. Which version of TLS is used?
3. What is the size of the TLS record SDU?
4. Is a CLIENTHELLO TLS record PDU? Why?
5. Is there a TLS session to resume? Please verify your answer.
6. Can you determine the number of cipher suite? Please verify your answer.

5. Use wireshark to open the pcap file “https_facebook.pcap”, please finish the following task.

- Find first TLS session. Please print the following packets for this TLS session.
    a. Client and server hello messages
    b. The cipher suites that this client supports
    c. The cipher suite that this server chooses
    d. The server certificate message
- How many sessions are used? Please show the respective session id.
- How many connections belong to each session?