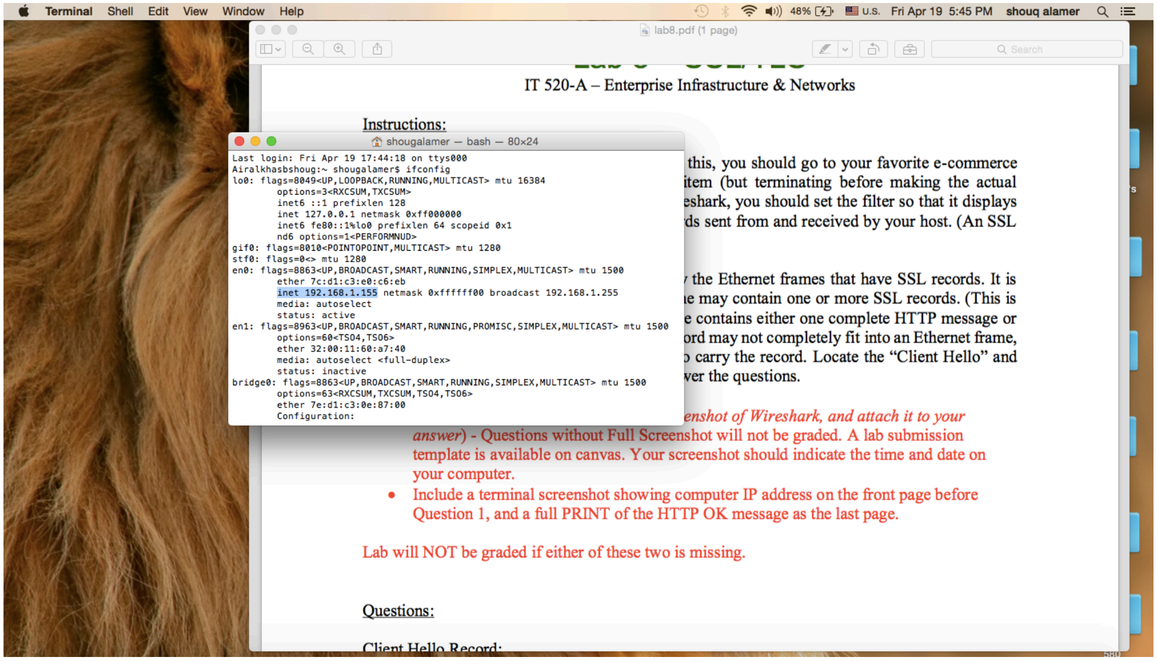


IT 520-A – Enterprise Infrastructure & Networks

Instructions:

```
Last login: Fri Apr 19 17:44:18 on ttys000
Airalkhasbshoug:~ shougalamer$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 7c:d1:c3:e0:c6:eb
        inet 192.168.1.155 netmask 0xffffff00 broadcast 192.168.1.255
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=60<TSO4,TSO6>
        ether 32:00:11:60:a7:40
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 7e:d1:c3:0e:87:00
        Configuration:
```

this, you should go to your favorite e-commerce
item (but terminating before making the actual
eshark, you should set the filter so that it displays
ds sent from and received by your host. (An SSL

the Ethernet frames that have SSL records. It is
e may contain one or more SSL records. (This is
e contains either one complete HTTP message or
ord may not completely fit into an Ethernet frame,
carry the record. Locate the “Client Hello” and
ver the questions.

enshot 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.

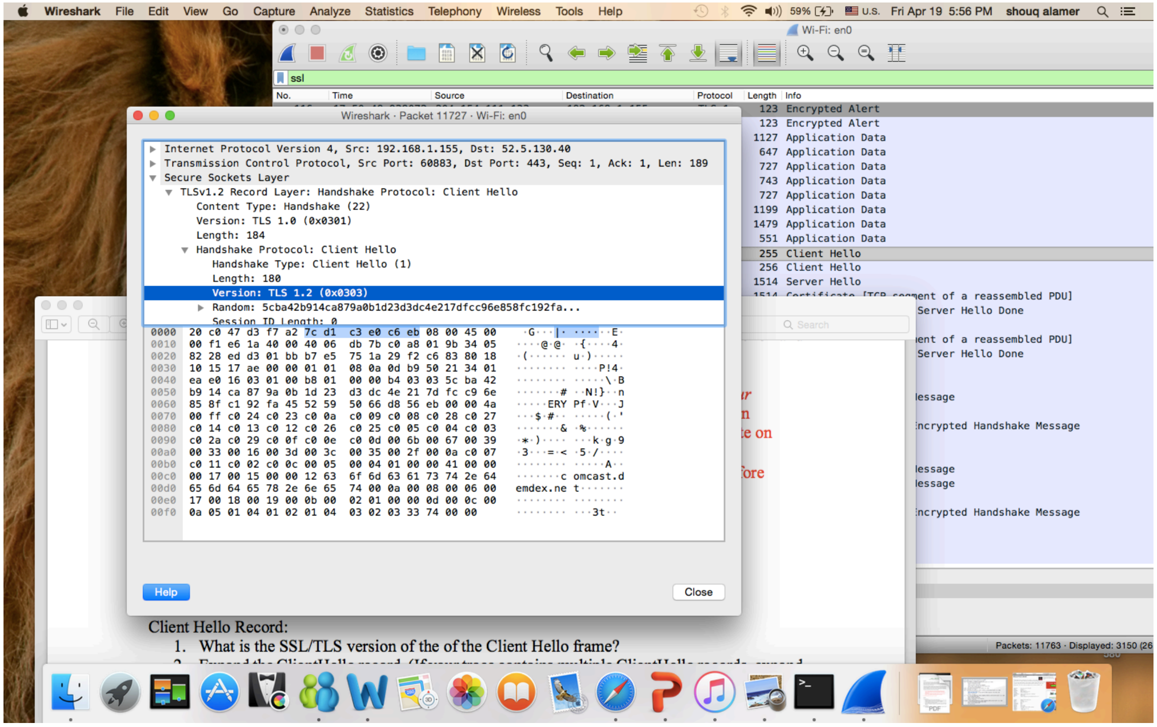
Lab will NOT be graded if either of these two is missing.

Questions:

Client Hello Record:

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

1.2



Filter: ssl

No.	Time	Source	Destination	Protocol	Length	Info
					123	Encrypted Alert
					123	Encrypted Alert
					1127	Application Data
					647	Application Data
					727	Application Data
					743	Application Data
					727	Application Data
					1199	Application Data
					1479	Application Data
					551	Application Data
					255	Client Hello
					256	Client Hello
					1514	Server Hello
					1514	Certificate [TCP segment of a reassembled PDU]
						Server Hello Done
						ent of a reassembled PDU]
						Server Hello Done
						lessage
						ncrypted Handshake Message
						lessage
						lessage
						ncrypted Handshake Message

Wireshark · Packet 11727 · Wi-Fi: en0

```
▶ Internet Protocol Version 4, Src: 192.168.1.155, Dst: 52.5.130.40
▶ Transmission Control Protocol, Src Port: 60883, Dst Port: 443, Seq: 1, Ack: 1, Len: 189
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 184
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 180
        Version: TLS 1.2 (0x0303)
      ▶ Random: 5cba42b914ca879a0b1d23d3dc4e217dfcc96e858fc192fa...
        Session ID Length: 0
```

```
0000  20 c0 47 d3 f7 a2 7c d1  c3 e0 c6 eb 08 00 45 00   ·G···|·  ······E·
0010  00 f1 e6 1a 40 00 40 06  db 7b c0 a8 01 9b 34 05   ····@·@·  ·{····4·
0020  82 28 ed d3 01 bb b7 e5  75 1a 29 f2 c6 83 80 18   ·(······  u·)·····
0030  10 15 17 ae 00 00 01 01  08 0a 0d b9 50 21 34 01   ········  ····P!4·
0040  ea e0 16 03 01 00 b8 01  00 00 b4 03 03 5c ba 42   ········  ·····\·B
0050  b9 14 ca 87 9a 0b 1d 23  d3 dc 4e 21 7d fc c9 6e   ·······#  ··N!}··n
0060  85 8f c1 92 fa 45 52 59  50 66 d8 56 eb 00 00 4a   ·····ERY  Pf·V···J
0070  00 ff c0 24 c0 23 c0 0a  c0 09 c0 08 c0 28 c0 27   ···$·#··  ·····(·'
0080  c0 14 c0 13 c0 12 c0 26  c0 25 c0 05 c0 04 c0 03   ·······&  ·%······
0090  c0 2a c0 29 c0 0f c0 0e  c0 0d 00 6b 00 67 00 39   ·*·)····  ···k·g·9
00a0  00 33 00 16 00 3d 00 3c  00 35 00 2f 00 0a c0 07   ·3···=·<  ·5·/····
00b0  c0 11 c0 02 c0 0c 00 05  00 04 01 00 00 41 00 00   ········  ·····A··
00c0  00 17 00 15 00 00 12 63  6f 6d 63 61 73 74 2e 64   ·······c  omcast.d
00d0  65 6d 64 65 78 2e 6e 65  74 00 0a 00 08 00 06 00   emdex.ne  t·······
00e0  17 00 18 00 19 00 0b 00  02 01 00 00 0d 00 0c 00   ········  ········
00f0  0a 05 01 04 01 02 01 04  03 02 03 33 74 00 00      ········  ···3t··
```

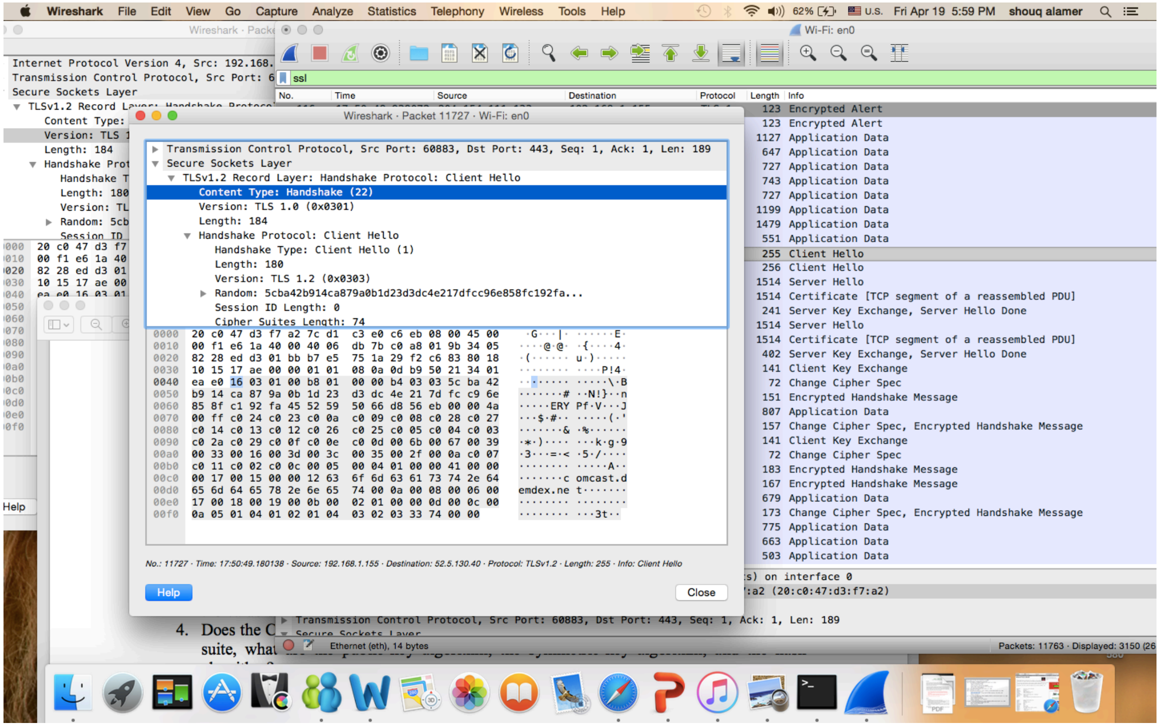
Client Hello Record:

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

Packets: 11763 · Displayed: 3150 (26

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?

Handshake (22)


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
62% U.S. Fri Apr 19 5:59 PM shouq alamer
Wi-Fi: en0
ssl
No. Time Source Destination Protocol Length Info
Wireshark · Packet 11727 · Wi-Fi: en0
Help
Close
Packets: 11763 · Displayed: 3150 (26

```
▶ Transmission Control Protocol, Src Port: 60883, Dst Port: 443, Seq: 1, Ack: 1, Len: 189
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 184
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 180
        Version: TLS 1.2 (0x0303)
      ▶ Random: 5cba42b914ca879a0b1d23d3dc4e217dfcc96e858fc192fa...
        Session ID Length: 0
        Cipher Suites Length: 74
```

```
0000  20 c0 47 d3 f7 a2 7c d1  c3 e0 c6 eb 08 00 45 00   ·G···|· ······E·
0010  00 f1 e6 1a 40 00 40 06  db 7b c0 a8 01 9b 34 05   ····@·@· ·{····4·
0020  82 28 ed d3 01 bb b7 e5  75 1a 29 f2 c6 83 80 18   ·(······ u·)·····
0030  10 15 17 ae 00 00 01 01  08 0a 0d b9 50 21 34 01   ········ ····P!4·
0040  ea e0 16 03 01 00 b8 01  00 00 b4 03 03 5c ba 42   ········ ·····\·B
0050  b9 14 ca 87 9a 0b 1d 23  d3 dc 4e 21 7d fc c9 6e   ·······# ··N!}··n
0060  85 8f c1 92 fa 45 52 59  50 66 d8 56 eb 00 00 4a   ·····ERY Pf·V···J
0070  00 ff c0 24 c0 23 c0 0a  c0 09 c0 08 c0 28 c0 27   ···$·#·· ·····(·'
0080  c0 14 c0 13 c0 12 c0 26  c0 25 c0 05 c0 04 c0 03   ·······& ·%······
0090  c0 2a c0 29 c0 0f c0 0e  c0 0d 00 6b 00 67 00 39   ·*·)···· ···k·g·9
00a0  00 33 00 16 00 3d 00 3c  00 35 00 2f 00 0a c0 07   ·3···=·< ·5·/····
00b0  c0 11 c0 02 c0 0c 00 05  00 04 01 00 00 41 00 00   ········ ·····A··
00c0  00 17 00 15 00 00 12 63  6f 6d 63 61 73 74 2e 64   ·······c omcast.d
00d0  65 6d 64 65 78 2e 6e 65  74 00 0a 00 08 00 06 00   emdex.ne t·······
00e0  17 00 18 00 19 00 0b 00  02 01 00 00 0d 00 0c 00   ········ ········
00f0  0a 05 01 04 01 02 01 04  03 02 03 33 74 00 00      ········ ···3t··
```

No.: 11727 · Time: 17:50:49.180138 · Source: 192.168.1.155 · Destination: 52.5.130.40 · Protocol: TLSv1.2 · Length: 255 · Info: Client Hello

```
 123 Encrypted Alert
 123 Encrypted Alert
1127 Application Data
 647 Application Data
 727 Application Data
 743 Application Data
 727 Application Data
1199 Application Data
1479 Application Data
 551 Application Data
 255 Client Hello
 256 Client Hello
1514 Server Hello
1514 Certificate [TCP segment of a reassembled PDU]
 241 Server Key Exchange, Server Hello Done
1514 Server Hello
1514 Certificate [TCP segment of a reassembled PDU]
 402 Server Key Exchange, Server Hello Done
 141 Client Key Exchange
  72 Change Cipher Spec
 151 Encrypted Handshake Message
 807 Application Data
 157 Change Cipher Spec, Encrypted Handshake Message
 141 Client Key Exchange
  72 Change Cipher Spec
 183 Encrypted Handshake Message
 167 Encrypted Handshake Message
 679 Application Data
 173 Change Cipher Spec, Encrypted Handshake Message
 775 Application Data
 663 Application Data
 503 Application Data
```

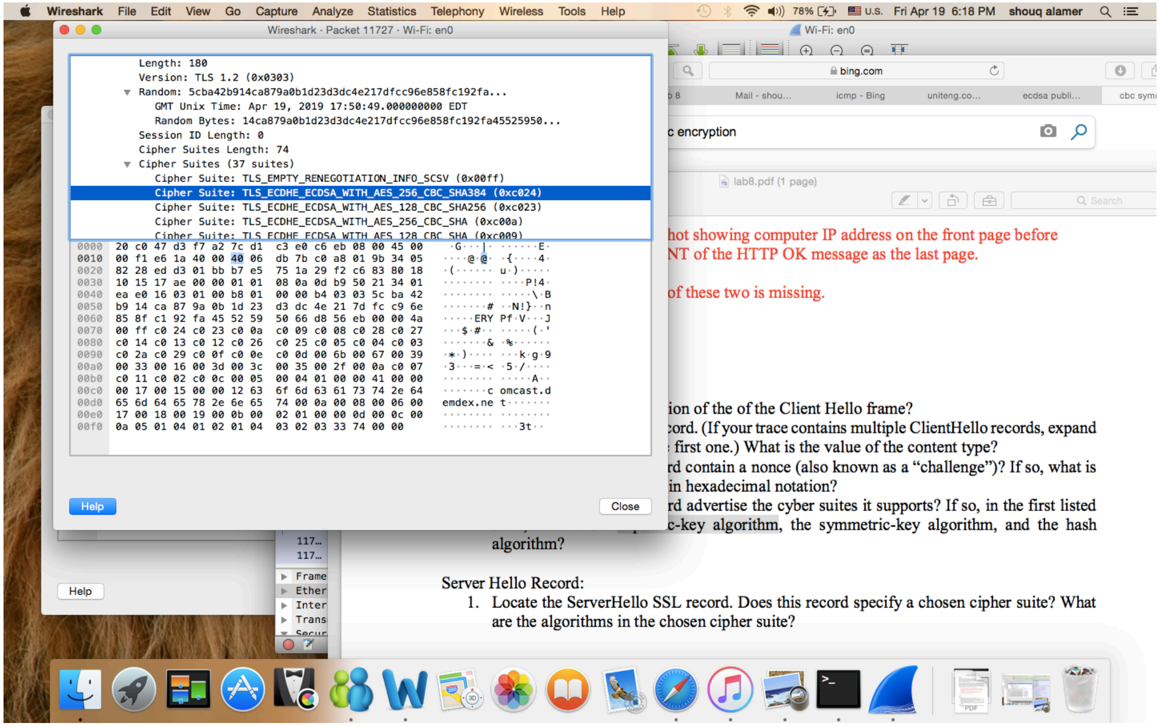
```
Internet Protocol Version 4, Src: 192.168.
Transmission Control Protocol, Src Port: 60883, Dst Port: 443, Seq: 1, Ack: 1, Len: 189
Secure Sockets Layer
```

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?

NO

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?

ECDSA public key algorithm
CBC symmetric key algorithm
SHA384 hash algorithm


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
78% U.S. Fri Apr 19 6:18 PM shouq alamer
Wireshark · Packet 11727 · Wi-Fi: en0
Wi-Fi: en0
bing.com
Mail - shou... icmp - Bing uniteng.co... ecdsa publi... cbc sym
c encryption
lab8.pdf (1 page)
Search
Help
Close
Help
117...
117...
Frame
Ether
Inter
Trans
Secur

```
        Length: 180
        Version: TLS 1.2 (0x0303)
      ▼ Random: 5cba42b914ca879a0b1d23d3dc4e217dfcc96e858fc192fa...
          GMT Unix Time: Apr 19, 2019 17:50:49.000000000 EDT
          Random Bytes: 14ca879a0b1d23d3dc4e217dfcc96e858fc192fa45525950...
        Session ID Length: 0
        Cipher Suites Length: 74
      ▼ Cipher Suites (37 suites)
          Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
          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_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
```

```
0000  20 c0 47 d3 f7 a2 7c d1  c3 e0 c6 eb 08 00 45 00    ·G···|· ······E·
0010  00 f1 e6 1a 40 00 40 06  db 7b c0 a8 01 9b 34 05   ····@·@· ·{····4·
0020  82 28 ed d3 01 bb b7 e5  75 1a 29 f2 c6 83 80 18   ·(······ u·)·····
0030  10 15 17 ae 00 00 01 01  08 0a 0d b9 50 21 34 01   ········ ····P!4·
0040  ea e0 16 03 01 00 b8 01  00 00 b4 03 03 5c ba 42   ········ ·····\·B
0050  b9 14 ca 87 9a 0b 1d 23  d3 dc 4e 21 7d fc c9 6e   ·······# ··N!}··n
0060  85 8f c1 92 fa 45 52 59  50 66 d8 56 eb 00 00 4a   ·····ERY Pf·V···J
0070  00 ff c0 24 c0 23 c0 0a  c0 09 c0 08 c0 28 c0 27   ···$·#·· ·····(·'
0080  c0 14 c0 13 c0 12 c0 26  c0 25 c0 05 c0 04 c0 03   ·······& ·%······
0090  c0 2a c0 29 c0 0f c0 0e  c0 0d 00 6b 00 67 00 39   ·*·)···· ···k·g·9
00a0  00 33 00 16 00 3d 00 3c  00 35 00 2f 00 0a c0 07   ·3···=·< ·5·/····
00b0  c0 11 c0 02 c0 0c 00 05  00 04 01 00 00 41 00 00   ········ ·····A··
00c0  00 17 00 15 00 00 12 63  6f 6d 63 61 73 74 2e 64   ·······c omcast.d
00d0  65 6d 64 65 78 2e 6e 65  74 00 0a 00 08 00 06 00   emdex.ne t·······
00e0  17 00 18 00 19 00 0b 00  02 01 00 00 0d 00 0c 00   ········ ········
00f0  0a 05 01 04 01 02 01 04  03 02 03 33 74 00 00      ········ ···3t··
```

hot showing computer IP address on the front page before
NT of the HTTP OK message as the last page.

of these two is missing.

ion of the of the Client Hello frame?
cord. (If your trace contains multiple ClientHello records, expand
first one.) What is the value of the content type?
rd contain a nonce (also known as a "challenge")? If so, what is
in hexadecimal notation?
rd advertise the cyber suites it supports? If so, in the first listed
c-key algorithm, the symmetric-key algorithm, and the 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?

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

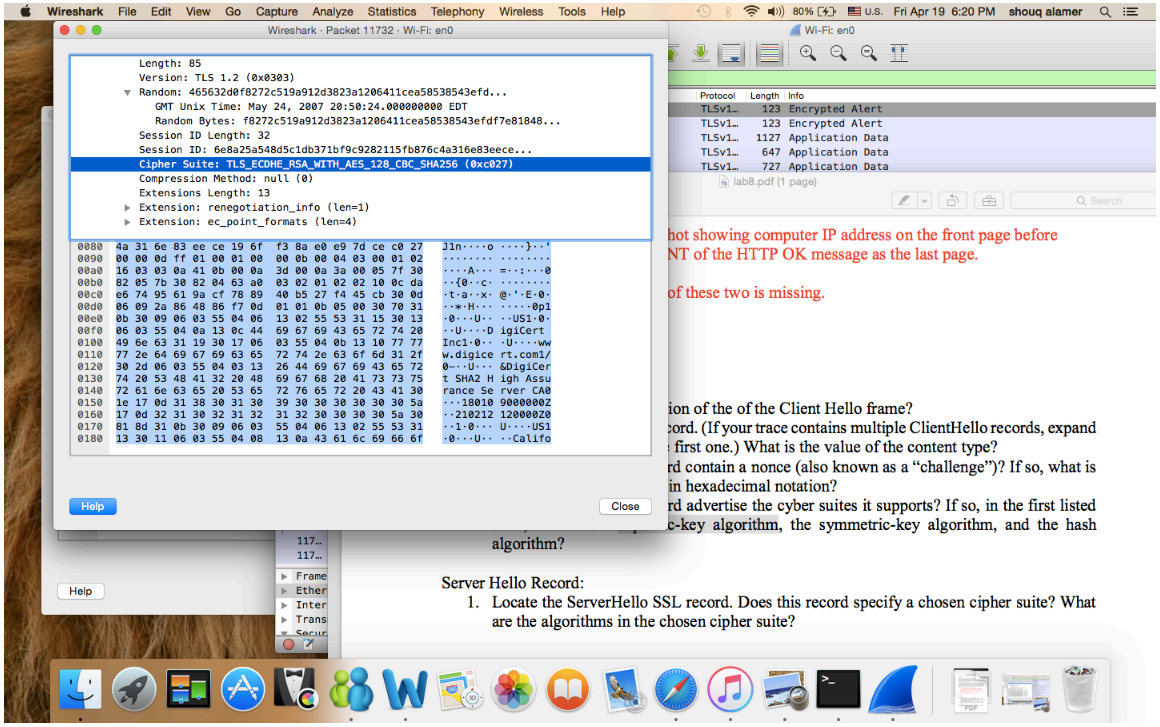
YES

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

RSA public key algorithm

CBC symmetric key algorithm

SHA256 hash algorithm


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Fri Apr 19 6:20 PM shouq alamer
Wireshark · Packet 11732 · Wi-Fi: en0
Wi-Fi: en0
Help
Close
lab8.pdf (1 page)
Search

```
        Length: 85
        Version: TLS 1.2 (0x0303)
      ▼ Random: 465632d0f8272c519a912d3823a1206411cea58538543efd...
          GMT Unix Time: May 24, 2007 20:50:24.000000000 EDT
          Random Bytes: f8272c519a912d3823a1206411cea58538543efdf7e81848...
        Session ID Length: 32
        Session ID: 6e8a25a548d5c1db371bf9c9282115fb876c4a316e83eece...
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
        Compression Method: null (0)
        Extensions Length: 13
      ▶ Extension: renegotiation_info (len=1)
      ▶ Extension: ec_point_formats (len=4)
```

```
0080  4a 31 6e 83 ee ce 19 6f  f3 8a e0 e9 7d ce c0 27   J1n····o ····}··'
0090  00 00 0d ff 01 00 01 00  00 0b 00 04 03 00 01 02   ········ ········
00a0  16 03 03 0a 41 0b 00 0a  3d 00 0a 3a 00 05 7f 30   ····A··· =··:···0
00b0  82 05 7b 30 82 04 63 a0  03 02 01 02 02 10 0c da   ··{0··c· ········
00c0  e6 74 95 61 9a cf 78 89  40 b5 27 f4 45 cb 30 0d   ·t·a··x· @·'·E·0·
00d0  06 09 2a 86 48 86 f7 0d  01 01 0b 05 00 30 70 31   ··*·H··· ·····0p1
00e0  0b 30 09 06 03 55 04 06  13 02 55 53 31 15 30 13   ·0···U·· ··US1·0·
00f0  06 03 55 04 0a 13 0c 44  69 67 69 43 65 72 74 20   ··U····D igiCert
0100  49 6e 63 31 19 30 17 06  03 55 04 0b 13 10 77 77   Inc1·0·· ·U····ww
0110  77 2e 64 69 67 69 63 65  72 74 2e 63 6f 6d 31 2f   w.digice rt.com1/
0120  30 2d 06 03 55 04 03 13  26 44 69 67 69 43 65 72   0-··U··· &DigiCer
0130  74 20 53 48 41 32 20 48  69 67 68 20 41 73 73 75   t SHA2 H igh Assu
0140  72 61 6e 63 65 20 53 65  72 76 65 72 20 43 41 30   rance Se rver CA0
0150  1e 17 0d 31 38 30 31 30  39 30 30 30 30 30 30 5a   ···18010 9000000Z
0160  17 0d 32 31 30 32 31 32  31 32 30 30 30 30 5a 30   ··210212 120000Z0
0170  81 8d 31 0b 30 09 06 03  55 04 06 13 02 55 53 31   ··1·0··· U····US1
0180  13 30 11 06 03 55 04 08  13 0a 43 61 6c 69 66 6f   ·0···U·· ··Califo
```

```
Protocol  Length  Info
TLSv1…       123  Encrypted Alert
TLSv1…       123  Encrypted Alert
TLSv1…      1127  Application Data
TLSv1…       647  Application Data
TLSv1…       727  Application Data
```

hot showing computer IP address on the front page before NT of the HTTP OK message as the last page.

of these two is missing.

ion of the of the Client Hello frame?
cord. (If your trace contains multiple ClientHello records, expand first one.) What is the value of the content type?
rd contain a nonce (also known as a "challenge")? If so, what is in hexadecimal notation?
rd advertise the cyber suites it supports? If so, in the first listed c-key algorithm, the symmetric-key algorithm, and the 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?

```
No.     Time               Source                Destination           Protocol Length Info
   9835 17:50:46.460242    192.138.218.207       192.168.1.155         HTTP/XML 1134   HTTP/1.1
200 OK
Frame 9835: 1134 bytes on wire (9072 bits), 1134 bytes captured (9072 bits) on interface 0
Ethernet II, Src: Verizon_d3:f7:a2 (20:c0:47:d3:f7:a2), Dst: Apple_e0:c6:eb (7c:d1:c3:e0:c6:eb)
Internet Protocol Version 4, Src: 192.138.218.207, Dst: 192.168.1.155
Transmission Control Protocol, Src Port: 80, Dst Port: 60865, Seq: 1369, Ack: 736, Len: 1068
[2 Reassembled TCP Segments (2436 bytes): #9834(1368), #9835(1068)]
Hypertext Transfer Protocol
eXtensible Markup Language
```