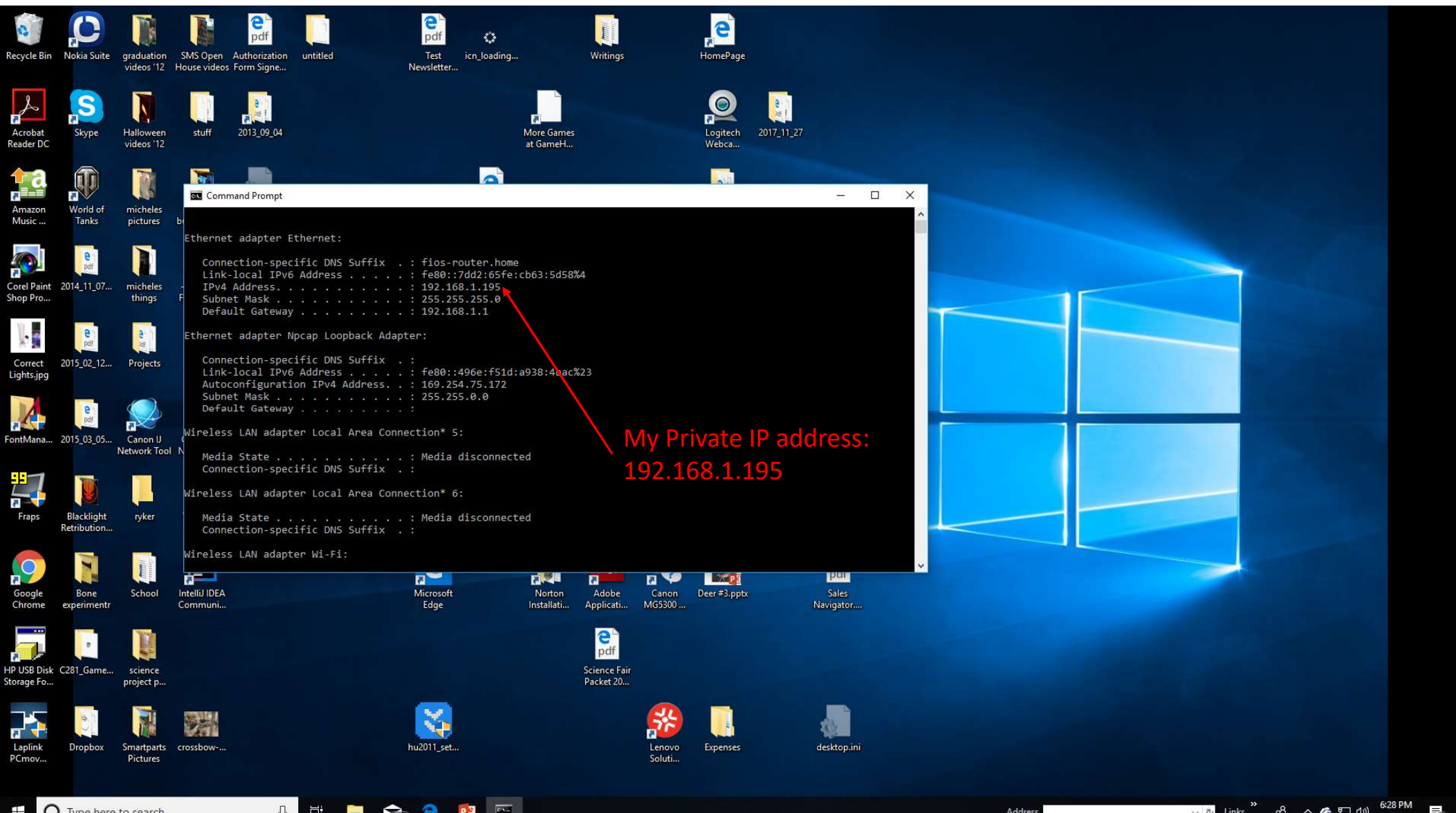


Wireshark Lab 8 – SSL / TLS

IT 520 –A – Enterprise Infrastructure & Networks

David Gogolkiewicz



Question 1

Wireshark Lab 8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
17	1.491840	192.168.1.195	13.107.42.12	TLSv1.2	234	Client Hello
25	1.502519	13.107.42.12	192.168.1.195	TLSv1.2	1348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
27	1.505990	192.168.1.195	13.107.42.12	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	1.521131	13.107.42.12	192.168.1.195	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
30	1.521975	192.168.1.195	13.107.42.12	TLSv1.2	1673	Application Data
31	1.522006	192.168.1.195	13.107.42.12	TLSv1.2	305	Application Data
34	1.561956	13.107.42.12	192.168.1.195	TLSv1.2	887	Application Data
35	1.561957	13.107.42.12	192.168.1.195	TLSv1.2	111	Application Data
49	5.233894	192.168.1.195	52.242.211.89	TLSv1.2	97	Application Data
50	5.298797	52.242.211.89	192.168.1.195	TLSv1.2	179	Application Data
65	7.326627	192.168.1.195	40.122.162.208	TLSv1.2	230	Client Hello
70	7.379406	40.122.162.208	192.168.1.195	TLSv1.2	1346	Server Hello, Certificate, Server Key Exchange, Server Hello Done
71	7.381808	192.168.1.195	40.122.162.208	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
72	7.426495	40.122.162.208	192.168.1.195	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
73	7.427872	192.168.1.195	40.122.162.208	TLSv1.2	1269	Application Data
74	7.476453	40.122.162.208	192.168.1.195	TLSv1.2	439	Application Data
75	7.477393	40.122.162.208	192.168.1.195	TLSv1.2	88	Application Data

Destination: 13.107.42.12

Transmission Control Protocol, Src Port: 58139, Dst Port: 443, Seq: 1, Ack: 1, Len: 180

Source Port: 58139

Destination Port: 443

[Stream index: 0]

[TCP Segment Len: 180]

Sequence number: 1 (relative sequence number)

[Next sequence number: 181 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 258

[Calculated window size: 66048]

[Window size scaling factor: 256]

Checksum: 0xfab0 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[Timestamps]

TCP payload (180 bytes)

Transport Layer Security

TLSv1.2 Record Layer: Handshake Protocol: Client Hello

0000 48 5d 36 68 c5 b8 00 01 6c d1 d3 8c 08 00 45 00 H]6h... 1....E-

0010 00 dc 63 a1 40 00 80 06 00 00 c0 a8 01 c3 0d 6b ..c.@@... ..k

0020 2a 0c e3 1b 01 bb a9 d1 c9 d8 dc 36 ec 26 50 18 *......6.&P

0030 01 02 fa b0 00 00 16 03 03 00 af 01 00 00 ab 03 .\A..\ ..u7I)

0040 03 5c be 41 ed d3 5c 83 1c da ed ef 75 37 49 29 D...Q...f...m...

0050 44 c9 d5 f7 00 51 04 0c 66 91 d7 97 6d 02 07 a7 ...*,+ :0./.....

0060 ab 00 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e .\$.#.(.....

0070 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13< :5./.....

0080 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00 .X.....d.doc

0090 00 58 00 00 00 14 00 12 00 00 0f 64 2e 64 6f 63 s.live.n et.....

00a0 73 2e 6c 69 76 65 2e 6e 65 74 00 05 00 05 01 00#

00b0 00 00 00 0a 00 08 00 06 00 1d 00 17 00 18 00#

00c0 0b 00 02 01 00 00 0d 00 14 00 12 04 01 05 01 02#

00d0 01 04 03 05 03 02 03 02 02 06 01 06 03 00 23 00#

Packets: 250/40 · Displayed: 11292 (45.1%) · Dropped: 0 (0.0%)

Profile: Default

Address Links

6:41 PM 4/22/2019

What is the SSL/TLS version of the of the Client Hello frame?

- Version 1.2

Question 2

Wireshark Lab 8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
17	1.491840	192.168.1.195	13.107.42.12	TLSv1.2	234	Client Hello
25	1.502519	13.107.42.12	192.168.1.195	TLSv1.2	1348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
27	1.505990	192.168.1.195	13.107.42.12	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	1.521131	13.107.42.12	192.168.1.195	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
30	1.521975	192.168.1.195	13.107.42.12	TLSv1.2	1673	Application Data
31	1.522006	192.168.1.195	13.107.42.12	TLSv1.2	305	Application Data
34	1.561956	13.107.42.12	192.168.1.195	TLSv1.2	887	Application Data
35	1.561957	13.107.42.12	192.168.1.195	TLSv1.2	111	Application Data
49	5.233894	192.168.1.195	52.242.211.89	TLSv1.2	97	Application Data
50	5.298797	52.242.211.89	192.168.1.195	TLSv1.2	179	Application Data
65	7.326627	192.168.1.195	40.122.162.208	TLSv1.2	230	Client Hello
70	7.379406	40.122.162.208	192.168.1.195	TLSv1.2	1346	Server Hello, Certificate, Server Key Exchange, Server Hello Done
71	7.381808	192.168.1.195	40.122.162.208	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
72	7.426495	40.122.162.208	192.168.1.195	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
73	7.427872	192.168.1.195	40.122.162.208	TLSv1.2	1269	Application Data
74	7.476453	40.122.162.208	192.168.1.195	TLSv1.2	439	Application Data
75	7.477393	40.122.162.208	192.168.1.195	TLSv1.2	88	Application Data

0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 258
[Calculated window size: 66048]
[Window size scaling factor: 256]
Checksum: 0xfab0 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
v [SEQ/ACK analysis]
[iRTT: 0.007866000 seconds]
[Bytes in flight: 180]
[Bytes sent since last PSH flag: 180]
v [Timestamps]
[Time since first frame in this TCP stream: 0.008289000 seconds]
[Time since previous frame in this TCP stream: 0.000423000 seconds]
TCP payload (180 bytes)
v Transport Layer Security
v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 175
> Handshake Protocol: Client Hello

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?

- Handshake (22)

0010 00 dc 63 a1 40 00 80 06 00 00 c0 a8 01 c3 0d 6b ...c.@.....k
0020 2a 0c e3 1b 01 bb a9 d1 c9 d8 dc 36 ec 26 50 18 *.....6.&p
0030 01 02 fa b0 00 00 16 03 03 00 af 01 00 00 ab 03f.....
0040 03 5c be 41 ed d3 5c 83 1c da ed ef 75 37 49 29 ..\A..\.....u7I
0050 44 c9 d5 f7 00 51 04 0c 66 91 d7 97 6d 02 07 a7 D...Q...f...m...
0060 ab 00 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e ...*.,+..0./...
0070 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 \$.#.(.'.....
0080 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00<..5./...
0090 00 58 00 00 00 14 00 12 00 00 0f 64 2e 64 6f 63 -X.....d.doc
00a0 73 2e 6c 69 76 65 2e 6e 65 74 00 05 00 05 01 00 s.live.n et.....
00b0 00 00 00 00 0a 00 00 00 06 00 1d 00 17 00 18 00
00c0 0b 00 02 01 00 00 0d 00 14 00 12 04 01 05 01 02
00d0 01 04 03 05 03 02 03 02 02 06 01 06 03 00 23 00#..
00e0 00 00 17 00 00 ff 01 00 01 00

Content Type (tls.record.content_type), 1 byte

Packets: 250/40 · Displayed: 11292 (45.1%) · Dropped: 0 (0.0%) Profile: Default

Address Links 6:43 PM 4/22/2019

Question 3

Wireshark Lab 8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssll

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
17	1.491840	192.168.1.195	13.107.42.12	TLSv1.2	234	Client Hello
25	1.502519	13.107.42.12	192.168.1.195	TLSv1.2	1348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
27	1.505990	192.168.1.195	13.107.42.12	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	1.521131	13.107.42.12	192.168.1.195	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
30	1.521975	192.168.1.195	13.107.42.12	TLSv1.2	1673	Application Data
31	1.522006	192.168.1.195	13.107.42.12	TLSv1.2	305	Application Data
34	1.561956	13.107.42.12	192.168.1.195	TLSv1.2	887	Application Data
35	1.561957	13.107.42.12	192.168.1.195	TLSv1.2	111	Application Data
49	5.233894	192.168.1.195	52.242.211.89	TLSv1.2	97	Application Data
50	5.298797	52.242.211.89	192.168.1.195	TLSv1.2	179	Application Data
65	7.326627	192.168.1.195	40.122.162.208	TLSv1.2	230	Client Hello
70	7.379406	40.122.162.208	192.168.1.195	TLSv1.2	1346	Server Hello, Certificate, Server Key Exchange, Server Hello Done
71	7.381808	192.168.1.195	40.122.162.208	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
72	7.426495	40.122.162.208	192.168.1.195	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
73	7.427872	192.168.1.195	40.122.162.208	TLSv1.2	1269	Application Data
74	7.476453	40.122.162.208	192.168.1.195	TLSv1.2	439	Application Data

> Frame 17: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
> Internet Protocol Version 4, Src: 192.168.1.195, Dst: 13.107.42.12
> Transmission Control Protocol, Src Port: 58139, Dst Port: 443, Seq: 1, Ack: 1, Len: 180
> Transport Layer Security
 > TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 175
 > Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 171
 Version: TLS 1.2 (0x0303)
 > Random: 5cbe41edd35c831cdaedef7537492944c9d5f70051040c6691d7976d0207a7ab
 GMT Unix Time: Apr 22, 2019 18:36:29.000000000 Eastern Daylight Time
 Random Bytes: d35c831cdaedef7537492944c9d5f70051040c6691d7976d0207a7ab
 Session ID Length: 0
 Cipher Suites Length: 42
 > Cipher Suites (21 suites)
 Compression Methods Length: 1
 > Compression Methods (1 method)
 Compression Method: null (0)

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

5cbe41edd35c831cdaedef7537492944c9d5f70051040c6691d7976d0207a7ab

0010 00 dc 63 a1 40 00 00 06 00 00 c0 a8 01 c3 0d 6b ...c:@... ..k
0020 2a 0c e3 1b 01 bb a9 d1 c9 d8 dc 36 ec 26 50 18 *.....6.&P.
0030 01 02 fa b0 00 00 16 03 03 00 af 01 00 00 ab 03
0040 03 5c be 41 ed d3 5c 83 1c da ed ef 75 37 49 29 \A..\..u(I)
0050 44 c9 d5 f7 00 51 04 0c 66 91 d7 97 6d 02 07 a7 D...Q..f...m..
0060 ab 00 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e ...*...+0./...
0070 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 \$#:(...
0080 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00<5./...
0090 00 58 00 00 00 14 00 12 00 00 0f 64 2e 64 6f 63 .X.....d.doc
00a0 73 2e 6c 69 76 65 2e 6e 65 74 00 05 00 05 01 00 s.live.n et.....
00b0 00 00 00 00 0a 00 08 00 06 00 1d 00 17 00 18 00
00c0 0b 00 02 01 00 00 0d 00 14 00 12 04 01 05 01 02
00d0 01 04 03 05 03 02 03 02 02 06 01 06 03 00 23 00#
00e0 00 00 17 00 00 ff 01 00 01 00
Random values used for deriving keys (tls.handshake.random), 32 bytes

Packets: 250/40 · Displayed: 11292 (45.1%) · Dropped: 0 (0.0%) Profile: Default

Address Links 7:07 PM 4/22/2019

Question 4

Wireshark Lab 8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
17	1.491840	192.168.1.195	13.107.42.12	TLSv1.2	234	Client Hello
25	1.502519	13.107.42.12	192.168.1.195	TLSv1.2	1348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
27	1.505990	192.168.1.195	13.107.42.12	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	1.521131	13.107.42.12	192.168.1.195	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
30	1.521975	192.168.1.195	13.107.42.12	TLSv1.2	1673	Application Data
31	1.522006	192.168.1.195	13.107.42.12	TLSv1.2	305	Application Data
34	1.561956	13.107.42.12	192.168.1.195	TLSv1.2	887	Application Data
35	1.561957	13.107.42.12	192.168.1.195	TLSv1.2	111	Application Data
49	5.233894	192.168.1.195	52.242.211.89	TLSv1.2	97	Application Data
50	5.298797	52.242.211.89	192.168.1.195	TLSv1.2	179	Application Data
65	7.326627	192.168.1.195	40.122.162.208	TLSv1.2	230	Client Hello
70	7.379406	40.122.162.208	192.168.1.195	TLSv1.2	1346	Server Hello, Certificate, Server Key Exchange, Server Hello Done
71	7.381808	192.168.1.195	40.122.162.208	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
72	7.426495	40.122.162.208	192.168.1.195	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
73	7.427872	192.168.1.195	40.122.162.208	TLSv1.2	1269	Application Data
74	7.476453	40.122.162.208	192.168.1.195	TLSv1.2	439	Application Data

▼ Cipher Suites (21 suites)

- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

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

- TLS
- RSA
- AES 256
- AES 128
- GCM
- SHA256
- SHA384
- CBC

0010 00 dc 63 a1 40 00 00 06 00 00 c0 a8 01 c3 0d 6b ...c@... ..k

0020 2a 0c e3 1b 01 bb a9 d1 c9 d8 dc 36 ec 26 50 18 *.....6.&P-

0030 01 02 fa b0 00 00 16 03 03 00 af 01 00 00 ab 03u7I)

0040 03 5c be 41 ed d3 5c 83 1c da ed ef 75 37 49 29 \A...Q...f...m...

0050 44 c9 d5 f7 00 51 04 0c 66 91 d7 97 6d 02 07 a7 D...Q...f...m...

0060 ab 00 00 2a c0 2c c0 2b c0 30 c0 2f 00 9f 00 9e ...*...+...@.../...

0070 c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 \$.#...('.....

0080 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00<\$./.....

0090 00 58 00 00 00 14 00 12 00 00 0f 64 2e 64 6f 63 .X.....d.doc

00a0 73 2e 6c 69 76 65 2e 6e 65 74 00 05 00 05 01 00 s.live.n et.....

00b0 00 00 00 00 0a 00 08 00 06 00 1d 00 17 00 18 00

00c0 0b 00 02 01 00 00 0d 00 14 00 12 04 01 05 01 02

00d0 01 04 03 05 03 02 03 02 02 06 01 06 03 00 23 00#.....

00e0 00 00 17 00 00 ff 01 00 01 00

Cipher Suite (tls.handshake.ciphersuite), 2 bytes

Packets: 250/40 · Displayed: 11292 (45.1%) · Dropped: 0 (0.0%) Profile: Default

Address Links 7:14 PM 4/22/2019

Wireshark Lab 8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
17	1.491840	192.168.1.195	13.107.42.12	TLSv1.2	234	Client Hello
25	1.502519	13.107.42.12	192.168.1.195	TLSv1.2	1348	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
27	1.505990	192.168.1.195	13.107.42.12	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	1.521131	13.107.42.12	192.168.1.195	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
30	1.521975	192.168.1.195	13.107.42.12	TLSv1.2	1673	Application Data
31	1.522006	192.168.1.195	13.107.42.12	TLSv1.2	305	Application Data
34	1.561956	13.107.42.12	192.168.1.195	TLSv1.2	887	Application Data
35	1.561957	13.107.42.12	192.168.1.195	TLSv1.2	111	Application Data
49	5.233894	192.168.1.195	52.242.211.89	TLSv1.2	97	Application Data
50	5.298797	52.242.211.89	192.168.1.195	TLSv1.2	179	Application Data
65	7.326627	192.168.1.195	40.122.162.208	TLSv1.2	230	Client Hello
70	7.379406	40.122.162.208	192.168.1.195	TLSv1.2	1346	Server Hello, Certificate, Server Key Exchange, Server Hello Done
71	7.381808	192.168.1.195	40.122.162.208	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
72	7.426495	40.122.162.208	192.168.1.195	TLSv1.2	165	Change Cipher Spec, Encrypted Handshake Message
73	7.427872	192.168.1.195	40.122.162.208	TLSv1.2	1269	Application Data
74	7.476453	40.122.162.208	192.168.1.195	TLSv1.2	439	Application Data

Length: 8589

- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 89
 - Version: TLS 1.2 (0x0303)
 - Random: 5cbe41ee6fe33de531261f1c62d2767cf3a2102bd86f719b...
 - GMT Unix Time: Apr 22, 2019 18:36:30.000000000 Eastern Daylight Time
 - Random Bytes: 6fe33de531261f1c62d2767cf3a2102bd86f719bca32c834...
 - Session ID Length: 32
 - Session ID: 6b03000093f7a59cebbcb885d9e4a00d7f544d898f373805c...
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Compression Method: null (0)
 - Extensions Length: 17
 - Extension: status_request (len=0)
 - Extension: session_ticket (len=0)
 - Extension: extended_master_secret (len=0)
 - Extension: renegotiation_info (len=1)
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 6349
 - Certificates Length: 6346
 - Certificates (6346 bytes)

0040 f3 73 80 5c 3b 7c 58 41 d5 ce 03 f3 c0 2f 00 00 s-;|XA/..

0050 11 00 05 00 00 00 23 00 00 00 17 00 00 ff 01 00#.....

0060 01 00 0b 00 18 cd 00 18 ca 00 13 0c 30 82 13 080.....

0070 30 82 10 f0 a0 03 02 01 02 02 13 2d 00 00 dc e80.....

0080 c7 b4 9d 60 1d c8 03 be 00 00 00 00 dc e8 30 0dH.....

0090 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 81 8b0.....

00a0 31 0b 30 09 06 03 55 04 06 13 02 55 31 13 30 1-0...U...US1.0

00b0 11 06 03 55 04 08 13 0a 57 61 73 68 09 6e 67 74 ...U...Washingt

00c0 6f 6e 31 10 30 0e 06 03 55 04 07 13 07 52 65 64 on1.0...U...Red

00d0 6d 6f 6e 64 31 1e 30 1c 06 03 55 04 0a 13 15 4d mond1.0...U...M

00e0 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 icrosoft Corpora

00f0 74 69 6f 6e 31 15 30 13 06 03 55 04 0b 13 0c tion1.0...U...-

Frame (1348 bytes) Reassembled TCP (8594 bytes)

Cipher Suite (tls.handshake.ciphersuite), 2 bytes

Packets: 250/40 · Displayed: 11292 (45.1%) · Dropped: 0 (0.0%) Profile: Default

Address Links 7:23 PM 4/22/2019

Question 1

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?

-TLS
-ECDHE
-RSA
-AES 128
-GCM
-SHA 256

C:\Users\dgogo\OneDrive\Masters\Computer Networking Course\Presentation 2\Project Files\Wireshark Lab 8.pcapng 25040 total packets, 20 shown

No.	Time	Source	Destination	Protocol	Length	Info
13662	42.778948	104.119.136.209	192.168.1.195	OCSP	967	Response

Frame 13662: 967 bytes on wire (7736 bits), 967 bytes captured (7736 bits) on interface 0
Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: Foxconn_d1:d3:8c (08:01:6c:d1:d3:8c)
Internet Protocol Version 4, Src: 104.119.136.209, Dst: 192.168.1.195
Transmission Control Protocol, Src Port: 80, Dst Port: 58328, Seq: 1461, Ack: 230, Len: 913
[2 Reassembled TCP Segments (2373 bytes): #13661(1460), #13662(913)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Content-Type: application/ocsp-response\r\n
Content-Transfer-Encoding: Binary\r\n
Content-Length: 1991\r\n
Last-Modified: Mon, 22 Apr 2019 18:12:47 GMT\r\n
ETag: "AF09CB2DD88BD9A8A701A538317C06E76B76F521"\r\n
Cache-Control: public, no-transform, must-revalidate, max-age=1797\r\n
Expires: Mon, 22 Apr 2019 23:07:08 GMT\r\n
Date: Mon, 22 Apr 2019 22:37:11 GMT\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.018729000 seconds]
[Request in frame: 13657]
[Request URI: http://ocsp.entrust.net/
ME0wSzBjMEcwRTAJBgUrDgMCGGUABBTXNCzdvBhHecWjg701jBw0InyWQanImetAe733n021R1GyNnSASZqsCDGGH59IAAAAUdNmpg%3D%3D]
File Data: 1991 bytes
Online Certificate Status Protocol