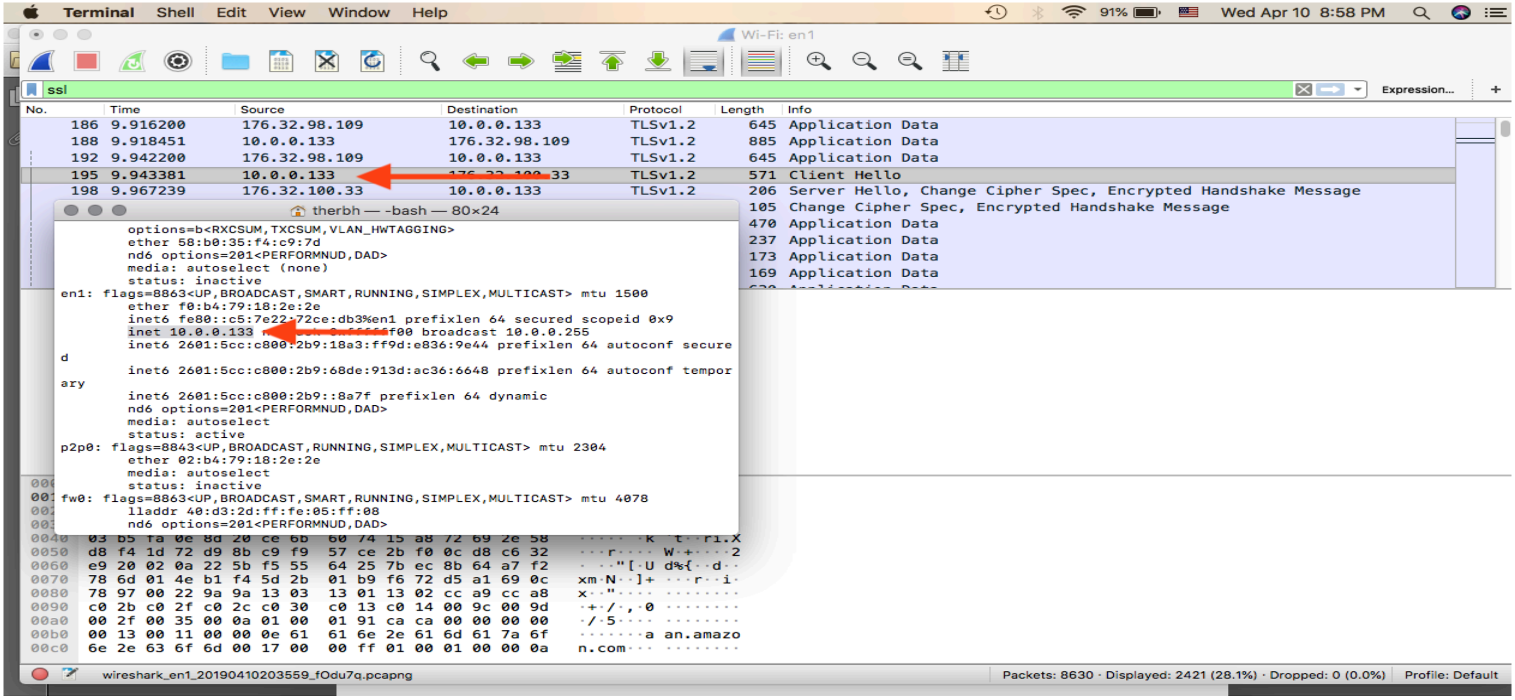
Shahad bin himd
Lab8

MY IP
10.0.0.133



Filter: ssl

```
No.   Time      Source          Destination     Protocol Length Info
  186 9.916200  176.32.98.109   10.0.0.133      TLSv1.2  645 Application Data
  188 9.918451  10.0.0.133      176.32.98.109   TLSv1.2  885 Application Data
  192 9.942200  176.32.98.109   10.0.0.133      TLSv1.2  645 Application Data
  195 9.943381  10.0.0.133      176.32.100.33   TLSv1.2  571 Client Hello
  198 9.967239  176.32.100.33   10.0.0.133      TLSv1.2  206 Server Hello, Change Cipher Spec, Encrypted Handshake Message
                                                         105 Change Cipher Spec, Encrypted Handshake Message
                                                         470 Application Data
                                                         237 Application Data
                                                         173 Application Data
                                                         169 Application Data
```

therbh — -bash — 80×24

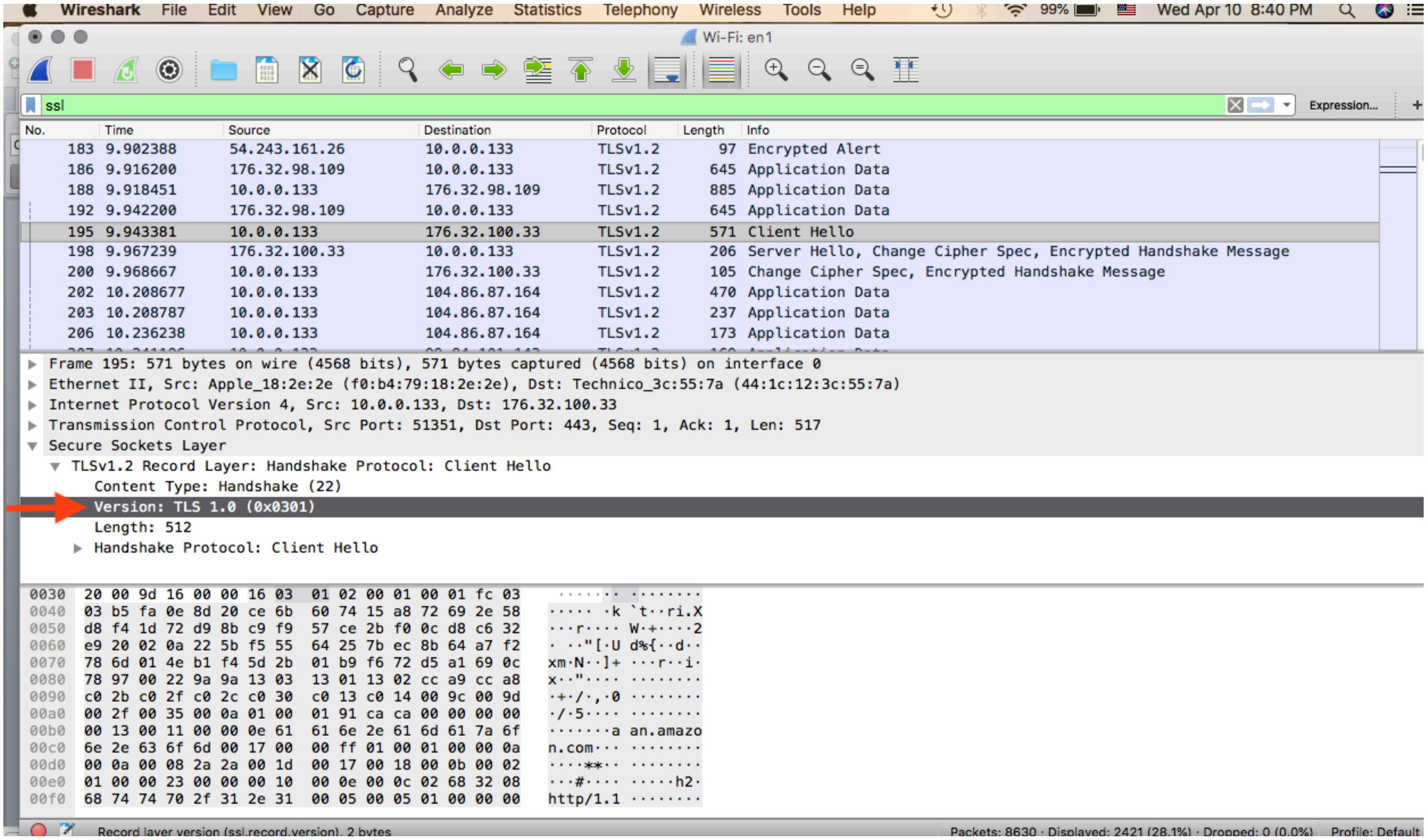
```
        options=b<RXCSUM,TXCSUM,VLAN_HWTAGGING>
        ether 58:b0:35:f4:c9:7d
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (none)
        status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether f0:b4:79:18:2e:2e
        inet6 fe80::c5:7e22:72ce:db3%en1 prefixlen 64 secured scopeid 0x9
        inet 10.0.0.133 netmask 0xffffff00 broadcast 10.0.0.255
        inet6 2601:5cc:c800:2b9:18a3:ff9d:e836:9e44 prefixlen 64 autoconf secure
d
        inet6 2601:5cc:c800:2b9:68de:913d:ac36:6648 prefixlen 64 autoconf tempor
ary
        inet6 2601:5cc:c800:2b9::8a7f prefixlen 64 dynamic
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 02:b4:79:18:2e:2e
        media: autoselect
        status: inactive
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr 40:d3:2d:ff:fe:05:ff:08
        nd6 options=201<PERFORMNUD,DAD>
```

```
0040  03 b5 fa 0e 8d 20 ce 6b  60 74 15 a8 72 69 2e 58   ······k `t··ri.X
0050  d8 f4 1d 72 d9 8b c9 f9  57 ce 2b f0 0c d8 c6 32   ···r···· W·+····2
0060  e9 20 02 0a 22 5b f5 55  64 25 7b ec 8b 64 a7 f2   · ··"[·U d%{··d··
0070  78 6d 01 4e b1 f4 5d 2b  01 b9 f6 72 d5 a1 69 0c   xm·N··]+ ···r··i·
0080  78 97 00 22 9a 9a 13 03  13 01 13 02 cc a9 cc a8   x··"···· ········
0090  c0 2b c0 2f c0 2c c0 30  c0 13 c0 14 00 9c 00 9d   ·+·/·,·0 ········
00a0  00 2f 00 35 00 0a 01 00  01 91 ca ca 00 00 00 00   ·/·5···· ········
00b0  00 13 00 11 00 00 0e 61  61 6e 2e 61 6d 61 7a 6f   ·······a an.amazo
00c0  6e 2e 63 6f 6d 00 17 00  00 ff 01 00 01 00 00 0a   n.com··· ········
```

wireshark_en1_20190410203559_fOdu7q.pcapng   Packets: 8630 · Displayed: 2421 (28.1%) · Dropped: 0 (0.0%)   Profile: Default

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

TLS 1.0



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
99% Wed Apr 10 8:40 PM
Wi-Fi: en1
Expression…

Filter: ssl

```
No.   Time       Source          Destination     Protocol Length Info
  183 9.902388   54.243.161.26   10.0.0.133      TLSv1.2   97 Encrypted Alert
  186 9.916200   176.32.98.109   10.0.0.133      TLSv1.2  645 Application Data
  188 9.918451   10.0.0.133      176.32.98.109   TLSv1.2  885 Application Data
  192 9.942200   176.32.98.109   10.0.0.133      TLSv1.2  645 Application Data
  195 9.943381   10.0.0.133      176.32.100.33   TLSv1.2  571 Client Hello
  198 9.967239   176.32.100.33   10.0.0.133      TLSv1.2  206 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  200 9.968667   10.0.0.133      176.32.100.33   TLSv1.2  105 Change Cipher Spec, Encrypted Handshake Message
  202 10.208677  10.0.0.133      104.86.87.164   TLSv1.2  470 Application Data
  203 10.208787  10.0.0.133      104.86.87.164   TLSv1.2  237 Application Data
  206 10.236238  10.0.0.133      104.86.87.164   TLSv1.2  173 Application Data
```

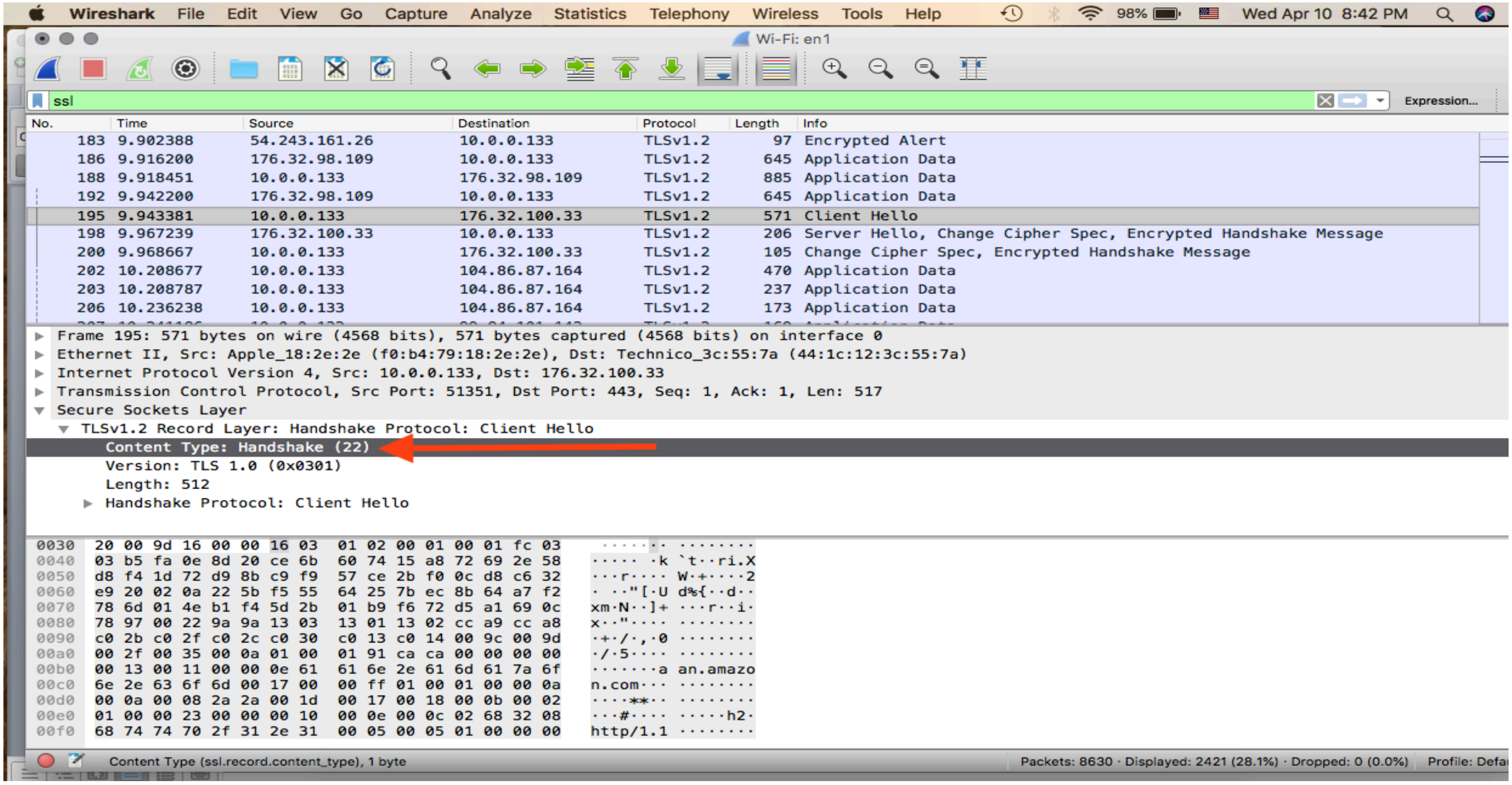
```
▶ Frame 195: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
▶ Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)
▶ Internet Protocol Version 4, Src: 10.0.0.133, Dst: 176.32.100.33
▶ Transmission Control Protocol, Src Port: 51351, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    ▶ Handshake Protocol: Client Hello
```

```
0030  20 00 9d 16 00 00 16 03  01 02 00 01 00 01 fc 03    ······· ········
0040  03 b5 fa 0e 8d 20 ce 6b  60 74 15 a8 72 69 2e 58   ····· ·k `t··ri.X
0050  d8 f4 1d 72 d9 8b c9 f9  57 ce 2b f0 0c d8 c6 32   ···r···· W·+····2
0060  e9 20 02 0a 22 5b f5 55  64 25 7b ec 8b 64 a7 f2   · ··"[·U d%{··d··
0070  78 6d 01 4e b1 f4 5d 2b  01 b9 f6 72 d5 a1 69 0c   xm·N··]+ ···r··i·
0080  78 97 00 22 9a 9a 13 03  13 01 13 02 cc a9 cc a8   x··"···· ········
0090  c0 2b c0 2f c0 2c c0 30  c0 13 c0 14 00 9c 00 9d   ·+·/·,·0 ········
00a0  00 2f 00 35 00 0a 01 00  01 91 ca ca 00 00 00 00   ·/·5···· ········
00b0  00 13 00 11 00 00 0e 61  61 6e 2e 61 6d 61 7a 6f   ·······a an.amazo
00c0  6e 2e 63 6f 6d 00 17 00  00 ff 01 00 01 00 00 0a   n.com··· ········
00d0  00 0a 00 08 2a 2a 00 1d  00 17 00 18 00 0b 00 02   ····**·· ········
00e0  01 00 00 23 00 00 00 10  00 0e 00 0c 02 68 32 08   ···#···· ·····h2·
00f0  68 74 74 70 2f 31 2e 31  00 05 00 05 01 00 00 00   http/1.1 ········
```

Record layer version (ssl.record.version), 2 bytes   Packets: 8630 · Displayed: 2421 (28.1%) · Dropped: 0 (0.0%)   Profile: Default

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
98%
Wed Apr 10 8:42 PM
Wi-Fi: en1
ssl
Expression…

```
No.   Time       Source          Destination     Protocol  Length  Info
  183 9.902388   54.243.161.26   10.0.0.133      TLSv1.2     97  Encrypted Alert
  186 9.916200   176.32.98.109   10.0.0.133      TLSv1.2    645  Application Data
  188 9.918451   10.0.0.133      176.32.98.109   TLSv1.2    885  Application Data
  192 9.942200   176.32.98.109   10.0.0.133      TLSv1.2    645  Application Data
  195 9.943381   10.0.0.133      176.32.100.33   TLSv1.2    571  Client Hello
  198 9.967239   176.32.100.33   10.0.0.133      TLSv1.2    206  Server Hello, Change Cipher Spec, Encrypted Handshake Message
  200 9.968667   10.0.0.133      176.32.100.33   TLSv1.2    105  Change Cipher Spec, Encrypted Handshake Message
  202 10.208677  10.0.0.133      104.86.87.164   TLSv1.2    470  Application Data
  203 10.208787  10.0.0.133      104.86.87.164   TLSv1.2    237  Application Data
  206 10.236238  10.0.0.133      104.86.87.164   TLSv1.2    173  Application Data
```

```
▶ Frame 195: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
▶ Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)
▶ Internet Protocol Version 4, Src: 10.0.0.133, Dst: 176.32.100.33
▶ Transmission Control Protocol, Src Port: 51351, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▼ Secure Sockets Layer
   ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
         Content Type: Handshake (22)
         Version: TLS 1.0 (0x0301)
         Length: 512
      ▶ Handshake Protocol: Client Hello
```

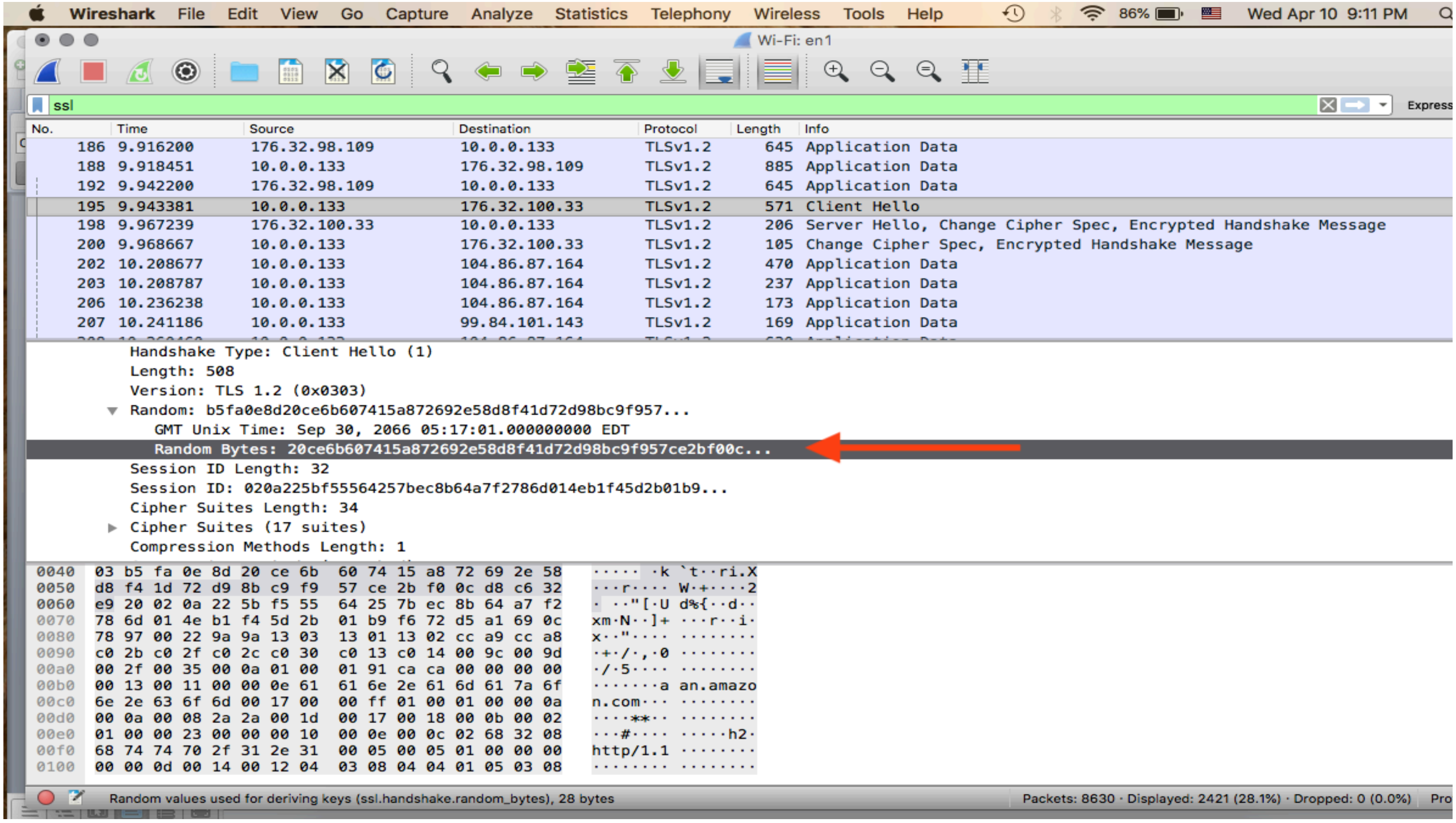
```
0030  20 00 9d 16 00 00 16 03  01 02 00 01 00 01 fc 03    ······ ·· ········
0040  03 b5 fa 0e 8d 20 ce 6b  60 74 15 a8 72 69 2e 58   ·····  ·k `t··ri.X
0050  d8 f4 1d 72 d9 8b c9 f9  57 ce 2b f0 0c d8 c6 32   ···r···· W·+····2
0060  e9 20 02 0a 22 5b f5 55  64 25 7b ec 8b 64 a7 f2   ·  ··"[·U d%{··d··
0070  78 6d 01 4e b1 f4 5d 2b  01 b9 f6 72 d5 a1 69 0c   xm·N··]+ ···r··i·
0080  78 97 00 22 9a 9a 13 03  13 01 13 02 cc a9 cc a8   x··"···· ········
0090  c0 2b c0 2f c0 2c c0 30  c0 13 c0 14 00 9c 00 9d   ·+·/·,·0 ········
00a0  00 2f 00 35 00 0a 01 00  01 91 ca ca 00 00 00 00   ·/·5···· ········
00b0  00 13 00 11 00 00 0e 61  61 6e 2e 61 6d 61 7a 6f   ·······a an.amazo
00c0  6e 2e 63 6f 6d 00 17 00  00 ff 01 00 01 00 00 0a   n.com··· ········
00d0  00 0a 00 08 2a 2a 00 1d  00 17 00 18 00 0b 00 02   ····**·· ········
00e0  01 00 00 23 00 00 00 10  00 0e 00 0c 02 68 32 08   ···#···· ·····h2·
00f0  68 74 74 70 2f 31 2e 31  00 05 00 05 01 00 00 00   http/1.1 ········
```

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

Packets: 8630 · Displayed: 2421 (28.1%) · Dropped: 0 (0.0%)   Profile: Defa

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?

Yes it does 20ce6b607…………………………


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
86%
Wed Apr 10 9:11 PM
Wi-Fi: en1
ssl
Express

```
No.   Time       Source          Destination     Protocol  Length  Info
  186 9.916200   176.32.98.109   10.0.0.133      TLSv1.2    645  Application Data
  188 9.918451   10.0.0.133      176.32.98.109   TLSv1.2    885  Application Data
  192 9.942200   176.32.98.109   10.0.0.133      TLSv1.2    645  Application Data
  195 9.943381   10.0.0.133      176.32.100.33   TLSv1.2    571  Client Hello
  198 9.967239   176.32.100.33   10.0.0.133      TLSv1.2    206  Server Hello, Change Cipher Spec, Encrypted Handshake Message
  200 9.968667   10.0.0.133      176.32.100.33   TLSv1.2    105  Change Cipher Spec, Encrypted Handshake Message
  202 10.208677  10.0.0.133      104.86.87.164   TLSv1.2    470  Application Data
  203 10.208787  10.0.0.133      104.86.87.164   TLSv1.2    237  Application Data
  206 10.236238  10.0.0.133      104.86.87.164   TLSv1.2    173  Application Data
  207 10.241186  10.0.0.133      99.84.101.143   TLSv1.2    169  Application Data
```

```
         Handshake Type: Client Hello (1)
         Length: 508
         Version: TLS 1.2 (0x0303)
       ▼ Random: b5fa0e8d20ce6b607415a872692e58d8f41d72d98bc9f957...
            GMT Unix Time: Sep 30, 2066 05:17:01.000000000 EDT
            Random Bytes: 20ce6b607415a872692e58d8f41d72d98bc9f957ce2bf00c...
         Session ID Length: 32
         Session ID: 020a225bf55564257bec8b64a7f2786d014eb1f45d2b01b9...
         Cipher Suites Length: 34
       ▶ Cipher Suites (17 suites)
         Compression Methods Length: 1
```

```
0040  03 b5 fa 0e 8d 20 ce 6b  60 74 15 a8 72 69 2e 58   ·····  ·k `t··ri.X
0050  d8 f4 1d 72 d9 8b c9 f9  57 ce 2b f0 0c d8 c6 32   ···r···· W·+····2
0060  e9 20 02 0a 22 5b f5 55  64 25 7b ec 8b 64 a7 f2   ·  ··"[·U d%{··d··
0070  78 6d 01 4e b1 f4 5d 2b  01 b9 f6 72 d5 a1 69 0c   xm·N··]+ ···r··i·
0080  78 97 00 22 9a 9a 13 03  13 01 13 02 cc a9 cc a8   x··"···· ········
0090  c0 2b c0 2f c0 2c c0 30  c0 13 c0 14 00 9c 00 9d   ·+·/·,·0 ········
00a0  00 2f 00 35 00 0a 01 00  01 91 ca ca 00 00 00 00   ·/·5···· ········
00b0  00 13 00 11 00 00 0e 61  61 6e 2e 61 6d 61 7a 6f   ·······a an.amazo
00c0  6e 2e 63 6f 6d 00 17 00  00 ff 01 00 01 00 00 0a   n.com··· ········
00d0  00 0a 00 08 2a 2a 00 1d  00 17 00 18 00 0b 00 02   ····**·· ········
00e0  01 00 00 23 00 00 00 10  00 0e 00 0c 02 68 32 08   ···#···· ·····h2·
00f0  68 74 74 70 2f 31 2e 31  00 05 00 05 01 00 00 00   http/1.1 ········
0100  00 00 0d 00 14 00 12 04  03 08 04 04 01 05 03 08   ········ ········
```

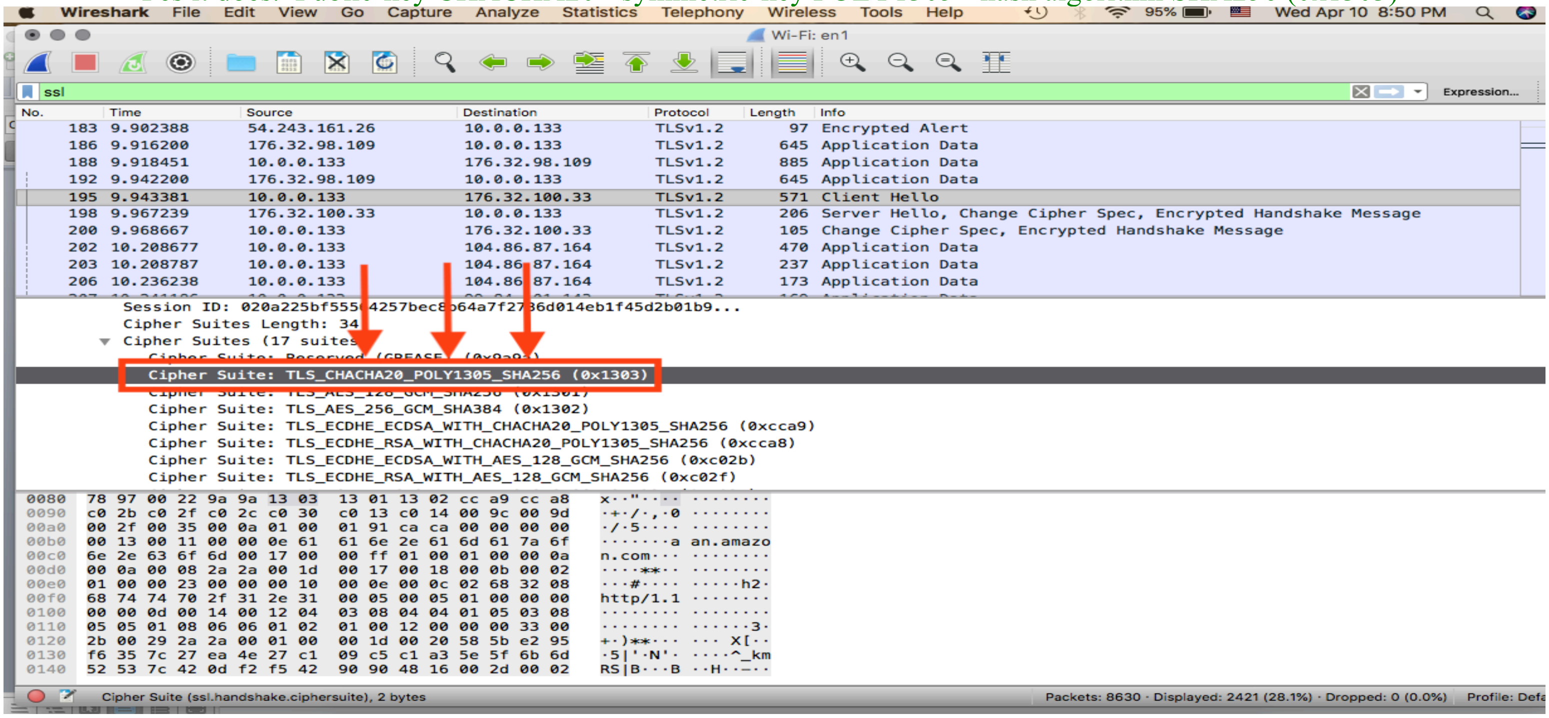
Random values used for deriving keys (ssl.handshake.random_bytes), 28 bytes

Packets: 8630 · Displayed: 2421 (28.1%) · Dropped: 0 (0.0%)   Pro

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?

Server Hello Record:

Yes it does. Public-key CHACHA20 - symmetric-key POLY1305 - hash algorithm SHA256 (0x1303)



```
No.   Time        Source           Destination      Protocol  Length  Info
  183 9.902388    54.243.161.26    10.0.0.133       TLSv1.2      97  Encrypted Alert
  186 9.916200    176.32.98.109    10.0.0.133       TLSv1.2     645  Application Data
  188 9.918451    10.0.0.133       176.32.98.109    TLSv1.2     885  Application Data
  192 9.942200    176.32.98.109    10.0.0.133       TLSv1.2     645  Application Data
  195 9.943381    10.0.0.133       176.32.100.33    TLSv1.2     571  Client Hello
  198 9.967239    176.32.100.33    10.0.0.133       TLSv1.2     206  Server Hello, Change Cipher Spec, Encrypted Handshake Message
  200 9.968667    10.0.0.133       176.32.100.33    TLSv1.2     105  Change Cipher Spec, Encrypted Handshake Message
  202 10.208677   10.0.0.133       104.86.87.164    TLSv1.2     470  Application Data
  203 10.208787   10.0.0.133       104.86.87.164    TLSv1.2     237  Application Data
  206 10.236238   10.0.0.133       104.86.87.164    TLSv1.2     173  Application Data
```

```
        Session ID: 020a225bf555 4257bec8 64a7f27 36d014eb1f45d2b01b9...
        Cipher Suites Length: 34
      ▼ Cipher Suites (17 suites)
          Cipher Suite: Reserved (GREASE) (0x9a9a)
          Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
          Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
          Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
          Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
```

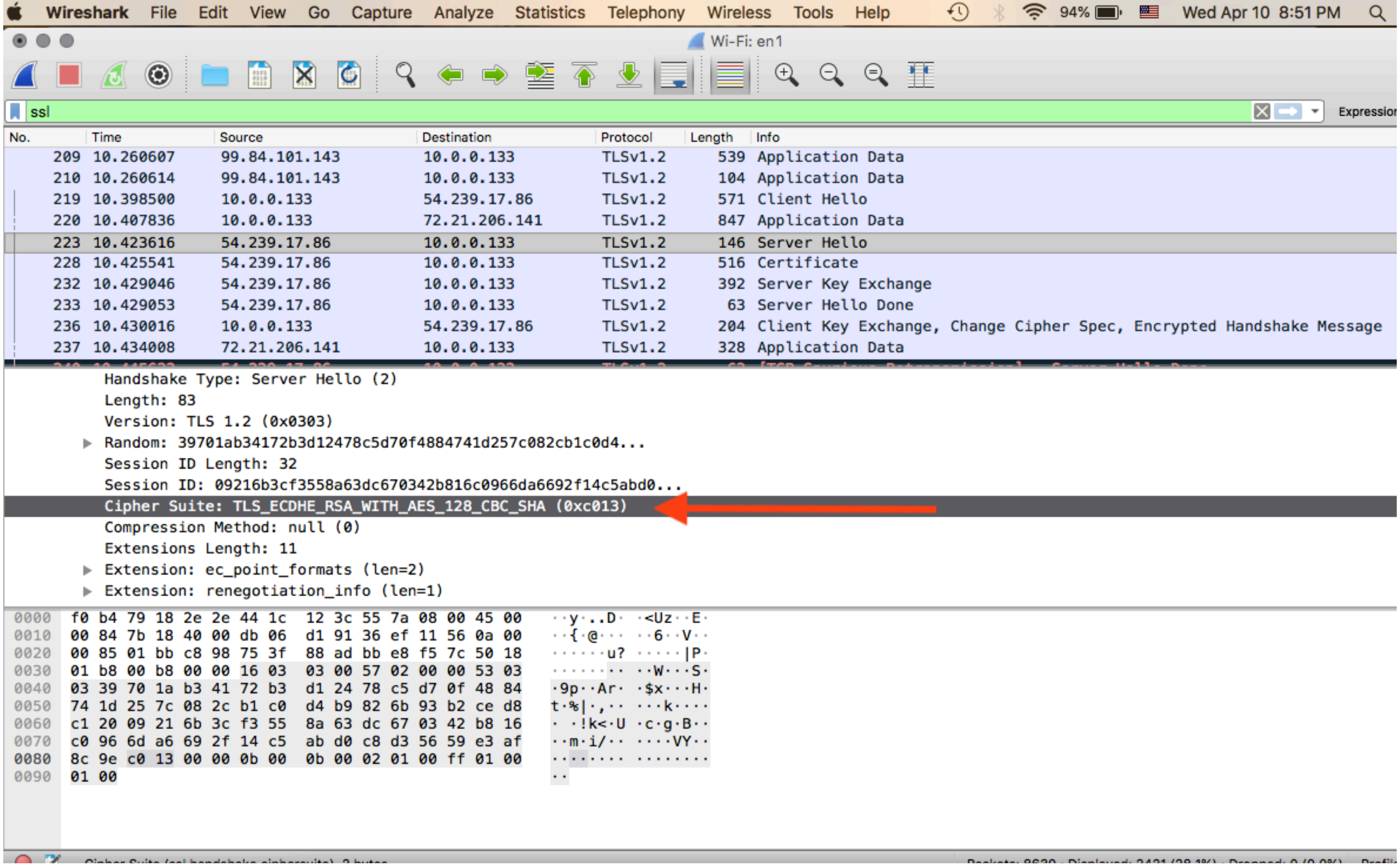
```
0080  78 97 00 22 9a 9a 13 03  13 01 13 02 cc a9 cc a8   x··"····  ········
0090  c0 2b c0 2f c0 2c c0 30  c0 13 c0 14 00 9c 00 9d   ·+·/·,·0  ········
00a0  00 2f 00 35 00 0a 01 00  01 91 ca ca 00 00 00 00   ·/·5····  ········
00b0  00 13 00 11 00 00 0e 61  61 6e 2e 61 6d 61 7a 6f   ·······a  an.amazo
00c0  6e 2e 63 6f 6d 00 17 00  00 ff 01 00 01 00 00 0a   n.com···  ········
00d0  00 0a 00 08 2a 2a 00 1d  00 17 00 18 00 0b 00 02   ····**··  ········
00e0  01 00 00 23 00 00 00 10  00 0e 00 0c 02 68 32 08   ···#····  ·····h2·
00f0  68 74 74 70 2f 31 2e 31  00 05 00 05 01 00 00 00   http/1.1  ········
0100  00 00 0d 00 14 00 12 04  03 08 04 04 01 05 03 08   ········  ········
0110  05 05 01 08 06 06 01 02  01 00 12 00 00 00 33 00   ········  ······3·
0120  2b 00 29 2a 2a 00 01 00  00 1d 00 20 58 5b e2 95   +·)**···  ··· X[··
0130  f6 35 7c 27 ea 4e 27 c1  09 c5 c1 a3 5e 5f 6b 6d   ·5|'·N'·  ····^_km
0140  52 53 7c 42 0d f2 f5 42  90 90 48 16 00 2d 00 02   RS|B···B  ··H··-··
```

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

Packets: 8630 · Displayed: 2421 (28.1%) · Dropped: 0 (0.0%) · Profile: Defa

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

Yes it does. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)



```
No.   Time        Source           Destination      Protocol  Length  Info
  209 10.260607   99.84.101.143    10.0.0.133       TLSv1.2     539  Application Data
  210 10.260614   99.84.101.143    10.0.0.133       TLSv1.2     104  Application Data
  219 10.398500   10.0.0.133       54.239.17.86     TLSv1.2     571  Client Hello
  220 10.407836   10.0.0.133       72.21.206.141    TLSv1.2     847  Application Data
  223 10.423616   54.239.17.86     10.0.0.133       TLSv1.2     146  Server Hello
  228 10.425541   54.239.17.86     10.0.0.133       TLSv1.2     516  Certificate
  232 10.429046   54.239.17.86     10.0.0.133       TLSv1.2     392  Server Key Exchange
  233 10.429053   54.239.17.86     10.0.0.133       TLSv1.2      63  Server Hello Done
  236 10.430016   10.0.0.133       54.239.17.86     TLSv1.2     204  Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  237 10.434008   72.21.206.141    10.0.0.133       TLSv1.2     328  Application Data
```

```
        Handshake Type: Server Hello (2)
        Length: 83
        Version: TLS 1.2 (0x0303)
      ▶ Random: 39701ab34172b3d12478c5d70f4884741d257c082cb1c0d4...
        Session ID Length: 32
        Session ID: 09216b3cf3558a63dc670342b816c0966da6692f14c5abd0...
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Compression Method: null (0)
        Extensions Length: 11
      ▶ Extension: ec_point_formats (len=2)
      ▶ Extension: renegotiation_info (len=1)
```

```
0000  f0 b4 79 18 2e 2e 44 1c  12 3c 55 7a 08 00 45 00   ··y·..D·  ·<Uz··E·
0010  00 84 7b 18 40 00 db 06  d1 91 36 ef 11 56 0a 00   ··{·@···  ··6··V··
0020  00 85 01 bb c8 98 75 3f  88 ad bb e8 f5 7c 50 18   ······u?  ·····|P·
0030  01 b8 00 b8 00 00 16 03  03 00 57 02 00 00 53 03   ········  ··W···S·
0040  03 39 70 1a b3 41 72 b3  d1 24 78 c5 d7 0f 48 84   ·9p··Ar·  ·$x···H·
0050  74 1d 25 7c 08 2c b1 c0  d4 b9 82 6b 93 b2 ce d8   t·%|·,··  ···k····
0060  c1 20 09 21 6b 3c f3 55  8a 63 dc 67 03 42 b8 16   · ·!k<·U  ·c·g·B··
0070  c0 96 6d a6 69 2f 14 c5  ab d0 c8 d3 56 59 e3 af   ··m·i/··  ····VY··
0080  8c 9e c0 13 00 00 0b 00  0b 00 02 01 00 ff 01 00   ········  ········
0090  01 00                                              ··
```

```
No.     Time           Source                Destination           Protocol Length Info
    195 9.943381       10.0.0.133            176.32.100.33         TLSv1.2  571    Client Hello
Frame 195: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:
55:7a)
Internet Protocol Version 4, Src: 10.0.0.133, Dst: 176.32.100.33
Transmission Control Protocol, Src Port: 51351, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 512
        Handshake Protocol: Client Hello
            Handshake Type: Client Hello (1)
            Length: 508
            Version: TLS 1.2 (0x0303)
            Random: b5fa0e8d20ce6b607415a872692e58d8f41d72d98bc9f957...
            Session ID Length: 32
            Session ID: 020a225bf55564257bec8b64a7f2786d014eb1f45d2b01b9...
            Cipher Suites Length: 34
            Cipher Suites (17 suites)
                Cipher Suite: Reserved (GREASE) (0x9a9a)
                Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
                Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
                Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
                Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
                Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
                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_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: 401
            Extension: Reserved (GREASE) (len=0)
            Extension: server_name (len=19)
            Extension: extended_master_secret (len=0)
            Extension: renegotiation_info (len=1)
            Extension: supported_groups (len=10)
            Extension: ec_point_formats (len=2)
            Extension: SessionTicket TLS (len=0)
            Extension: application_layer_protocol_negotiation (len=14)
            Extension: status_request (len=5)
            Extension: signature_algorithms (len=20)
            Extension: signed_certificate_timestamp (len=0)
            Extension: key_share (len=43)
            Extension: psk_key_exchange_modes (len=2)
            Extension: supported_versions (len=11)
            Extension: Unknown type 27 (len=3)
            Extension: Reserved (GREASE) (len=1)
            Extension: padding (len=202)
```