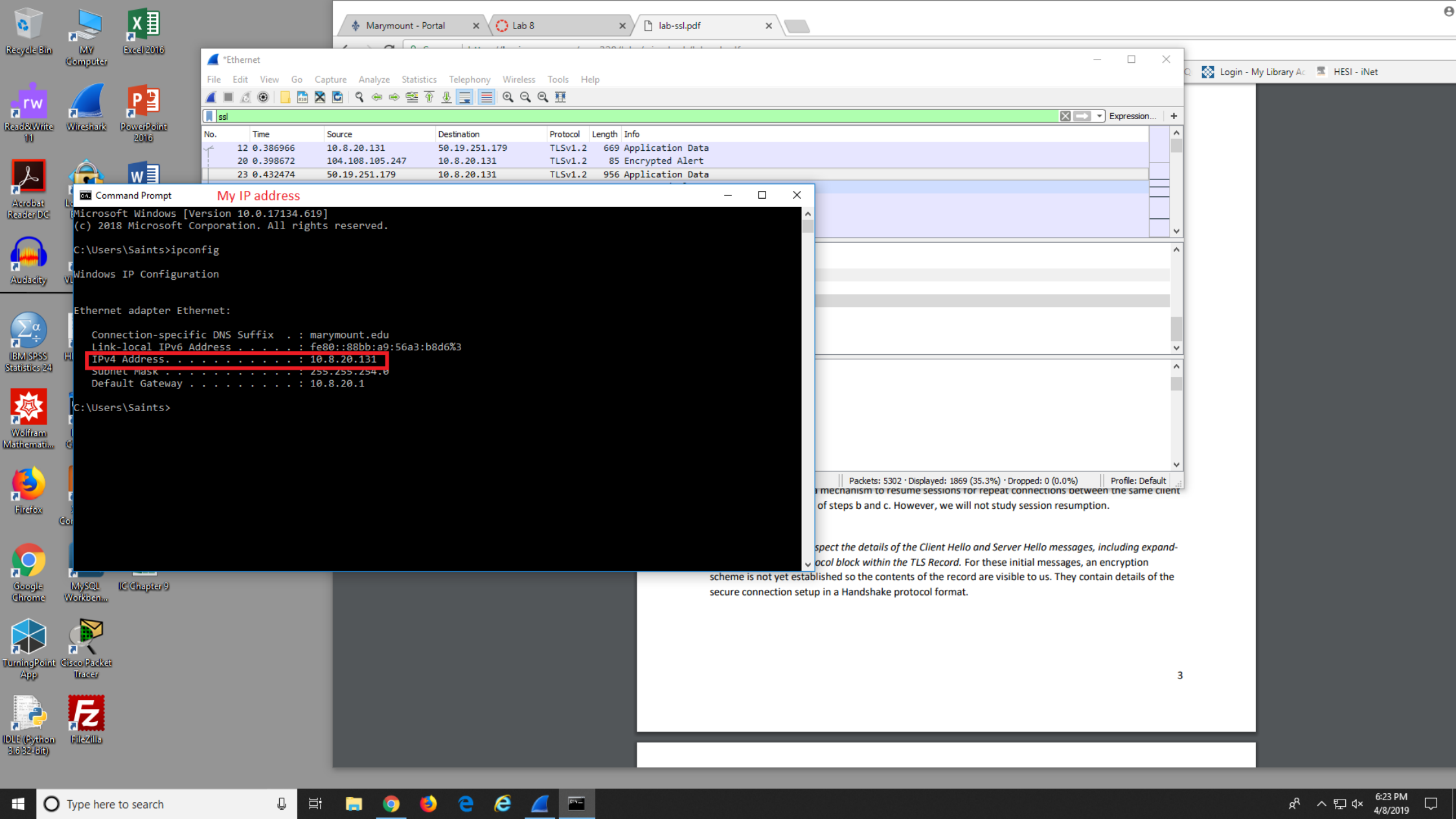
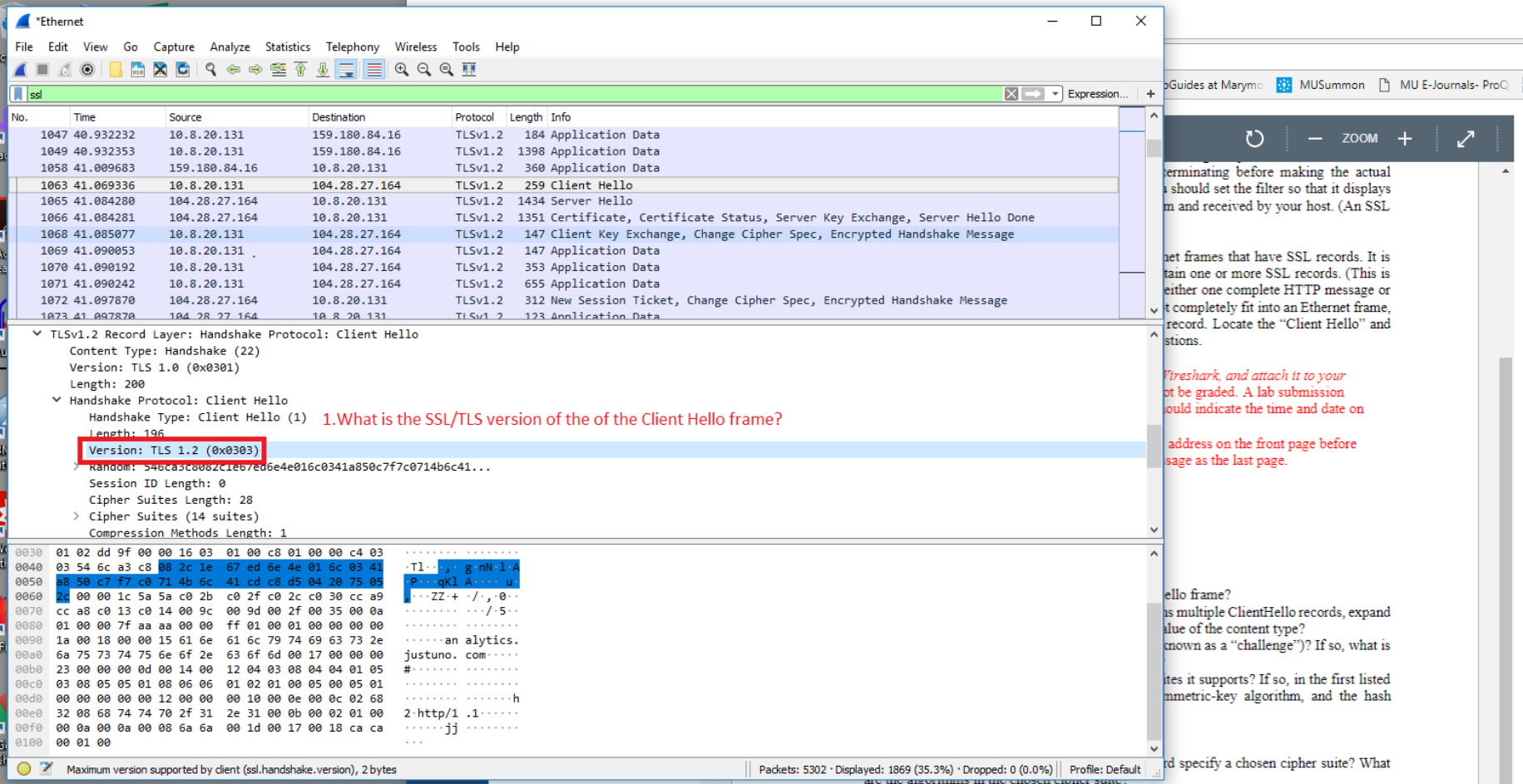

Marymount - Portal
Lab 8
lab-ssl.pdf
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...
No. Time Source Destination Protocol Length Info
12 0.386966 10.8.20.131 50.19.251.179 TLSv1.2 669 Application Data
20 0.398672 104.108.105.247 10.8.20.131 TLSv1.2 85 Encrypted Alert
23 0.432474 50.19.251.179 10.8.20.131 TLSv1.2 956 Application Data
Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%)
Profile: Default
Command Prompt
My IP address
Microsoft Windows [Version 10.0.17134.619]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Saints>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : marymount.edu
Link-local IPv6 Address . . . . . : fe80::88bb:a9:56a3:b8d6%3
IPv4 Address. . . . . : 10.8.20.131
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 10.8.20.1
C:\Users\Saints>
of steps b and c. However, we will not study session resumption.
scheme is not yet established so the contents of the record are visible to us. They contain details of the
secure connection setup in a Handshake protocol format.
3
Recycle Bin
MY Computer
Excel 2016
Read&Write 11
Wireshark
PowerPoint 2016
Acrobat Reader DC
Audacity
IBM SPSS Statistics 24
Wolfram Mathemati...
Firefox
Google Chrome
MySQL Workben...
IC Chapter 9
TurningPoint App
Cisco Packet Tracer
IDLE (Python 3.6 32-bit)
FileZilla
Type here to search
6:23 PM
4/8/2019


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...
No. Time Source Destination Protocol Length Info
1047 40.932232 10.8.20.131 159.180.84.16 TLSv1.2 184 Application Data
1049 40.932353 10.8.20.131 159.180.84.16 TLSv1.2 1398 Application Data
1058 41.009683 159.180.84.16 10.8.20.131 TLSv1.2 360 Application Data
1063 41.069336 10.8.20.131 104.28.27.164 TLSv1.2 259 Client Hello
1065 41.084280 104.28.27.164 10.8.20.131 TLSv1.2 1434 Server Hello
1066 41.084281 104.28.27.164 10.8.20.131 TLSv1.2 1351 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1068 41.085077 10.8.20.131 104.28.27.164 TLSv1.2 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1069 41.090053 10.8.20.131 104.28.27.164 TLSv1.2 147 Application Data
1070 41.090192 10.8.20.131 104.28.27.164 TLSv1.2 353 Application Data
1071 41.090242 10.8.20.131 104.28.27.164 TLSv1.2 655 Application Data
1072 41.097870 104.28.27.164 10.8.20.131 TLSv1.2 312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 200
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
1.What is the SSL/TLS version of the of the Client Hello frame?
Length: 196
Version: TLS 1.2 (0x0303)
Random: 546ca3c8082c1e67ed6e4e016c0341a850c7f7c0714b6c41...
Session ID Length: 0
Cipher Suites Length: 28
Cipher Suites (14 suites)
Compression Methods Length: 1
0030 01 02 dd 9f 00 00 16 03 01 00 c8 01 00 00 c4 03
0040 03 54 6c a3 c8 08 2c 1e 67 ed 6e 4e 01 6c 03 41
0050 a8 50 c7 f7 c0 71 4b 6c 41 cd c8 d5 04 20 75 05
0060 2c 00 00 1c 5a 5a c0 2b c0 2f c0 2c c0 30 cc a9
0070 cc a8 c0 13 c0 14 00 9c 00 9d 00 2f 00 35 00 0a
0080 01 00 00 7f aa aa 00 00 ff 01 00 01 00 00 00 00
0090 1a 00 18 00 00 15 61 6e 61 6c 79 74 69 63 73 2e
00a0 6a 75 73 74 75 6e 6f 2e 63 6f 6d 00 17 00 00 00
00b0 23 00 00 00 0d 00 14 00 12 04 03 08 04 04 01 05
00c0 03 08 05 05 01 08 06 06 01 02 01 00 05 00 05 01
00d0 00 00 00 00 00 12 00 00 00 10 00 0e 00 0c 02 68
00e0 32 08 68 74 74 70 2f 31 2e 31 00 0b 00 02 01 00
00f0 00 0a 00 0a 00 08 6a 6a 00 1d 00 17 00 18 ca ca
0100 00 01 00
Maximum version supported by client (ssl.handshake.version), 2 bytes
Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%)
Profile: Default
ZOOM
terminating before making the actual
should set the filter so that it displays
m and received by your host. (An SSL
net frames that have SSL records. It is
tain one or more SSL records. (This is
either one complete HTTP message or
t completely fit into an Ethernet frame,
record. Locate the "Client Hello" and
stions.
Wireshark, and attach it to your
ot be graded. A lab submission
ould indicate the time and date on
address on the front page before
sage as the last page.
ello frame?
s multiple ClientHello records, expand
alue of the content type?
known as a "challenge")? If so, what is
ites it supports? If so, in the first listed
mmetric-key algorithm, and the hash
rd specify a chosen cipher suite? What
Previous
Next
TurningPoint App
Cisco Packet Tracer
IDLE (Python 3.6 32-bit)
FileZilla
Type here to search
6:30 PM
4/8/2019

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1047	40.932232	10.8.20.131	159.180.84.16	TLSv1.2	184	Application Data
1049	40.932353	10.8.20.131	159.180.84.16	TLSv1.2	1398	Application Data
1058	41.009683	159.180.84.16	10.8.20.131	TLSv1.2	360	Application Data
1063	41.069336	10.8.20.131	104.28.27.164	TLSv1.2	259	Client Hello
1065	41.084280	104.28.27.164	10.8.20.131	TLSv1.2	1434	Server Hello
1066	41.084281	104.28.27.164	10.8.20.131	TLSv1.2	1351	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1068	41.085077	10.8.20.131	104.28.27.164	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1069	41.090053	10.8.20.131	104.28.27.164	TLSv1.2	147	Application Data
1070	41.090192	10.8.20.131	104.28.27.164	TLSv1.2	353	Application Data
1071	41.090242	10.8.20.131	104.28.27.164	TLSv1.2	655	Application Data
1072	41.097870	104.28.27.164	10.8.20.131	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1073	41.097870	104.28.27.164	10.8.20.131	TLSv1.2	123	Application Data

```
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (205 bytes)
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 200
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 196
```

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?

```
0030  01 02 dd 9f 00 00 16 03  01 00 c8 01 00 00 c4 03   ........ ........
0040  03 54 6c a3 c8 08 2c 1e  67 ed 6e 4e 01 6c 03 41   ·Tl···,· g·nN·l·A
0050  a8 50 c7 f7 c0 71 4b 6c  41 cd c8 d5 04 20 75 05   ·P···qKl A···· u·
0060  2c 00 00 1c 5a 5a c0 2b  c0 2f c0 2c c0 30 cc a9   ,···ZZ·+ ·/·,·0··
0070  cc a8 c0 13 c0 14 00 9c  00 9d 00 2f 00 35 00 0a   ........ ···/·5··
0080  01 00 00 7f aa aa 00 00  ff 01 00 01 00 00 00 00   ........ ........
0090  1a 00 18 00 00 15 61 6e  61 6c 79 74 69 63 73 2e   ......an alytics.
00a0  6a 75 73 74 75 6e 6f 2e  63 6f 6d 00 17 00 00 00   justuno. com·····
00b0  23 00 00 00 0d 00 14 00  12 04 03 08 04 04 01 05   #····... ........
00c0  03 08 05 05 01 08 06 06  01 02 01 00 05 00 05 01   ........ ........
00d0  00 00 00 00 00 12 00 00  00 10 00 0e 00 0c 02 68   ........ .......h
00e0  32 08 68 74 74 70 2f 31  2e 31 00 0b 00 02 01 00   2·http/1 .1·····
00f0  00 0a 00 0a 00 08 6a 6a  00 1d 00 17 00 18 ca ca   ......jj ........
0100  00 01 00                                          ···
```

Content Type (ssl.record.content_type), 1 byte | Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%) | Profile: Default

...tain one or more SSL records. (This is ...either one complete HTTP message or ...t completely fit into an Ethernet frame, ...record. Locate the "Client Hello" and ...stions.

...Wireshark, and attach it to your ...ot be graded. A lab submission ...ould indicate the time and date on

... address on the front page before ...sage as the last page.

...ello frame?
...s multiple ClientHello records, expand
...alue of the content type?
...known as a "challenge")? If so, what is

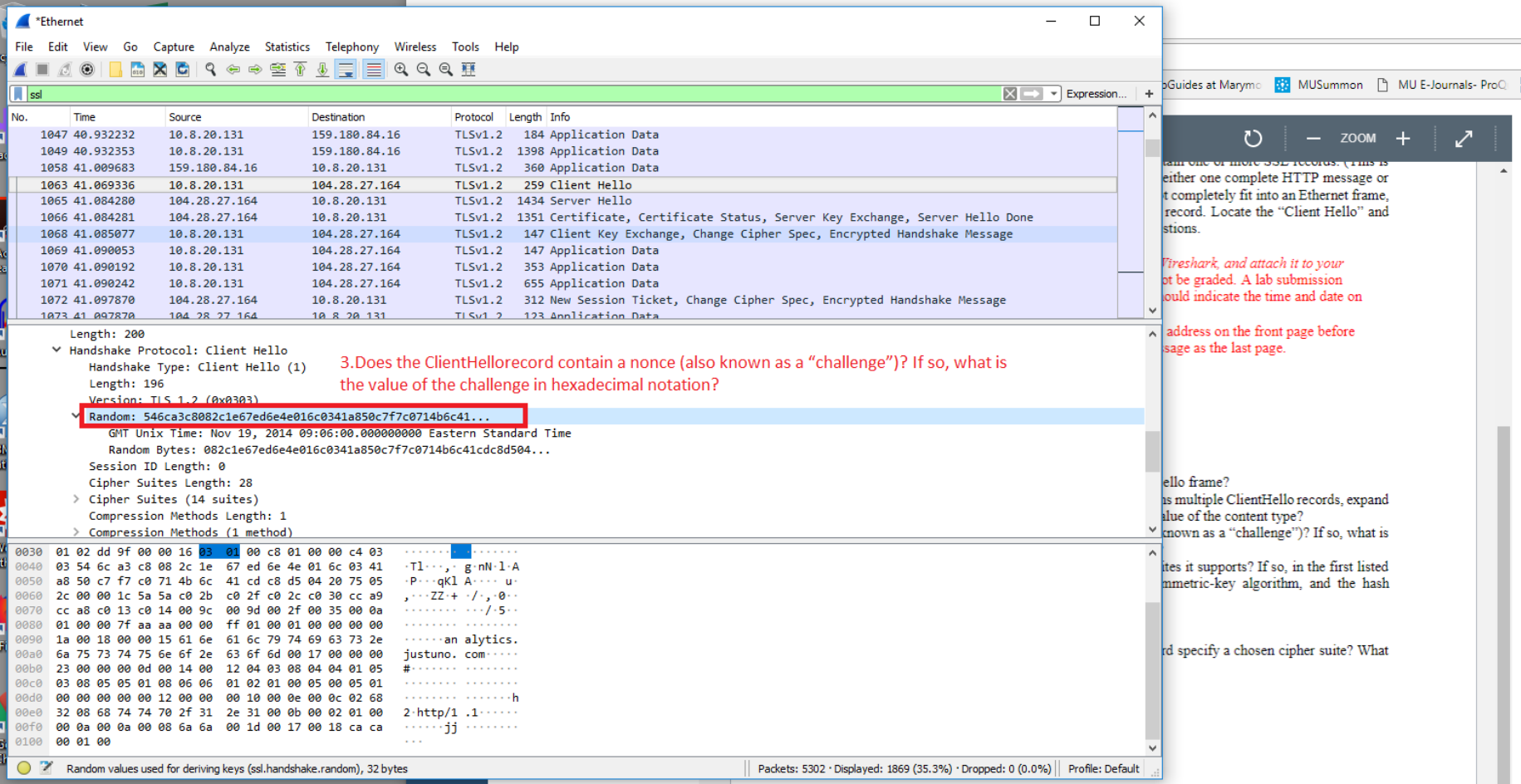
...ites it supports? If so, in the first listed
...mmetric-key algorithm, and the hash

...rd specify a chosen cipher suite? What

◂ Previous Next ▸

Type here to search

6:32 PM
4/8/2019


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...
No. Time Source Destination Protocol Length Info
1047 40.932232 10.8.20.131 159.180.84.16 TLSv1.2 184 Application Data
1049 40.932353 10.8.20.131 159.180.84.16 TLSv1.2 1398 Application Data
1058 41.009683 159.180.84.16 10.8.20.131 TLSv1.2 360 Application Data
1063 41.069336 10.8.20.131 104.28.27.164 TLSv1.2 259 Client Hello
1065 41.084280 104.28.27.164 10.8.20.131 TLSv1.2 1434 Server Hello
1066 41.084281 104.28.27.164 10.8.20.131 TLSv1.2 1351 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1068 41.085077 10.8.20.131 104.28.27.164 TLSv1.2 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1069 41.090053 10.8.20.131 104.28.27.164 TLSv1.2 147 Application Data
1070 41.090192 10.8.20.131 104.28.27.164 TLSv1.2 353 Application Data
1071 41.090242 10.8.20.131 104.28.27.164 TLSv1.2 655 Application Data
1072 41.097870 104.28.27.164 10.8.20.131 TLSv1.2 312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
Length: 200
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 196
Version: TLS 1.2 (0x0303)
Random: 546ca3c8082c1e67ed6e4e016c0341a850c7f7c0714b6c41...
GMT Unix Time: Nov 19, 2014 09:06:00.000000000 Eastern Standard Time
Random Bytes: 082c1e67ed6e4e016c0341a850c7f7c0714b6c41cdc8d504...
Session ID Length: 0
Cipher Suites Length: 28
Cipher Suites (14 suites)
Compression Methods Length: 1
Compression Methods (1 method)
3.Does the ClientHellorecord contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?
0030 01 02 dd 9f 00 00 16 03 01 00 c8 01 00 00 c4 03
0040 03 54 6c a3 c8 08 2c 1e 67 ed 6e 4e 01 6c 03 41
0050 a8 50 c7 f7 c0 71 4b 6c 41 cd c8 d5 04 20 75 05
0060 2c 00 00 1c 5a 5a c0 2b c0 2f c0 2c c0 30 cc a9
0070 cc a8 c0 13 c0 14 00 9c 00 9d 00 2f 00 35 00 0a
0080 01 00 00 7f aa aa 00 00 ff 01 00 01 00 00 00 00
0090 1a 00 18 00 00 15 61 6e 61 6c 79 74 69 63 73 2e
00a0 6a 75 73 74 75 6e 6f 2e 63 6f 6d 00 17 00 00 00
00b0 23 00 00 00 0d 00 14 00 12 04 03 08 04 04 01 05
00c0 03 08 05 05 01 08 06 06 01 02 01 00 05 00 05 01
00d0 00 00 00 00 00 12 00 00 00 10 00 0e 00 0c 02 68
00e0 32 08 68 74 74 70 2f 31 2e 31 00 0b 00 02 01 00
00f0 00 0a 00 0a 00 08 6a 6a 00 1d 00 17 00 18 ca ca
0100 00 01 00
Random values used for deriving keys (ssl.handshake.random), 32 bytes
Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%)
Profile: Default
ZOOM
either one complete HTTP message or
t completely fit into an Ethernet frame,
record. Locate the “Client Hello” and
stions.
Wireshark, and attach it to your
ot be graded. A lab submission
ould indicate the time and date on
address on the front page before
sage as the last page.
ello frame?
s multiple ClientHello records, expand
alue of the content type?
known as a “challenge”)? If so, what is
tes it supports? If so, in the first listed
mmetric-key algorithm, and the hash
rd specify a chosen cipher suite? What
Previous
Next
TurningPoint App
Cisco Packet Tracer
IDLE (Python 3.6 32-bit)
FileZilla
Type here to search
6:34 PM
4/8/2019

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1038	40.807708	10.8.20.131	50.19.251.179	TLSv1.2	1256	Application Data
1039	40.858675	50.19.251.179	10.8.20.131	TLSv1.2	958	Application Data
1044	40.932061	10.8.20.131	159.180.84.16	TLSv1.2	1081	Application Data
1047	40.932232	10.8.20.131	159.180.84.16	TLSv1.2	184	Application Data
1049	40.932353	10.8.20.131	159.180.84.16	TLSv1.2	1398	Application Data
1058	41.009683	159.180.84.16	10.8.20.131	TLSv1.2	360	Application Data
1063	41.069336	10.8.20.131	104.28.27.164	TLSv1.2	259	Client Hello
1065	41.084280	104.28.27.164	10.8.20.131	TLSv1.2	1434	Server Hello
1066	41.084281	104.28.27.164	10.8.20.131	TLSv1.2	1351	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1068	41.085077	10.8.20.131	104.28.27.164	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1069	41.090053	10.8.20.131	104.28.27.164	TLSv1.2	147	Application Data
1070	41.090192	10.8.20.131	104.28.27.164	TLSv1.2	353	Application Data
1071	41.090242	10.8.20.131	104.28.27.164	TLSv1.2	655	Application Data
1072	41.097870	104.28.27.164	10.8.20.131	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1073	41.097870	104.28.27.164	10.8.20.131	TLSv1.2	123	Application Data
1075	41.098092	10.8.20.131	104.28.27.164	TLSv1.2	92	Application Data
1077	41.107089	104.28.27.164	10.8.20.131	TLSv1.2	92	Application Data

```
Cipher Suites (14 suites)
    Cipher Suite: Reserved (GREASE) (0x5a5a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 127
```

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?

-No public-key algorithm
-the symmetric-key algorithm AES_128_GSM
-hash algorithm SHA256

```
0000  00 2c c8 59 ec bf 14 b3  1f 14 c0 18 08 00 45 00   ·,·Y···· ·····E·
0010  00 f5 2e f8 40 00 80 06  28 c0 0a 08 14 83 68 1c   ····@··· (·····h·
0020  1b a4 f7 36 01 bb 28 5a  74 a4 78 8b dc 5a 50 18   ···6··(Z t·x··ZP·
0030  01 02 dd 9f 00 00 16 03  01 00 c8 01 00 00 c4 03   ········ ········
0040  03 54 6c a3 c8 08 2c 1e  67 ed 6e 4e 01 6c 03 41   ·Tl···,· g·nN·l·A
0050  a8 50 c7 f7 c0 71 4b 6c  41 cd c8 d5 04 20 75 05   ·P···qKl A···· u·
0060  2c 00 00 1c 5a 5a c0 2b  c0 2f c0 2c c0 30 cc a9   ,···ZZ·+ ·/·,·0··
0070  cc a8 c0 13 c0 14 00 9c  00 9d 00 2f 00 35 00 0a   ········ ···/·5··
0080  01 00 00 7f aa aa 00 00  ff 01 00 01 00 00 00 00   ········ ········
0090  1a 00 18 00 00 15 61 6e  61 6c 79 74 69 63 73 2e   ·····an alytics.
00a0  6a 75 73 74 75 6e 6f 2e  63 6f 6d 00 17 00 00 00   justuno. com·····
00b0  23 00 00 00 0d 00 14 00  12 04 03 08 04 04 01 05   #······ ········
00c0  03 08 05 05 01 08 06 06  01 02 01 00 05 00 05 01   ········ ········
00d0  00 00 00 00 00 12 00 00  00 10 00 0e 00 0c 02 68   ········ ·······h
00e0  32 08 68 74 74 70 2f 31  2e 31 00 0b 00 02 01 00   2·http/1 .1······
00f0  00 0a 00 0a 00 08 5a 6a  00 1d 00 17 00 18 ca ca   ·····Zj ········
0100  00 01 00                                          ···
```

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%) | Profile: Default

Type here to search

9:11 PM
4/8/2019

Marymount - Portal | Lab 8 | Chapter 8 - Slide: 19/SP | Inbox (6,998) - g0e62891

Secure | https://marymount.instructure.com/courses/14356/assignments/89453?module_item_id=219954

Apps | Marymount Universit | Library & Learning Se | MU Gmail | MU Portal

Account | Dashboard | Courses | Groups | Calendar | Inbox 11 | Help

very different from HTTP,
a portion of a HTTP messa
in which case multiple fra
"Server Hello" frame and

- *(For each of these answer)* - Question template is availab your computer.
- Include a terminal Question 1, and a f

Lab will NOT be graded if

Questions:

Client Hello Record:

1. What is the SSL/TL
2. Expand the ClientH the frame that cont
3. Does the ClientHel the value of the cha
4. Does the ClientHel suite, what are th algorithm?

Server Hello Record:

1. Locate the ServerH are the algorithms

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1047	40.932232	10.8.20.131	159.180.84.16	TLSv1.2	184	Application Data
1049	40.932353	10.8.20.131	159.180.84.16	TLSv1.2	1398	Application Data
1058	41.009683	159.180.84.16	10.8.20.131	TLSv1.2	360	Application Data
1063	41.069336	10.8.20.131	104.28.27.164	TLSv1.2	259	Client Hello
1065	41.084280	104.28.27.164	10.8.20.131	TLSv1.2	1434	Server Hello
1066	41.084281	104.28.27.164	10.8.20.131	TLSv1.2	1351	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1068	41.085077	10.8.20.131	104.28.27.164	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1069	41.090053	10.8.20.131	104.28.27.164	TLSv1.2	147	Application Data
1070	41.090192	10.8.20.131	104.28.27.164	TLSv1.2	353	Application Data
1071	41.090242	10.8.20.131	104.28.27.164	TLSv1.2	655	Application Data
1072	41.097870	104.28.27.164	10.8.20.131	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1073	41.097870	104.28.27.164	10.8.20.131	TLSv1.2	123	Application Data

```
Handshake Type: Server Hello (2)
Length: 72
Version: TLS 1.2 (0x0303)
Random: 5cabc79b556cee5f80de4012c40f59e56de7186287b418e0...
   GMT Unix Time: Apr  8, 2019 18:13:47.000000000 Eastern Daylight Time
   Random Bytes: 556cee5f80de4012c40f59e56de7186287b418e0444f574e...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Compression Method: null (0)
Extensions Length: 32
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=2)
```

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

-Cipher suite TLS ECDHE ECDSA WITH AES 128 GSM SHA256
-Public key algorithm ECDHE
-Symmetric key algorithm AES
-hash algorhitm SHA256

```
0000  14 b3 1f 14 c0 18 00 2c  c8 59 ec bf 08 00 45 00   .......,  .Y....E.
0010  05 8c 83 54 40 00 3a 06  15 cd 68 1c 1b a4 0a 08   ...T@.:.  ..h.....
0020  14 83 01 bb f7 36 78 8b  dc 5a 28 5a 75 71 50 10   .....6x.  .Z(ZuqP.
0030  00 1e 49 b2 00 00 16 03  03 00 4c 02 00 00 48 03   ..I.....  ..L...H.
0040  03 5c ab c7 9b 55 6c ee  5f 80 de 40 12 c4 0f 59   .\...Ul.  _..@...Y
0050  e5 6d e7 18 62 87 b4 18  e0 44 4f 57 4e 47 52 44   .m..b...  .DOWNGRD
0060  01 00 c0 2b 00 00 20 00  17 00 00 ff 01 00 01 00   ...+..  .  ........
0070  00 0b 00 02 01 00 00 23  00 00 00 10 00 05 00 03   .......#  ........
0080  02 68 32 00 05 00 00 16  03 03 08 79 0b 00 08 75   .h2.....  ...y...u
0090  00 08 72 00 04 c5 30 82  04 c1 30 82 04 68 a0 03   ..r...0.  ..0..h..
00a0  02 01 02 02 10 0f 5d 56  5c 95 4a 66 91 6e e2 4e   ......]V  \.Jf.n.N
00b0  62 57 70 7c 18 30 0a 06  08 2a 86 48 ce 3d 04 03   bWp|.0..  .*.H.=..
00c0  02 30 6f 31 0b 30 09 06  03 55 04 06 13 02 55 53   .0o1.0..  .U....US
00d0  31 0b 30 09 06 03 55 04  08 13 02 43 41 31 16 30   1.0...U.  ...CA1.0
```

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%) | Profile: Default

aded on

◂ Previous | Next ▸

Type here to search

9:14 PM
4/8/2019

Marymount - Portal | Lab 8 | Chapter 8 - Slide: 19/SP | Inbox (6,998) - g0e62891

Secure | https://marymount.instructure.com/courses/14356/assignments/89453?module_item_id=219954

Apps | Marymount Universit | Library & Learning Sc | MU Gmail | MU Portal | Marynet | WRLC Catalog | LibGuides at Marymo | MUSummon | MU E-Journals- ProQ | Login - My Library A | HESL - iNet

Account
Dashboard
Courses
Groups
Calendar
Inbox 11
Help

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1047	40.932232	10.8.20.131	159.180.84.16	TLSv1.2	184	Application Data
1049	40.932353	10.8.20.131	159.180.84.16	TLSv1.2	1398	Application Data
1058	41.009683	159.180.84.16	10.8.20.131			
1063	41.069336	10.8.20.131	104.28.27.164			
1065	41.084280	104.28.27.164	10.8.20.131			
1066	41.084281	104.28.27.164	10.8.20.131			ange, Server Hello Done
1068	41.085077	10.8.20.131	104.28.27.164			ed Handshake Message
1069	41.090053	10.8.20.131	104.28.27.164			
1070	41.090192	10.8.20.131	104.28.27.164			
1071	41.090242	10.8.20.131	104.28.27.164			
1072	41.097870	104.28.27.164	10.8.20.131			d Handshake Message
1073	41.097870	104.28.27.164	10.8.20.131			

Handshake Type: Server Hello (2)
Length: 72
Version: TLS 1.2 (0x0303)
Random: 5cabc79b556cee5f80de4012c40f59e56de71
GMT Unix Time: Apr 8, 2019 18:13:47.00000
Random Bytes: 556cee5f80de4012c40f59e56de7
Session ID Length: 0
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GC
Compression Method: null (0)
Extensions Length: 32
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)
Extension: ec point formats (len=2)

```
0000  14 b3 1f 14 c0 18 00 2c  c8 59 ec bf 08 00 45 00   ·····,· ·Y····E·
0010  05 8c 83 54 40 00 3a 06  15 cd 68 1c 1b a4 0a 08   ···T@·:· ··h·····
0020  14 83 01 bb f7 36 78 8b  dc 5a 28 5a 75 71 50 10   ·····6x· ·Z(ZuqP·
0030  00 1e 49 b2 00 00 16 03  03 00 4c 02 00 00 48 03   ··I····· ··L···H·
0040  03 5c ab c7 9b 55 6c ee  5f 80 de 40 12 c4 0f 59   ·\···Ul· _··@···Y
0050  e5 6d e7 18 62 87 b4 18  e0 44 4f 57 4e 47 52 44   ·m··b··· ·DOWNGRD
0060  01 00 c0 2b 00 00 20 00  17 00 00 ff 01 00 01 00   ···+·· · ········
0070  00 0b 00 02 01 00 00 23  00 00 00 10 00 05 00 03   ·······# ········
0080  02 68 32 00 05 00 00 16  03 03 08 79 0b 00 08 75   ·h2····· ···y···u
0090  00 08 72 00 04 c5 30 82  04 c1 30 82 04 68 a0 03   ··r···0· ··0··h··
00a0  02 01 02 02 10 0f 5d 56  5c 95 4a 66 91 6e e2 4e   ·····]V \·Jf·n·N
00b0  62 57 70 7c 18 30 0a 06  08 2a 86 48 ce 3d 04 03   bWp|·0·· ·*·H·=··
00c0  02 30 6f 31 0b 30 09 06  03 55 04 06 13 02 55 53   ·0o1·0·· ·U····US
00d0  31 0b 30 09 06 03 55 04  08 13 02 43 41 31 16 30   1·0···U· ···CA1·0
```

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 5302 · Displayed: 1869 (35.3%) · Dropped: 0 (0.0%) | Profile: Default

Wireshark · Print

Packet Format
- [x] Summary line
- [x] 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	5302	1869
(•) 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

◂ Previous | Next ▸

Type here to search

9:14 PM
4/8/2019

```
   1065 41.084280      104.28.27.164         10.8.20.131           TLSv1.2  1434   Server Hello
Frame 1065: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
Ethernet II, Src: Cisco_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell_14:c0:18 (14:b3:1f:14:c0:18)
Internet Protocol Version 4, Src: 104.28.27.164, Dst: 10.8.20.131
Transmission Control Protocol, Src Port: 443, Dst Port: 63286, Seq: 1, Ack: 206, Len: 1380
    Source Port: 443
    Destination Port: 63286
    [Stream index: 185]
    [TCP Segment Len: 1380]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1381    (relative sequence number)]
    Acknowledgment number: 206    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window size value: 30
    [Calculated window size: 30720]
    [Window size scaling factor: 1024]
    Checksum: 0x49b2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (1380 bytes)
    TCP segment data (1299 bytes)
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 76
        Handshake Protocol: Server Hello
            Handshake Type: Server Hello (2)
            Length: 72
            Version: TLS 1.2 (0x0303)
            Random: 5cabc79b556cee5f80de4012c40f59e56de7186287b418e0...
                GMT Unix Time: Apr  8, 2019 18:13:47.000000000 Eastern Daylight Time
                Random Bytes: 556cee5f80de4012c40f59e56de7186287b418e0444f574e...
            Session ID Length: 0
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
            Compression Method: null (0)
            Extensions Length: 32
            Extension: extended_master_secret (len=0)
            Extension: renegotiation_info (len=1)
            Extension: ec_point_formats (len=2)
            Extension: SessionTicket TLS (len=0)
            Extension: application_layer_protocol_negotiation (len=5)
            Extension: status_request (len=0)
```