Tasks

1. Perform `ping` of various packet length (`0B` , `32B` , `65500B`) and observe.
2. `tracert` to IP/Name to local and external server
3. Observer web request with 3-tabs (TCP/HTTP - ports)

Task 1: ping to 10.1.3.17

Source Machine: 10.1.3.33
Destination Machine: 10.1.3.17

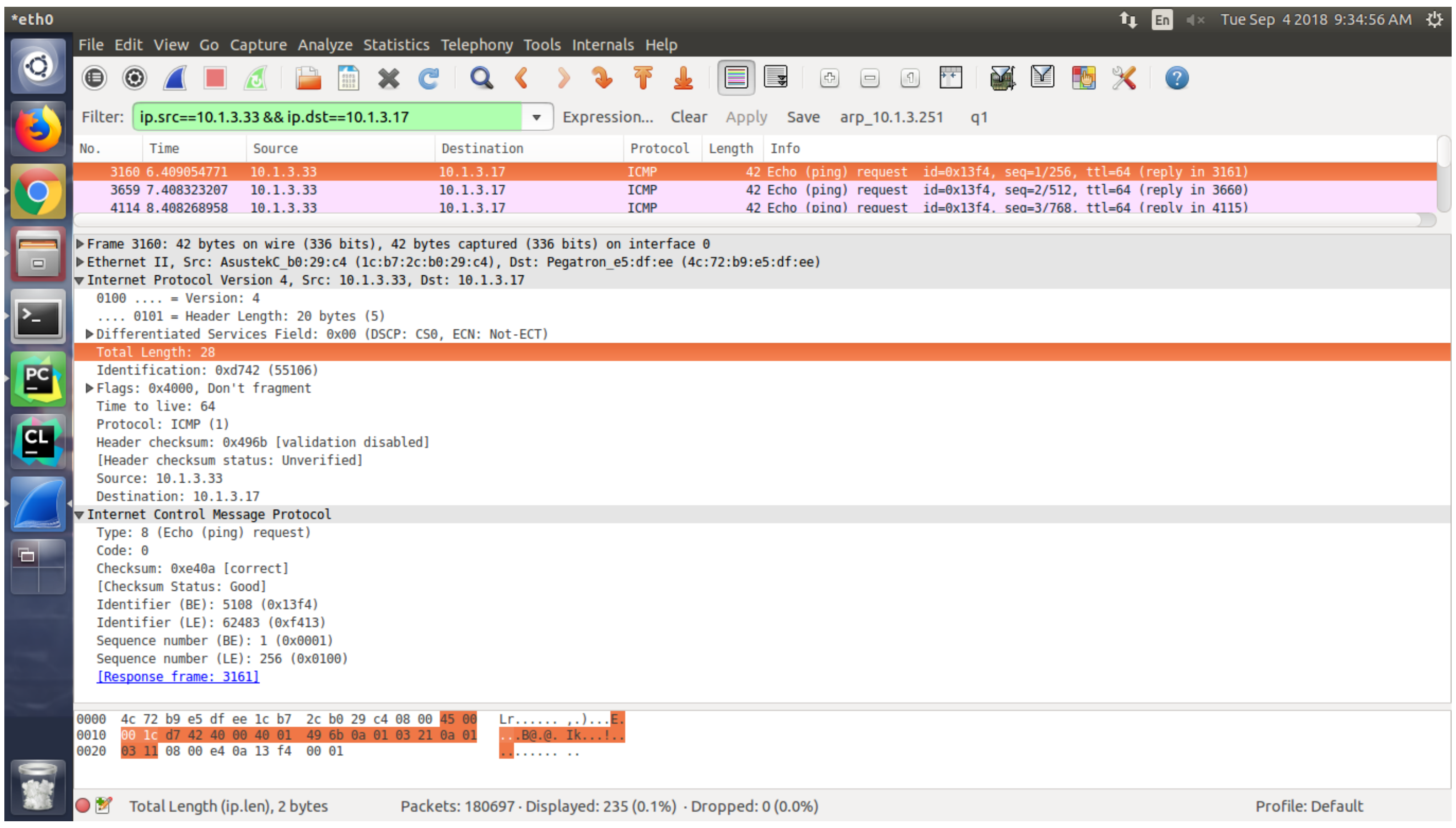
Ping with payload `0 bytes`

```
ping -s 0 10.1.3.17
```

Wireshark Filter:

```
ip.src == 10.1.3.33 && ip.dst == 10.1.3.17
```

Result:


*eth0
Tue Sep 4 2018 9:34:56 AM
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save arp_10.1.3.251 q1

```
Filter: ip.src==10.1.3.33 && ip.dst==10.1.3.17

No.  Time         Source      Destination  Protocol  Length  Info
3160 6.409054771  10.1.3.33   10.1.3.17    ICMP      42 Echo (ping) request  id=0x13f4, seq=1/256, ttl=64 (reply in 3161)
3659 7.408323207  10.1.3.33   10.1.3.17    ICMP      42 Echo (ping) request  id=0x13f4, seq=2/512, ttl=64 (reply in 3660)
4114 8.408268958  10.1.3.33   10.1.3.17    ICMP      42 Echo (ping) request  id=0x13f4, seq=3/768, ttl=64 (reply in 4115)

▶Frame 3160: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Pegatron_e5:df:ee (4c:72:b9:e5:df:ee)
▼Internet Protocol Version 4, Src: 10.1.3.33, Dst: 10.1.3.17
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
  ▶Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 28
   Identification: 0xd742 (55106)
  ▶Flags: 0x4000, Don't fragment
   Time to live: 64
   Protocol: ICMP (1)
   Header checksum: 0x496b [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.1.3.33
   Destination: 10.1.3.17
▼Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xe40a [correct]
   [Checksum Status: Good]
   Identifier (BE): 5108 (0x13f4)
   Identifier (LE): 62483 (0xf413)
   Sequence number (BE): 1 (0x0001)
   Sequence number (LE): 256 (0x0100)
   [Response frame: 3161]

0000  4c 72 b9 e5 df ee 1c b7  2c b0 29 c4 08 00 45 00   Lr...... ,.)...E.
0010  00 1c d7 42 40 00 40 01  49 6b 0a 01 03 21 0a 01   ...B@.@. Ik...!..
0020  03 11 08 00 e4 0a 13 f4  00 01                     ........ ..

Total Length (ip.len), 2 bytes    Packets: 180697 · Displayed: 235 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

ICMP echo request or echo reply packet's minimum size is `28 bytes` as described below:

> 20 byte IP header + 4 byte ICMP header + 4 byte echo request/reply header data + 0 bytes of ICMP payload data.

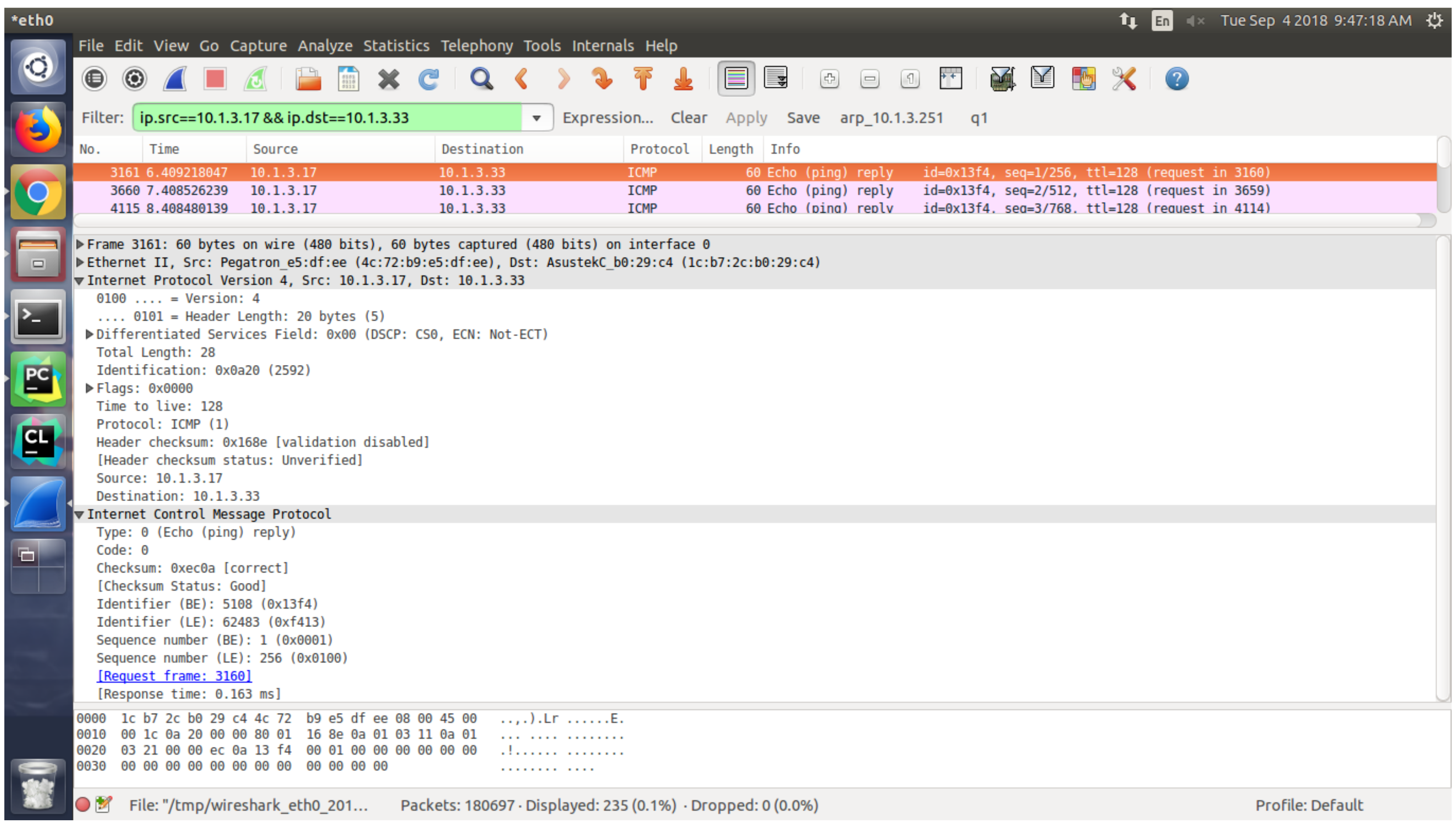
Ethernet frame header will be `18 bytes` (`14 B` MAC header and `4 B` checksum)
As shown in above snapshot packet length of `0 B` payload is `42 B` total (as wireshark ignores checksum)

However for response the packet size would be `60 B` (ignoring `4 B` checksum) because minimum frame size in
Ethernet is `64 B` and hence before transmitting the packets source ethernet will pad dummy bytes and hence response in wireshark is observed as below:

Wireshark Filter:

```
ip.src == 10.1.3.17 && ip.dst == 10.1.3.33
```

Result:



```
Filter: ip.src==10.1.3.17 && ip.dst==10.1.3.33

No.   Time         Source       Destination  Protocol Length Info
 3161 6.409218047  10.1.3.17    10.1.3.33    ICMP     60 Echo (ping) reply   id=0x13f4, seq=1/256, ttl=128 (request in 3160)
 3660 7.408526239  10.1.3.17    10.1.3.33    ICMP     60 Echo (ping) reply   id=0x13f4, seq=2/512, ttl=128 (request in 3659)
 4115 8.408480139  10.1.3.17    10.1.3.33    ICMP     60 Echo (ping) reply   id=0x13f4, seq=3/768, ttl=128 (request in 4114)

▶Frame 3161: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶Ethernet II, Src: Pegatron_e5:df:ee (4c:72:b9:e5:df:ee), Dst: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4)
▼Internet Protocol Version 4, Src: 10.1.3.17, Dst: 10.1.3.33
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
  ▶Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 28
   Identification: 0x0a20 (2592)
  ▶Flags: 0x0000
   Time to live: 128
   Protocol: ICMP (1)
   Header checksum: 0x168e [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.1.3.17
   Destination: 10.1.3.33
▼Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: 0xec0a [correct]
   [Checksum Status: Good]
   Identifier (BE): 5108 (0x13f4)
   Identifier (LE): 62483 (0xf413)
   Sequence number (BE): 1 (0x0001)
   Sequence number (LE): 256 (0x0100)
   [Request frame: 3160]
   [Response time: 0.163 ms]

0000  1c b7 2c b0 29 c4 4c 72  b9 e5 df ee 08 00 45 00   ..,.).Lr ......E.
0010  00 1c 0a 20 00 00 80 01  16 8e 0a 01 03 11 0a 01   ... .... ........
0020  03 21 00 00 ec 0a 13 f4  00 01 00 00 00 00 00 00   .!...... ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "/tmp/wireshark_eth0_201...   Packets: 180697 · Displayed: 235 (0.1%) · Dropped: 0 (0.0%)   Profile: Default
```

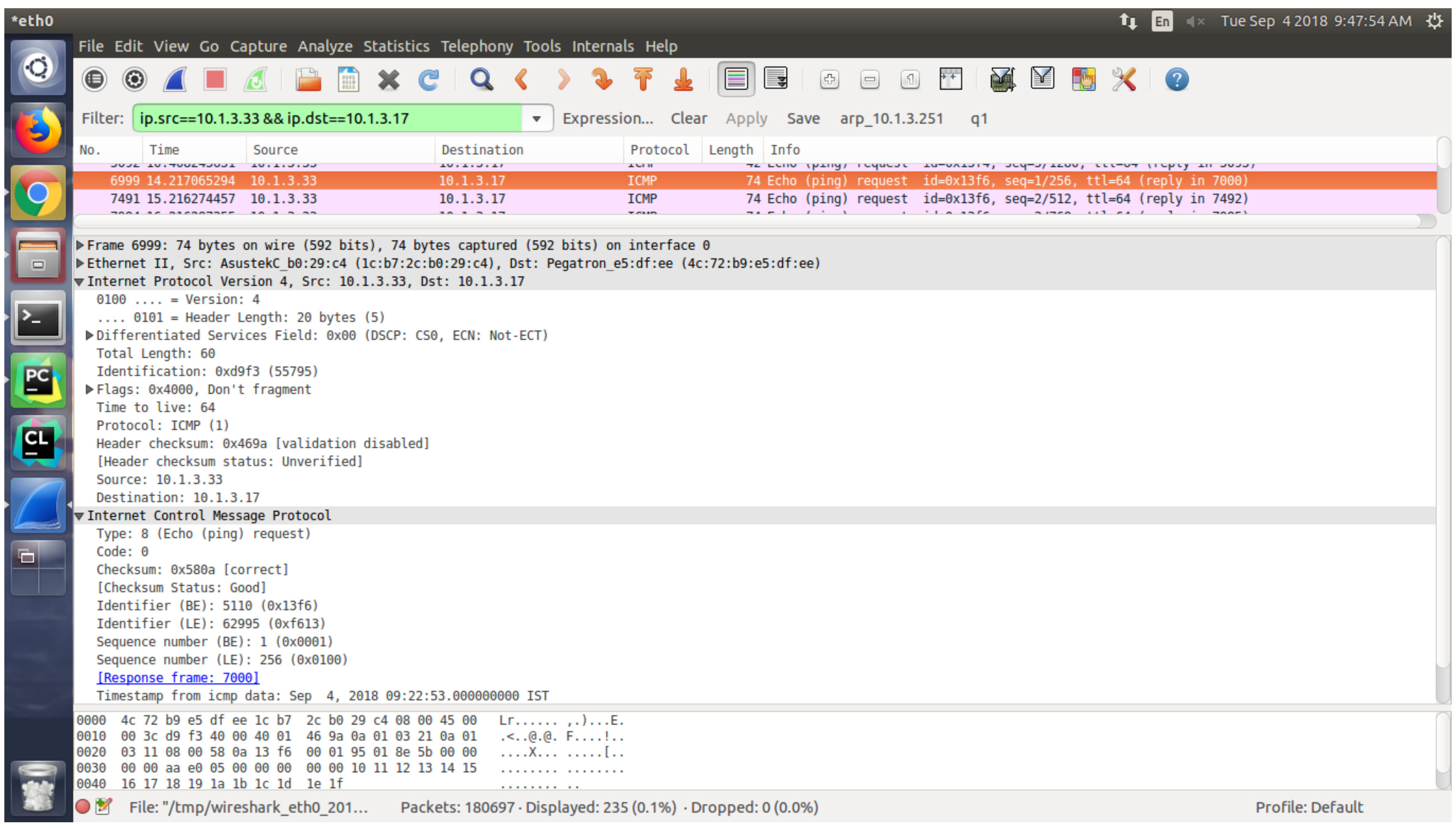
Ping with payload `32 bytes`

```
ping -s 32 10.1.3.17
```

Wireshark Filter:

```
ip.src == 10.1.3.33 && ip.dst == 10.1.3.17
```

Result:



```
Filter: ip.src==10.1.3.33 && ip.dst==10.1.3.17

No.   Time          Source       Destination  Protocol Length Info
 6999 14.217065294  10.1.3.33    10.1.3.17    ICMP     74 Echo (ping) request  id=0x13f6, seq=1/256, ttl=64 (reply in 7000)
 7491 15.216274457  10.1.3.33    10.1.3.17    ICMP     74 Echo (ping) request  id=0x13f6, seq=2/512, ttl=64 (reply in 7492)

▶Frame 6999: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Pegatron_e5:df:ee (4c:72:b9:e5:df:ee)
▼Internet Protocol Version 4, Src: 10.1.3.33, Dst: 10.1.3.17
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
  ▶Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0xd9f3 (55795)
  ▶Flags: 0x4000, Don't fragment
   Time to live: 64
   Protocol: ICMP (1)
   Header checksum: 0x469a [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.1.3.33
   Destination: 10.1.3.17
▼Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x580a [correct]
   [Checksum Status: Good]
   Identifier (BE): 5110 (0x13f6)
   Identifier (LE): 62995 (0xf613)
   Sequence number (BE): 1 (0x0001)
   Sequence number (LE): 256 (0x0100)
   [Response frame: 7000]
   Timestamp from icmp data: Sep  4, 2018 09:22:53.000000000 IST

0000  4c 72 b9 e5 df ee 1c b7  2c b0 29 c4 08 00 45 00   Lr...... ,.)...E.
0010  00 3c d9 f3 40 00 40 01  46 9a 0a 01 03 21 0a 01   .<..@.@. F....!..
0020  03 11 08 00 58 0a 13 f6  00 01 95 01 8e 5b 00 00   ....X... .....[..
0030  00 00 aa e0 05 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f                     ........ ..

File: "/tmp/wireshark_eth0_201...   Packets: 180697 · Displayed: 235 (0.1%) · Dropped: 0 (0.0%)   Profile: Default
```

- No padding will be observed in this case as packet length `74 B` is greater than minimum ethernet frame size.

Ping with payload `65500 bytes`

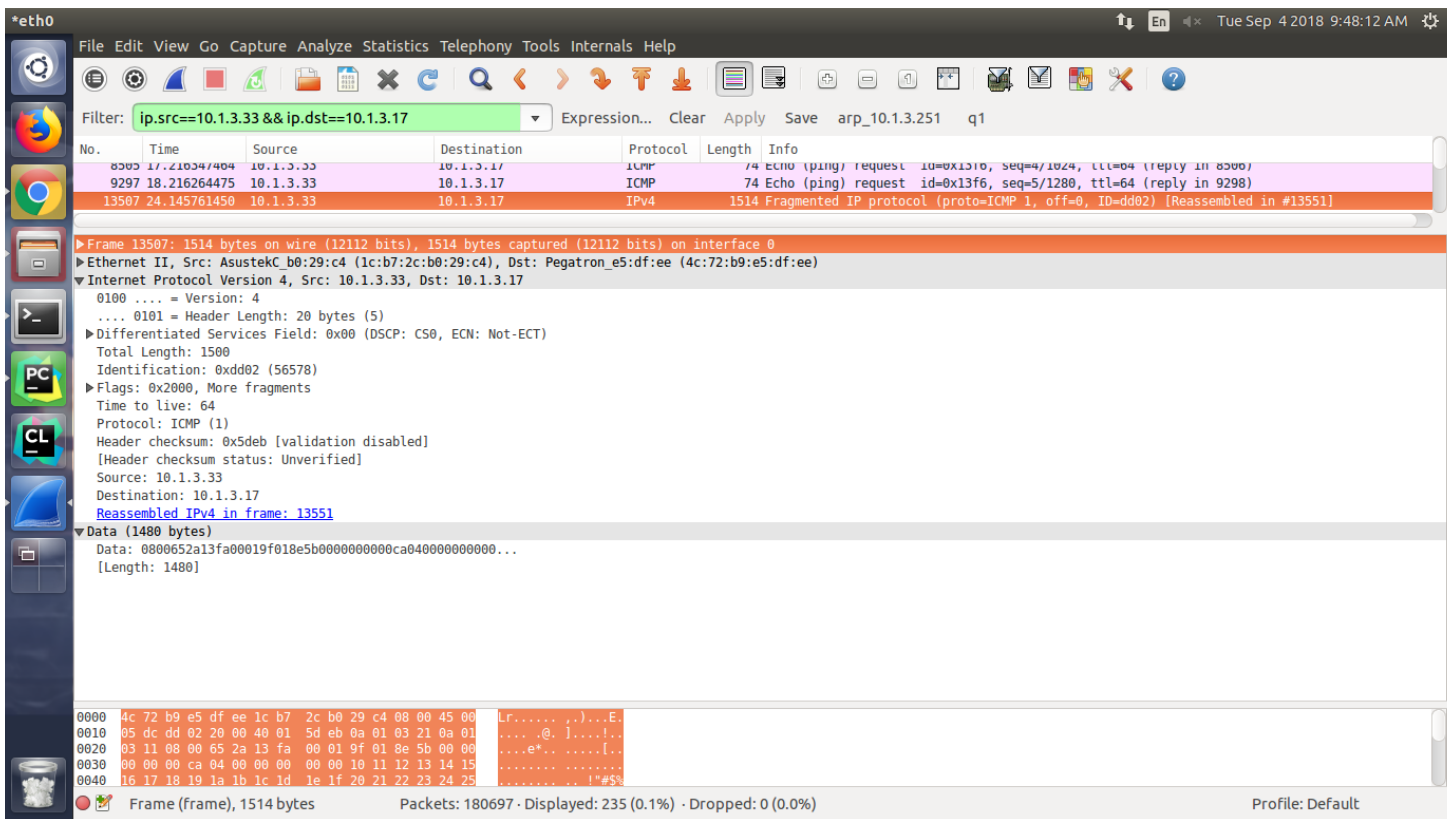
```
ping -s 65500 10.1.3.17
```

Wireshark Filter:

```
ip.src == 10.1.3.33 && ip.dst == 10.1.3.17
```

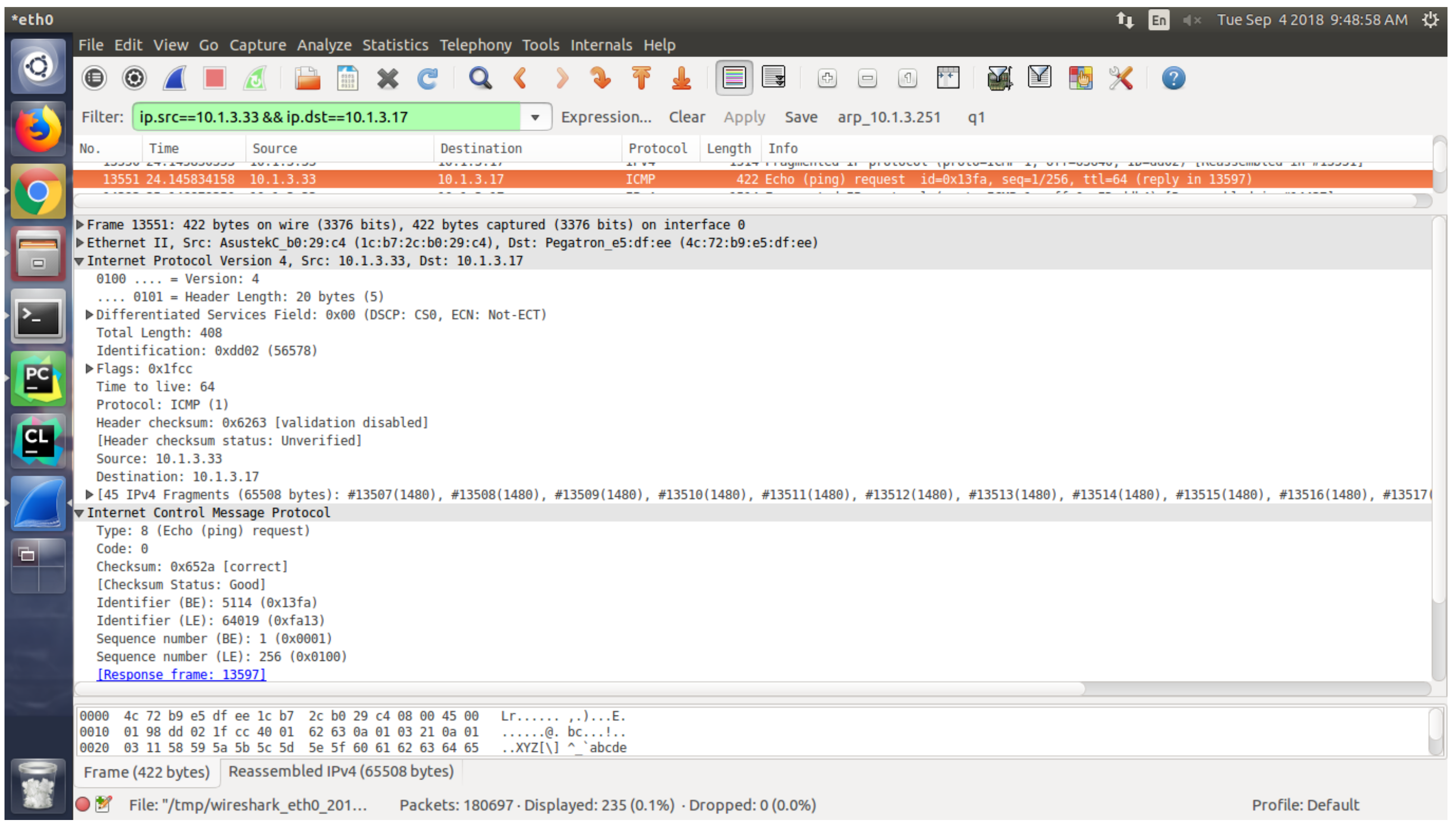
- In this scenario payload size `65500 B` is greater than MTU size `1480 B` hence the payload is fragmented and all other packets except last one are IP packets
  whereas last packet of remaining payload bytes will be ICMP packet as observed in below result.

Result:



```
*eth0                                                      Tue Sep 4 2018 9:48:12 AM
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Internals  Help
Filter: ip.src==10.1.3.33 && ip.dst==10.1.3.17   Expression...  Clear  Apply  Save  arp_10.1.3.251  q1

No.    Time             Source      Destination  Protocol  Length  Info
 8505 17.216347464     10.1.3.33   10.1.3.17    ICMP          74  Echo (ping) request  id=0x13f6, seq=4/1024, ttl=64 (reply in 8506)
 9297 18.216264475     10.1.3.33   10.1.3.17    ICMP          74  Echo (ping) request  id=0x13f6, seq=5/1280, ttl=64 (reply in 9298)
13507 24.145761450     10.1.3.33   10.1.3.17    IPv4        1514  Fragmented IP protocol (proto=ICMP 1, off=0, ID=dd02) [Reassembled in #13551]

▶Frame 13507: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Pegatron_e5:df:ee (4c:72:b9:e5:df:ee)
▼Internet Protocol Version 4, Src: 10.1.3.33, Dst: 10.1.3.17
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
  ▶Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 1500
   Identification: 0xdd02 (56578)
  ▶Flags: 0x2000, More fragments
   Time to live: 64
   Protocol: ICMP (1)
   Header checksum: 0x5deb [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.1.3.33
   Destination: 10.1.3.17
   Reassembled IPv4 in frame: 13551
▼Data (1480 bytes)
   Data: 0800652a13fa00019f018e5b0000000000ca040000000000...
   [Length: 1480]

0000  4c 72 b9 e5 df ee 1c b7  2c b0 29 c4 08 00 45 00   Lr...... ,.)...E.
0010  05 dc dd 02 20 00 40 01  5d eb 0a 01 03 21 0a 01   .... .@. ]....!..
0020  03 11 08 00 65 2a 13 fa  00 01 9f 01 8e 5b 00 00   ....e*.. .....[..
0030  00 00 00 ca 04 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%

Frame (frame), 1514 bytes    Packets: 180697 · Displayed: 235 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig: 65500 bytes payload (1st packet) IP



```
*eth0                                                      Tue Sep 4 2018 9:48:58 AM
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Internals  Help
Filter: ip.src==10.1.3.33 && ip.dst==10.1.3.17   Expression...  Clear  Apply  Save  arp_10.1.3.251  q1

No.    Time             Source      Destination  Protocol  Length  Info
13551 24.145834158     10.1.3.33   10.1.3.17    ICMP         422  Echo (ping) request  id=0x13fa, seq=1/256, ttl=64 (reply in 13597)

▶Frame 13551: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Pegatron_e5:df:ee (4c:72:b9:e5:df:ee)
▼Internet Protocol Version 4, Src: 10.1.3.33, Dst: 10.1.3.17
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
  ▶Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 408
   Identification: 0xdd02 (56578)
  ▶Flags: 0x1fcc
   Time to live: 64
   Protocol: ICMP (1)
   Header checksum: 0x6263 [validation disabled]
   [Header checksum status: Unverified]
   Source: 10.1.3.33
   Destination: 10.1.3.17
  ▶[45 IPv4 Fragments (65508 bytes): #13507(1480), #13508(1480), #13509(1480), #13510(1480), #13511(1480), #13512(1480), #13513(1480), #13514(1480), #13515(1480), #13516(1480), #13517(
▼Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x652a [correct]
   [Checksum Status: Good]
   Identifier (BE): 5114 (0x13fa)
   Identifier (LE): 64019 (0xfa13)
   Sequence number (BE): 1 (0x0001)
   Sequence number (LE): 256 (0x0100)
   [Response frame: 13597]

0000  4c 72 b9 e5 df ee 1c b7  2c b0 29 c4 08 00 45 00   Lr...... ,.)...E.
0010  01 98 dd 02 1f cc 40 01  62 63 0a 01 03 21 0a 01   ......@. bc...!..
0020  03 11 58 59 5a 5b 5c 5d  5e 5f 60 61 62 63 64 65   ..XYZ[\] ^_`abcde

Frame (422 bytes)  Reassembled IPv4 (65508 bytes)
File: "/tmp/wireshark_eth0_201...    Packets: 180697 · Displayed: 235 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig: 65500 bytes payload (last packet) ICMP

Task 2: Trace Route to 8.8.8.8

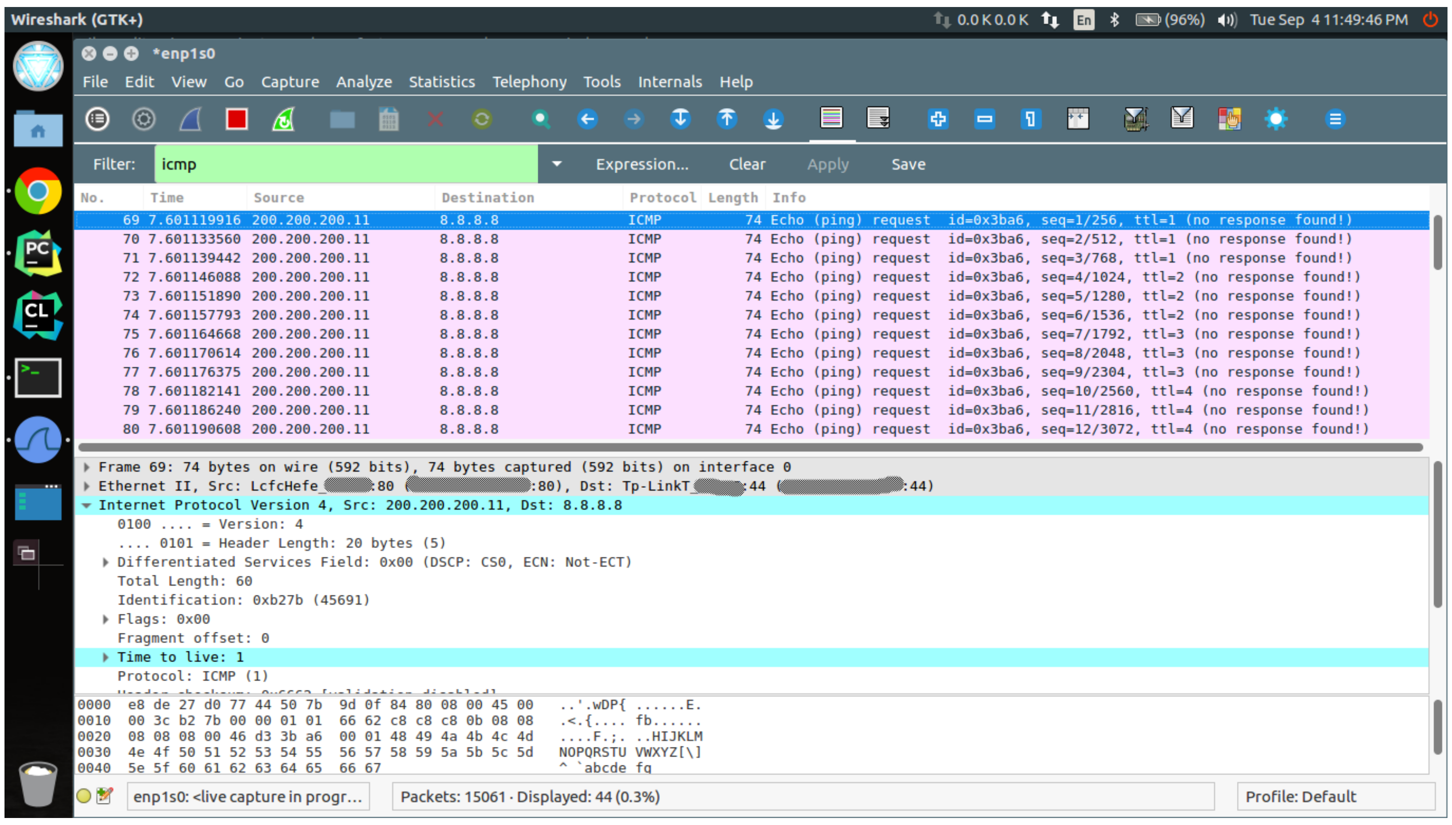
```
jarvis@jarvis:~$ sudo traceroute -I 8.8.8.8
```

Result:

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  200.200.200.1 (200.200.200.1)  0.237 ms  0.256 ms  0.302 ms
 2  27.116.51.70 (27.116.51.70)  8.255 ms  8.273 ms  8.278 ms
 3  182.237.15.149 (182.237.15.149)  8.429 ms  8.417 ms  8.352 ms
 4  10.221.221.37 (10.221.221.37)  9.845 ms * *
 5  * * *
 6  * 103.241.47.130 (103.241.47.130)  16.370 ms *
 7  * 108.170.248.193 (108.170.248.193)  16.816 ms *
 8  * * *
 9  google-public-dns-a.google.com (8.8.8.8)  13.722 ms  13.488 ms  13.481 ms
```

> TTL is not measured by the no of seconds but the no of hops. Its the maximum number of hops that a packet can travel through across the internet, before its discarded.

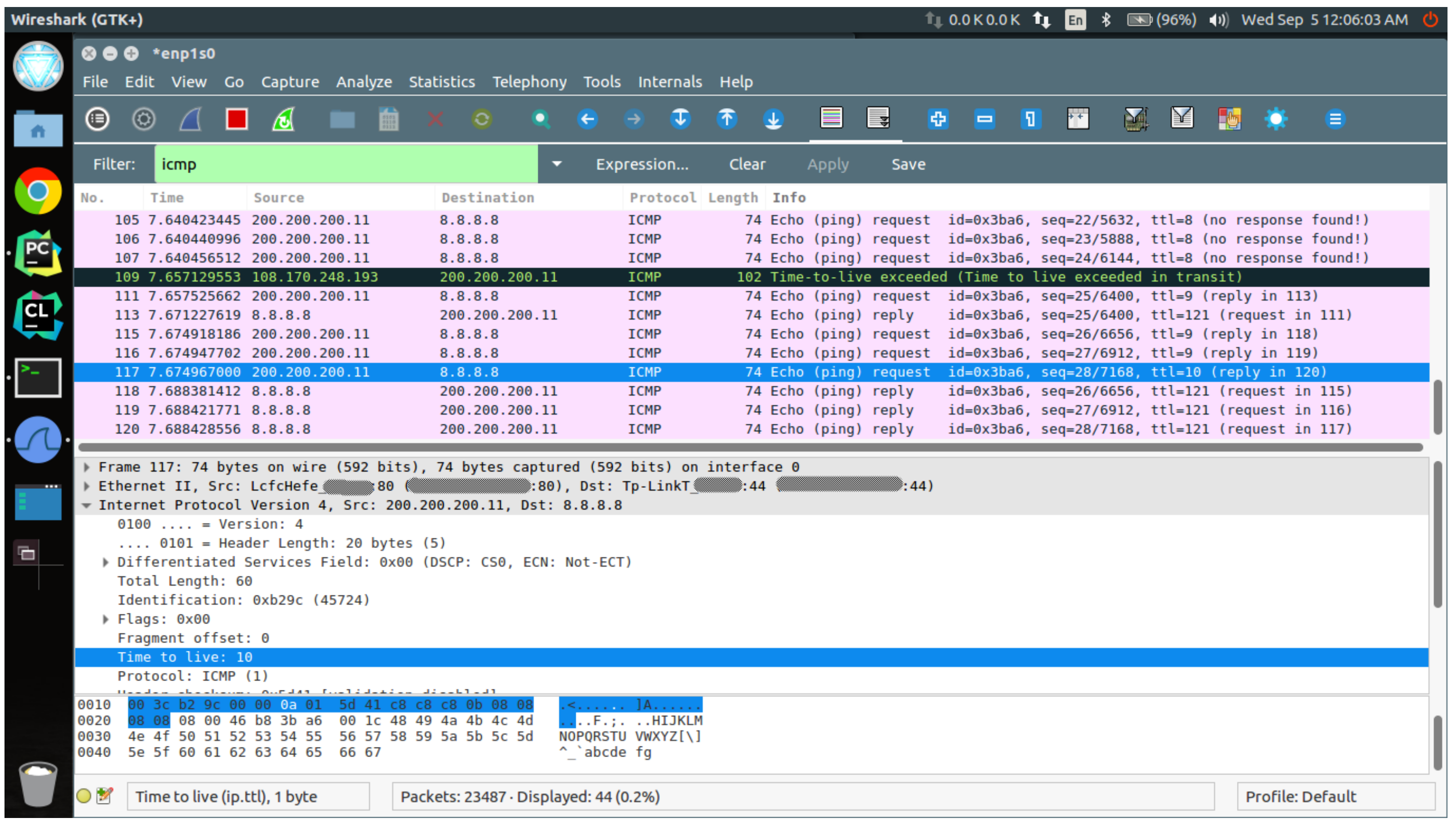
- Trace Route works by initially setting the TTL for a packet to `1` as observed in below figure:



```
Filter: icmp
No.  Time        Source          Destination     Protocol Length Info
  69 7.601119916 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=1/256, ttl=1 (no response found!)
  70 7.601133560 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=2/512, ttl=1 (no response found!)
  71 7.601139442 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=3/768, ttl=1 (no response found!)
  72 7.601146088 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=4/1024, ttl=2 (no response found!)
  73 7.601151890 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=5/1280, ttl=2 (no response found!)
  74 7.601157793 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=6/1536, ttl=2 (no response found!)
  75 7.601164668 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=7/1792, ttl=3 (no response found!)
  76 7.601170614 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=8/2048, ttl=3 (no response found!)
  77 7.601176375 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=9/2304, ttl=3 (no response found!)
  78 7.601182141 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=10/2560, ttl=4 (no response found!)
  79 7.601186240 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=11/2816, ttl=4 (no response found!)
  80 7.601190608 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=12/3072, ttl=4 (no response found!)

▸ Frame 69: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: LcfcHefe_[redacted]:80 ([redacted]:80), Dst: Tp-LinkT_[redacted]:44 ([redacted]:44)
▾ Internet Protocol Version 4, Src: 200.200.200.11, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb27b (45691)
  ▸ Flags: 0x00
    Fragment offset: 0
  ▸ Time to live: 1
    Protocol: ICMP (1)

0000  e8 de 27 d0 77 44 50 7b  9d 0f 84 80 08 00 45 00   ..'.wDP{ ......E.
0010  00 3c b2 7b 00 00 01 01  66 62 c8 c8 c8 0b 08 08   .<.{.... fb......
0020  08 08 08 00 46 d3 3b a6  00 01 48 49 4a 4b 4c 4d   ....F.;. ..HIJKLM
0030  4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040  5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg

enp1s0: <live capture in progr...   Packets: 15061 · Displayed: 44 (0.3%)   Profile: Default
```

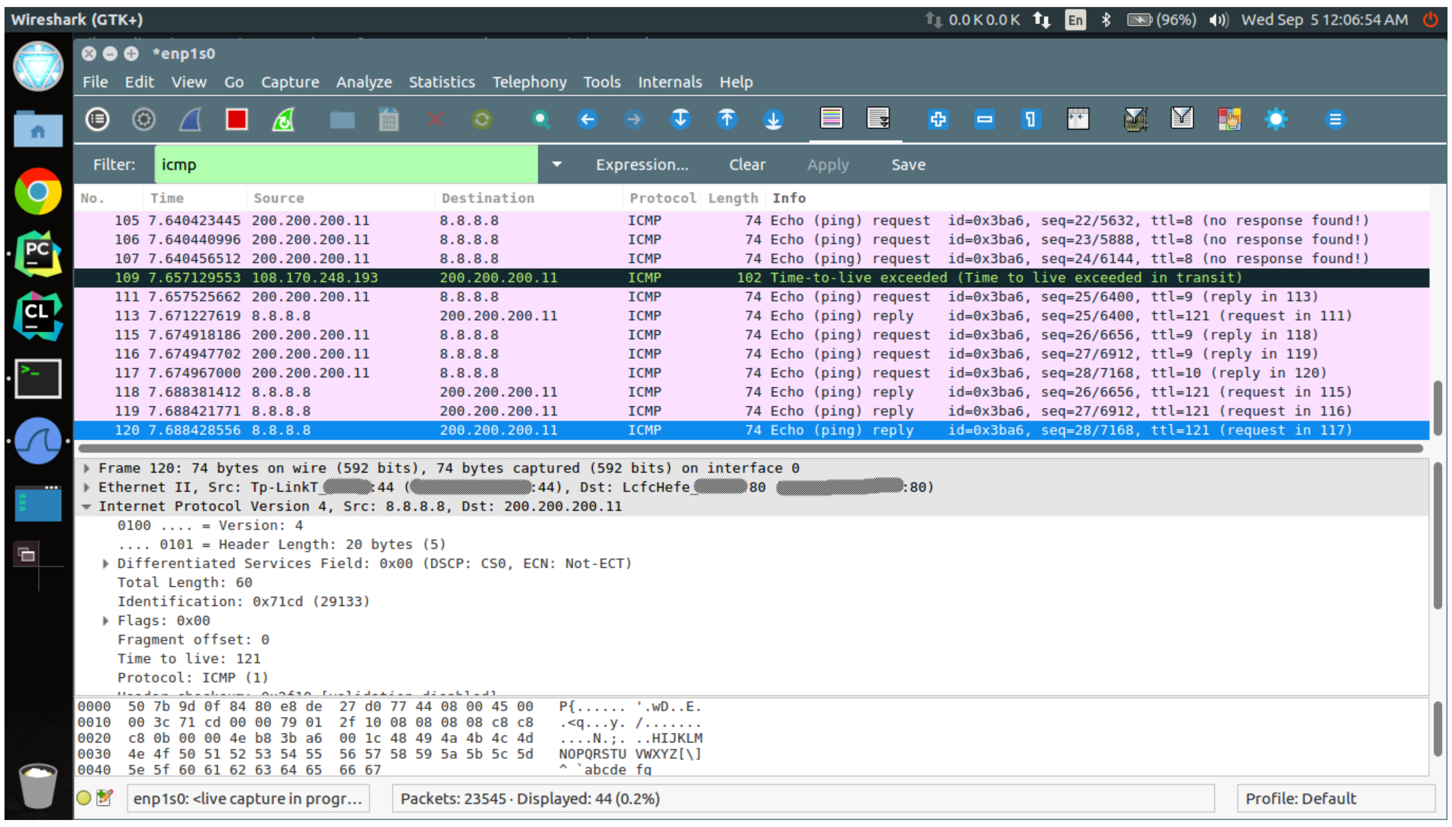
Fig: TTL packet set to 1

- Router's job here is to decrease TTL by `1` (so that packet won't flow endlessly and it can be discarded when TTL reaches to `0`)
- When TTL value becomes `0` (no further travel) the receiving router will drop the packet and informs the original sender (informed that `the TTL value exceeded and it cannot forward the packet further`).



```
Filter: icmp
No.  Time        Source          Destination     Protocol Length Info
 105 7.640423445 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=22/5632, ttl=8 (no response found!)
 106 7.640440996 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=23/5888, ttl=8 (no response found!)
 107 7.640456512 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=24/6144, ttl=8 (no response found!)
 109 7.657129553 108.170.248.193 200.200.200.11  ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 111 7.657525662 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=25/6400, ttl=9 (reply in 113)
 113 7.671227619 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=25/6400, ttl=121 (request in 111)
 115 7.674918186 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=26/6656, ttl=9 (reply in 118)
 116 7.674947702 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=27/6912, ttl=9 (reply in 119)
 117 7.674967000 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=28/7168, ttl=10 (reply in 120)
 118 7.688381412 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=26/6656, ttl=121 (request in 115)
 119 7.688421771 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=27/6912, ttl=121 (request in 116)
 120 7.688428556 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=28/7168, ttl=121 (request in 117)

▸ Frame 117: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: LcfcHefe_[redacted]:80 ([redacted]:80), Dst: Tp-LinkT_[redacted]:44 [redacted]:44)
▾ Internet Protocol Version 4, Src: 200.200.200.11, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb29c (45724)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 10
    Protocol: ICMP (1)

0010  00 3c b2 9c 00 00 0a 01  5d 41 c8 c8 c8 0b 08 08   .<...... ]A......
0020  08 08 08 00 46 b8 3b a6  00 1c 48 49 4a 4b 4c 4d   ....F.;. ..HIJKLM
0030  4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040  5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg

Time to live (ip.ttl), 1 byte   Packets: 23487 · Displayed: 44 (0.2%)   Profile: Default
```

Fig: TTL where no value exceeded



```
Filter: icmp
No.  Time        Source          Destination     Protocol Length Info
 105 7.640423445 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=22/5632, ttl=8 (no response found!)
 106 7.640440996 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=23/5888, ttl=8 (no response found!)
 107 7.640456512 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=24/6144, ttl=8 (no response found!)
 109 7.657129553 108.170.248.193 200.200.200.11  ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 111 7.657525662 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=25/6400, ttl=9 (reply in 113)
 113 7.671227619 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=25/6400, ttl=121 (request in 111)
 115 7.674918186 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=26/6656, ttl=9 (reply in 118)
 116 7.674947702 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=27/6912, ttl=9 (reply in 119)
 117 7.674967000 200.200.200.11  8.8.8.8         ICMP      74 Echo (ping) request  id=0x3ba6, seq=28/7168, ttl=10 (reply in 120)
 118 7.688381412 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=26/6656, ttl=121 (request in 115)
 119 7.688421771 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=27/6912, ttl=121 (request in 116)
 120 7.688428556 8.8.8.8         200.200.200.11  ICMP      74 Echo (ping) reply    id=0x3ba6, seq=28/7168, ttl=121 (request in 117)

▸ Frame 120: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Tp-LinkT_[redacted]:44 ([redacted]:44), Dst: LcfcHefe_[redacted]80 [redacted]:80)
▾ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 200.200.200.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x71cd (29133)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 121
    Protocol: ICMP (1)

0000  50 7b 9d 0f 84 80 e8 de  27 d0 77 44 08 00 45 00   P{...... '.wD..E.
0010  00 3c 71 cd 00 00 79 01  2f 10 08 08 08 08 c8 c8   .<q...y. /.......
0020  c8 0b 00 00 4e b8 3b a6  00 1c 48 49 4a 4b 4c 4d   ....N.;. ..HIJKLM
0030  4e 4f 50 51 52 53 54 55  56 57 58 59 5a 5b 5c 5d   NOPQRSTU VWXYZ[\]
0040  5e 5f 60 61 62 63 64 65  66 67                     ^_`abcde fg

enp1s0: <live capture in progr...   Packets: 23545 · Displayed: 44 (0.2%)   Profile: Default
```

Fig: TTL response

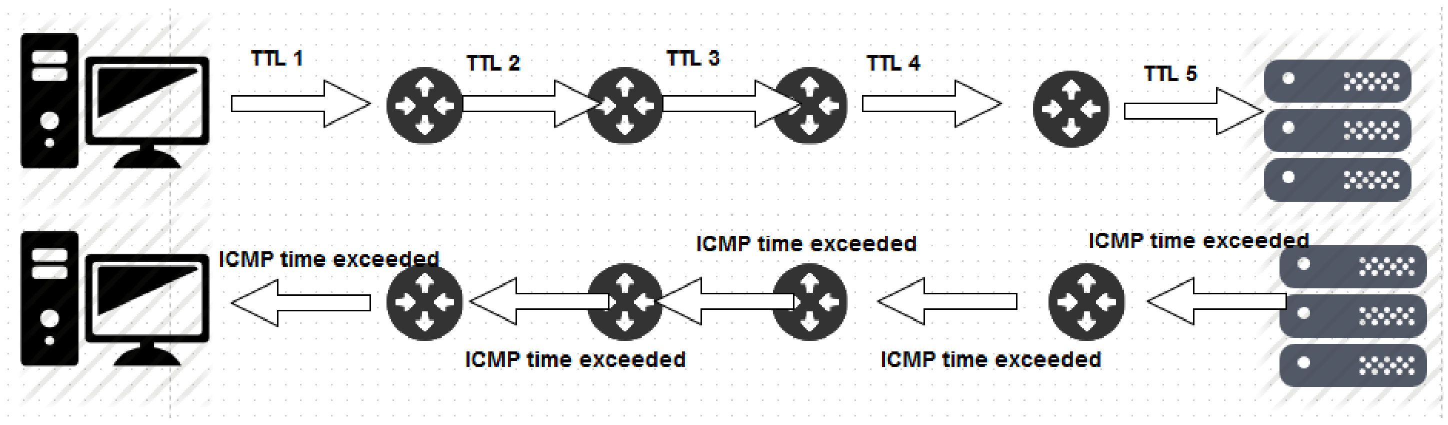


Fig: TTL (working of traceroute)

Task 3: Observer web request communication on ports with 3-tabs

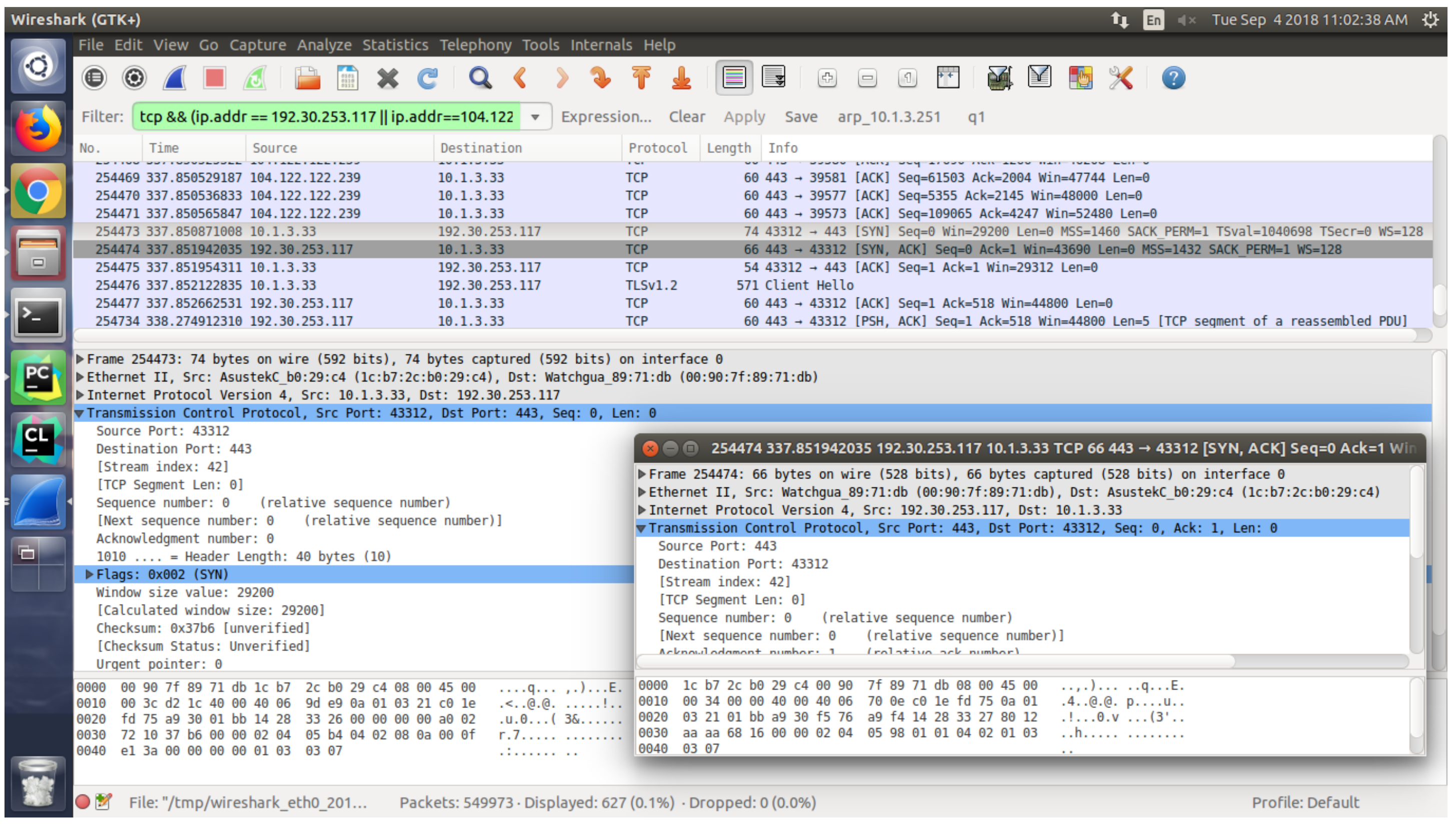
Browsing to below three websites in three different tabs simultaneously:

Domain	IP Address	Web-URL
github.com	192.30.253.117	https://github.com/
www.apple.com	104.122.122.239	https://www.apple.com/
www.sherlockology.com	109.228.21.63	http://www.sherlockology.com/

Below are the details of service connection for above websites from source machine `10.1.3.33`

Source IP	Source Port	Destination IP	Destination Port
10.1.3.33	43312	192.30.253.117	443
10.1.3.33	39573	104.122.122.239	443
10.1.3.33	56127	109.228.21.63	80

As shown in above tabular data destination server like github, apple has their fixed port for communication but from the source machine `10.1.3.33` Operating System has opened a free available port on system to establish TCP connection with different server with different browser tab.
Ex. - for IP address `192.30.253.117` (github) operating system of source machine (`10.1.3.33`) has opened a port `43312` hence all packet will now communicate not only with IP address but with port too so that packets can be delivered to correct browser tab. similarly connection to `109.228.21.63` established on source machine's port `56127`. The Illustration is shown in below results captured in wireshark:



Wireshark (GTK+)
Tue Sep 4 2018 11:02:38 AM
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save arp_10.1.3.251 q1

Filter: tcp && (ip.addr == 192.30.253.117 || ip.addr==104.122

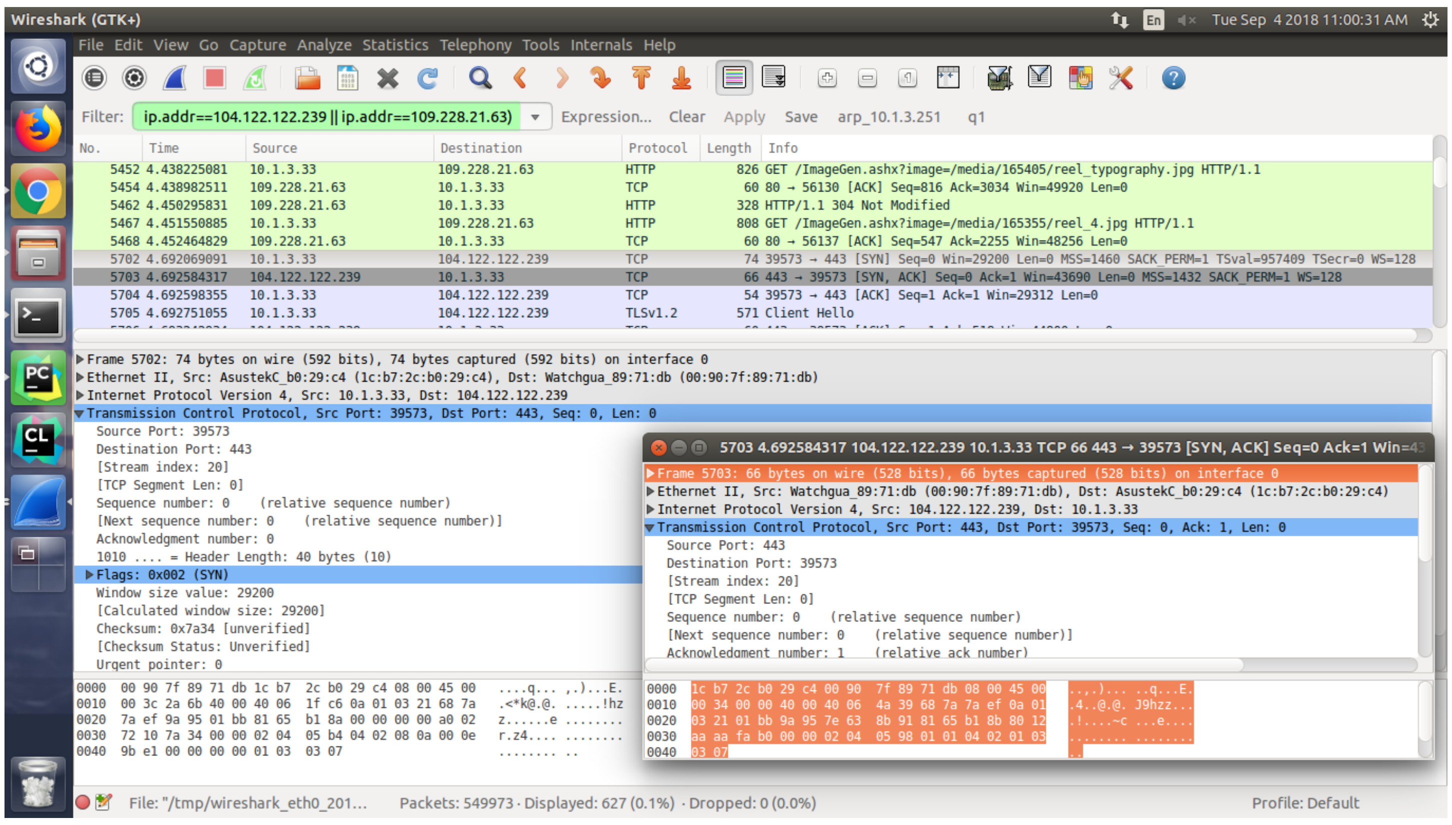
```
No.    Time          Source          Destination     Protocol Length Info
254469 337.850529187 104.122.122.239 10.1.3.33       TCP        60 443 → 39581 [ACK] Seq=61503 Ack=2004 Win=47744 Len=0
254470 337.850536833 104.122.122.239 10.1.3.33       TCP        60 443 → 39577 [ACK] Seq=5355 Ack=2145 Win=48000 Len=0
254471 337.850565847 104.122.122.239 10.1.3.33       TCP        60 443 → 39573 [ACK] Seq=109065 Ack=4247 Win=52480 Len=0
254473 337.850871008 10.1.3.33       192.30.253.117  TCP        74 43312 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1040698 TSecr=0 WS=128
254474 337.851942035 192.30.253.117  10.1.3.33       TCP        66 443 → 43312 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=1432 SACK_PERM=1 WS=128
254475 337.851954311 10.1.3.33       192.30.253.117  TCP        54 43312 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
254476 337.852122835 10.1.3.33       192.30.253.117  TLSv1.2   571 Client Hello
254477 337.852662531 192.30.253.117  10.1.3.33       TCP        60 443 → 43312 [ACK] Seq=1 Ack=518 Win=44800 Len=0
254734 338.274912310 192.30.253.117  10.1.3.33       TCP        60 443 → 43312 [PSH, ACK] Seq=1 Ack=518 Win=44800 Len=5 [TCP segment of a reassembled PDU]
```

```
▶Frame 254473: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Watchgua_89:71:db (00:90:7f:89:71:db)
▶Internet Protocol Version 4, Src: 10.1.3.33, Dst: 192.30.253.117
▼Transmission Control Protocol, Src Port: 43312, Dst Port: 443, Seq: 0, Len: 0
   Source Port: 43312
   Destination Port: 443
   [Stream index: 42]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   [Next sequence number: 0    (relative sequence number)]
   Acknowledgment number: 0
   1010 .... = Header Length: 40 bytes (10)
  ▶Flags: 0x002 (SYN)
   Window size value: 29200
   [Calculated window size: 29200]
   Checksum: 0x37b6 [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0

0000  00 90 7f 89 71 db 1c b7  2c b0 29 c4 08 00 45 00   ....q... ,.)...E.
0010  00 3c d2 1c 40 00 40 06  9d e9 0a 01 03 21 c0 1e   .<..@.@. .....!..
0020  fd 75 a9 30 01 bb 14 28  33 26 00 00 00 00 a0 02   .u.0...( 3&......
0030  72 10 37 b6 00 00 02 04  05 b4 04 02 08 0a 00 0f   r.7..... ........
0040  e1 3a 00 00 00 00 01 03  03 07                     .:...... ..
```

```
254474 337.851942035 192.30.253.117 10.1.3.33 TCP 66 443 → 43312 [SYN, ACK] Seq=0 Ack=1 Win
▶Frame 254474: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶Ethernet II, Src: Watchgua_89:71:db (00:90:7f:89:71:db), Dst: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4)
▶Internet Protocol Version 4, Src: 192.30.253.117, Dst: 10.1.3.33
▼Transmission Control Protocol, Src Port: 443, Dst Port: 43312, Seq: 0, Ack: 1, Len: 0
   Source Port: 443
   Destination Port: 43312
   [Stream index: 42]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   [Next sequence number: 0    (relative sequence number)]
   Acknowledgment number: 1    (relative ack number)

0000  1c b7 2c b0 29 c4 00 90  7f 89 71 db 08 00 45 00   ..,.)... ..q...E.
0010  00 34 00 00 40 00 40 06  70 0e c0 1e fd 75 0a 01   .4..@.@. p....u..
0020  03 21 01 bb a9 30 f5 76  a9 f4 14 28 33 27 80 12   .!...0.v ...(3'..
0030  aa aa 68 16 00 00 02 04  05 98 01 01 04 02 01 03   ..h..... ........
0040  03 07                                              ..
```

File: "/tmp/wireshark_eth0_201... Packets: 549973 · Displayed: 627 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Source Machine `10.1.3.33` opened port `43312` to communicate with `192.30.253.117:443`



Wireshark (GTK+)
Tue Sep 4 2018 11:00:31 AM
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save arp_10.1.3.251 q1

Filter: ip.addr==104.122.122.239 || ip.addr==109.228.21.63)

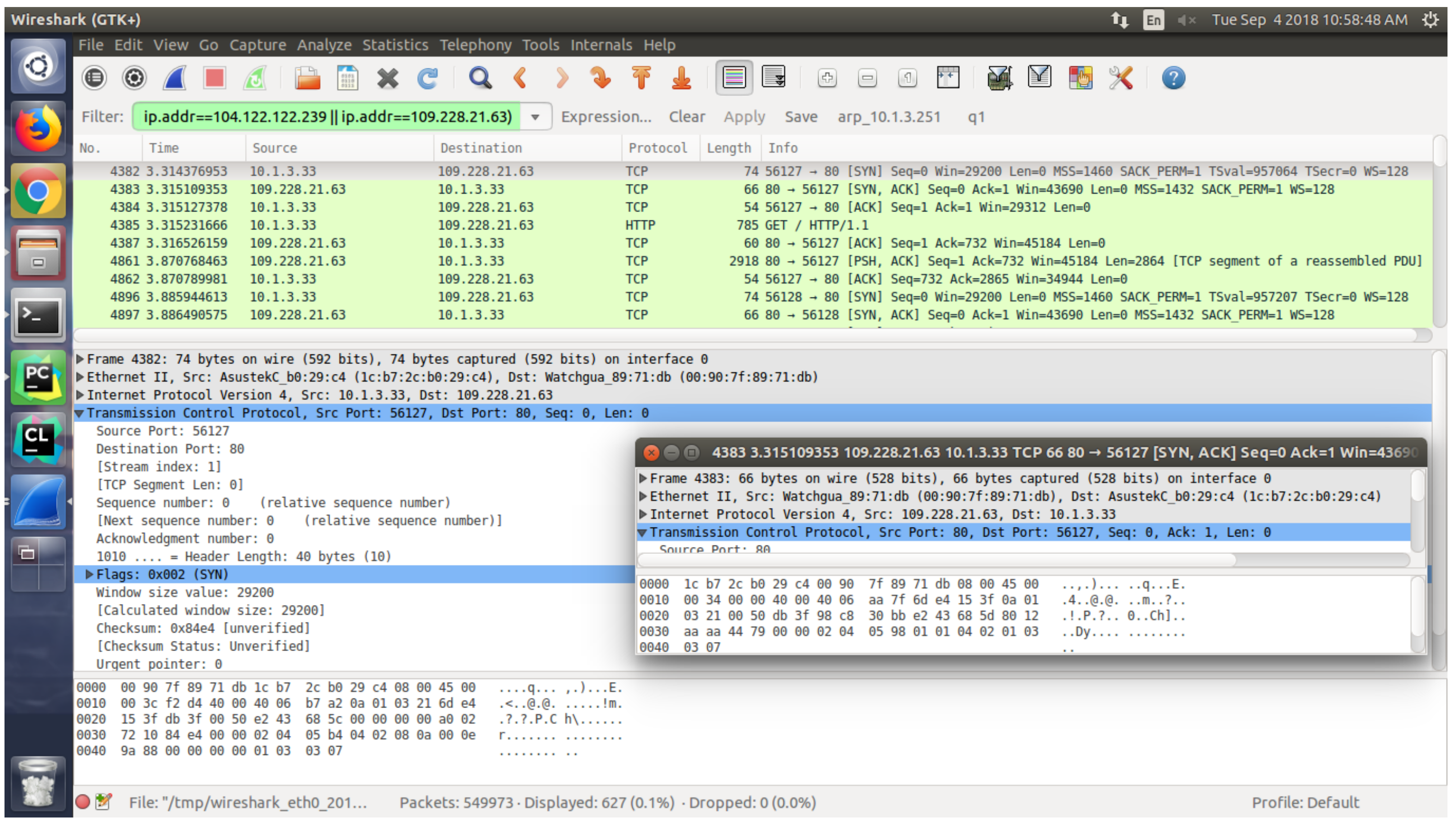
```
No.  Time        Source          Destination     Protocol Length Info
5452 4.438225081 10.1.3.33       109.228.21.63   HTTP      826 GET /ImageGen.ashx?image=/media/165405/reel_typography.jpg HTTP/1.1
5454 4.438982511 109.228.21.63   10.1.3.33       TCP        60 80 → 56130 [ACK] Seq=816 Ack=3034 Win=49920 Len=0
5462 4.450295831 109.228.21.63   10.1.3.33       HTTP      328 HTTP/1.1 304 Not Modified
5467 4.451550885 10.1.3.33       109.228.21.63   HTTP      808 GET /ImageGen.ashx?image=/media/165355/reel_4.jpg HTTP/1.1
5468 4.452464829 109.228.21.63   10.1.3.33       TCP        60 80 → 56137 [ACK] Seq=547 Ack=2255 Win=48256 Len=0
5702 4.692069091 10.1.3.33       104.122.122.239 TCP        74 39573 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=957409 TSecr=0 WS=128
5703 4.692584317 104.122.122.239 10.1.3.33       TCP        66 443 → 39573 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=1432 SACK_PERM=1 WS=128
5704 4.692598355 10.1.3.33       104.122.122.239 TCP        54 39573 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
5705 4.692751055 10.1.3.33       104.122.122.239 TLSv1.2   571 Client Hello
```

```
▶Frame 5702: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Watchgua_89:71:db (00:90:7f:89:71:db)
▶Internet Protocol Version 4, Src: 10.1.3.33, Dst: 104.122.122.239
▼Transmission Control Protocol, Src Port: 39573, Dst Port: 443, Seq: 0, Len: 0
   Source Port: 39573
   Destination Port: 443
   [Stream index: 20]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   [Next sequence number: 0    (relative sequence number)]
   Acknowledgment number: 0
   1010 .... = Header Length: 40 bytes (10)
  ▶Flags: 0x002 (SYN)
   Window size value: 29200
   [Calculated window size: 29200]
   Checksum: 0x7a34 [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0

0000  00 90 7f 89 71 db 1c b7  2c b0 29 c4 08 00 45 00   ....q... ,.)...E.
0010  00 3c 2a 6b 40 00 40 06  1f c6 0a 01 03 21 68 7a   .<*k@.@. .....!hz
0020  7a ef 9a 95 01 bb 81 65  b1 8a 00 00 00 00 a0 02   z......e ........
0030  72 10 7a 34 00 00 02 04  05 b4 04 02 08 0a 00 0e   r.z4.... ........
0040  9b e1 00 00 00 00 01 03  03 07                     ........ ..
```

```
5703 4.692584317 104.122.122.239 10.1.3.33 TCP 66 443 → 39573 [SYN, ACK] Seq=0 Ack=1 Win=43
▶Frame 5703: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶Ethernet II, Src: Watchgua_89:71:db (00:90:7f:89:71:db), Dst: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4)
▶Internet Protocol Version 4, Src: 104.122.122.239, Dst: 10.1.3.33
▼Transmission Control Protocol, Src Port: 443, Dst Port: 39573, Seq: 0, Ack: 1, Len: 0
   Source Port: 443
   Destination Port: 39573
   [Stream index: 20]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   [Next sequence number: 0    (relative sequence number)]
   Acknowledgment number: 1    (relative ack number)

0000  1c b7 2c b0 29 c4 00 90  7f 89 71 db 08 00 45 00   ..,.)... ..q...E.
0010  00 34 00 00 40 00 40 06  4a 39 68 7a 7a ef 0a 01   .4..@.@. J9hzz...
0020  03 21 01 bb 9a 95 7e 63  8b 91 81 65 b1 8b 80 12   .!....~c ...e....
0030  aa aa fa b0 00 00 02 04  05 98 01 01 04 02 01 03   ........ ........
0040  03 07                                              ..
```

File: "/tmp/wireshark_eth0_201... Packets: 549973 · Displayed: 627 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Source Machine `10.1.3.33` opened port `39573` to communicate with `104.122.122.239:443`



Wireshark (GTK+)
Tue Sep 4 2018 10:58:48 AM
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save arp_10.1.3.251 q1

Filter: ip.addr==104.122.122.239 || ip.addr==109.228.21.63)

```
No.  Time        Source          Destination     Protocol Length Info
4382 3.314376953 10.1.3.33       109.228.21.63   TCP        74 56127 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=957064 TSecr=0 WS=128
4383 3.315109353 109.228.21.63   10.1.3.33       TCP        66 80 → 56127 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=1432 SACK_PERM=1 WS=128
4384 3.315127378 10.1.3.33       109.228.21.63   TCP        54 56127 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
4385 3.315231666 10.1.3.33       109.228.21.63   HTTP      785 GET / HTTP/1.1
4387 3.316526159 109.228.21.63   10.1.3.33       TCP        60 80 → 56127 [ACK] Seq=1 Ack=732 Win=45184 Len=0
4861 3.870768463 109.228.21.63   10.1.3.33       TCP      2918 80 → 56127 [PSH, ACK] Seq=1 Ack=732 Win=45184 Len=2864 [TCP segment of a reassembled PDU]
4862 3.870789981 10.1.3.33       109.228.21.63   TCP        54 56127 → 80 [ACK] Seq=732 Ack=2865 Win=34944 Len=0
4896 3.885944613 10.1.3.33       109.228.21.63   TCP        74 56128 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=957207 TSecr=0 WS=128
4897 3.886490575 109.228.21.63   10.1.3.33       TCP        66 80 → 56128 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=1432 SACK_PERM=1 WS=128
```

```
▶Frame 4382: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶Ethernet II, Src: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4), Dst: Watchgua_89:71:db (00:90:7f:89:71:db)
▶Internet Protocol Version 4, Src: 10.1.3.33, Dst: 109.228.21.63
▼Transmission Control Protocol, Src Port: 56127, Dst Port: 80, Seq: 0, Len: 0
   Source Port: 56127
   Destination Port: 80
   [Stream index: 1]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   [Next sequence number: 0    (relative sequence number)]
   Acknowledgment number: 0
   1010 .... = Header Length: 40 bytes (10)
  ▶Flags: 0x002 (SYN)
   Window size value: 29200
   [Calculated window size: 29200]
   Checksum: 0x84e4 [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0

0000  00 90 7f 89 71 db 1c b7  2c b0 29 c4 08 00 45 00   ....q... ,.)...E.
0010  00 3c f2 d4 40 00 40 06  b7 a2 0a 01 03 21 6d e4   .<..@.@. .....!m.
0020  15 3f db 3f 00 50 e2 43  68 5c 00 00 00 00 a0 02   .?.?.P.C h\......
0030  72 10 84 e4 00 00 02 04  05 b4 04 02 08 0a 00 0e   r....... ........
0040  9a 88 00 00 00 00 01 03  03 07                     ........ ..
```

```
4383 3.315109353 109.228.21.63 10.1.3.33 TCP 66 80 → 56127 [SYN, ACK] Seq=0 Ack=1 Win=4369
▶Frame 4383: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶Ethernet II, Src: Watchgua_89:71:db (00:90:7f:89:71:db), Dst: AsustekC_b0:29:c4 (1c:b7:2c:b0:29:c4)
▶Internet Protocol Version 4, Src: 109.228.21.63, Dst: 10.1.3.33
▼Transmission Control Protocol, Src Port: 80, Dst Port: 56127, Seq: 0, Ack: 1, Len: 0
   Source Port: 80

0000  1c b7 2c b0 29 c4 00 90  7f 89 71 db 08 00 45 00   ..,.)... ..q...E.
0010  00 34 00 00 40 00 40 06  aa 7f 6d e4 15 3f 0a 01   .4..@.@. ..m..?..
0020  03 21 00 50 db 3f 98 c8  30 bb e2 43 68 5d 80 12   .!.P.?.. 0..Ch]..
0030  aa aa 44 79 00 00 02 04  05 98 01 01 04 02 01 03   ..Dy.... ........
0040  03 07                                              ..
```

File: "/tmp/wireshark_eth0_201... Packets: 549973 · Displayed: 627 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Source Machine `10.1.3.33` opened port `56127` to communicate with `109.228.21.63:80`