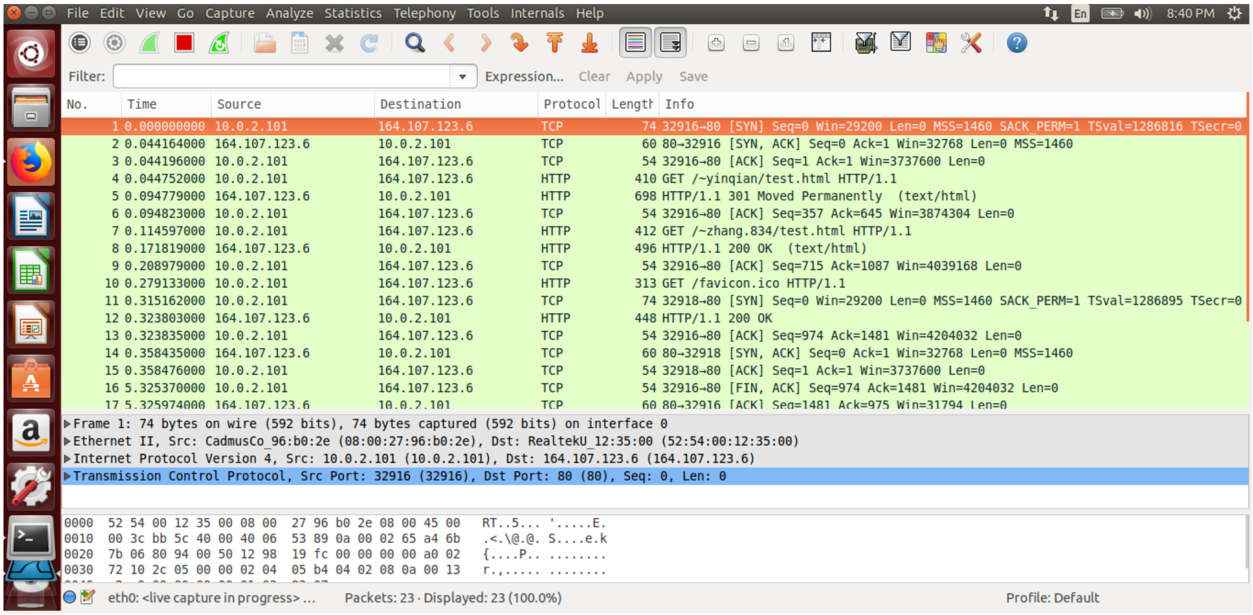
Joseph Shaffer

Shaffer.567

CSE 5473

Lab 1

Task 2.2


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
En
8:40 PM
Filter:
Expression...
Clear
Apply
Save

```
No.   Time        Source          Destination     Protocol Length Info
    1 0.000000000 10.0.2.101      164.107.123.6   TCP       74 32916→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1286816 TSecr=0
    2 0.044164000 164.107.123.6   10.0.2.101      TCP       60 80→32916 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
    3 0.044196000 10.0.2.101      164.107.123.6   TCP       54 32916→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
    4 0.044752000 10.0.2.101      164.107.123.6   HTTP     410 GET /~yinqian/test.html HTTP/1.1
    5 0.094779000 164.107.123.6   10.0.2.101      HTTP     698 HTTP/1.1 301 Moved Permanently  (text/html)
    6 0.094823000 10.0.2.101      164.107.123.6   TCP       54 32916→80 [ACK] Seq=357 Ack=645 Win=3874304 Len=0
    7 0.114597000 10.0.2.101      164.107.123.6   HTTP     412 GET /~zhang.834/test.html HTTP/1.1
    8 0.171819000 164.107.123.6   10.0.2.101      HTTP     496 HTTP/1.1 200 OK  (text/html)
    9 0.208979000 10.0.2.101      164.107.123.6   TCP       54 32916→80 [ACK] Seq=715 Ack=1087 Win=4039168 Len=0
   10 0.279133000 10.0.2.101      164.107.123.6   HTTP     313 GET /favicon.ico HTTP/1.1
   11 0.315162000 10.0.2.101      164.107.123.6   TCP       74 32918→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1286895 TSecr=0
   12 0.323803000 164.107.123.6   10.0.2.101      HTTP     448 HTTP/1.1 200 OK
   13 0.323835000 10.0.2.101      164.107.123.6   TCP       54 32916→80 [ACK] Seq=974 Ack=1481 Win=4204032 Len=0
   14 0.358435000 164.107.123.6   10.0.2.101      TCP       60 80→32918 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
   15 0.358476000 10.0.2.101      164.107.123.6   TCP       54 32918→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
   16 5.325370000 10.0.2.101      164.107.123.6   TCP       54 32916→80 [FIN, ACK] Seq=974 Ack=1481 Win=4204032 Len=0
   17 5.325974000 164.107.123.6   10.0.2.101      TCP       60 80→32916 [ACK] Seq=1481 Ack=975 Win=31794 Len=0
```

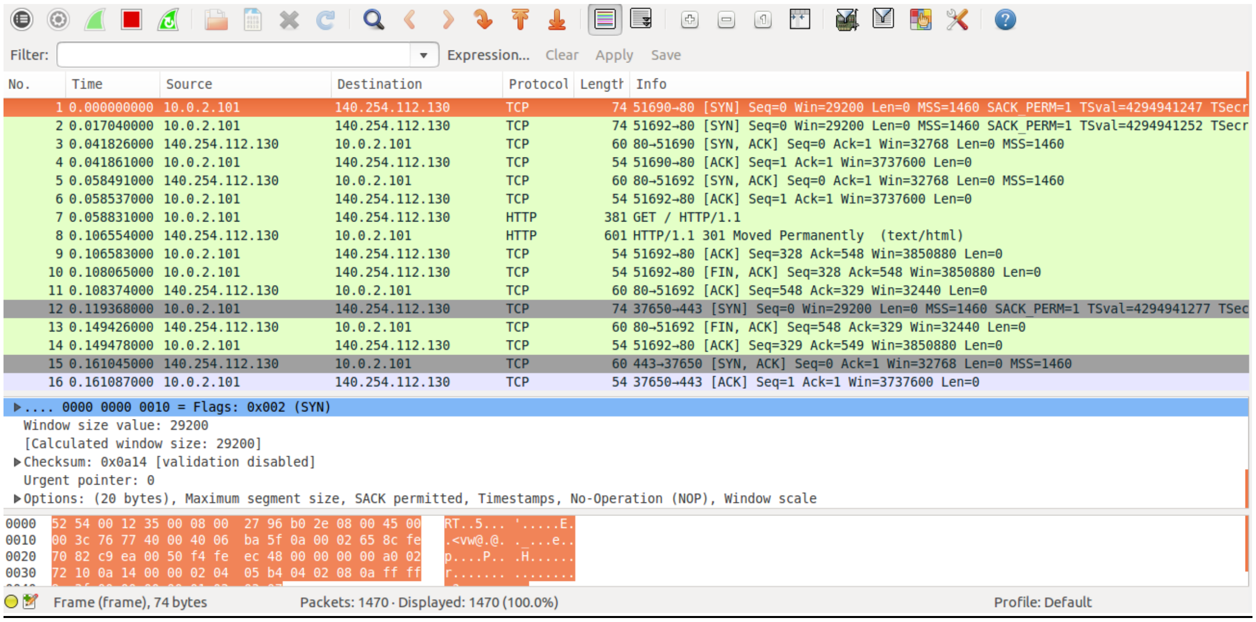
```
▶Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶Ethernet II, Src: CadmusCo_96:b0:2e (08:00:27:96:b0:2e), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 164.107.123.6 (164.107.123.6)
▶Transmission Control Protocol, Src Port: 32916 (32916), Dst Port: 80 (80), Seq: 0, Len: 0
```

```
0000  52 54 00 12 35 00 08 00  27 96 b0 2e 08 00 45 00   RT..5... '.....E.
0010  00 3c bb 5c 40 00 40 06  53 89 0a 00 02 65 a4 6b   .<.\@.@. S....e.k
0020  7b 06 80 94 00 50 12 98  19 fc 00 00 00 00 a0 02   {....P.. ........
0030  72 10 2c 05 00 00 02 04  05 b4 04 02 08 0a 00 13   r.,..... ........
```

eth0: <live capture in progress> ...   Packets: 23 · Displayed: 23 (100.0%)   Profile: Default

From the screenshot, it can be seen that the TCP handshake begins with client and the OSU server for the webpage http://web.cse.ohio-state.edu/~yinqian/test.html. This begins with the client sending a SYN and the server responding with a SYN and an ACK to which the client responds with an ACK, which is an example of the TCP three way handshake. It can also be seen that the client sends packets for the HTTP protocol to the server with a GET to request information from the server and the server responds to that HTTP protocol with a HTTP protocol with the information requested from the client. The session terminates with the TCP handshake that has [FIN, ACK] and [FIN] messages from both the client to the server and the server to the client. The handshake ends with an ACK from the client to the server.

Task 2.3

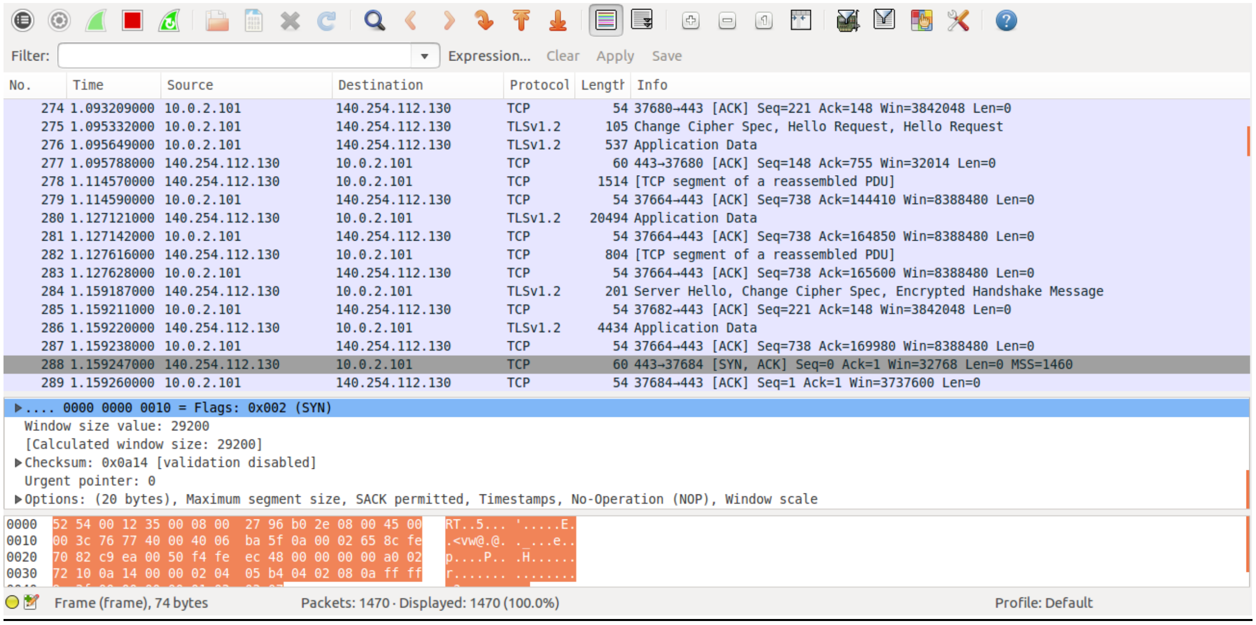


```
No.   Time        Source          Destination     Protocol Length Info
    1 0.000000000 10.0.2.101      140.254.112.130 TCP        74 51690→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294941247 TSecr
    2 0.017040000 10.0.2.101      140.254.112.130 TCP        74 51692→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294941252 TSecr
    3 0.041826000 140.254.112.130 10.0.2.101      TCP        60 80→51690 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
    4 0.041861000 10.0.2.101      140.254.112.130 TCP        54 51690→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
    5 0.058491000 140.254.112.130 10.0.2.101      TCP        60 80→51692 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
    6 0.058537000 10.0.2.101      140.254.112.130 TCP        54 51692→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
    7 0.058831000 10.0.2.101      140.254.112.130 HTTP      381 GET / HTTP/1.1
    8 0.106554000 140.254.112.130 10.0.2.101      HTTP      601 HTTP/1.1 301 Moved Permanently  (text/html)
    9 0.106583000 10.0.2.101      140.254.112.130 TCP        54 51692→80 [ACK] Seq=328 Ack=548 Win=3850880 Len=0
   10 0.108065000 10.0.2.101      140.254.112.130 TCP        54 51692→80 [FIN, ACK] Seq=328 Ack=548 Win=3850880 Len=0
   11 0.108374000 140.254.112.130 10.0.2.101      TCP        60 80→51692 [ACK] Seq=548 Ack=329 Win=32440 Len=0
   12 0.119368000 10.0.2.101      140.254.112.130 TCP        74 37650→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294941277 TSec
   13 0.149426000 140.254.112.130 10.0.2.101      TCP        60 80→51692 [FIN, ACK] Seq=548 Ack=329 Win=32440 Len=0
   14 0.149478000 10.0.2.101      140.254.112.130 TCP        54 51692→80 [ACK] Seq=329 Ack=549 Win=3850880 Len=0
   15 0.161045000 140.254.112.130 10.0.2.101      TCP        60 443→37650 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
   16 0.161087000 10.0.2.101      140.254.112.130 TCP        54 37650→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
```

```
▶.... 0000 0000 0010 = Flags: 0x002 (SYN)
  Window size value: 29200
  [Calculated window size: 29200]
▶Checksum: 0x0a14 [validation disabled]
  Urgent pointer: 0
▶Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

```
0000  52 54 00 12 35 00 08 00  27 96 b0 2e 08 00 45 00   RT..5... '.....E.
0010  00 3c 76 77 40 00 40 06  ba 5f 0a 00 02 65 8c fe   .<vw@.@. ._...e..
0020  70 82 c9 ea 00 50 f4 fe  ec 48 00 00 00 00 a0 02   p....P.. .H......
0030  72 10 0a 14 00 00 02 04  05 b4 04 02 08 0a ff ff   r....... ........
```

Frame (frame), 74 bytes   Packets: 1470 · Displayed: 1470 (100.0%)   Profile: Default

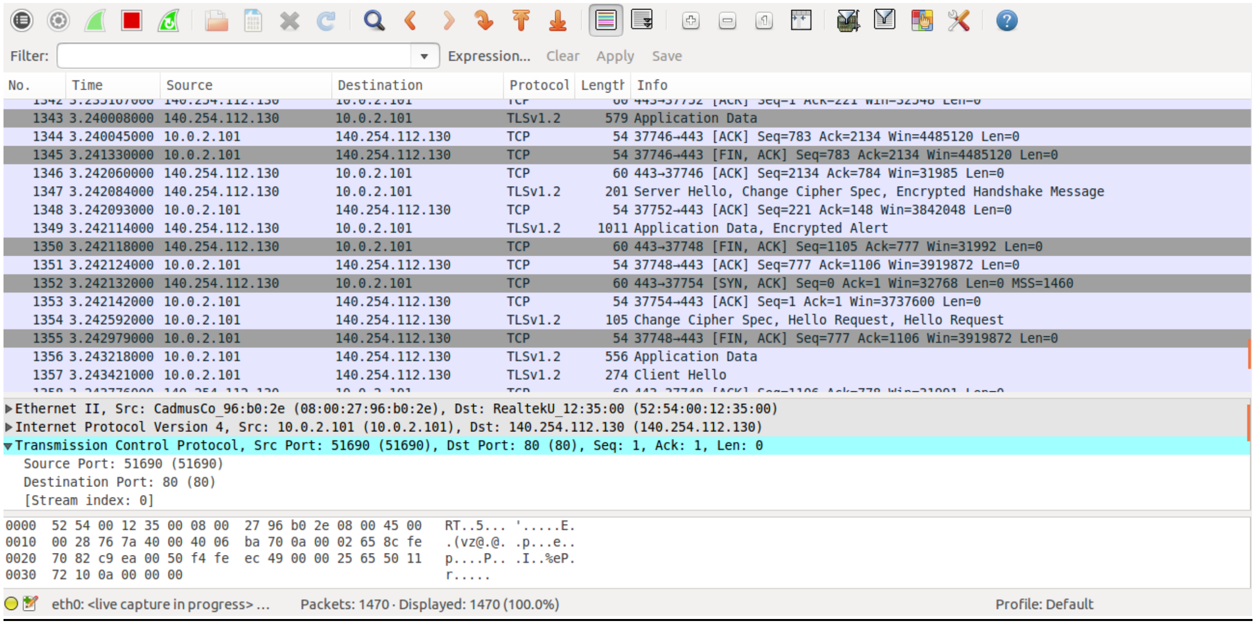


```
No.   Time        Source          Destination     Protocol Length Info
  274 1.093209000 10.0.2.101      140.254.112.130 TCP         54 37680→443 [ACK] Seq=221 Ack=148 Win=3842048 Len=0
  275 1.095332000 10.0.2.101      140.254.112.130 TLSv1.2    105 Change Cipher Spec, Hello Request, Hello Request
  276 1.095649000 10.0.2.101      140.254.112.130 TLSv1.2    537 Application Data
  277 1.095788000 140.254.112.130 10.0.2.101      TCP         60 443→37680 [ACK] Seq=148 Ack=755 Win=32014 Len=0
  278 1.114570000 140.254.112.130 10.0.2.101      TCP       1514 [TCP segment of a reassembled PDU]
  279 1.114590000 10.0.2.101      140.254.112.130 TCP         54 37664→443 [ACK] Seq=738 Ack=144410 Win=8388480 Len=0
  280 1.127121000 140.254.112.130 10.0.2.101      TLSv1.2  20494 Application Data
  281 1.127142000 10.0.2.101      140.254.112.130 TCP         54 37664→443 [ACK] Seq=738 Ack=164850 Win=8388480 Len=0
  282 1.127616000 140.254.112.130 10.0.2.101      TCP        804 [TCP segment of a reassembled PDU]
  283 1.127628000 10.0.2.101      140.254.112.130 TCP         54 37664→443 [ACK] Seq=738 Ack=165600 Win=8388480 Len=0
  284 1.159187000 140.254.112.130 10.0.2.101      TLSv1.2    201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  285 1.159211000 10.0.2.101      140.254.112.130 TCP         54 37682→443 [ACK] Seq=221 Ack=148 Win=3842048 Len=0
  286 1.159220000 140.254.112.130 10.0.2.101      TLSv1.2   4434 Application Data
  287 1.159238000 10.0.2.101      140.254.112.130 TCP         54 37664→443 [ACK] Seq=738 Ack=169980 Win=8388480 Len=0
  288 1.159247000 140.254.112.130 10.0.2.101      TCP         60 443→37684 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
  289 1.159260000 10.0.2.101      140.254.112.130 TCP         54 37684→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
```

```
▶.... 0000 0000 0010 = Flags: 0x002 (SYN)
  Window size value: 29200
  [Calculated window size: 29200]
▶Checksum: 0x0a14 [validation disabled]
  Urgent pointer: 0
▶Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

```
0000  52 54 00 12 35 00 08 00  27 96 b0 2e 08 00 45 00   RT..5... '.....E.
0010  00 3c 76 77 40 00 40 06  ba 5f 0a 00 02 65 8c fe   .<vw@.@. ._...e..
0020  70 82 c9 ea 00 50 f4 fe  ec 48 00 00 00 00 a0 02   p....P.. .H......
0030  72 10 0a 14 00 00 02 04  05 b4 04 02 08 0a ff ff   r....... ........
```

Frame (frame), 74 bytes   Packets: 1470 · Displayed: 1470 (100.0%)   Profile: Default

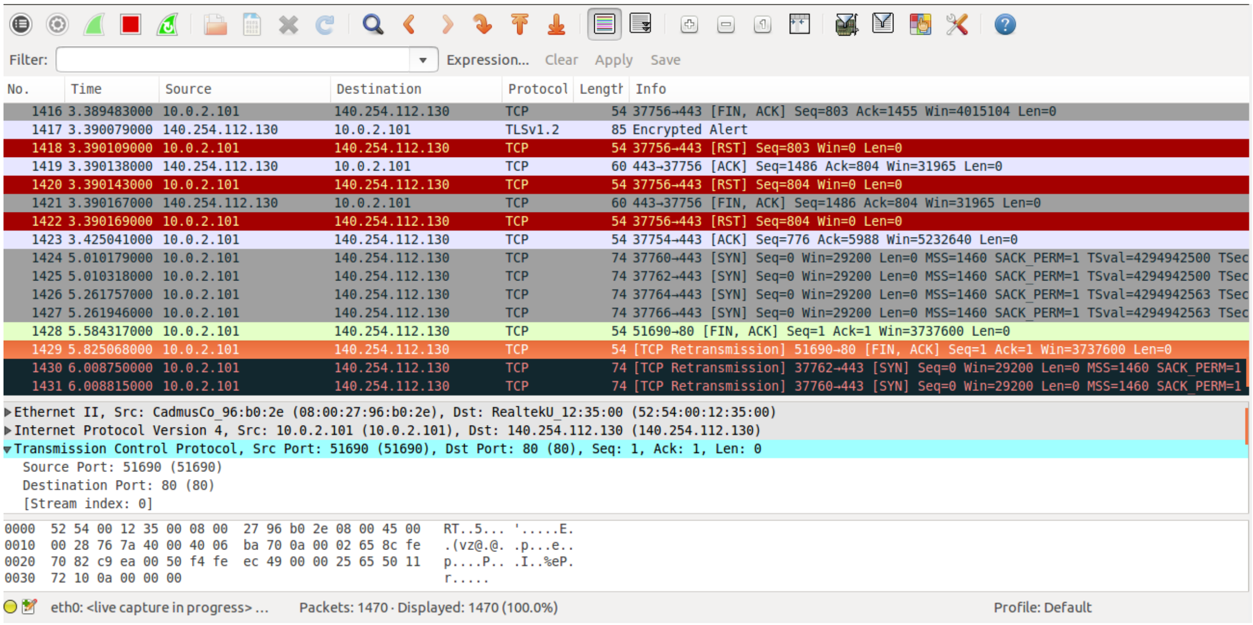


```
No.   Time        Source          Destination     Protocol Length Info
 1343 3.240008000 140.254.112.130 10.0.2.101      TLSv1.2    579 Application Data
 1344 3.240045000 10.0.2.101      140.254.112.130 TCP         54 37746→443 [ACK] Seq=783 Ack=2134 Win=4485120 Len=0
 1345 3.241330000 10.0.2.101      140.254.112.130 TCP         54 37746→443 [FIN, ACK] Seq=783 Ack=2134 Win=4485120 Len=0
 1346 3.242060000 140.254.112.130 10.0.2.101      TCP         60 443→37746 [ACK] Seq=2134 Ack=784 Win=31985 Len=0
 1347 3.242084000 140.254.112.130 10.0.2.101      TLSv1.2    201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
 1348 3.242093000 10.0.2.101      140.254.112.130 TCP         54 37752→443 [ACK] Seq=221 Ack=148 Win=3842048 Len=0
 1349 3.242114000 140.254.112.130 10.0.2.101      TLSv1.2   1011 Application Data, Encrypted Alert
 1350 3.242118000 140.254.112.130 10.0.2.101      TCP         60 443→37748 [FIN, ACK] Seq=1105 Ack=777 Win=31992 Len=0
 1351 3.242124000 10.0.2.101      140.254.112.130 TCP         54 37748→443 [ACK] Seq=777 Ack=1106 Win=3919872 Len=0
 1352 3.242132000 140.254.112.130 10.0.2.101      TCP         60 443→37754 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
 1353 3.242142000 10.0.2.101      140.254.112.130 TCP         54 37754→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
 1354 3.242592000 10.0.2.101      140.254.112.130 TLSv1.2    105 Change Cipher Spec, Hello Request, Hello Request
 1355 3.242979000 10.0.2.101      140.254.112.130 TCP         54 37748→443 [FIN, ACK] Seq=777 Ack=1106 Win=3919872 Len=0
 1356 3.243218000 10.0.2.101      140.254.112.130 TLSv1.2    556 Application Data
 1357 3.243421000 10.0.2.101      140.254.112.130 TLSv1.2    274 Client Hello
```

```
▶Ethernet II, Src: CadmusCo_96:b0:2e (08:00:27:96:b0:2e), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 140.254.112.130 (140.254.112.130)
▼Transmission Control Protocol, Src Port: 51690 (51690), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0
  Source Port: 51690 (51690)
  Destination Port: 80 (80)
  [Stream index: 0]
```

```
0000  52 54 00 12 35 00 08 00  27 96 b0 2e 08 00 45 00   RT..5... '.....E.
0010  00 28 76 7a 40 00 40 06  ba 70 0a 00 02 65 8c fe   .(vz@.@. .p...e..
0020  70 82 c9 ea 00 50 f4 fe  ec 49 00 00 25 65 50 11   p....P.. .I..%eP.
0030  72 10 0a 00 00 00                                  r.....
```

eth0: <live capture in progress> ...   Packets: 1470 · Displayed: 1470 (100.0%)   Profile: Default

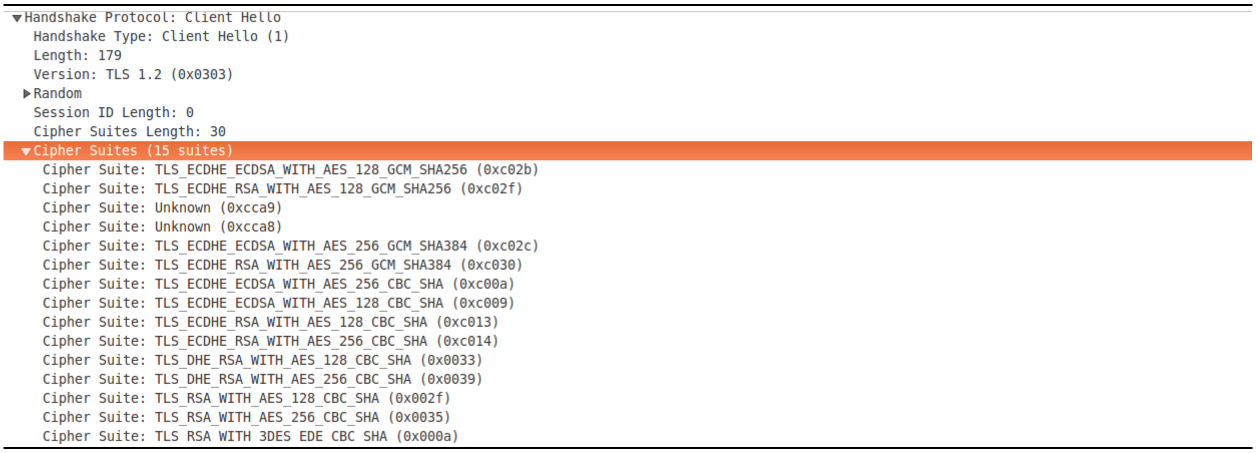


```
No.     Time         Source          Destination     Protocol Length Info
   1416 3.389483000 10.0.2.101      140.254.112.130  TCP      54 37756→443 [FIN, ACK] Seq=803 Ack=1455 Win=4015104 Len=0
   1417 3.390079000 140.254.112.130 10.0.2.101       TLSv1.2  85 Encrypted Alert
   1418 3.390109000 10.0.2.101      140.254.112.130  TCP      54 37756→443 [RST] Seq=803 Win=0 Len=0
   1419 3.390138000 140.254.112.130 10.0.2.101       TCP      60 443→37756 [ACK] Seq=1486 Ack=804 Win=31965 Len=0
   1420 3.390143000 10.0.2.101      140.254.112.130  TCP      54 37756→443 [RST] Seq=804 Win=0 Len=0
   1421 3.390167000 140.254.112.130 10.0.2.101       TCP      60 443→37756 [FIN, ACK] Seq=1486 Ack=804 Win=31965 Len=0
   1422 3.390169000 10.0.2.101      140.254.112.130  TCP      54 37756→443 [RST] Seq=804 Win=0 Len=0
   1423 3.425041000 10.0.2.101      140.254.112.130  TCP      54 37754→443 [ACK] Seq=776 Ack=5988 Win=5232640 Len=0
   1424 5.010179000 10.0.2.101      140.254.112.130  TCP      74 37760→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294942500 TSec
   1425 5.010318000 10.0.2.101      140.254.112.130  TCP      74 37762→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294942500 TSec
   1426 5.261757000 10.0.2.101      140.254.112.130  TCP      74 37764→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294942563 TSec
   1427 5.261946000 10.0.2.101      140.254.112.130  TCP      74 37766→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294942563 TSec
   1428 5.584317000 10.0.2.101      140.254.112.130  TCP      54 51690→80 [FIN, ACK] Seq=1 Ack=1 Win=3737600 Len=0
   1429 5.825068000 10.0.2.101      140.254.112.130  TCP      54 [TCP Retransmission] 51690→80 [FIN, ACK] Seq=1 Ack=1 Win=3737600 Len=0
   1430 6.008750000 10.0.2.101      140.254.112.130  TCP      74 [TCP Retransmission] 37762→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
   1431 6.008815000 10.0.2.101      140.254.112.130  TCP      74 [TCP Retransmission] 37760→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
```

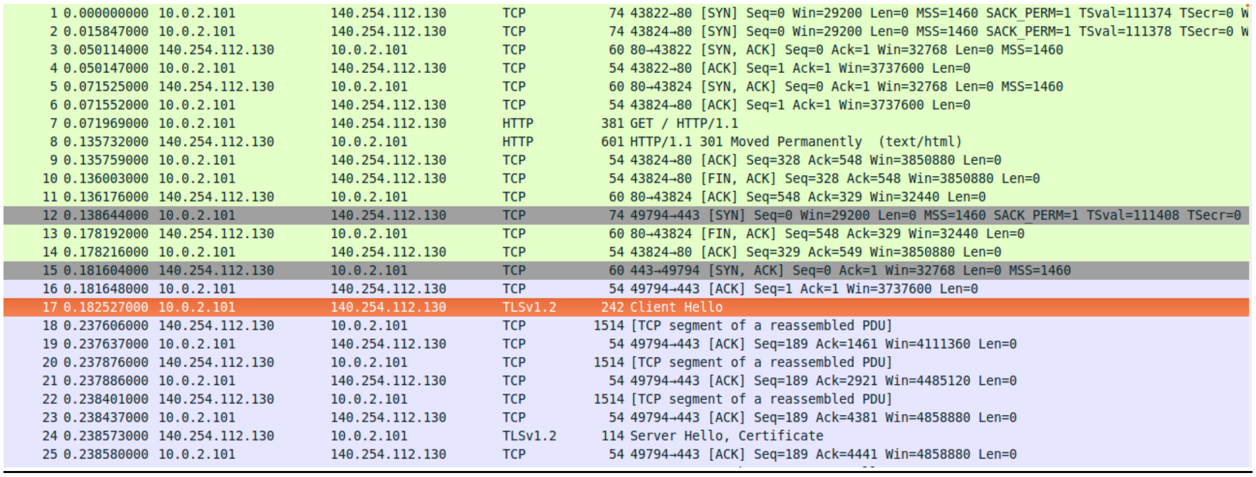
```
▶Ethernet II, Src: CadmusCo_96:b0:2e (08:00:27:96:b0:2e), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 140.254.112.130 (140.254.112.130)
▼Transmission Control Protocol, Src Port: 51690 (51690), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0
   Source Port: 51690 (51690)
   Destination Port: 80 (80)
   [Stream index: 0]
```

```
0000  52 54 00 12 35 00 08 00  27 96 b0 2e 08 00 45 00   RT..5... '.....E.
0010  00 28 76 7a 40 00 40 06  ba 70 0a 00 02 65 8c fe   .(vz@.@. .p...e..
0020  70 82 c9 ea 00 50 f4 fe  ec 49 00 00 25 65 50 11   p....P.. .I..%eP.
0030  72 10 0a 00 00 00                                  r.....
```

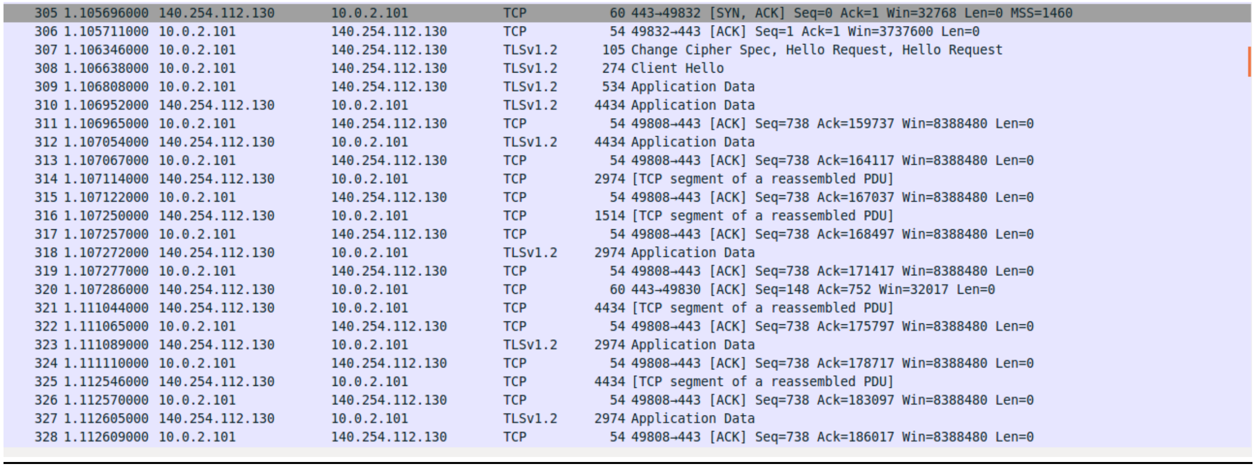
eth0: <live capture in progress> … Packets: 1470 · Displayed: 1470 (100.0%) Profile: Default



```
 ▼Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 179
    Version: TLS 1.2 (0x0303)
   ▶Random
    Session ID Length: 0
    Cipher Suites Length: 30
   ▼Cipher Suites (15 suites)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: Unknown (0xcca9)
      Cipher Suite: Unknown (0xcca8)
      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_AES_256_CBC_SHA (0xc00a)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      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_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
      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)
```



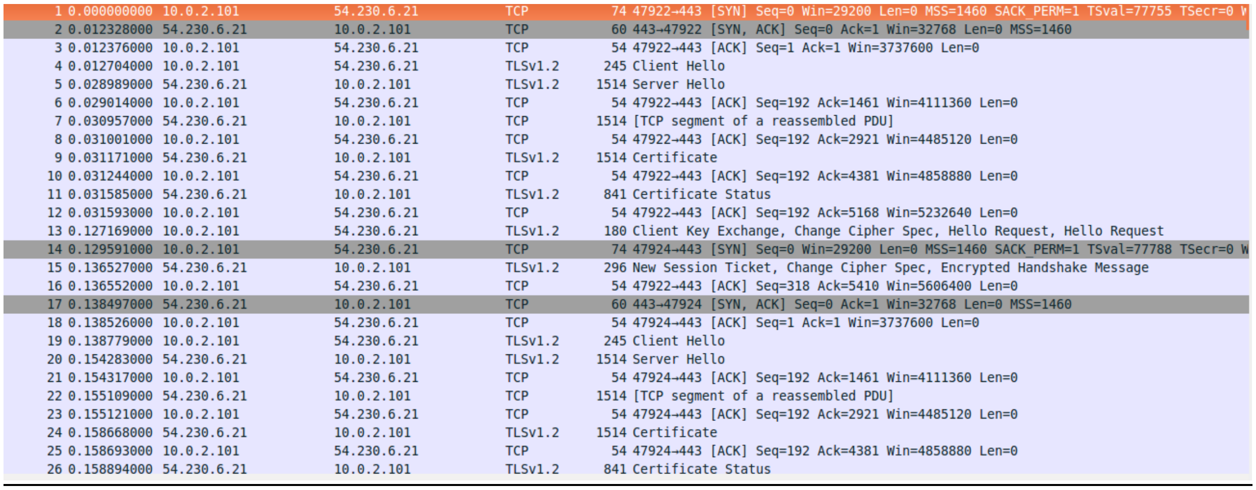
```
  1 0.000000000 10.0.2.101        140.254.112.130   TCP       74 43822→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=111374 TSecr=0 W
  2 0.015847000 10.0.2.101        140.254.112.130   TCP       74 43824→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=111378 TSecr=0 W
  3 0.050114000 140.254.112.130   10.0.2.101        TCP       60 80→43822 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
  4 0.050147000 10.0.2.101        140.254.112.130   TCP       54 43822→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
  5 0.071525000 140.254.112.130   10.0.2.101        TCP       60 80→43824 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
  6 0.071552000 10.0.2.101        140.254.112.130   TCP       54 43824→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
  7 0.071969000 10.0.2.101        140.254.112.130   HTTP     381 GET / HTTP/1.1
  8 0.135732000 140.254.112.130   10.0.2.101        HTTP     601 HTTP/1.1 301 Moved Permanently  (text/html)
  9 0.135759000 10.0.2.101        140.254.112.130   TCP       54 43824→80 [ACK] Seq=328 Ack=548 Win=3850880 Len=0
 10 0.136003000 10.0.2.101        140.254.112.130   TCP       54 43824→80 [FIN, ACK] Seq=328 Ack=548 Win=3850880 Len=0
 11 0.136176000 140.254.112.130   10.0.2.101        TCP       60 80→43824 [ACK] Seq=548 Ack=329 Win=32440 Len=0
 12 0.138644000 10.0.2.101        140.254.112.130   TCP       74 49794→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=111408 TSecr=0
 13 0.178192000 140.254.112.130   10.0.2.101        TCP       60 80→43824 [FIN, ACK] Seq=548 Ack=329 Win=32440 Len=0
 14 0.178216000 10.0.2.101        140.254.112.130   TCP       54 43824→80 [ACK] Seq=329 Ack=549 Win=3850880 Len=0
 15 0.181604000 140.254.112.130   10.0.2.101        TCP       60 443→49794 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
 16 0.181648000 10.0.2.101        140.254.112.130   TCP       54 49794→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
 17 0.182527000 10.0.2.101        140.254.112.130   TLSv1.2  242 Client Hello
 18 0.237606000 140.254.112.130   10.0.2.101        TCP     1514 [TCP segment of a reassembled PDU]
 19 0.237637000 10.0.2.101        140.254.112.130   TCP       54 49794→443 [ACK] Seq=189 Ack=1461 Win=4111360 Len=0
 20 0.237876000 140.254.112.130   10.0.2.101        TCP     1514 [TCP segment of a reassembled PDU]
 21 0.237886000 10.0.2.101        140.254.112.130   TCP       54 49794→443 [ACK] Seq=189 Ack=2921 Win=4485120 Len=0
 22 0.238401000 140.254.112.130   10.0.2.101        TCP     1514 [TCP segment of a reassembled PDU]
 23 0.238437000 10.0.2.101        140.254.112.130   TCP       54 49794→443 [ACK] Seq=189 Ack=4381 Win=4858880 Len=0
 24 0.238573000 140.254.112.130   10.0.2.101        TLSv1.2  114 Server Hello, Certificate
 25 0.238580000 10.0.2.101        140.254.112.130   TCP       54 49794→443 [ACK] Seq=189 Ack=4441 Win=4858880 Len=0
```



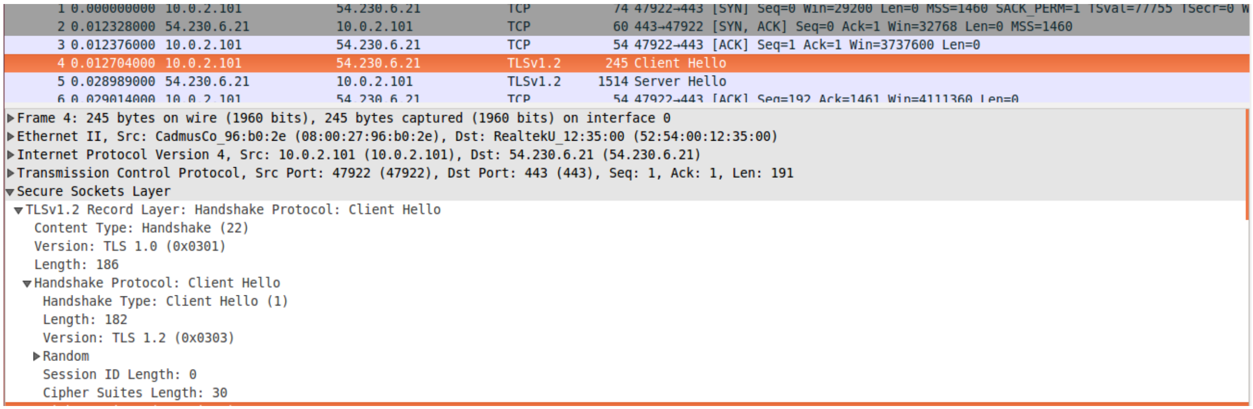
```
305 1.105696000 140.254.112.130   10.0.2.101        TCP       60 443→49832 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
306 1.105711000 10.0.2.101        140.254.112.130   TCP       54 49832→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
307 1.106346000 10.0.2.101        140.254.112.130   TLSv1.2  105 Change Cipher Spec, Hello Request, Hello Request
308 1.106638000 10.0.2.101        140.254.112.130   TLSv1.2  274 Client Hello
309 1.106808000 10.0.2.101        140.254.112.130   TLSv1.2  534 Application Data
310 1.106952000 140.254.112.130   10.0.2.101        TLSv1.2 4434 Application Data
311 1.106965000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=159737 Win=8388480 Len=0
312 1.107054000 140.254.112.130   10.0.2.101        TLSv1.2 4434 Application Data
313 1.107067000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=164117 Win=8388480 Len=0
314 1.107114000 140.254.112.130   10.0.2.101        TCP     2974 [TCP segment of a reassembled PDU]
315 1.107122000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=167037 Win=8388480 Len=0
316 1.107250000 140.254.112.130   10.0.2.101        TCP     1514 [TCP segment of a reassembled PDU]
317 1.107257000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=168497 Win=8388480 Len=0
318 1.107272000 140.254.112.130   10.0.2.101        TLSv1.2 2974 Application Data
319 1.107277000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=171417 Win=8388480 Len=0
320 1.107286000 140.254.112.130   10.0.2.101        TCP       60 443→49830 [ACK] Seq=148 Ack=752 Win=32017 Len=0
321 1.111044000 140.254.112.130   10.0.2.101        TCP     4434 [TCP segment of a reassembled PDU]
322 1.111065000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=175797 Win=8388480 Len=0
323 1.111089000 140.254.112.130   10.0.2.101        TLSv1.2 2974 Application Data
324 1.111110000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=178717 Win=8388480 Len=0
325 1.112546000 140.254.112.130   10.0.2.101        TCP     4434 [TCP segment of a reassembled PDU]
326 1.112570000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=183097 Win=8388480 Len=0
327 1.112605000 140.254.112.130   10.0.2.101        TLSv1.2 2974 Application Data
328 1.112609000 10.0.2.101        140.254.112.130   TCP       54 49808→443 [ACK] Seq=738 Ack=186017 Win=8388480 Len=0
```

The HTTP traffic is upgraded to the HTTPS because HTTPS is encrypted with TLS protocols, which can be seen throughout the screenshots, which was not used in the HTTP traffic. After the initial TCP handshakes, the client sends a Client Hello packet to the server with the TLS protocol. This packet includes 15 cipher suites. The server responds with a TLS protocol packet with a Server Hello Certificate that includes a cipher suite that was included in the Client Hello packet from the client to the server. The chosen cipher suite is the first cipher suite in the list from the client that the server can also support. The server then also sends a packet with the TSL protocol with the Server Key Exchange, which includes the ending of the Server Hello Done from the server to the client. The client also sends a Client Key Exchange to the server and the server responds with a Change Cipher Spec and Encrypted message. Thus, the cipher suite and the key exchange are both encrypted. These message continuously are transmitted between the client and the server along with Application Date from the client to the server and the server to the client. These messages show that HTTPS traffic is encrypted unlike HTTP traffic, meaning that the Client and Server are exchanging requests and cipher suites and keys between each other. The choices of ciphers are about 15 cipher suites, which are different encryption schemes that are TLS encryptions. The 15 cipher suites are have different options such as ECDSA with AES and RSA with AES or RSA with 3 DES, as well as different cipher key lengths which are either 128 or 256. This all shows the difference in HTTP and HTTPS traffic as HTTPS uses encryption and exchanges encryption schemes and keys between the client and the server.

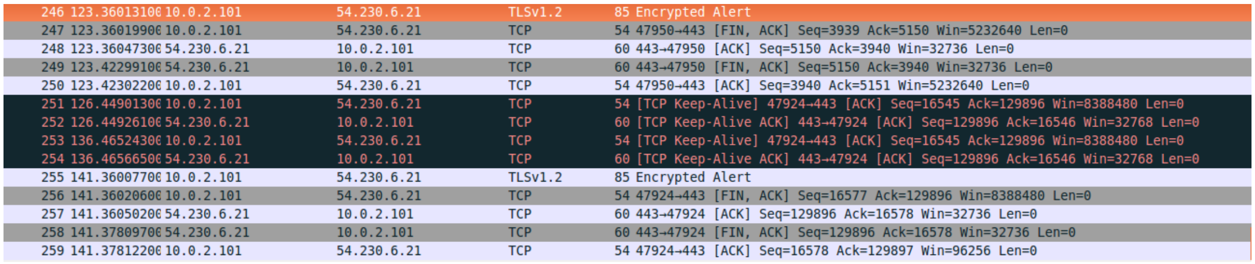
Task 2.4



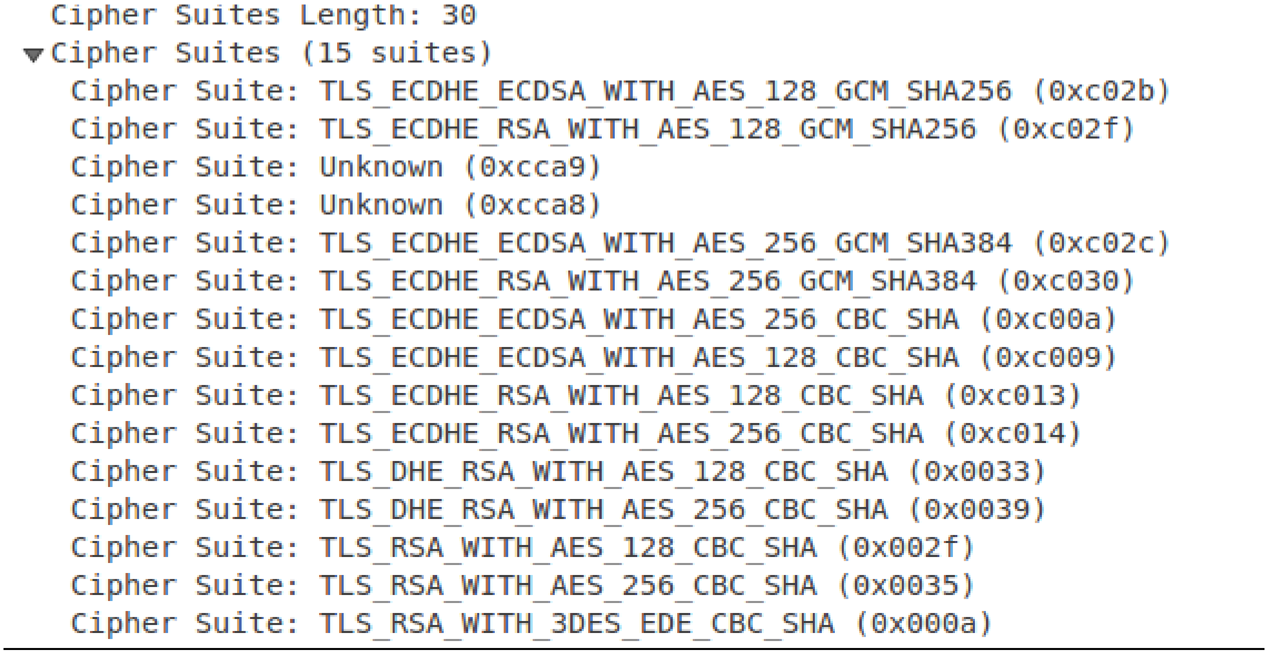
```
 1 0.000000000 10.0.2.101   54.230.6.21  TCP       74 47922→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=77755 TSecr=0 W
 2 0.012328000 54.230.6.21  10.0.2.101   TCP       60 443→47922 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
 3 0.012376000 10.0.2.101   54.230.6.21  TCP       54 47922→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
 4 0.012704000 10.0.2.101   54.230.6.21  TLSv1.2  245 Client Hello
 5 0.028989000 54.230.6.21  10.0.2.101   TLSv1.2 1514 Server Hello
 6 0.029014000 10.0.2.101   54.230.6.21  TCP       54 47922→443 [ACK] Seq=192 Ack=1461 Win=4111360 Len=0
 7 0.030957000 54.230.6.21  10.0.2.101   TCP     1514 [TCP segment of a reassembled PDU]
 8 0.031001000 10.0.2.101   54.230.6.21  TCP       54 47922→443 [ACK] Seq=192 Ack=2921 Win=4485120 Len=0
 9 0.031171000 54.230.6.21  10.0.2.101   TLSv1.2 1514 Certificate
10 0.031244000 10.0.2.101   54.230.6.21  TCP       54 47922→443 [ACK] Seq=192 Ack=4381 Win=4858880 Len=0
11 0.031585000 54.230.6.21  10.0.2.101   TLSv1.2  841 Certificate Status
12 0.031593000 10.0.2.101   54.230.6.21  TCP       54 47922→443 [ACK] Seq=192 Ack=5168 Win=5232640 Len=0
13 0.127169000 10.0.2.101   54.230.6.21  TLSv1.2  180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
14 0.129591000 10.0.2.101   54.230.6.21  TCP       74 47924→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=77788 TSecr=0 W
15 0.136527000 54.230.6.21  10.0.2.101   TLSv1.2  296 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
16 0.136552000 10.0.2.101   54.230.6.21  TCP       54 47922→443 [ACK] Seq=318 Ack=5410 Win=5606400 Len=0
17 0.138497000 54.230.6.21  10.0.2.101   TCP       60 443→47924 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
18 0.138526000 10.0.2.101   54.230.6.21  TCP       54 47924→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
19 0.138779000 10.0.2.101   54.230.6.21  TLSv1.2  245 Client Hello
20 0.154283000 54.230.6.21  10.0.2.101   TLSv1.2 1514 Server Hello
21 0.154317000 10.0.2.101   54.230.6.21  TCP       54 47924→443 [ACK] Seq=192 Ack=1461 Win=4111360 Len=0
22 0.155109000 54.230.6.21  10.0.2.101   TCP     1514 [TCP segment of a reassembled PDU]
23 0.155121000 10.0.2.101   54.230.6.21  TCP       54 47924→443 [ACK] Seq=192 Ack=2921 Win=4485120 Len=0
24 0.158668000 54.230.6.21  10.0.2.101   TLSv1.2 1514 Certificate
25 0.158693000 10.0.2.101   54.230.6.21  TCP       54 47924→443 [ACK] Seq=192 Ack=4381 Win=4858880 Len=0
26 0.158894000 54.230.6.21  10.0.2.101   TLSv1.2  841 Certificate Status
```



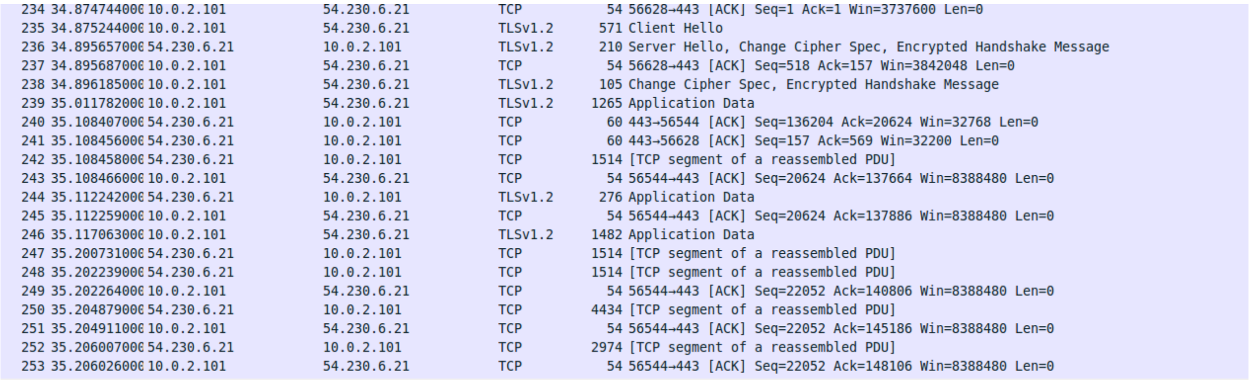
```
  1 0.000000000  10.0.2.101     54.230.6.21    TCP       74 47922→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=77755 TSecr=0 W
  2 0.012328000  54.230.6.21    10.0.2.101     TCP       60 443→47922 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
  3 0.012376000  10.0.2.101     54.230.6.21    TCP       54 47922→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
  4 0.012704000  10.0.2.101     54.230.6.21    TLSv1.2  245 Client Hello
  5 0.028989000  54.230.6.21    10.0.2.101     TLSv1.2 1514 Server Hello
  6 0.029014000  10.0.2.101     54.230.6.21    TCP       54 47922→443 [ACK] Seq=192 Ack=1461 Win=4111360 Len=0
▶Frame 4: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) on interface 0
▶Ethernet II, Src: CadmusCo_96:b0:2e (08:00:27:96:b0:2e), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 54.230.6.21 (54.230.6.21)
▶Transmission Control Protocol, Src Port: 47922 (47922), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 191
▼Secure Sockets Layer
 ▼TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 186
   ▼Handshake Protocol: Client Hello
     Handshake Type: Client Hello (1)
     Length: 182
     Version: TLS 1.2 (0x0303)
    ▶Random
     Session ID Length: 0
     Cipher Suites Length: 30
```



```
246 123.36013100 10.0.2.101    54.230.6.21    TLSv1.2  85 Encrypted Alert
247 123.36019900 10.0.2.101    54.230.6.21    TCP      54 47950→443 [FIN, ACK] Seq=3939 Ack=5150 Win=5232640 Len=0
248 123.36047300 54.230.6.21   10.0.2.101     TCP      60 443→47950 [ACK] Seq=5150 Ack=3940 Win=32736 Len=0
249 123.42299100 54.230.6.21   10.0.2.101     TCP      60 443→47950 [FIN, ACK] Seq=5150 Ack=3940 Win=32736 Len=0
250 123.42302200 10.0.2.101    54.230.6.21    TCP      54 47950→443 [ACK] Seq=3940 Ack=5151 Win=5232640 Len=0
251 126.44901300 10.0.2.101    54.230.6.21    TCP      54 [TCP Keep-Alive] 47924→443 [ACK] Seq=16545 Ack=129896 Win=8388480 Len=0
252 126.44926100 54.230.6.21   10.0.2.101     TCP      60 [TCP Keep-Alive ACK] 443→47924 [ACK] Seq=129896 Ack=16546 Win=32768 Len=0
253 136.46524300 10.0.2.101    54.230.6.21    TCP      54 [TCP Keep-Alive] 47924→443 [ACK] Seq=16545 Ack=129896 Win=8388480 Len=0
254 136.46566500 54.230.6.21   10.0.2.101     TCP      60 [TCP Keep-Alive ACK] 443→47924 [ACK] Seq=129896 Ack=16546 Win=32768 Len=0
255 141.36007700 10.0.2.101    54.230.6.21    TLSv1.2  85 Encrypted Alert
256 141.36020600 10.0.2.101    54.230.6.21    TCP      54 47924→443 [FIN, ACK] Seq=16577 Ack=129896 Win=8388480 Len=0
257 141.36050200 54.230.6.21   10.0.2.101     TCP      60 443→47924 [ACK] Seq=129896 Ack=16578 Win=32736 Len=0
258 141.37809700 54.230.6.21   10.0.2.101     TCP      60 443→47924 [FIN, ACK] Seq=129896 Ack=16578 Win=32736 Len=0
259 141.37812200 10.0.2.101    54.230.6.21    TCP      54 47924→443 [ACK] Seq=16578 Ack=129897 Win=96256 Len=0
```



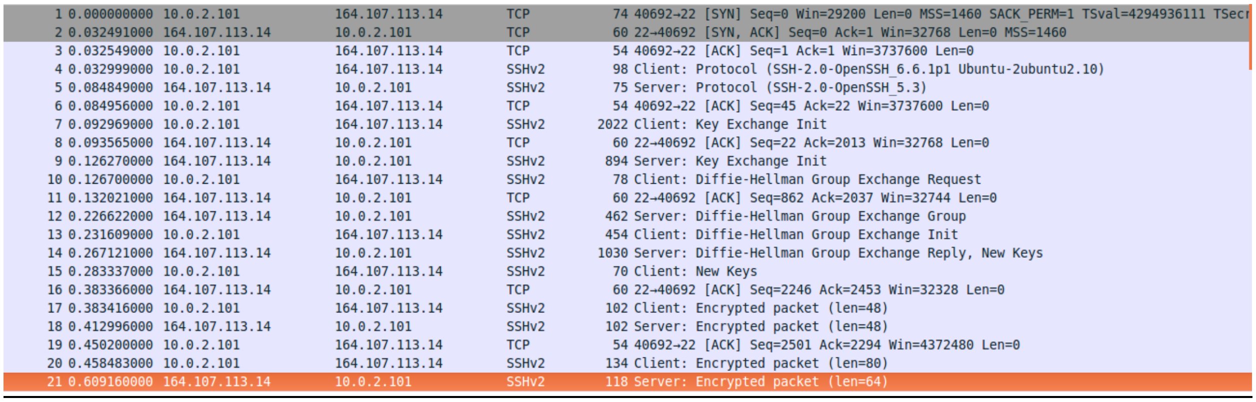
```
  Cipher Suites Length: 30
▼Cipher Suites (15 suites)
   Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
   Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
   Cipher Suite: Unknown (0xcca9)
   Cipher Suite: Unknown (0xcca8)
   Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
   Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
   Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
   Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
   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_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
   Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
   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)
```



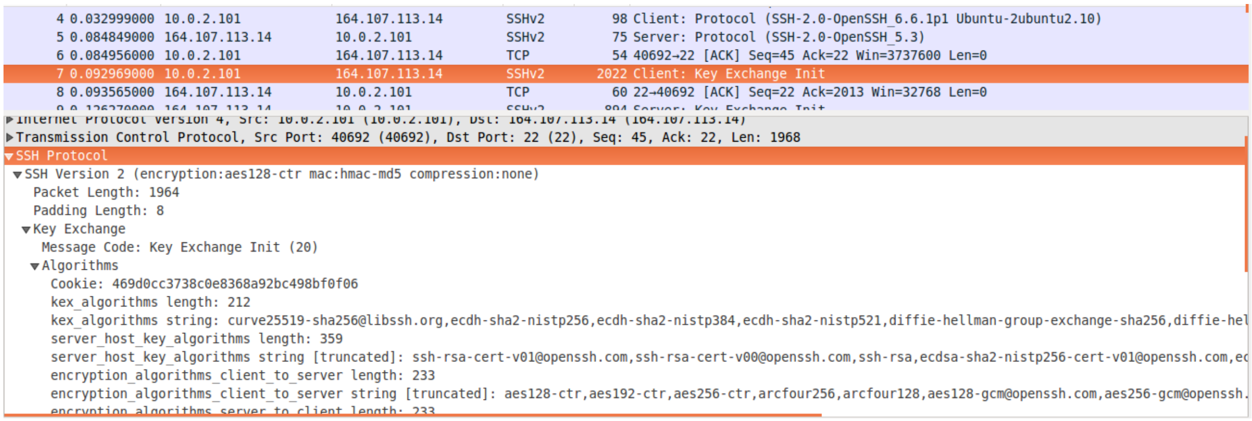
```
234 34.874744000 10.0.2.101          54.230.6.21         TCP          54 56628→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
235 34.875244000 10.0.2.101          54.230.6.21         TLSv1.2     571 Client Hello
236 34.895657000 54.230.6.21         10.0.2.101          TLSv1.2     210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
237 34.895687000 10.0.2.101          54.230.6.21         TCP          54 56628→443 [ACK] Seq=518 Ack=157 Win=3842048 Len=0
238 34.896185000 10.0.2.101          54.230.6.21         TLSv1.2     105 Change Cipher Spec, Encrypted Handshake Message
239 35.011782000 10.0.2.101          54.230.6.21         TLSv1.2    1265 Application Data
240 35.108407000 54.230.6.21         10.0.2.101          TCP          60 443→56544 [ACK] Seq=136204 Ack=20624 Win=32768 Len=0
241 35.108456000 54.230.6.21         10.0.2.101          TCP          60 443→56628 [ACK] Seq=157 Ack=569 Win=32200 Len=0
242 35.108458000 54.230.6.21         10.0.2.101          TCP        1514 [TCP segment of a reassembled PDU]
243 35.108466000 10.0.2.101          54.230.6.21         TCP          54 56544→443 [ACK] Seq=20624 Ack=137664 Win=8388480 Len=0
244 35.112242000 54.230.6.21         10.0.2.101          TLSv1.2     276 Application Data
245 35.112259000 10.0.2.101          54.230.6.21         TCP          54 56544→443 [ACK] Seq=20624 Ack=137886 Win=8388480 Len=0
246 35.117063000 10.0.2.101          54.230.6.21         TLSv1.2    1482 Application Data
247 35.200731000 54.230.6.21         10.0.2.101          TCP        1514 [TCP segment of a reassembled PDU]
248 35.202239000 54.230.6.21         10.0.2.101          TCP        1514 [TCP segment of a reassembled PDU]
249 35.202264000 10.0.2.101          54.230.6.21         TCP          54 56544→443 [ACK] Seq=22052 Ack=140806 Win=8388480 Len=0
250 35.204879000 54.230.6.21         10.0.2.101          TCP        4434 [TCP segment of a reassembled PDU]
251 35.204911000 10.0.2.101          54.230.6.21         TCP          54 56544→443 [ACK] Seq=22052 Ack=145186 Win=8388480 Len=0
252 35.206007000 54.230.6.21         10.0.2.101          TCP        2974 [TCP segment of a reassembled PDU]
253 35.206026000 10.0.2.101          54.230.6.21         TCP          54 56544→443 [ACK] Seq=22052 Ack=148106 Win=8388480 Len=0
```

The traffic for Amazon.com is actually very similar to task 2.3, thus all pages are protected by HTTPS. This can be seen in various ways. The first is that as you access the amazon webpage, by looking at the address bar, you can see the address has HTTPS in it. The second way this can be seen is in the record of communication between the client and the server from wireshark where it can be shown that the client and server send encrypted packets between each other beginning with a Client Hello packet from the client. As in task 2.3, the server responds with a Server Hello packet and a Certificate. The record of packets also shows a key exchange between the client and server. Basically it can be seen that the messages between the client and server are encrypted with an encryption and key that are agreed upon between the client and server. These messages are continuously sent between the client and server. Even as I logged in and looked through the amazon page and put items in my cart, the packets between the client and the server were encrypted. This leads me to believe that the website is secure as the webpage even before logging in requires an agreed upon encryption and key between the client and server to communicate with encrypted packets.

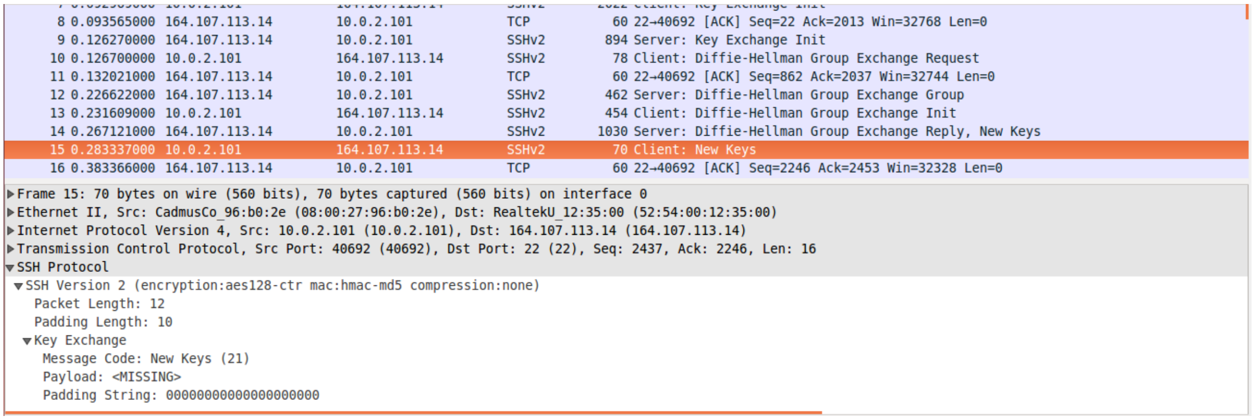
Task 2.5



```
  1 0.000000000  10.0.2.101       164.107.113.14     TCP          74 40692→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294936111 TSecr
  2 0.032491000  164.107.113.14   10.0.2.101         TCP          60 22→40692 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
  3 0.032549000  10.0.2.101       164.107.113.14     TCP          54 40692→22 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
  4 0.032999000  10.0.2.101       164.107.113.14     SSHv2        98 Client: Protocol (SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.10)
  5 0.084849000  164.107.113.14   10.0.2.101         SSHv2        75 Server: Protocol (SSH-2.0-OpenSSH_5.3)
  6 0.084956000  10.0.2.101       164.107.113.14     TCP          54 40692→22 [ACK] Seq=45 Ack=22 Win=3737600 Len=0
  7 0.092969000  10.0.2.101       164.107.113.14     SSHv2      2022 Client: Key Exchange Init
  8 0.093565000  164.107.113.14   10.0.2.101         TCP          60 22→40692 [ACK] Seq=22 Ack=2013 Win=32768 Len=0
  9 0.126270000  164.107.113.14   10.0.2.101         SSHv2       894 Server: Key Exchange Init
 10 0.126700000  10.0.2.101       164.107.113.14     SSHv2        78 Client: Diffie-Hellman Group Exchange Request
 11 0.132021000  164.107.113.14   10.0.2.101         TCP          60 22→40692 [ACK] Seq=862 Ack=2037 Win=32744 Len=0
 12 0.226622000  164.107.113.14   10.0.2.101         SSHv2       462 Server: Diffie-Hellman Group Exchange Group
 13 0.231609000  10.0.2.101       164.107.113.14     SSHv2       454 Client: Diffie-Hellman Group Exchange Init
 14 0.267121000  164.107.113.14   10.0.2.101         SSHv2      1030 Server: Diffie-Hellman Group Exchange Reply, New Keys
 15 0.283337000  10.0.2.101       164.107.113.14     SSHv2        70 Client: New Keys
 16 0.383366000  164.107.113.14   10.0.2.101         TCP          60 22→40692 [ACK] Seq=2246 Ack=2453 Win=32328 Len=0
 17 0.383416000  10.0.2.101       164.107.113.14     SSHv2       102 Client: Encrypted packet (len=48)
 18 0.412996000  164.107.113.14   10.0.2.101         SSHv2       102 Server: Encrypted packet (len=48)
 19 0.450200000  10.0.2.101       164.107.113.14     TCP          54 40692→22 [ACK] Seq=2501 Ack=2294 Win=4372480 Len=0
 20 0.458483000  10.0.2.101       164.107.113.14     SSHv2       134 Client: Encrypted packet (len=80)
 21 0.609160000  164.107.113.14   10.0.2.101         SSHv2       118 Server: Encrypted packet (len=64)
```

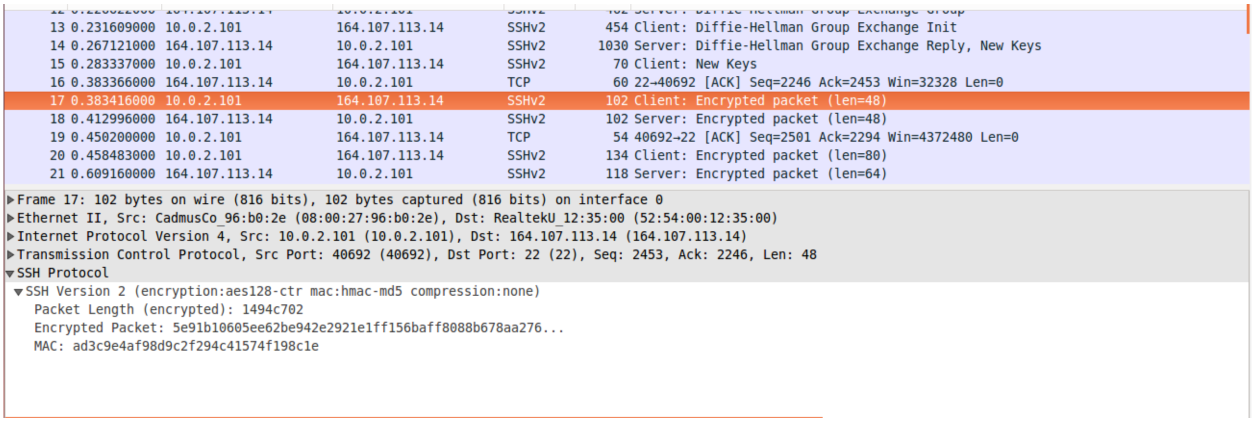


```
    4 0.032999000 10.0.2.101       164.107.113.14   SSHv2      98 Client: Protocol (SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.10)
    5 0.084849000 164.107.113.14   10.0.2.101       SSHv2      75 Server: Protocol (SSH-2.0-OpenSSH_5.3)
    6 0.084956000 10.0.2.101       164.107.113.14   TCP        54 40692→22 [ACK] Seq=45 Ack=22 Win=3737600 Len=0
    7 0.092969000 10.0.2.101       164.107.113.14   SSHv2    2022 Client: Key Exchange Init
    8 0.093565000 164.107.113.14   10.0.2.101       TCP        60 22→40692 [ACK] Seq=22 Ack=2013 Win=32768 Len=0
    9 0.126270000 164.107.113.14   10.0.2.101       SSHv2     894 Server: Key Exchange Init
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 164.107.113.14 (164.107.113.14)
▶Transmission Control Protocol, Src Port: 40692 (40692), Dst Port: 22 (22), Seq: 45, Ack: 22, Len: 1968
▼SSH Protocol
 ▼SSH Version 2 (encryption:aes128-ctr mac:hmac-md5 compression:none)
   Packet Length: 1964
   Padding Length: 8
  ▼Key Exchange
    Message Code: Key Exchange Init (20)
   ▼Algorithms
     Cookie: 469d0cc3738c0e8368a92bc498bf0f06
     kex_algorithms length: 212
     kex_algorithms string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hel
     server_host_key_algorithms length: 359
     server_host_key_algorithms string [truncated]: ssh-rsa-cert-v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-rsa,ecdsa-sha2-nistp256-cert-v01@openssh.com,ec
     encryption_algorithms_client_to_server length: 233
     encryption_algorithms_client_to_server string [truncated]: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.
     encryption_algorithms_server_to_client length: 233
```



```
    7 0.092969000 10.0.2.101       164.107.113.14   SSHv2    2022 Client: Key Exchange Init
    8 0.093565000 164.107.113.14   10.0.2.101       TCP        60 22→40692 [ACK] Seq=22 Ack=2013 Win=32768 Len=0
    9 0.126270000 164.107.113.14   10.0.2.101       SSHv2     894 Server: Key Exchange Init
   10 0.126700000 10.0.2.101       164.107.113.14   SSHv2      78 Client: Diffie-Hellman Group Exchange Request
   11 0.132021000 164.107.113.14   10.0.2.101       TCP        60 22→40692 [ACK] Seq=862 Ack=2037 Win=32744 Len=0
   12 0.226622000 164.107.113.14   10.0.2.101       SSHv2     462 Server: Diffie-Hellman Group Exchange Group
   13 0.231609000 10.0.2.101       164.107.113.14   SSHv2     454 Client: Diffie-Hellman Group Exchange Init
   14 0.267121000 164.107.113.14   10.0.2.101       SSHv2    1030 Server: Diffie-Hellman Group Exchange Reply, New Keys
   15 0.283337000 10.0.2.101       164.107.113.14   SSHv2      70 Client: New Keys
   16 0.383366000 164.107.113.14   10.0.2.101       TCP        60 22→40692 [ACK] Seq=2246 Ack=2453 Win=32328 Len=0

▶Frame 15: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶Ethernet II, Src: CadmusCo_96:b0:2e (08:00:27:96:b0:2e), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 164.107.113.14 (164.107.113.14)
▶Transmission Control Protocol, Src Port: 40692 (40692), Dst Port: 22 (22), Seq: 2437, Ack: 2246, Len: 16
▼SSH Protocol
 ▼SSH Version 2 (encryption:aes128-ctr mac:hmac-md5 compression:none)
   Packet Length: 12
   Padding Length: 10
  ▼Key Exchange
    Message Code: New Keys (21)
    Payload: <MISSING>
    Padding String: 00000000000000000000
```



```
   12 0.226622000 164.107.113.14   10.0.2.101       SSHv2     462 Server: Diffie-Hellman Group Exchange Group
   13 0.231609000 10.0.2.101       164.107.113.14   SSHv2     454 Client: Diffie-Hellman Group Exchange Init
   14 0.267121000 164.107.113.14   10.0.2.101       SSHv2    1030 Server: Diffie-Hellman Group Exchange Reply, New Keys
   15 0.283337000 10.0.2.101       164.107.113.14   SSHv2      70 Client: New Keys
   16 0.383366000 164.107.113.14   10.0.2.101       TCP        60 22→40692 [ACK] Seq=2246 Ack=2453 Win=32328 Len=0
   17 0.383416000 10.0.2.101       164.107.113.14   SSHv2     102 Client: Encrypted packet (len=48)
   18 0.412996000 164.107.113.14   10.0.2.101       SSHv2     102 Server: Encrypted packet (len=48)
   19 0.450200000 10.0.2.101       164.107.113.14   TCP        54 40692→22 [ACK] Seq=2501 Ack=2294 Win=4372480 Len=0
   20 0.458483000 10.0.2.101       164.107.113.14   SSHv2     134 Client: Encrypted packet (len=80)
   21 0.609160000 164.107.113.14   10.0.2.101       SSHv2     118 Server: Encrypted packet (len=64)

▶Frame 17: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
▶Ethernet II, Src: CadmusCo_96:b0:2e (08:00:27:96:b0:2e), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▶Internet Protocol Version 4, Src: 10.0.2.101 (10.0.2.101), Dst: 164.107.113.14 (164.107.113.14)
▶Transmission Control Protocol, Src Port: 40692 (40692), Dst Port: 22 (22), Seq: 2453, Ack: 2246, Len: 48
▼SSH Protocol
 ▼SSH Version 2 (encryption:aes128-ctr mac:hmac-md5 compression:none)
   Packet Length (encrypted): 1494c702
   Encrypted Packet: 5e91b10605ee62be942e2921e1ff156baff8088b678aa276...
   MAC: ad3c9e4af98d9c2f294c41574f198c1e
```

After the initial TCP handshake the client sends a SSH protocol message to the server with the info: Client: Protocol, to which the server responds with a Server: Protocol. After that the client initiates a Key Exchange with the server. The client sends encryption key algorithms to the server and the server also sends encryption algorithms to the client, where the algorithms all have different lengths. The client and server also send packets with the label of Diffie-Hellman Group Exchange to each other. Thus after agreeing encryption schemes and keys, the client and server send encrypted packets of differing lengths to each other. Other than ACK, TCP protocol messages, all the packets seem to be encrypted between the client and server, thus I am unable to intercept my own password.