WireShark Lab 8

Jennifer Hurst

Instructions:
Capture your packets in an SSL session. To do this, you should go to your favorite e-commerce site and begin the process of purchasing an item (but terminating before making the actual purpose!).

After capturing the packets with Wireshark, you should **set the filter so that it displays only the Ethernet frames that contain SSL records sent from and received by your host**. (An SSL record is the same thing as an SSL message.)

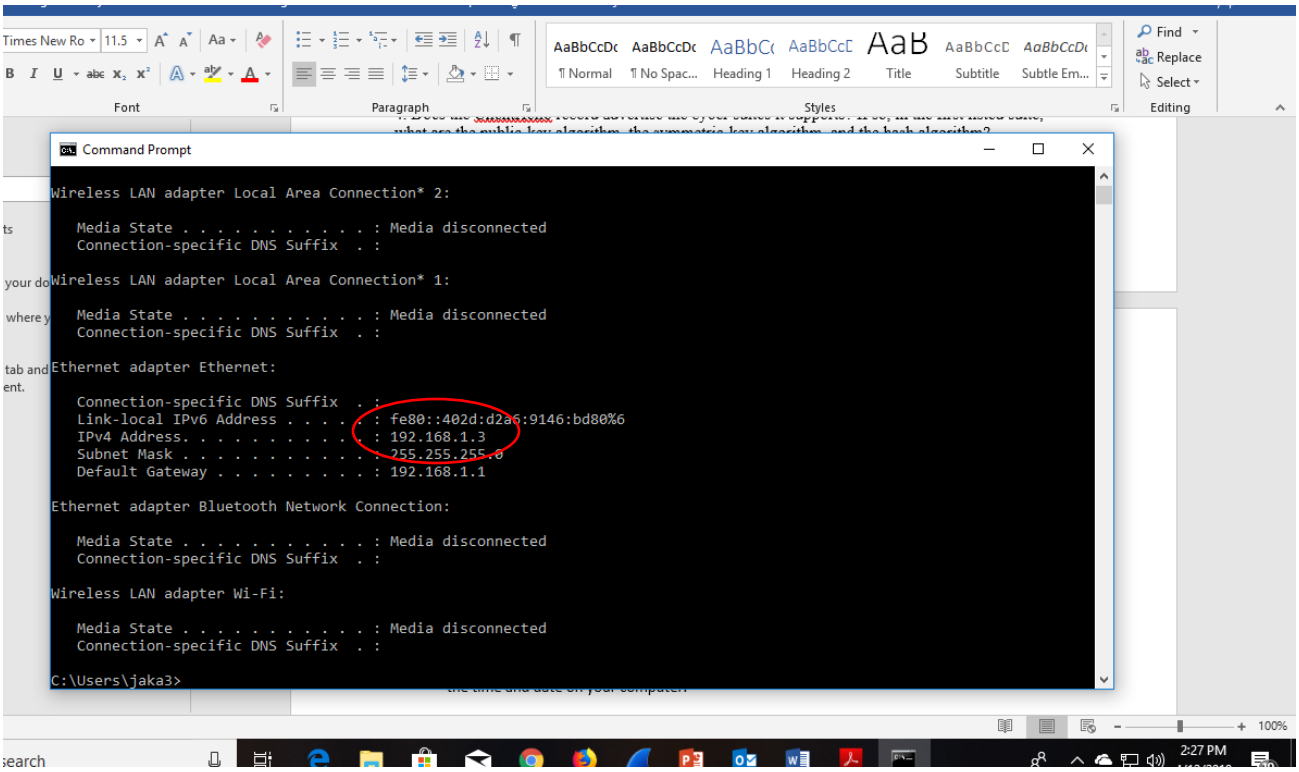
Your Wireshark GUI should be displaying only the Ethernet frames that have SSL records. It is important to keep in mind that an Ethernet frame may contain one or more SSL records. (This is very different from HTTP, for which each frame contains either one complete HTTP message or a portion of a HTTP message.) Also, an SSL record may not completely fit into an Ethernet frame, in which case multiple frames will be needed to carry the record. Locate the "Client Hello" and "Server Hello" frame and use the frames to answer the questions.

- • (*For each of these questions, take a screenshot of Wireshark, and attach it to your answer*) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- • Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Lab will NOT be graded if either of these two is missing.

What is the IP address of your computer? – **Wireshark screenshot not, Terminal**

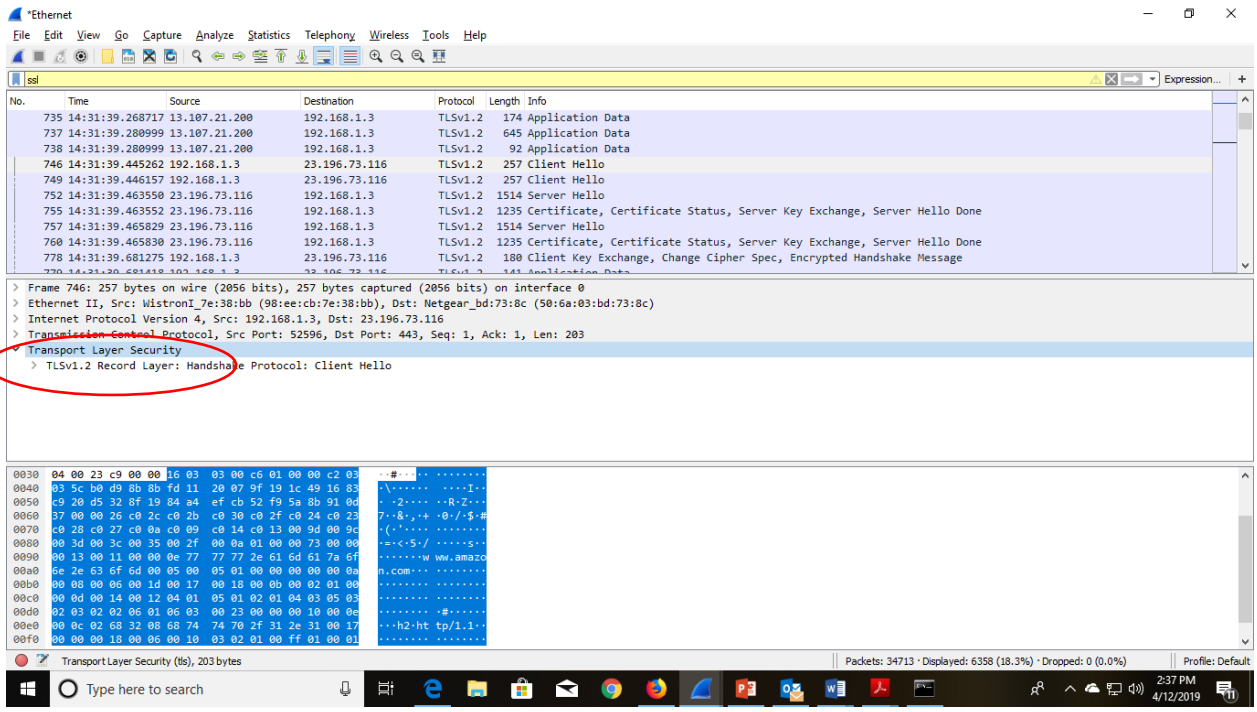
My IP address is 192.168.1.3



Questions:

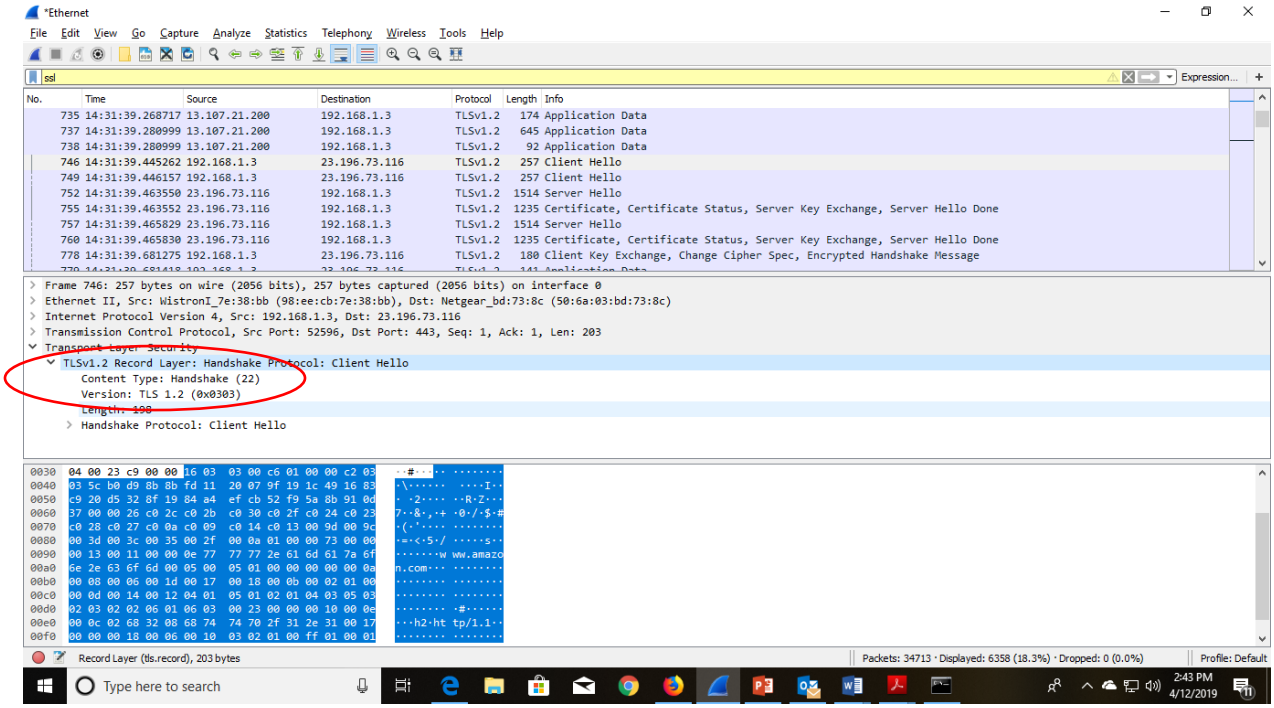
Client Hello Record:

1. What is the SSL/TLS version of the of the Client Hello frame?
   TLS v1.2



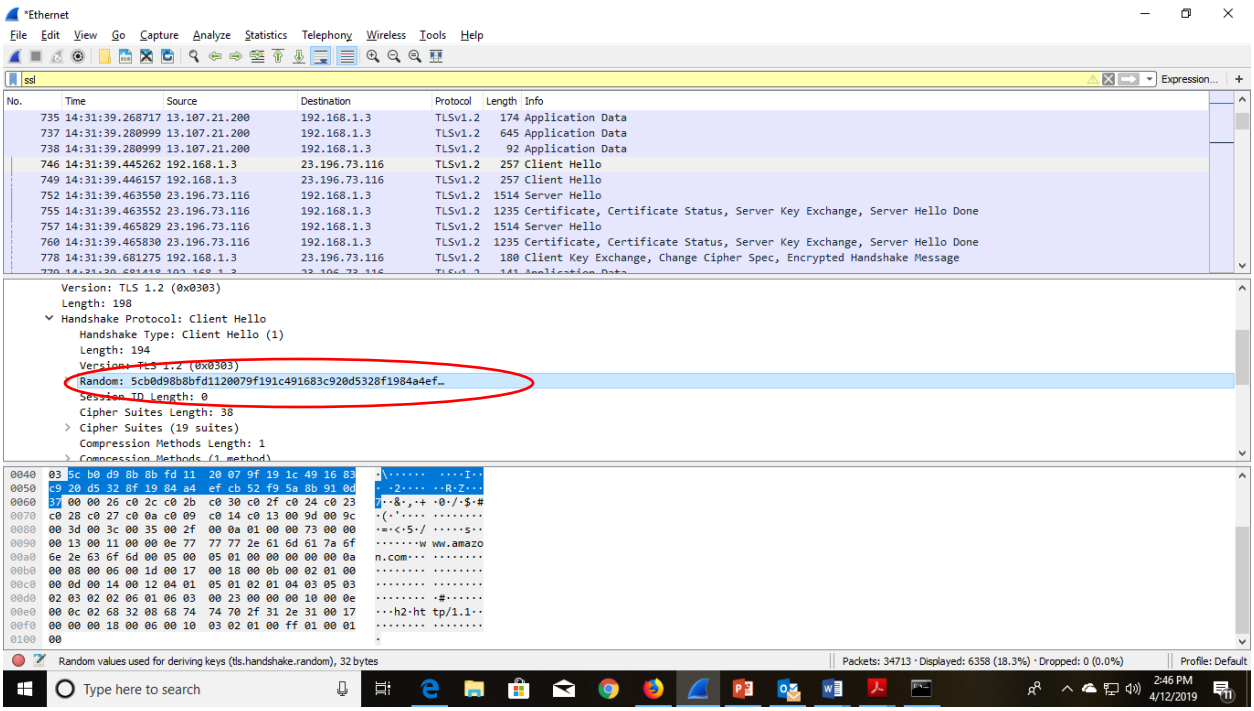
2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

The content type is 22, for handshake message



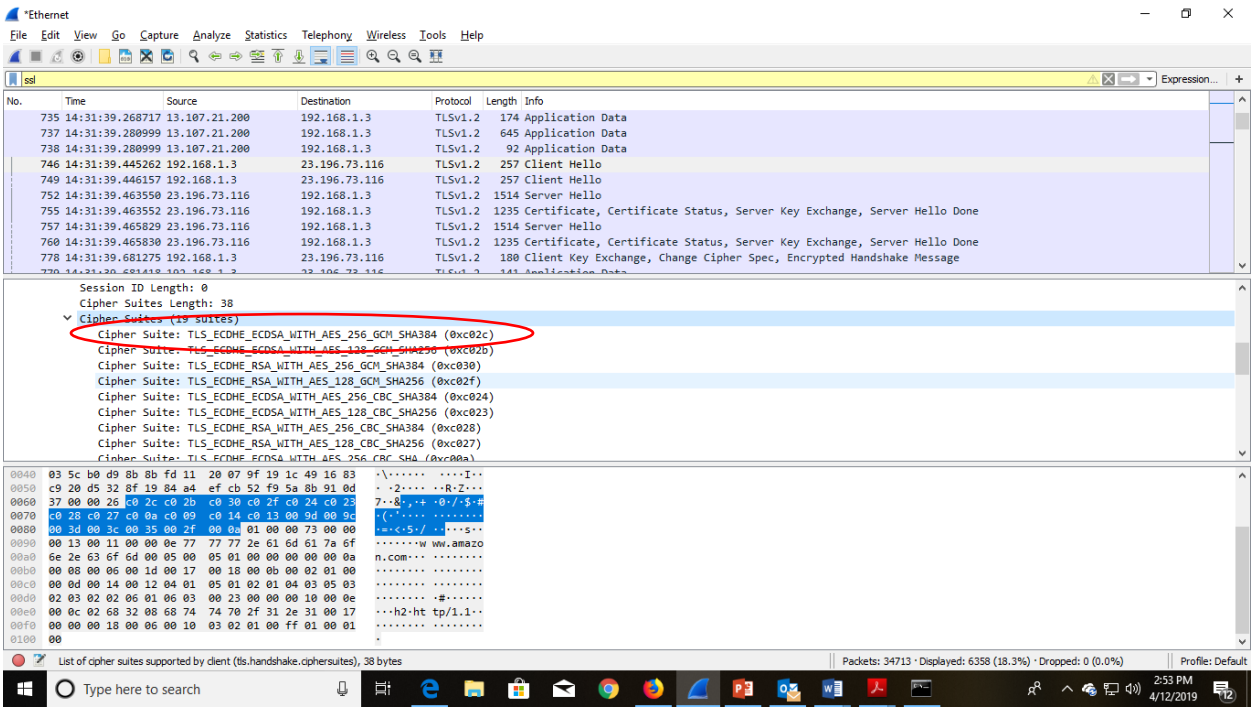
3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

The client hello challenge is Random Bytes:
8bfd1120079f191c491683c920d5328f1984a4efcb52f95a…



4. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

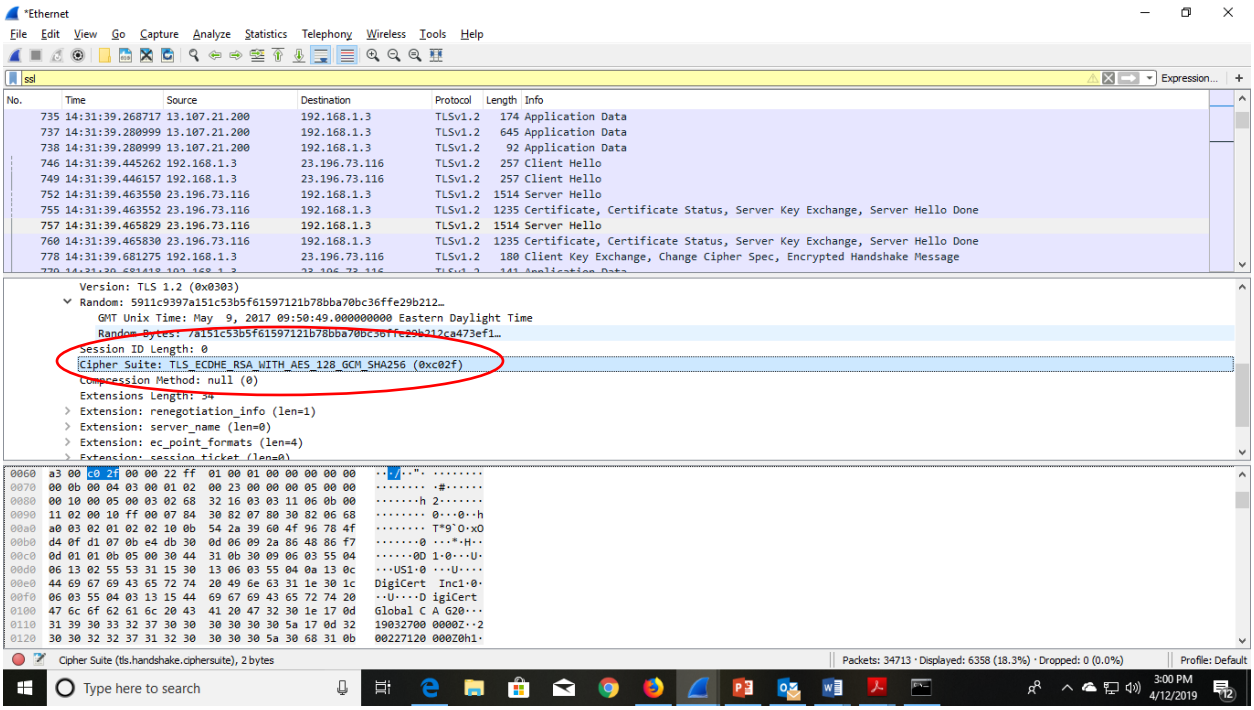
Yes it is listed. The first suite uses ECDHE_ECDSA for public key crypto, AES 256 GCM for the symmetric -key cipher and uses the SHA384 hash algorithm



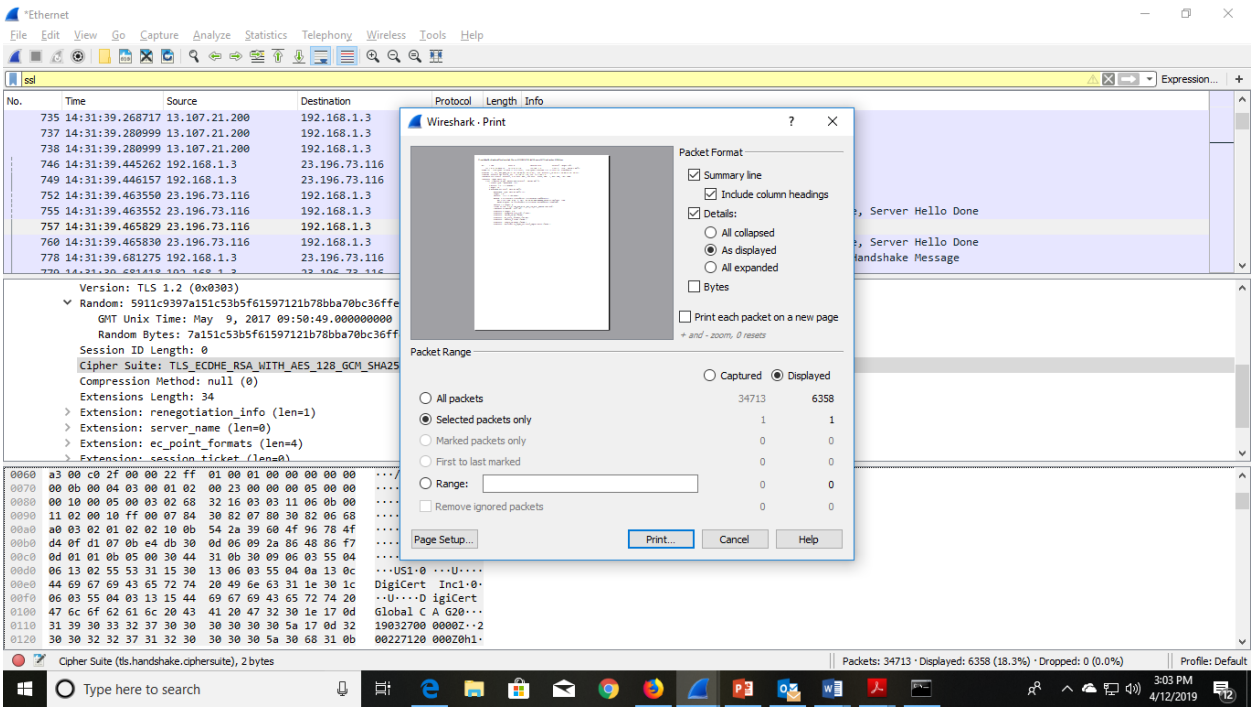
Server Hello Record:

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

The server hello cipher suite uses ECDHE_RSA for public key crypto, AES_128_GCM for the symmetric - key cipher and uses the SHA256 hash algorithm.



Screen print, final page


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...
No. Time Source Destination Protocol Length Info
735 14:31:39.268717 13.107.21.200 192.168.1.3
737 14:31:39.280999 13.107.21.200 192.168.1.3
738 14:31:39.280999 13.107.21.200 192.168.1.3
746 14:31:39.445262 192.168.1.3 23.196.73.116
749 14:31:39.446157 192.168.1.3 23.196.73.116
752 14:31:39.463550 23.196.73.116 192.168.1.3
755 14:31:39.463552 23.196.73.116 192.168.1.3
757 14:31:39.465829 23.196.73.116 192.168.1.3
760 14:31:39.465830 23.196.73.116 192.168.1.3
778 14:31:39.681275 192.168.1.3 23.196.73.116
Server Hello Done
Server Hello Done
Handshake Message
Wireshark · Print
Packet Format
Summary line
Include column headings
Details:
All collapsed
As displayed
All expanded
Bytes
Print each packet on a new page
+ and - zoom, 0 resets
Packet Range
Captured Displayed
All packets 34713 6358
Selected packets only 1 1
Marked packets only 0 0
First to last marked 0 0
Range: 0 0
Remove ignored packets 0 0
Page Setup... Print... Cancel Help
Version: TLS 1.2 (0x0303)
Random: 5911c9397a151c53b5f61597121b78bba70bc36ffe
GMT Unix Time: May 9, 2017 09:50:49.000000000
Random Bytes: 7a151c53b5f61597121b78bba70bc36ff
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA25
Compression Method: null (0)
Extensions Length: 34
Extension: renegotiation_info (len=1)
Extension: server_name (len=0)
Extension: ec_point_formats (len=4)
Extension: session_ticket (len=0)
0060 a3 00 c0 2f 00 00 22 ff 01 00 01 00 00 00 00 00
0070 00 0b 00 04 03 00 01 02 00 23 00 00 00 05 00 00
0080 00 10 00 05 00 03 02 68 32 16 03 03 11 06 0b 00
0090 11 02 00 10 ff 00 07 84 30 82 07 80 30 82 06 68
00a0 a0 03 02 01 02 02 10 0b 54 2a 39 60 4f 96 78 4f
00b0 d4 0f d1 07 0b e4 db 30 0d 06 09 2a 86 48 86 f7
00c0 0d 01 01 0b 05 00 30 44 31 0b 30 09 06 03 55 04
00d0 06 13 02 55 53 31 15 30 13 06 03 55 04 0a 13 0c ···US1·0 ···U····
00e0 44 69 67 69 43 65 72 74 20 49 6e 63 31 1e 30 1c DigiCert Inc1·0·
00f0 06 03 55 04 03 13 15 44 69 67 69 43 65 72 74 20 ··U····D igiCert
0100 47 6c 6f 62 61 6c 20 43 41 20 47 32 30 1e 17 0d Global C A G20···
0110 31 39 30 33 32 37 30 30 30 30 30 5a 17 0d 32 19032700 0000Z··2
0120 30 30 32 32 37 31 32 30 30 30 30 5a 30 68 31 0b 00227120 000Z0h1·
Cipher Suite (tls.handshake.ciphersuite), 2 bytes
Packets: 34713 · Displayed: 6358 (18.3%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
3:03 PM
4/12/2019