南昌大学实验报告

姓名：**陈华豪**

学号：**6130116238**

邮箱地址：**6130116238@email.ncu.edu.cn**

专业班级：**网络工程161班**

实验日期：**2018.**

课程名称：**网络协议分析与实现**

实验项目名称

Wireshark Lab: SSL

实验目的

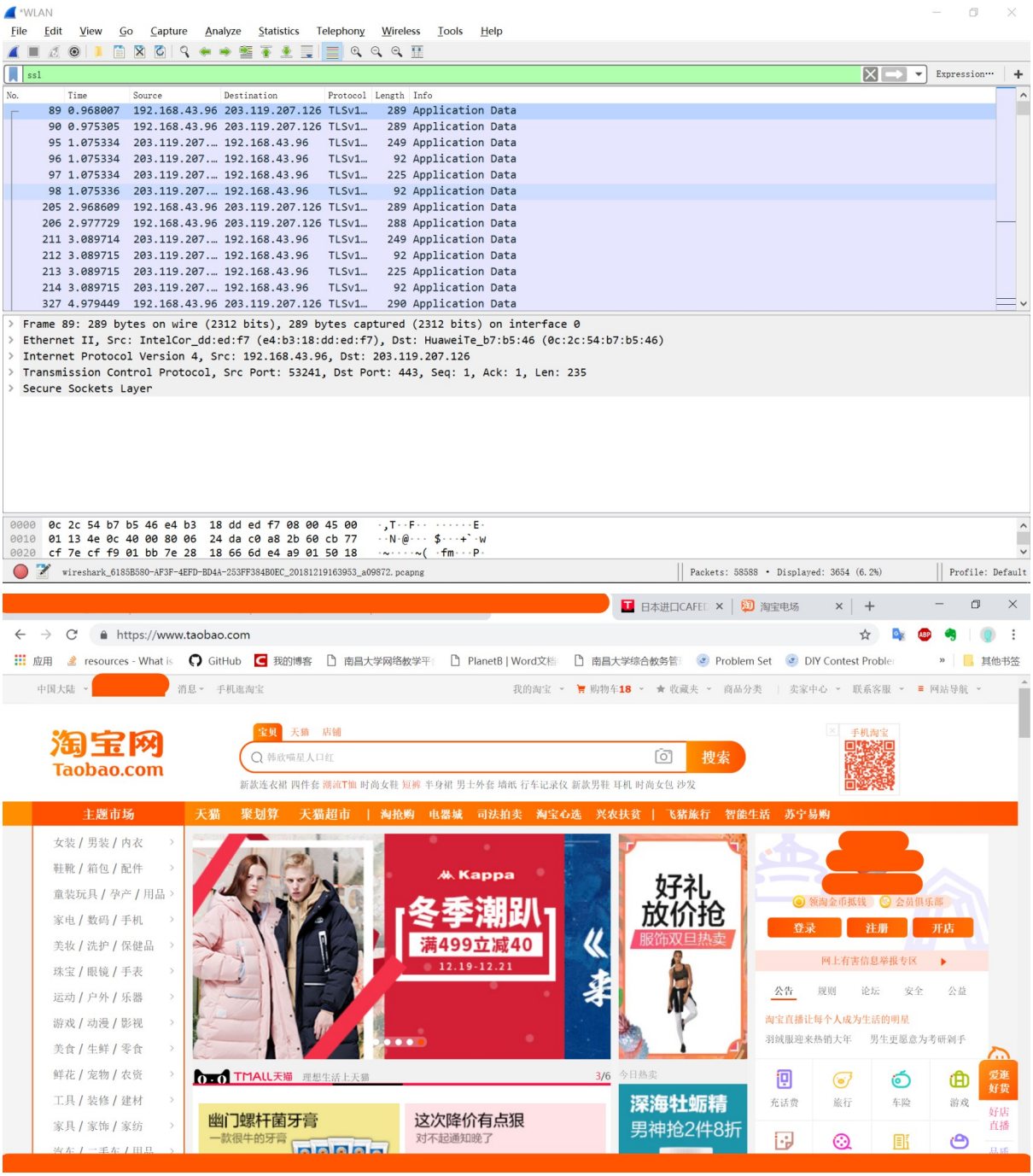
- **Investigate the Secure Sockets Layer (SSL) protocol**

实验基础

- http://www-net.cs.umass.edu/wireshark-labs/Wireshark_SSL_v7.0.pdf

实验步骤

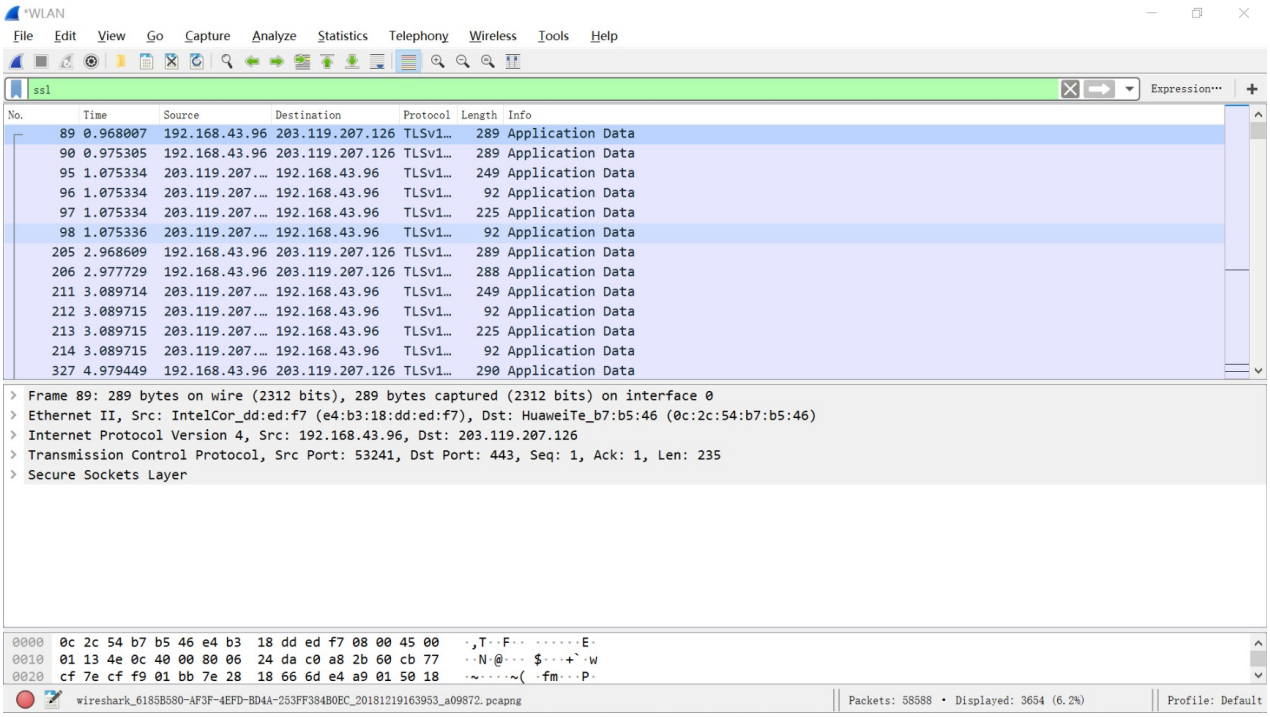
1. 在SSL会话中捕获数据包第一步是在SSL会话中捕获数据包。要做到这一点，你应该去你最喜欢的电子商务网站并开始购买物品的过程（但在实现目的之前终止！）。使用Wireshark捕获数据包后，应设置过滤器，使其仅显示包含主机发送和接收的SSL记录的以太网帧。（SSL记录与SSL消息相同。）



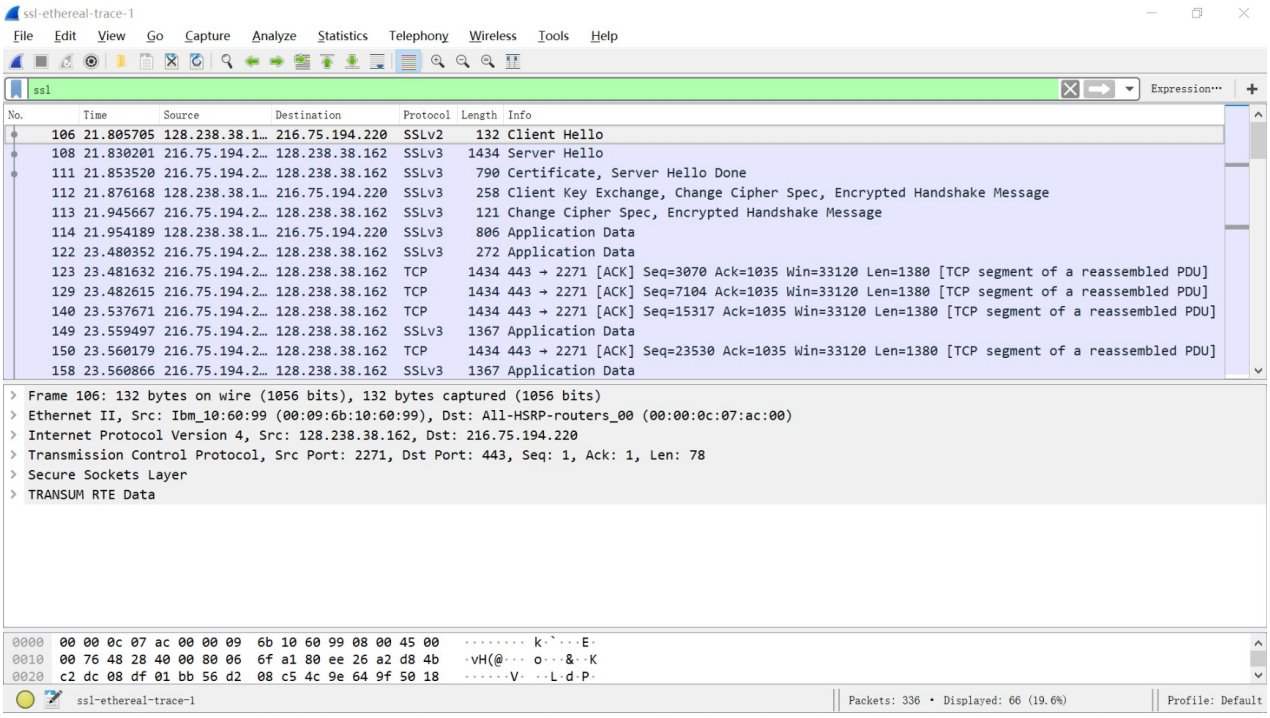
2. 查看捕获的跟踪您的Wireshark GUI应仅显示具有SSL记录的以太网帧。请记住，以太网帧可能包含一个或多个SSL记录，这一点很重要。 （这与HTTP非常不同，每个帧包含一个完整的HTTP消息或一部分HTTP消息。）此外，SSL记录可能不完全适合以太网帧，在这种情况下，将需要多个帧记载。
3. 回答实验思考部分的内容。

实验数据或结果

ssl.pcapng



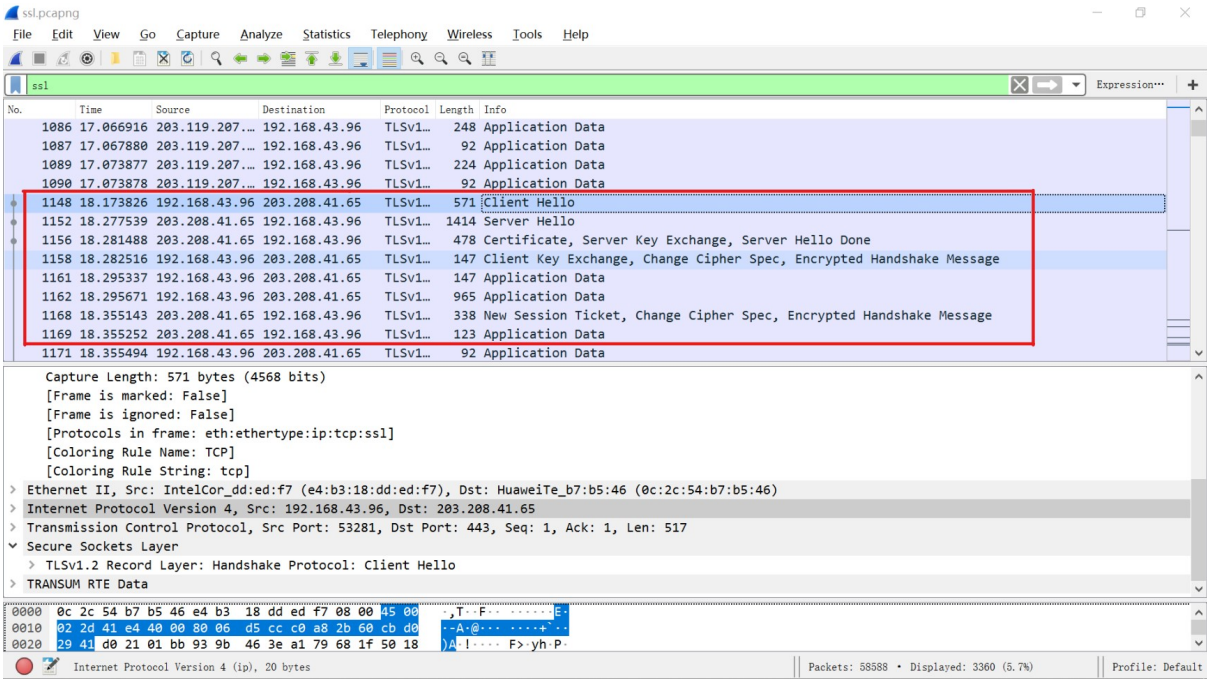
ssl-ethereal-trace-1



实验思考

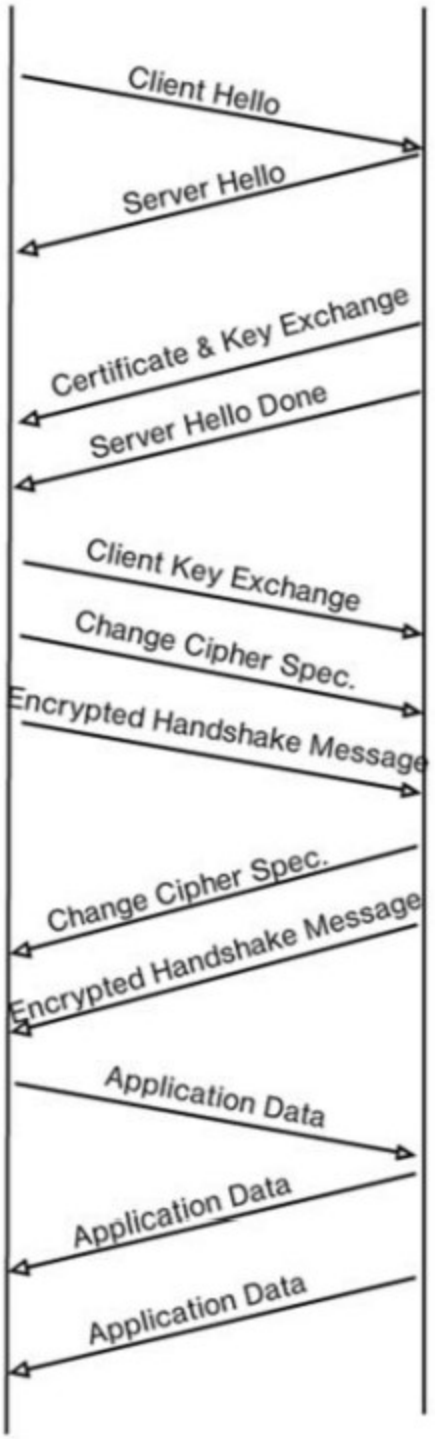
1. 对于前8个以太网帧中的每一个，指定帧的来源（客户端或服务器），确定帧中包含的SSL记录的数量，并列出帧中包含的SSL记录类型。在客户端和服务器之间绘制时序图，每个SSL记录都有一个箭头。

答：



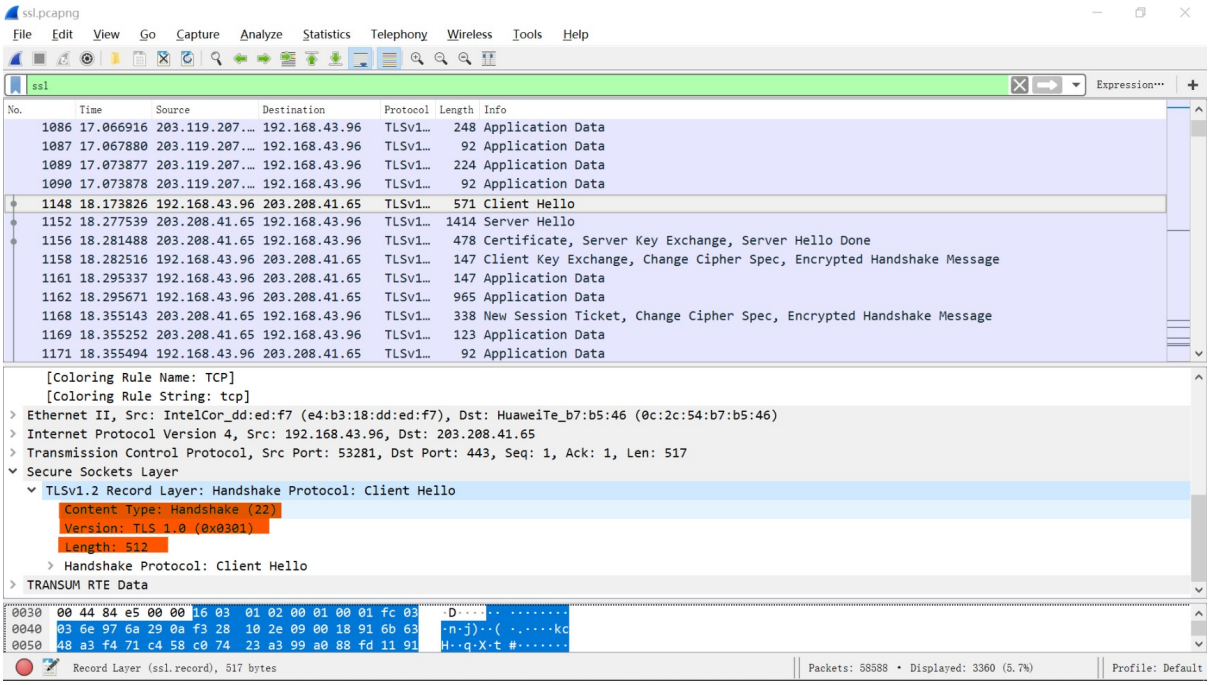
No.	Frame	Source	Destination	SSL Count	SSL Type
1	1148	192.168.43.96	203.208.41.65	1	Client Hello
2	1152	203.208.41.65	192.168.43.96	1	Server Hello
3	1156	203.208.41.65	192.168.43.96	2	Certificate, Sever Key Exchange, Server Hello Done
4	1158	192.168.43.96	203.208.41.65	1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

No.	Frame	Source	Destination	SSL Count	SSL Type
5	1161	192.168.43.96	203.208.41.65	1	Application Data
6	1162	192.168.43.96	203.208.41.65	1	Application Data
7	1168	203.208.41.65	192.168.43.96	1	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
8	1169	203.208.41.65	192.168.43.96	1	Application Data



2. 每个SSL记录都以相同的三个字段（可能具有不同的值）开头。其中一个字段是“内容类型”，长度为一个字节。列出所有三个字段及其长度。

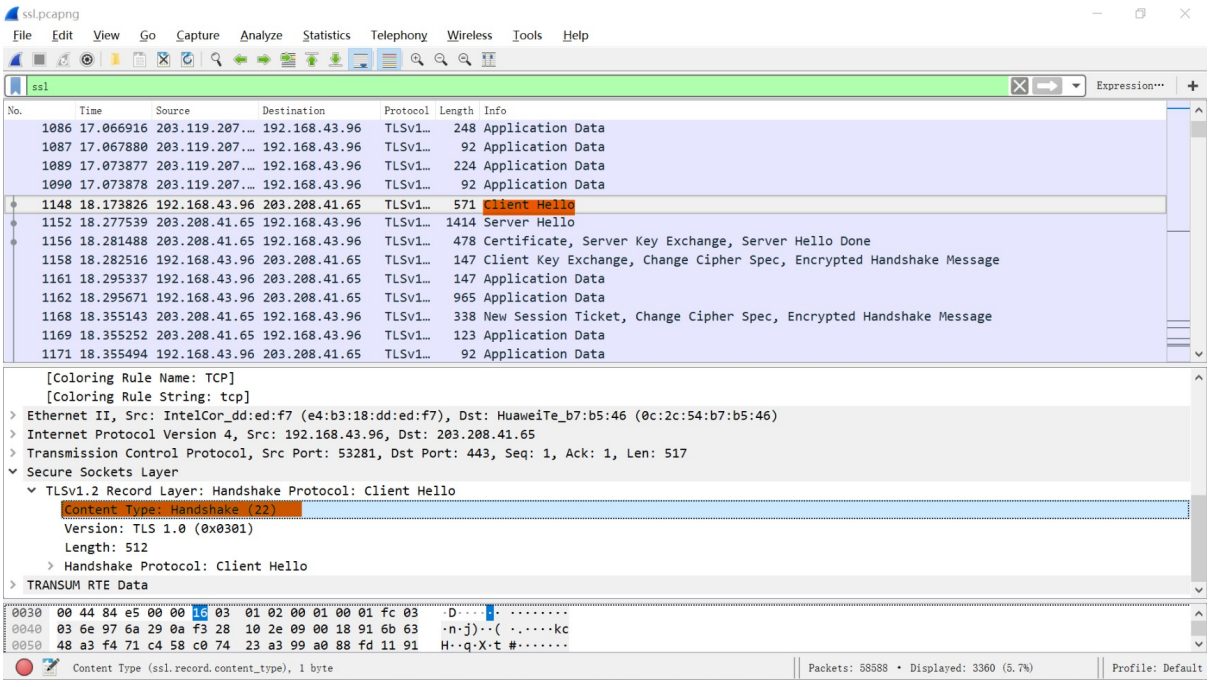
答：



ClientHello Record:

3. 展开ClientHello记录。 （如果您的跟踪包含多个ClientHello记录，请展开包含第一个记录的框架。）内容类型的值是多少?

> 答：Content Type: Handshake (22)



4. ClientHello记录是否包含nonce（也称为“挑战”）？ 如果是这样，十六进制表示法中的挑战价值是多少?

5. ClientHello记录是否广告它支持的网络套件？如果是这样，在第一个列出的套件中，什么是公钥算法，对称密钥算法和散列算法?

   ```
   答：公钥算法：RSA 对称密钥算法：RC4 哈希算法：MD5
   ```

   ServerHello Record:

6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

7. Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?
8. Does this record include a session ID? What is the purpose of the session ID?
9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

Client Key Exchange Record:

1. Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

Change Cipher Spec Record (sent by client) and Encrypted Handshake Record:

1. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?
2. In the encrypted handshake record, what is being encrypted? How?
3. Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?

Application Data

1. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?
2. Comment on and explain anything else that you found interesting in the trace.

参考资料

- http://www-net.cs.umass.edu/wireshark-labs/Wireshark_SSL_v7.0.pdf