

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。）

The screenshot displays two windows. The top window is Wireshark, showing a list of network packets. The selected packet (No. 89) is a TLSv1 Application Data packet. The bottom window is a web browser showing the Taobao.com homepage. The browser's address bar shows the URL https://www.taobao.com. The page content includes various promotional banners and navigation links.

No.	Time	Source	Destination	Protocol	Length	Info
89	0.968007	192.168.43.96	203.119.207.126	TLSv1...	289	Application Data
90	0.975305	192.168.43.96	203.119.207.126	TLSv1...	289	Application Data
95	1.075334	203.119.207...	192.168.43.96	TLSv1...	249	Application Data
96	1.075334	203.119.207...	192.168.43.96	TLSv1...	92	Application Data
97	1.075334	203.119.207...	192.168.43.96	TLSv1...	225	Application Data
98	1.075336	203.119.207...	192.168.43.96	TLSv1...	92	Application Data
205	2.968609	192.168.43.96	203.119.207.126	TLSv1...	289	Application Data
206	2.977729	192.168.43.96	203.119.207.126	TLSv1...	288	Application Data
211	3.089714	203.119.207...	192.168.43.96	TLSv1...	249	Application Data
212	3.089715	203.119.207...	192.168.43.96	TLSv1...	92	Application Data
213	3.089715	203.119.207...	192.168.43.96	TLSv1...	225	Application Data
214	3.089715	203.119.207...	192.168.43.96	TLSv1...	92	Application Data
327	4.979449	192.168.43.96	203.119.207.126	TLSv1...	290	Application Data

Frame 89: 289 bytes on wire (2312 bits), 289 bytes captured (2312 bits) on interface 0
> Ethernet II, Src: IntelCor_dd:ed:f7 (e4:b3:18:dd:ed:f7), Dst: HuaweiTe_b7:b5:46 (0c:2c:54:b7:b5:46)
> Internet Protocol Version 4, Src: 192.168.43.96, Dst: 203.119.207.126
> Transmission Control Protocol, Src Port: 53241, Dst Port: 443, Seq: 1, Ack: 1, Len: 235
> Secure Sockets Layer

Packets: 58588 • Displayed: 3654 (6.2%) Profile: Default

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。

ssl.pcapng

WLAN

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
89	0.968007	192.168.43.96	203.119.207.126	TLSv1...	289	Application Data
90	0.975305	192.168.43.96	203.119.207.126	TLSv1...	289	Application Data
95	1.075334	203.119.207.126	192.168.43.96	TLSv1...	249	Application Data
96	1.075334	203.119.207.126	192.168.43.96	TLSv1...	92	Application Data
97	1.075334	203.119.207.126	192.168.43.96	TLSv1...	225	Application Data
98	1.075336	203.119.207.126	192.168.43.96	TLSv1...	92	Application Data
205	2.968609	192.168.43.96	203.119.207.126	TLSv1...	289	Application Data
206	2.977729	192.168.43.96	203.119.207.126	TLSv1...	288	Application Data
211	3.089714	203.119.207.126	192.168.43.96	TLSv1...	249	Application Data
212	3.089715	203.119.207.126	192.168.43.96	TLSv1...	92	Application Data
213	3.089715	203.119.207.126	192.168.43.96	TLSv1...	225	Application Data
214	3.089715	203.119.207.126	192.168.43.96	TLSv1...	92	Application Data
327	4.979449	192.168.43.96	203.119.207.126	TLSv1...	290	Application Data

> Frame 89: 289 bytes on wire (2312 bits), 289 bytes captured (2312 bits) on interface 0

> Ethernet II, Src: IntelCor-dd:ed:f7 (e4:b3:18:dd:ed:f7), Dst: HuaweiTe_b7:b5:46 (0c:2c:54:b7:b5:46)

> Internet Protocol Version 4, Src: 192.168.43.96, Dst: 203.119.207.126

> Transmission Control Protocol, Src Port: 53241, Dst Port: 443, Seq: 1, Ack: 1, Len: 235

> Secure Sockets Layer

0000 0c 2c 54 b7 b5 46 e4 b3 18 dd ed f7 08 00 45 00 .T.F.E-
0010 01 13 4e 0c 40 00 80 06 24 da c0 a8 2b 60 cb 77 .N@...\$...W
0020 cf 7e cf f9 01 bb 7e 28 18 66 6d e4 a9 01 50 18 .~...~.fm..P.

wireshark_6185B580-AF3F-4EFD-BD4A-253FF384B0EC_20181219163953_a09872.pcapng

Packets: 58588 • Displayed: 3654 (6.2%)

Profile: Default

ssl-ethereal-trace-1

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The main display area is divided into three panes: Packet List, Packet Details, and Packet Bytes.

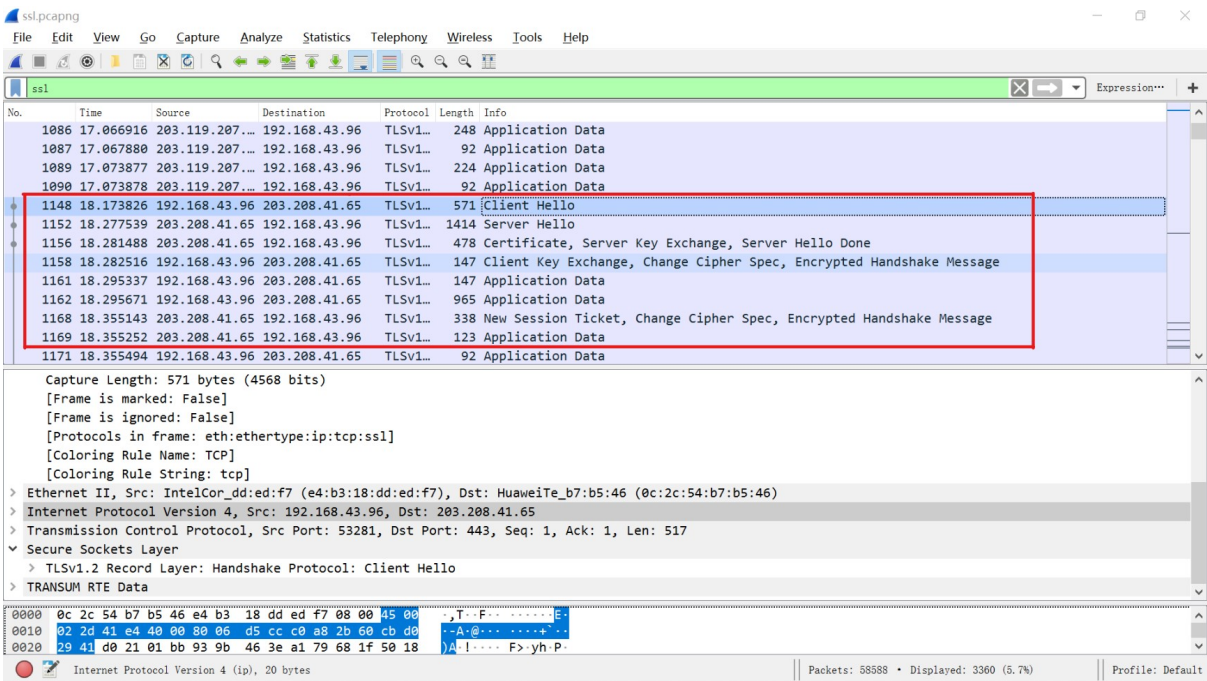
The Packet List pane shows a list of captured packets. The first packet (No. 106) is an SSLv2 Client Hello. The subsequent packets (No. 108 to 158) include a Server Hello, Certificate, Key Exchange, Change Cipher Spec, and Application Data. The details pane for the selected packet (No. 106) shows the structure of the Client Hello packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Secure Sockets Layer. The packet bytes pane shows the raw hex and ASCII data of the selected packet.

The status bar at the bottom indicates the current capture file is 'ssl-ethereal-trace-1', the number of packets is 336, the number of displayed packets is 66 (19.6%), and the profile is Default.

实验思考

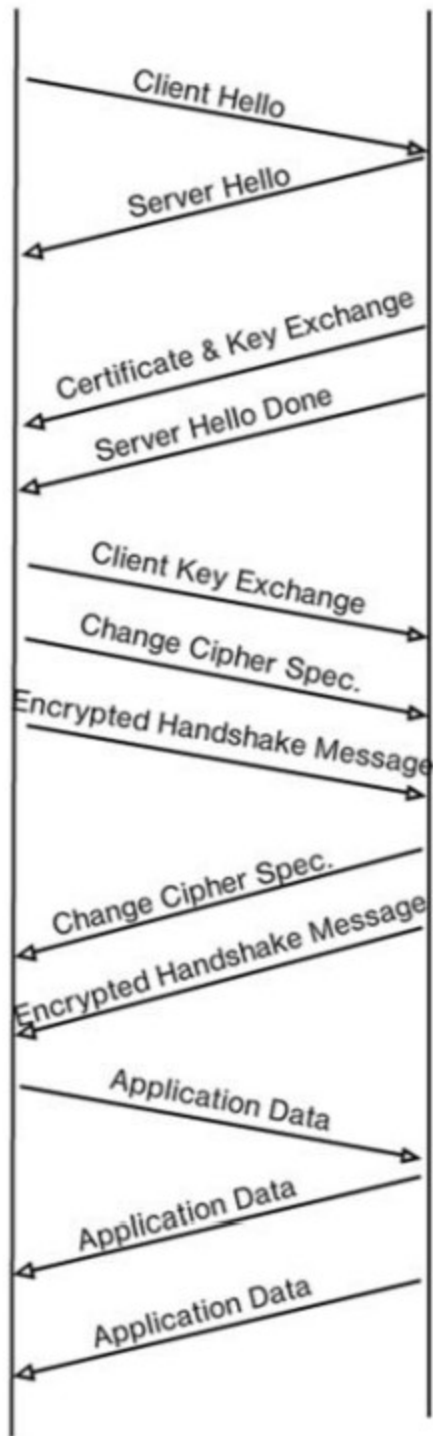
1. 对于前8个以太网帧中的每一个，指定帧的来源（客户端或服务器），确定帧中包含的SSL记录的数量，并列出帧中包含的SSL记录类型。在客户端和服务器之间绘制时序图，每个SSL记录都有一个箭头。

答：



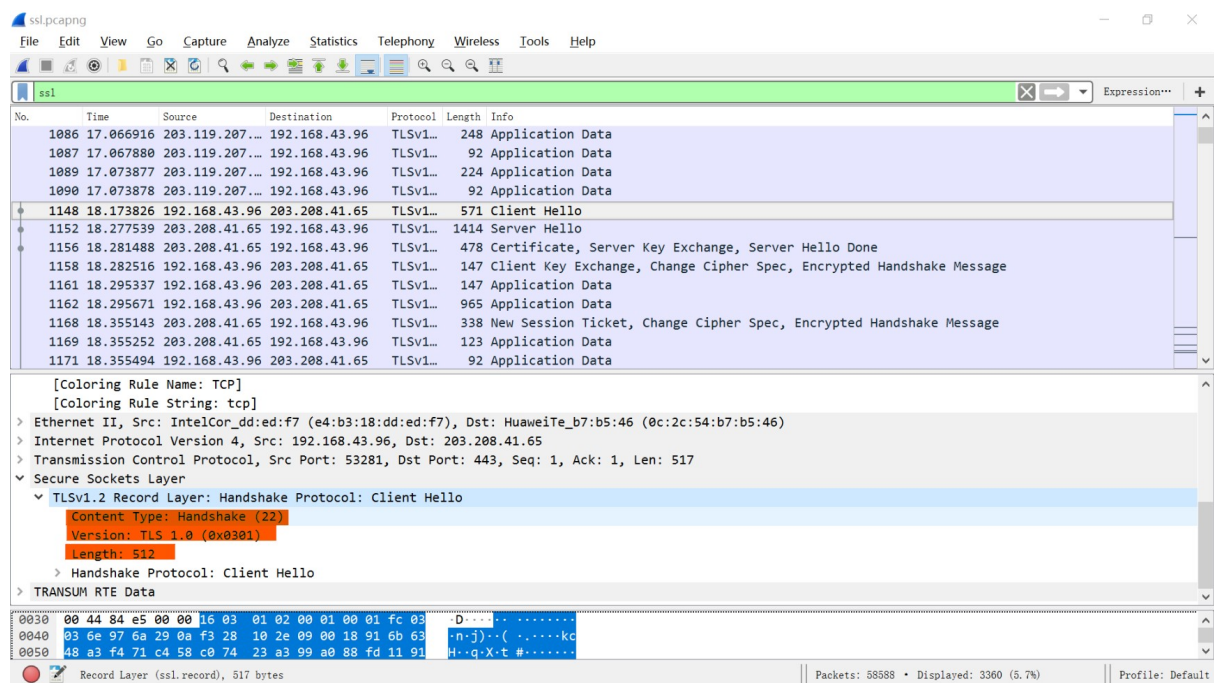
No.	Frame	Source	Destination	SSL Count	SSL Type
1	1148	192.168.43.96	203.208.41.65	1	Client Hello
2	1152	203.208.41.65	192.168.43.96	1	Server Hello
3	1156	203.208.41.65	192.168.43.96	2	Certificate, Sever Key Exchange, Server Hello Done
4	1158	192.168.43.96	203.208.41.65	1	Client Key Exchange, Change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

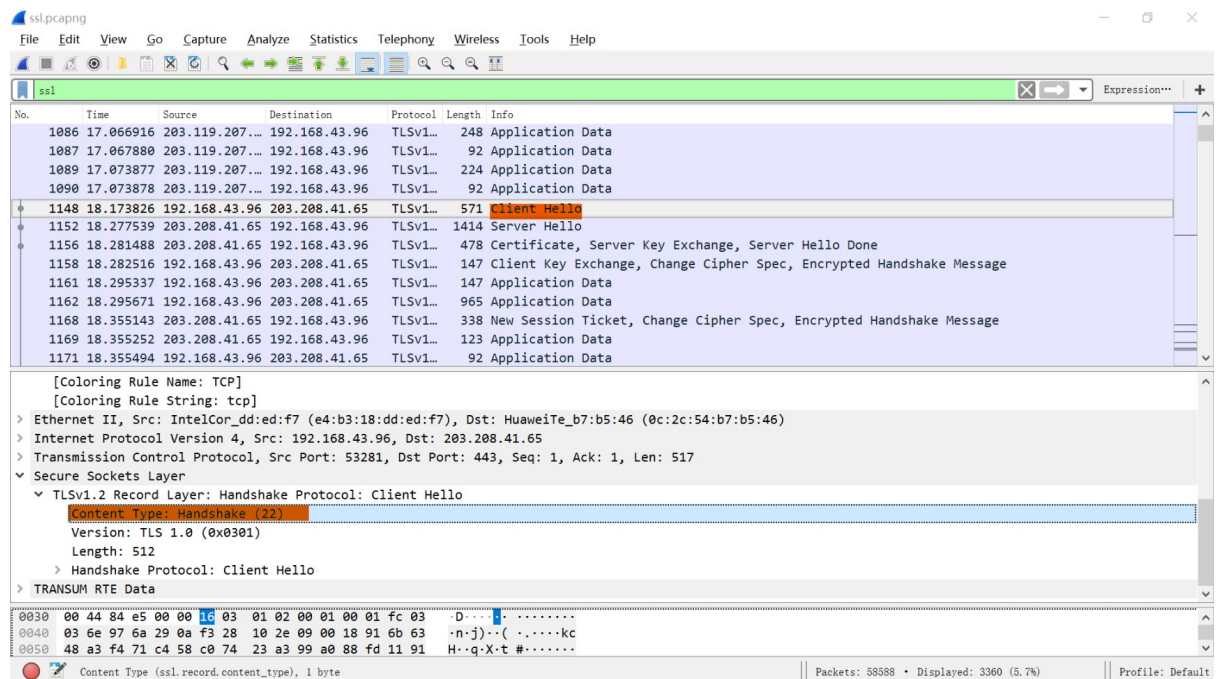
答：



ClientHello Record:

- 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)



- 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