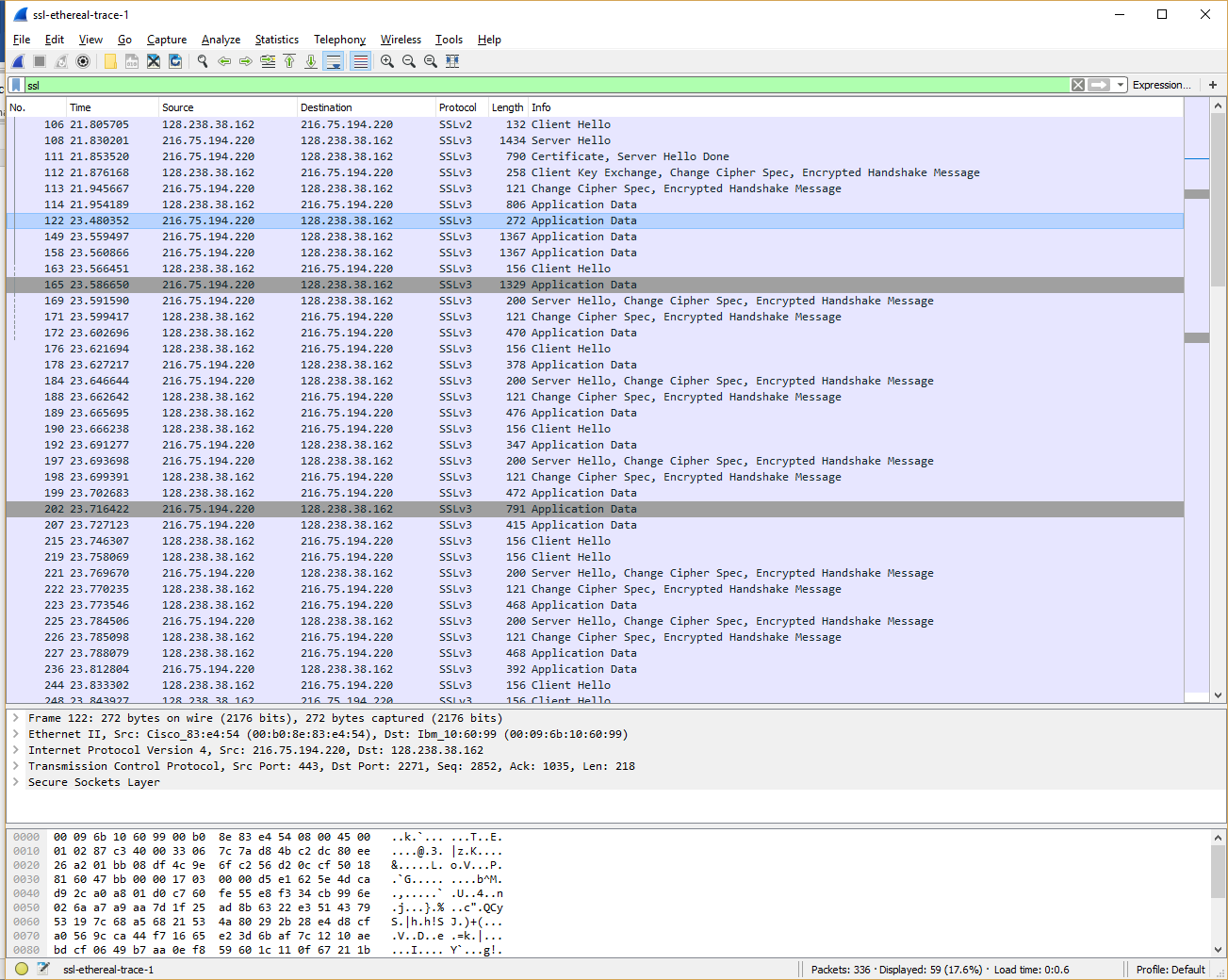
William Fu

4/15/18

Lab 4

I used the given trace by given by the lab cause I couldn’t get mine to work

1)



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 106 | 128.238.38.162 | 216.75.194.220 | 1 | Client Hello |
| 2 | 102 | 216.75.194.220 | 128.238.38.162 | 1 | Server Hello |
| 3 | 111 | 216.75.194.220 | 128.238.38.162 | 2 | Server Hello Done |
| 4 | 112 | 21.238.38.162 | 216.75.194.220 | 3 | Client Key Exchange |
| 5 | 113 | 216.75.194.220 | 128.238.38.162 | 2 | Change Cipher Spec |
| 6 | 114 | 128.238.38.162 | 216.75.194.220 | 1 | Application Data |
| 7 | 122 | 216.75.194.220 | 128.238.38.162 | 1 | Application Data |
| 8 | 149 | 216.75.194.220 | 128.238.38.162 | 1 | Application Data |

2)

Content Type = 1 Byte

Version = 2 bytes

Length = 2 bytes

3)

Content type is 22

4)

Challenge: 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

5)

Public Key: RSA

Symmetric Key: RC4

Hash: MD5

6)

Public Key: RSA

Symmetric Key: RC4

Hash: MD5

7)

32 bit long (28 Bit data + 4 bit time)

Used for attack prevention

8)

Yes the record include a session ID. Session Id in record is used as an identifier for SSL. Allows client to resume the session later by using session ID.

9)

No certificate. The certificate is in the separate record. The certificate fits into a single ethernet frame

10)

This record contains a pre-master secret. The master secret is created using this pre-master secret. Master key is used to create session key. The secret is encrypted by public key. The encrypted secret is 120 bytes