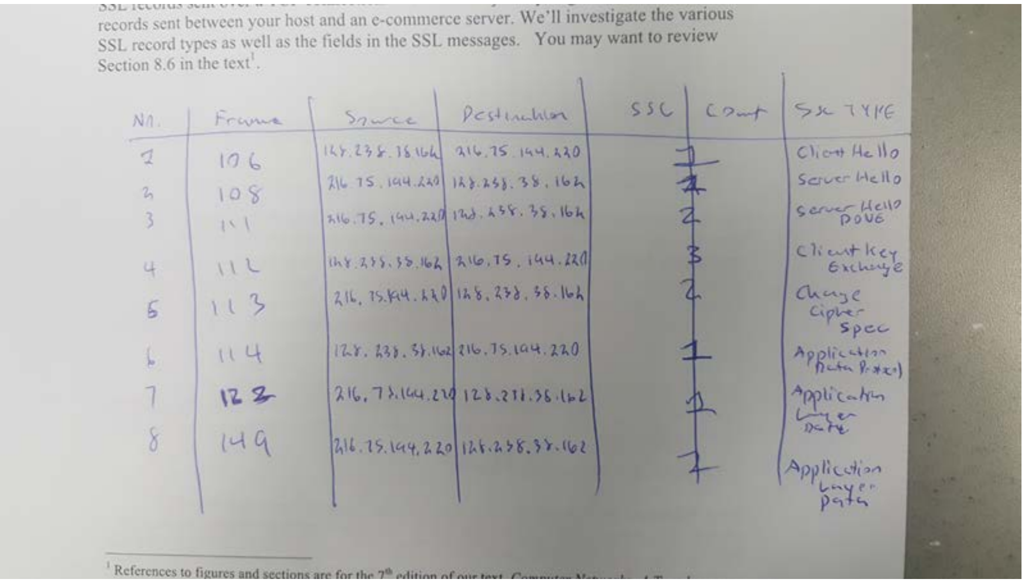
Franklin Nuth
Professor Ronny Bull
CSC323-A
November 21, 2017

SSL

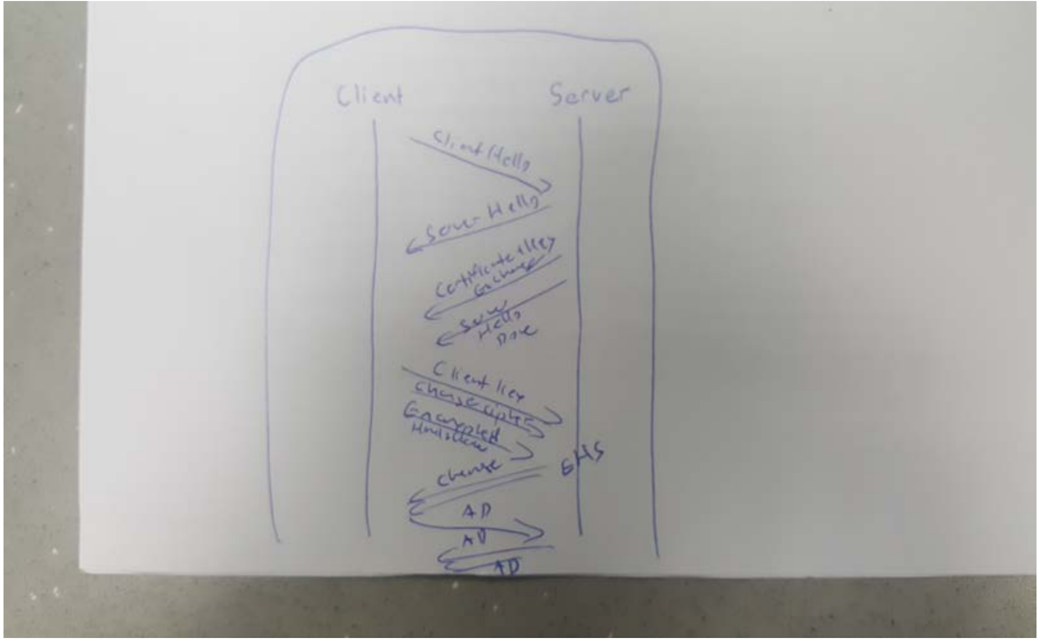
1)



records sent between your host and an e-commerce server. We'll investigate the various SSL record types as well as the fields in the SSL messages. You may want to review Section 8.6 in the text[1].

No.	Frame	Source	Destination	SSL Count	SSL TYPE
1	106	128.238.38.162	216.75.144.220	1	Client Hello
2	108	216.75.144.220	128.238.38.162	2	Server Hello
3	111	216.75.144.220	128.238.38.162	2	Server Hello DONE
4	112	128.238.38.162	216.75.144.220	3	Client Key Exchange
5	113	216.75.144.220	128.238.38.162	2	Change Cipher Spec
6	114	128.238.38.162	216.75.144.220	1	Application Data Protocol
7	122	216.75.144.220	128.238.38.162	1	Application Layer Data
8	149	216.75.144.220	128.238.38.162	1	Application Layer Data

[1] References to figures and sections are for the 7th edition of our text, Computer Networks



2) The three content fields and their lengths are Content Type (1), Version (2), and Length (2).
3) The value of the Content Type in ClientHello is 22.
4) Yes, the ClientHello record does contain a nonce. The value of the challenge in hexadecimal notation is 04 8c d6 04 35 dc 44 89 84 49 99 09.
5) No, it does not advertise the cyber suites it supports.
6) Yes, the record specified a chosen cipher suite. The algorithms in the cyber suite are RSA, RCH, and MD5.
7) No, the record does not contain a nonce. The purpose of nonces in SSL is used to prevent attacks.

8) Yes, it does include a session ID. The purpose of the session ID is to keep SSL sessions.
9) No, this record does not contain a certificate. The certificate is included in a different record. Yes, it can fit into a single Ethernet frame.
10) Yes, client key exchange record contains a pre-master secret. This secret is used for session key. It is encrypted, and it is 128 bits long.
11) The purpose of the Change Cipher Record is to indicate the next SSL record encryption. The record in the trace is 5 bits long.
12) In the encrypted handshake record, the handshakes messages and MACs are being encrypted by being sent to the server.
13) Yes, the server's encrypted handshake contains all messages. The records are different in that the client received the rest of the messages.
14) The application data is being encrypted through an algorithm. Yes, it included a MAC. No, Wireshark does not distinguish between the encrypted data and the MAC.
15) I find nothing strange about this trace.

```
    106 0.009406       128.238.38.162        216.75.194.220        SSLv2    132    Client Hello
Frame 106: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220
Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 1, Ack: 1, Len: 78
    Source Port: 2271
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 78]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 79    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xe755 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022082000 seconds]
        [Bytes in flight: 78]
        [Bytes sent since last PSH flag: 78]
    TCP payload (78 bytes)
Secure Sockets Layer
    SSLv2 Record Layer: Client Hello
        [Version: SSL 2.0 (0x0002)]
        Length: 76
        Handshake Message Type: Client Hello (1)
        Version: SSL 3.0 (0x0300)
        Cipher Spec Length: 51
        Session ID Length: 0
        Challenge Length: 16
        Cipher Specs (17 specs)
            Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
            Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)
            Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)
            Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
            Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
            Cipher Spec: SSL2_RC2_128_CBC_WITH_MD5 (0x030080)
            Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)
            Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
            Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x000064)
            Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x000062)
            Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x000003)
            Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x000006)
            Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
            Cipher Spec: SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 (0x040080)
            Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)
            Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)
            Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)
        Challenge
    108 0.002053       216.75.194.220        128.238.38.162        SSLv3    1434   Server Hello
Frame 108: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 18, 2005 11:11:12.648204000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1121710272.648204000 seconds
    [Time delta from previous captured frame: 0.002053000 seconds]
    [Time delta from previous displayed frame: 0.002053000 seconds]
    [Time since reference or first frame: 21.830201000 seconds]
    Frame Number: 108
    Frame Length: 1434 bytes (11472 bits)
    Capture Length: 1434 bytes (11472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssl]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09:6b:10:60:99)
    Destination: Ibm_10:60:99 (00:09:6b:10:60:99)
        Address: Ibm_10:60:99 (00:09:6b:10:60:99)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_83:e4:54 (00:b0:8e:83:e4:54)
        Address: Cisco_83:e4:54 (00:b0:8e:83:e4:54)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1420
    Identification: 0x87be (34750)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 51
    Protocol: TCP (6)
    Header checksum: 0x77f5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 216.75.194.220
    Destination: 128.238.38.162
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380
    Source Port: 443
    Destination Port: 2271
    [Stream index: 2]
    [TCP Segment Len: 1380]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1381    (relative sequence number)]
    Acknowledgment number: 79    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A····]
    Window size value: 33120
    [Calculated window size: 33120]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xcc13 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022082000 seconds]
        [Bytes in flight: 1380]
        [Bytes sent since last PSH flag: 1380]
    TCP payload (1380 bytes)
    TCP segment data (1301 bytes)
Secure Sockets Layer
    SSLv3 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 74
        Handshake Protocol: Server Hello
            Handshake Type: Server Hello (2)
            Length: 70
            Version: SSL 3.0 (0x0300)
            Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c3919...
                GMT Unix Time: Dec 31, 1969 16:00:00.000000000 Pacific Standard Time
                Random Bytes: 42dbed248b8831d04cc98c26e5badc4e267c391944f0f070...
            Session ID Length: 32
            Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86dd...
            Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
            Compression Method: null (0)
    112 0.022648       128.238.38.162        216.75.194.220        SSLv3    258    Client Key Exchange, Change Cipher Spec, Encrypted
Handshake Message
Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 18, 2005 11:11:12.694171000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1121710272.694171000 seconds
    [Time delta from previous captured frame: 0.022648000 seconds]
    [Time delta from previous displayed frame: 0.022648000 seconds]
    [Time since reference or first frame: 21.876168000 seconds]
    Frame Number: 112
    Frame Length: 258 bytes (2064 bits)
    Capture Length: 258 bytes (2064 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssl]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
    Destination: All-HSRP-routers_00 (00:00:0c:07:ac:00)
        Address: All-HSRP-routers_00 (00:00:0c:07:ac:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Ibm_10:60:99 (00:09:6b:10:60:99)
        Address: Ibm_10:60:99 (00:09:6b:10:60:99)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 244
    Identification: 0x482c (18476)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x6f1f [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.238.38.162
    Destination: 216.75.194.220
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 79, Ack: 2785, Len: 204
    Source Port: 2271
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 204]
    Sequence number: 79    (relative sequence number)
    [Next sequence number: 283    (relative sequence number)]
    Acknowledgment number: 2785    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window size value: 64799
    [Calculated window size: 64799]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xc2d9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 111]
        [The RTT to ACK the segment was: 0.022648000 seconds]
        [iRTT: 0.022082000 seconds]
        [Bytes in flight: 204]
        [Bytes sent since last PSH flag: 204]
    TCP payload (204 bytes)
Secure Sockets Layer
    SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 132
        Handshake Protocol: Client Key Exchange
            Handshake Type: Client Key Exchange (16)
            Length: 128
            RSA Encrypted PreMaster Secret
                Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c...
    SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: SSL 3.0 (0x0300)
        Length: 1
        Change Cipher Spec Message
    SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 56
        Handshake Protocol: Encrypted Handshake Message
```