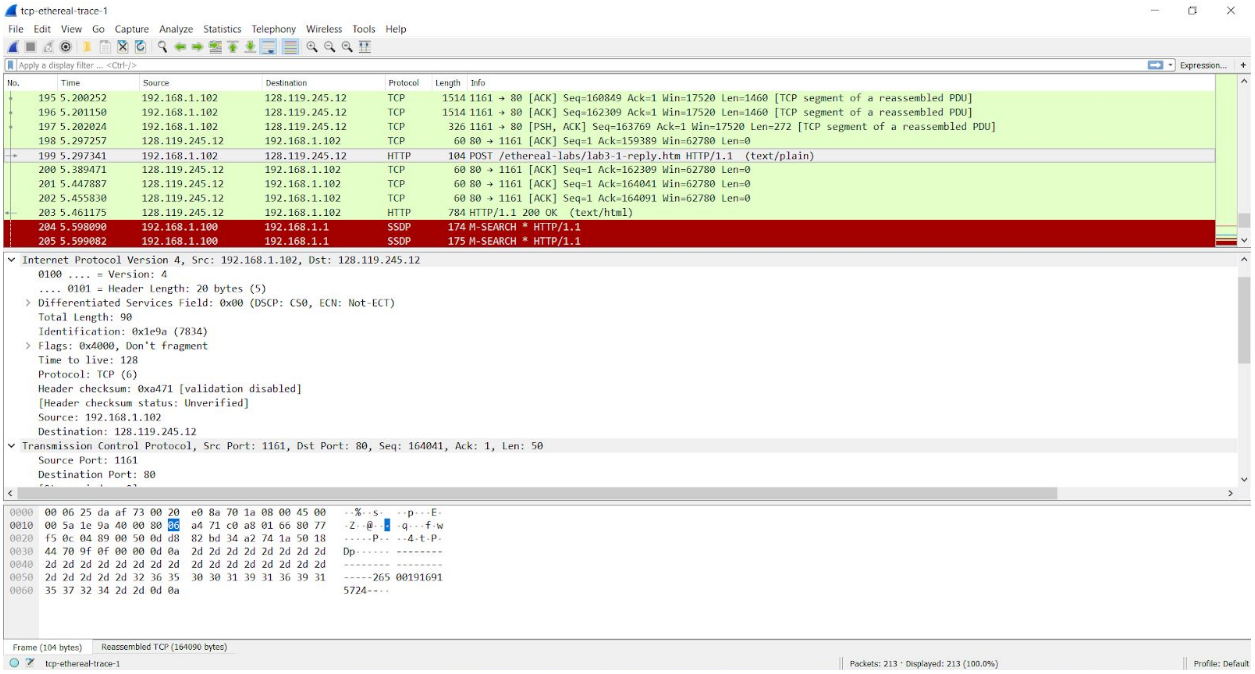
60-367 Assignment 2
Calvin Moras, Ryan Lebeau
104448832 - 104535367

TCP

1. The IP address used by the client computer is 192.168.1.102 and the TCP port used is 1161.
2. The IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP request is being received through port 80.

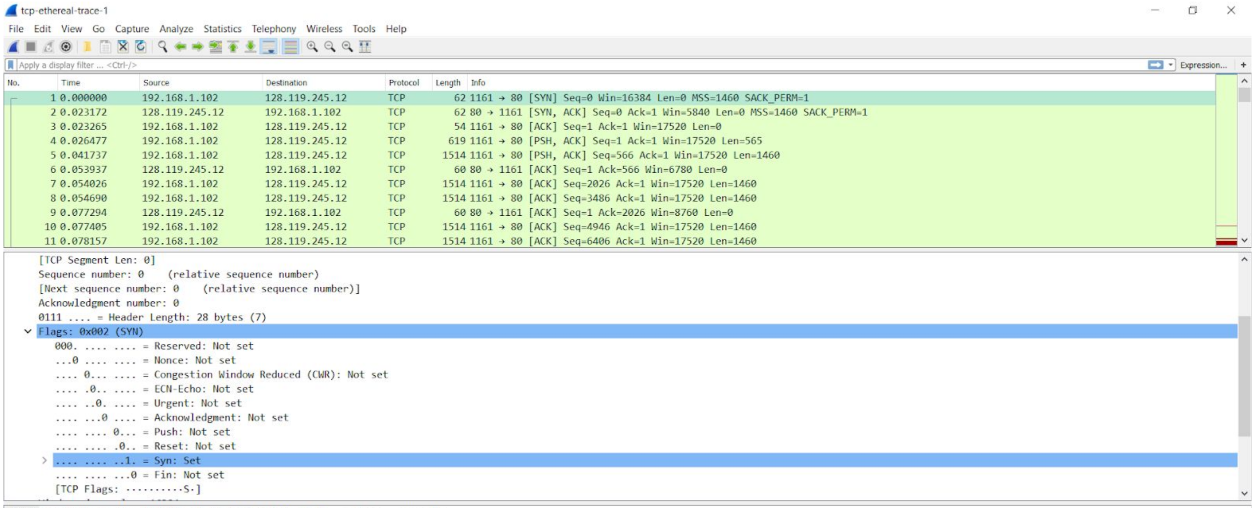


```
No.  Time      Source          Destination     Protocol Length Info
 195 5.200252  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=160849 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
 196 5.201150  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
 197 5.202024  192.168.1.102   128.119.245.12  TCP       326 1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=17520 Len=272 [TCP segment of a reassembled PDU]
 198 5.297257  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780 Len=0
 199 5.297341  192.168.1.102   128.119.245.12  HTTP      104 POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
 200 5.389471  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
 201 5.447887  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
 202 5.455830  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
 203 5.461175  128.119.245.12  192.168.1.102   HTTP      784 HTTP/1.1 200 OK  (text/html)
 204 5.598090  192.168.1.100   192.168.1.1     SSDP      174 M-SEARCH * HTTP/1.1
 205 5.599082  192.168.1.100   192.168.1.1     SSDP      175 M-SEARCH * HTTP/1.1
```

```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 90
    Identification: 0x1e9a (7834)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xa471 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
    Source Port: 1161
    Destination Port: 80
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  00 5a 1e 9a 40 00 80 06  a4 71 c0 a8 01 66 80 77   ·Z··@···  ·q···f·w
0020  f5 0c 04 89 00 50 0d d8  82 bd 34 a2 74 1a 50 18   ·····P··  ··4·t·P·
0030  44 70 9f 0f 00 00 0d 0a  2d 2d 2d 2d 2d 2d 2d 2d   Dp······  --------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0050  2d 2d 2d 2d 2d 32 36 35  30 30 31 39 31 36 39 31   -----265  00191691
0060  35 37 32 34 2d 2d 0d 0a                            5724--··
```

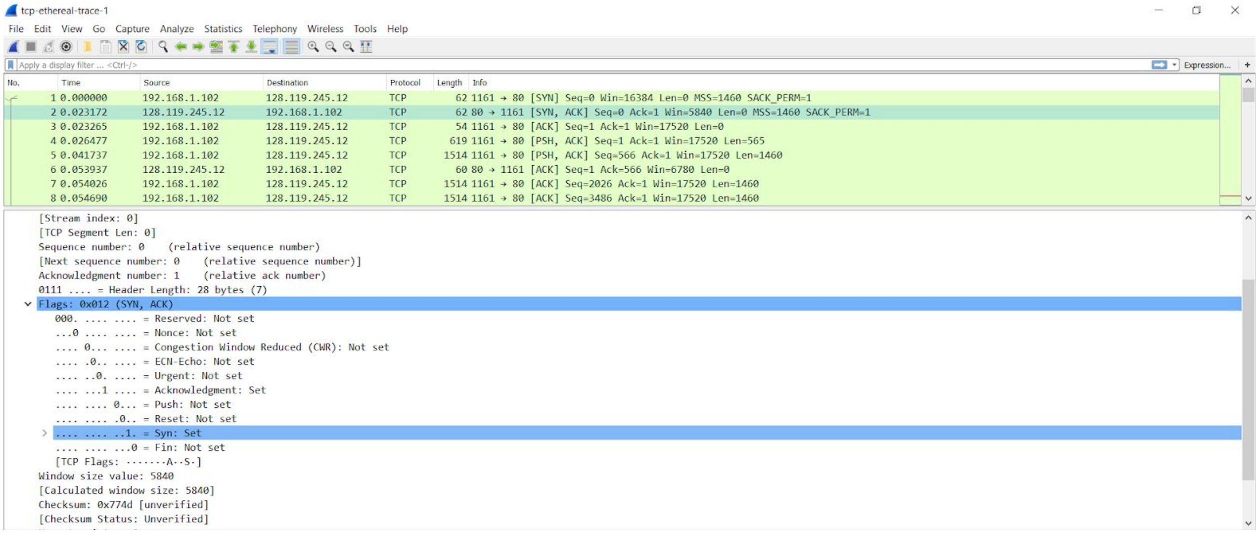
3. I have not been able to create my own trace.
4. The sequence number of the TCP SYN segment that initiated the connection is 0 and the SYN flag is set to 1 to identify that it is a SYN segment.



```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
   5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
   6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
   7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
   8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
   9 0.077294  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
  10 0.077405  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
  11 0.078157  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
```

```
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
```

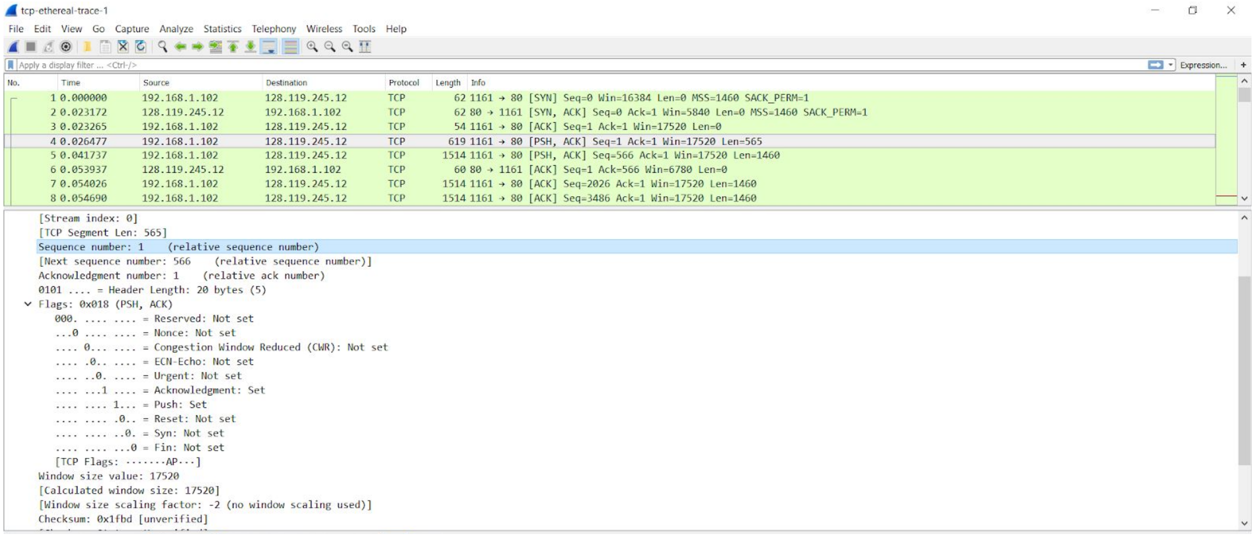
5. The sequence number of the TCP SYNACK is 0 and the acknowledgement field is set to 1, which is obtained by adding to the original SYN’s acknowledgement field. Both the SYN and the ACK fields are set to 1 to determine it is a SYNACK.


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time        Source           Destination      Protocol  Length  Info
   1 0.000000    192.168.1.102    128.119.245.12   TCP         62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   2 0.023172    128.119.245.12   192.168.1.102    TCP         62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.023265    192.168.1.102    128.119.245.12   TCP         54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   4 0.026477    192.168.1.102    128.119.245.12   TCP        619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
   5 0.041737    192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
   6 0.053937    128.119.245.12   192.168.1.102    TCP         60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
   7 0.054026    192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
   8 0.054690    192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
```

```
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0111 .... = Header Length: 28 bytes (7)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window size value: 5840
    [Calculated window size: 5840]
    Checksum: 0x774d [unverified]
    [Checksum Status: Unverified]
```

6. The sequence number of the TCP segment containing the HTTP POST is 1.


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time        Source           Destination      Protocol  Length  Info
   1 0.000000    192.168.1.102    128.119.245.12   TCP         62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   2 0.023172    128.119.245.12   192.168.1.102    TCP         62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.023265    192.168.1.102    128.119.245.12   TCP         54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   4 0.026477    192.168.1.102    128.119.245.12   TCP        619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
   5 0.041737    192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
   6 0.053937    128.119.245.12   192.168.1.102    TCP         60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
   7 0.054026    192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
   8 0.054690    192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
```

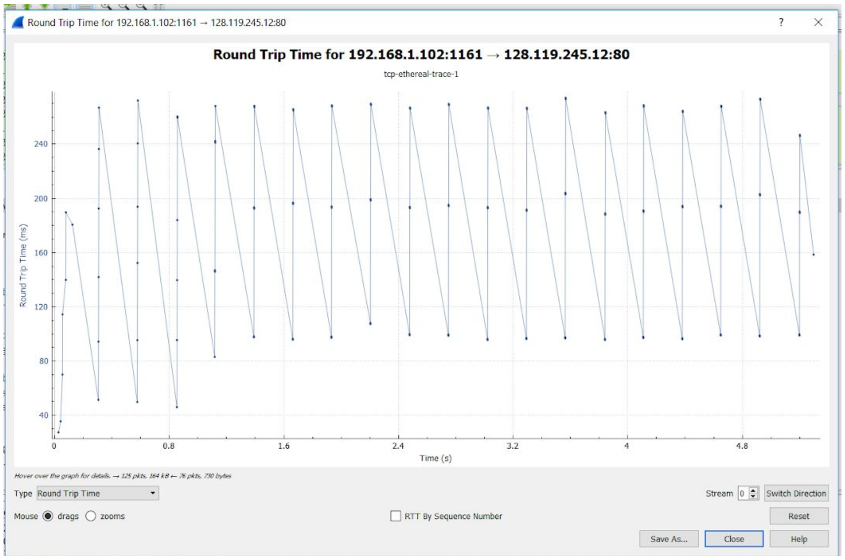
```
    [Stream index: 0]
    [TCP Segment Len: 565]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 566    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1fbd [unverified]
```

7. The first six segments have sequence numbers 1,566,2026,3486,4946,6406 respectively. The table outlines segment sent time, ACK received time, and RTT.

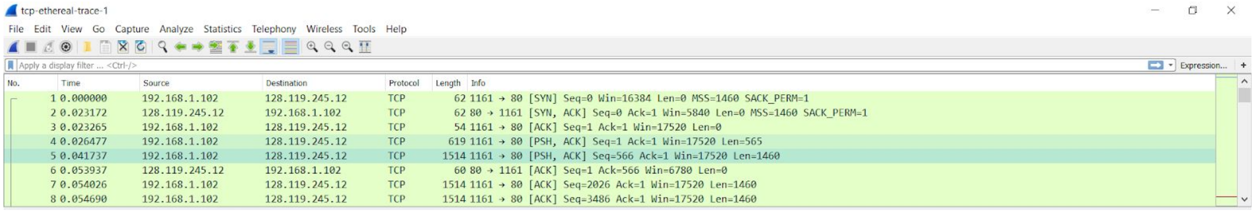
Segment	Time Sent(s)	ACK Time(s)	RTT(s)
1	0.0264	0.0539	0.027
2	0.0417	0.0772	0.035
3	0.0540	0.1240	0.070
4	0.0546	0.1691	0.114

5	0.0774	0.2172	0.139
6	0.0781	0.2678	0.189

Segment 1 EstimatedRTT=0.027
Segment 2 EstimatedRTT=0.029
Segment 3 EstimatedRTT=0.038
Segment 4 EstimatedRTT=0.044
Segment 5 EstimatedRTT=0.056
Segment 6 EstimatedRTT=0.073

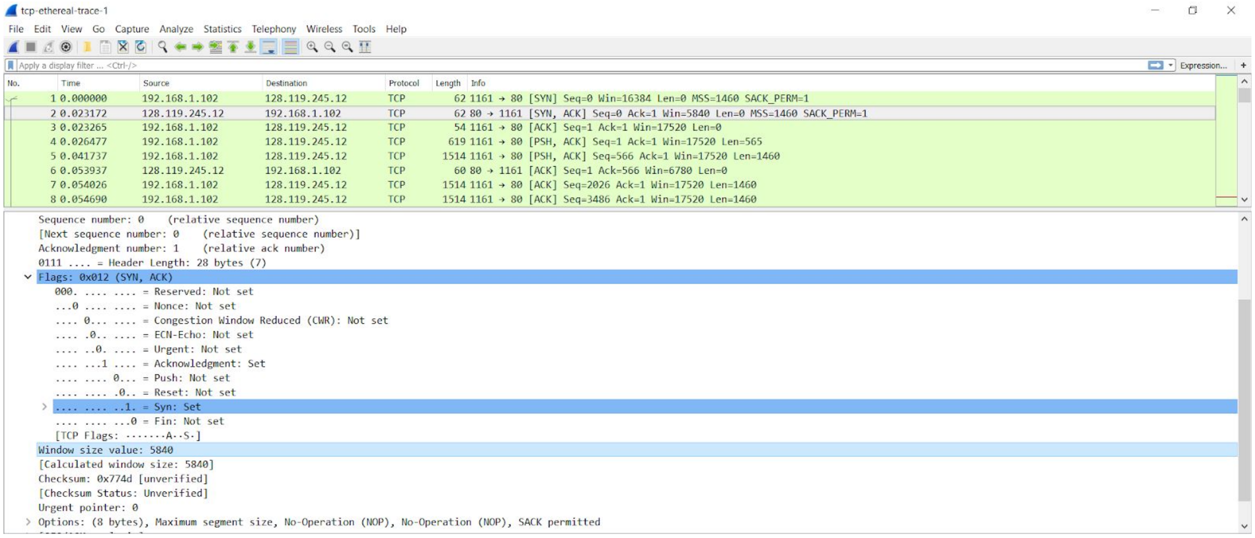


8. The first HTTP POST segment is only 565 bytes and the other 5 are all 1460 bytes.


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source           Destination      Protocol  Length  Info
    1 0.000000  192.168.1.102    128.119.245.12   TCP         62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
    2 0.023172  128.119.245.12   192.168.1.102    TCP         62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
    3 0.023265  192.168.1.102    128.119.245.12   TCP         54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
    4 0.026477  192.168.1.102    128.119.245.12   TCP        619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
    5 0.041737  192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
    6 0.053937  128.119.245.12   192.168.1.102    TCP         60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
    7 0.054026  192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
    8 0.054690  192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
```

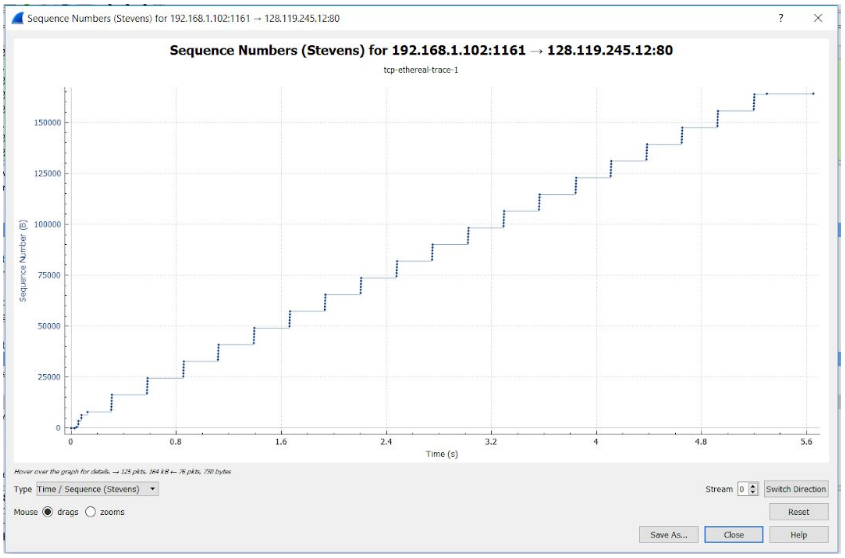
9. The first ACK sent shows a size value of 5840 bytes and the last segment is at size 62780 bytes with no slow down of growth within the segments, therefore the sender is never throttled.


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

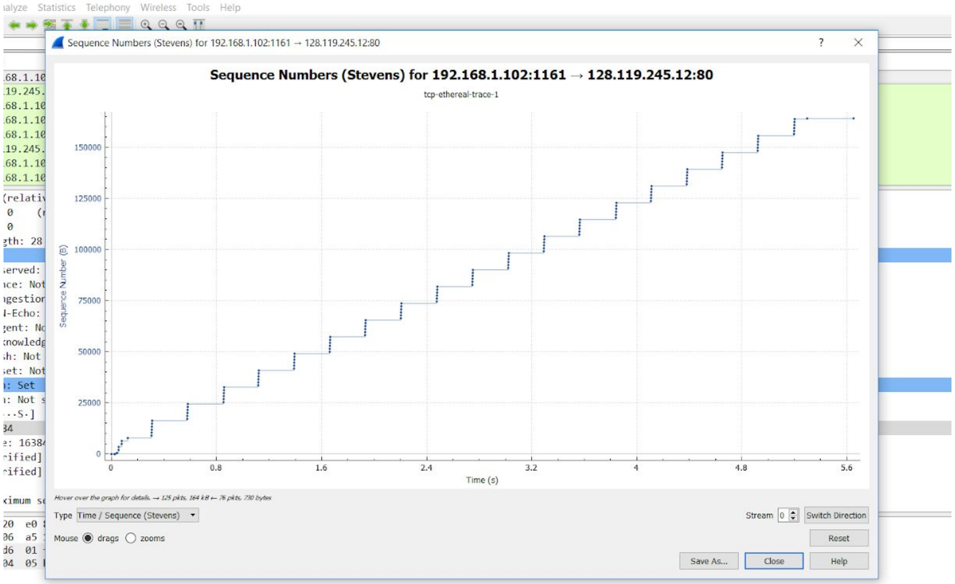
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
   5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
   6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
   7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
   8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
```

```
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0111 .... = Header Length: 28 bytes (7)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window size value: 5840
    [Calculated window size: 5840]
    Checksum: 0x774d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

10. The Time-Sequence graph (stevens) of this trace shows that there are no retransmitted segments, since every steadily increases with respect to time.



11. The receiver typically acknowledges the difference between the current and previous sequence number (eg. ack2 and ack1 sequence number are 2026 and 566, the acknowledged data for ack2 is 1460).
12. The throughput is calculated by TotalData/TotalTime=Throughput. The total data is 164091-1=164090bytes (last ACK - first ACK bytes) and the total time is 5.456-0.0265=5.429s (time of last ACK - time of first ACK). Therefore the throughput is 164090b/5.429s=30224b/s or 30.224kb/s.
13. The TCP slow start phase begins at the HTTP POST, and the end of slowstart / beginning of congestion state can not be clearly viewed since the sender never actually sends enough data to trigger a clear change in states. The main difference between studied TCP behaviour and the behaviour we experienced is that the idealized behaviour of TCP segments congest the network since mass amounts of data are being sent. In this trace example though, that is not happening and a clear change from slow start to congestion phase is never witnessed.



Hover over the graph for details. → 125 pkts, 164 kB ← 76 pkts, 730 bytes

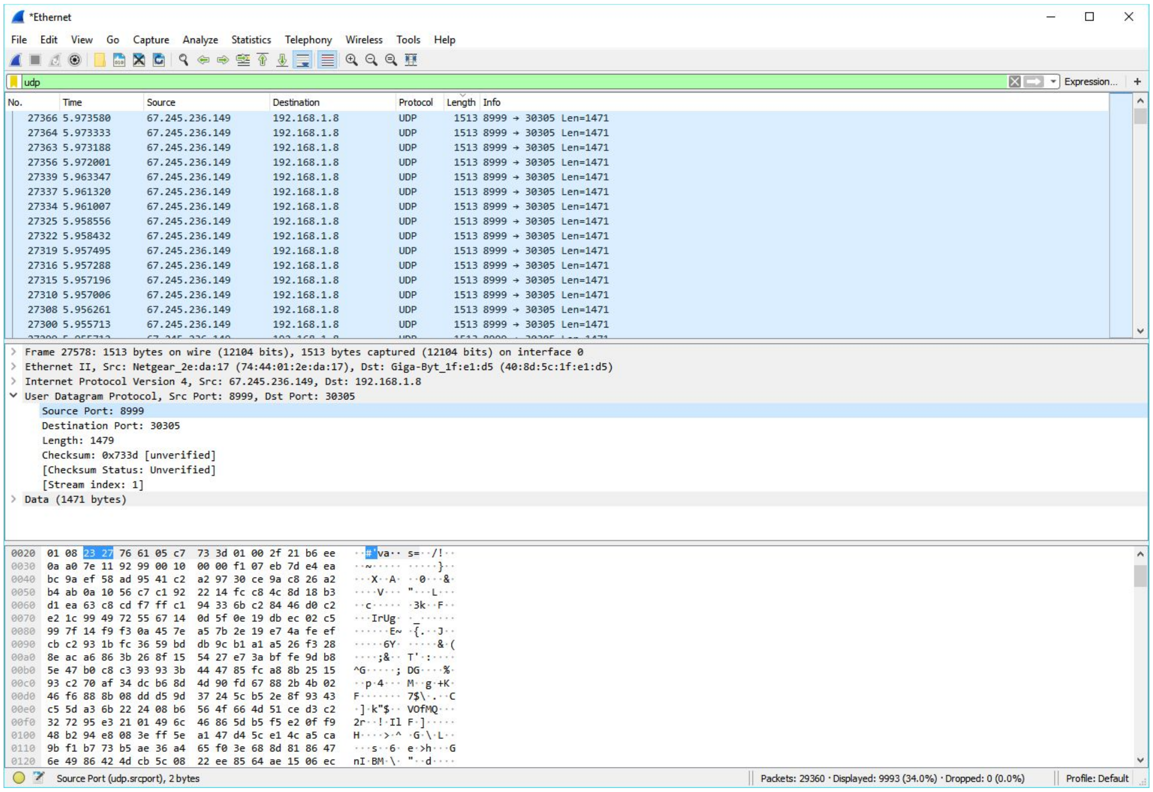
Type Time / Sequence (Stevens)

Stream 0

Mouse ● drags ○ zooms

UDP

1. Although the UDP field appears to contain 6 headers, headers enclosed with square brackets are fields generated by wireshark. The main fields contained in the UDP packet are therefore Source Port, Destination Port, Length, and Checksum. The last two are calculations made by wireshark after collecting the packet data, although the verification appears to be switched off by default.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp

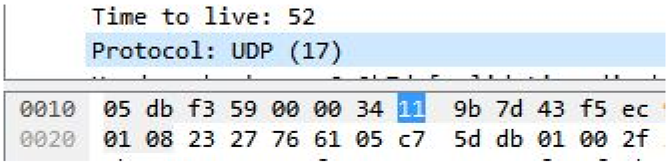
```
No.   Time     Source          Destination  Protocol Length Info
27366 5.973580 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27364 5.973333 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27363 5.973188 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27356 5.972001 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27339 5.963347 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27337 5.961320 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27334 5.961007 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27325 5.958556 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27322 5.958432 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27319 5.957495 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27316 5.957288 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27315 5.957196 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27310 5.957006 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27308 5.956261 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
27300 5.955713 67.245.236.149  192.168.1.8  UDP      1513 8999 → 30305 Len=1471
```

```
> Frame 27578: 1513 bytes on wire (12104 bits), 1513 bytes captured (12104 bits) on interface 0
> Ethernet II, Src: Netgear_2e:da:17 (74:44:01:2e:da:17), Dst: Giga-Byt_1f:e1:d5 (40:8d:5c:1f:e1:d5)
> Internet Protocol Version 4, Src: 67.245.236.149, Dst: 192.168.1.8
v User Datagram Protocol, Src Port: 8999, Dst Port: 30305
    Source Port: 8999
    Destination Port: 30305
    Length: 1479
    Checksum: 0x733d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
> Data (1471 bytes)
```

```
0020  01 08 23 27 76 61 05 c7  73 3d 01 00 2f 21 b6 ee   ··#'va·· s=··/!··
0030  0a a0 7e 11 92 99 00 10  00 00 f1 07 eb 7d e4 ea   ··~····· ·····}··
0040  bc 9a ef 58 ad 95 41 c2  a2 97 30 ce 9a c8 26 a2   ···X··A· ··0···&·
0050  b4 ab 0a 10 56 c7 c1 92  22 14 fc c8 4c 8d 18 b3   ····V··· "···L···
0060  d1 ea 63 c8 cd f7 ff c1  94 33 6b c2 84 46 d0 c2   ··c····· ·3k··F··
0070  e2 1c 99 49 72 55 67 14  0d 5f 0e 19 db ec 02 c5   ···IrUg· ·_······
0080  99 7f 14 f9 f3 0a 45 7e  a5 7b 2e 19 e7 4a fe ef   ······E~ ·{.··J··
0090  cb c2 93 1b fc 36 59 bd  db 9c b1 a1 a5 26 f3 28   ·····6Y· ·····&·(
00a0  8e ac a6 86 3b 26 8f 15  54 27 e7 3a bf fe 9d b8   ····;&·· T'·:····
00b0  5e 47 b0 c8 c3 93 93 3b  44 47 85 fc a8 8b 25 15   ^G·····; DG····%·
00c0  93 c2 70 af 34 dc b6 8d  4d 90 fd 67 88 2b 4b 02   ··p·4··· M··g·+K·
00d0  46 f6 88 8b 08 dd d5 9d  37 24 5c b5 2e 8f 93 43   F······· 7$\·.··C
00e0  c5 5d a3 6b 22 24 08 b6  56 4f 66 4d 51 ce d3 c2   ·]·k"$·· VOfMQ···
00f0  32 72 95 e3 21 01 49 6c  46 86 5d b5 f5 e2 0f f9   2r··!·Il F·]·····
0100  48 b2 94 e8 08 3e ff 5e  a1 47 d4 5c e1 4c a5 ca   H····>·^ ·G·\·L··
0110  9b f1 b7 73 b5 ae 36 a4  65 f0 3e 68 8d 81 86 47   ···s··6· e·>h···G
0120  6e 49 86 42 4d cb 5c 08  22 ee 85 64 ae 15 06 ec   nI·BM·\· "··d····
```

```
Source Port (udp.srcport), 2 bytes    Packets: 29360 · Displayed: 9993 (34.0%) · Dropped: 0 (0.0%)    Profile: Default
```

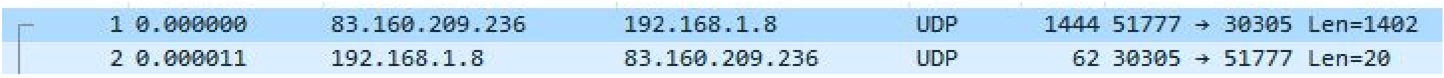
2. Using the same packet being referenced above, the initial source port header was 2 bytes, and the remaining 3 headers were also 2 bytes.
3. The value in the length field is the total size of the packet, that being the size of the data transmitted + the headers. In the case of my packet being examined above, the length is 1479 bytes, which come from 1471 bytes of data plus 8 bytes (4 headers x 2 bytes) of header information.
4. The maximum length of data that could possibly be contained in a UDP packet is 2^16 - 1 or 65535 bytes. One easy way to see this is by noting that the hex values displayed in wireshark have a maximum value of FFFF in hex in the left-hand column. It is worth noting however that is is the overall frame size and does not account for the 8 bytes required for the header, dropping the value to 65627. Further research into the UDP protocol however reveals that an additional 20 bytes are also reserved for a standard IPV4 IP header.
5. The largest source port number is also 2^16-1, 65535.
6. UDP is protocol number 17 or 0x11 in hex:



```
Time to live: 52
Protocol: UDP (17)

0010  05 db f3 59 00 00 34 11  9b 7d 43 f5 ec
0020  01 08 23 27 76 61 05 c7  5d db 01 00 2f
```

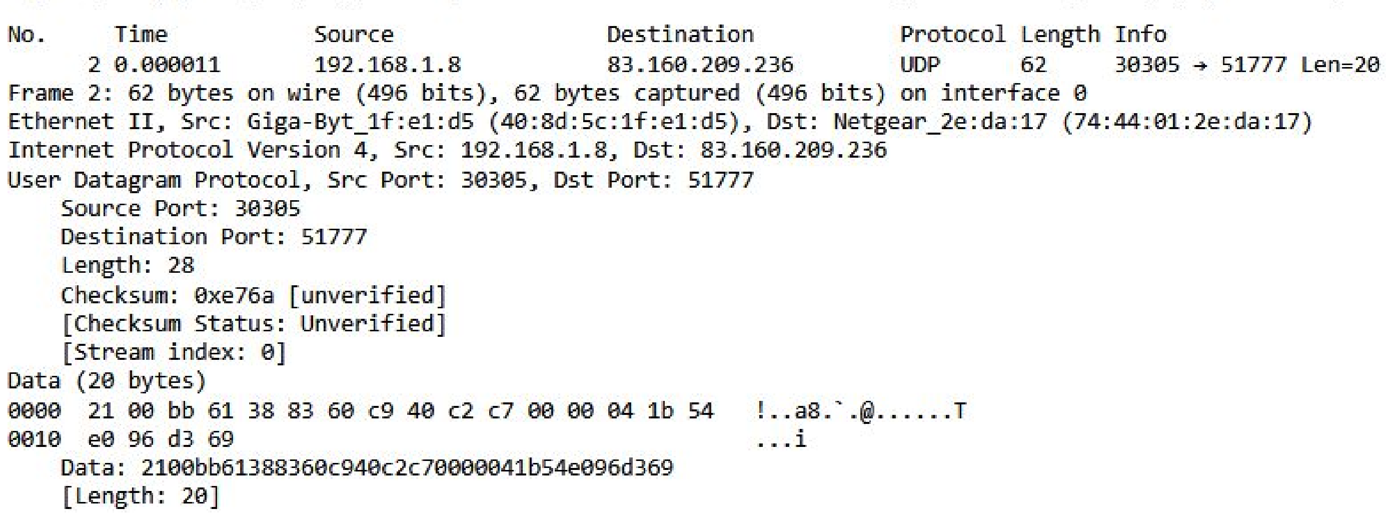
7.



```
1 0.000000    83.160.209.236    192.168.1.8       UDP    1444 51777 → 30305 Len=1402
2 0.000011    192.168.1.8       83.160.209.236    UDP      62 30305 → 51777 Len=20
```

For the two packets being examined above, it can be shown that the first packet was sent from the 83.160.209.236 IP on the 51777 source port, to the IP 192.168.1.8 (my machine's local IP on this network) on the 30305 destination port. This port is the port I have specificied my torrent client to direct UDP traffic through. The next packet is a 20 byte response from my machine through the destination port, to the other client's IP and source port (IE the source / destination information in the first packet is the opposite of the second). The length of this response is only 28 bytes, 8 being the headers. However it is worth mentioning that the remaining 20 bytes are not in fact from the IP header mentioned previously, as wireshark excludes this from the packet length field. Since this was the response for a torrent piece, it was more than likely my client telling the other client the checksum for the piece was correct, or something of this nature.

Also included is this snapshot of the response packet printout examined for 7:



```
No.     Time           Source                Destination           Protocol Length Info
      2 0.000011       192.168.1.8           83.160.209.236        UDP      62     30305 → 51777 Len=20
Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Giga-Byt_1f:e1:d5 (40:8d:5c:1f:e1:d5), Dst: Netgear_2e:da:17 (74:44:01:2e:da:17)
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 83.160.209.236
User Datagram Protocol, Src Port: 30305, Dst Port: 51777
    Source Port: 30305
    Destination Port: 51777
    Length: 28
    Checksum: 0xe76a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Data (20 bytes)
0000  21 00 bb 61 38 83 60 c9 40 c2 c7 00 00 04 1b 54   !..a8.`.@......T
0010  e0 96 d3 69                                       ...i
    Data: 2100bb61388360c940c2c70000041b54e096d369
    [Length: 20]
```