

First packet comparison - wireshark on the left, my output on the right

```
> Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
  > Ethernet II, Src: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2), Dst: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    > Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    > Source: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
      Type: IPv4 (0x0800)
      [Stream index: 0]
    > Internet Protocol Version 4, Src: 162.0.180.74, Dst: 192.168.1.99
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 54
        Identification: 0xe884 (59524)
      > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 117
        Protocol: UDP (17)
        Header Checksum: 0x44dc [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 162.0.180.74
        Destination Address: 192.168.1.99
        [Stream index: 0]
    > User Datagram Protocol, Src Port: 443, Dst Port: 55701
    > Data (26 bytes)
```

```
((base) ethianiannicelli@Mac-mini Ethan_Iannicelli_hw1 % python pktsniffer.py -r input
{'read': 'input.pcap', 'filter_type': None, 'filter_value': None, 'tcp': False, 'udp': True}
Ethernet Header:
  Packet Size: 68
  Destination MAC Address: 0e:83:01:0b:07:68
  Source MAC Address: 80:cc:9c:11:e2:c2
  Ethertype: 0x0800
IP Header:
  Version: 4
  Header Length: 20
  Type of Service: 0x00
  Total Length: 54
  Identification: 0xe884
  Flags: 0x00
  Fragment Offset: 0
  Time to Live: 117
  Protocol: 17
  Header Checksum: 0x44dc
  Source IP Address: 162.0.180.74
  Destination IP Address: 192.168.1.99
Layer UDP
:
  Source Port: 443
  Destination Port: 55701
  Length: 34
  Checksum: 0x3afe [unverified]
  Checksum Status: Unverified
  Stream index: 0
  Stream Packet Number: 1
Timestamps
Time since first frame: 0.000000000 seconds
Time since previous frame: 0.000000000 seconds
UDP payload (26 bytes)
```

((base) ethianiannicelli@Mac-mini Ethan_Iannicelli_hw1 %

Last packet comparison - wireshark on the left, my output on the right

```
> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
  > Ethernet II, Src: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2), Dst: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    > Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    > Source: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
      Type: IPv4 (0x0800)
      [Stream index: 0]
    > Internet Protocol Version 4, Src: 104.16.80.73, Dst: 192.168.1.99
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 52
        Identification: 0x357b (13691)
      > 010. .... = Flags: 0x2, Don't fragment
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 55
        Protocol: TCP (6)
        Header Checksum: 0x93e4 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 104.16.80.73
        Destination Address: 192.168.1.99
        [Stream index: 11]
    > Transmission Control Protocol, Src Port: 443, Dst Port: 49525, Seq: 1, Ack: 2, Len: 0
```

```
Ethernet Header:
  Packet Size: 66
  Destination MAC Address: 0e:83:01:0b:07:68
  Source MAC Address: 80:cc:9c:11:e2:c2
  Ethertype: 0x0800
IP Header:
  Version: 4
  Header Length: 20
  Type of Service: 0x00
  Total Length: 52
  Identification: 0x357b
  Flags: 0x02
  Fragment Offset: 0
  Time to Live: 55
  Protocol: 6
  Header Checksum: 0x93e4
  Source IP Address: 104.16.80.73
  Destination IP Address: 192.168.1.99
Layer TCP
:
  Source Port: 443
  Destination Port: 49525
  Stream index: 3
  Conversation completeness: Incomplete (4)
```

Filtering

Screenshots of the last packet for each filter - wireshark on right, my output on left

Filter: ip.host == 162.0.180.74, host 162.0.180.74

```
> Frame 91: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
  Ethernet II, Src: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68), Dst: Netgear_11:e2:c2
    Destination: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
    Source: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  Internet Protocol Version 4, Src: 192.168.1.99, Dst: 162.0.180.74
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x2259 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.99
    Destination Address: 162.0.180.74
    [Stream index: 0]
  User Datagram Protocol, Src Port: 55701, Dst Port: 443
  Data (34 bytes)
```

Ethernet Header:
Packet Size: 76
Destination MAC Address: 80:cc:9c:11:e2:c2
Source MAC Address: 0e:83:01:0b:07:68
Ethertype: 0x0800

IP Header:
Version: 4
Header Length: 20
Type of Service: 0x00
Total Length: 62
Identification: 0x0000
Flags: 0x02
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Header Checksum: 0x2259
Source IP Address: 192.168.1.99
Destination IP Address: 162.0.180.74

Layer UDP
:
Source Port: 55701
Destination Port: 443
Length: 42
Checksum: 0xff98 [unverified]
Checksum Status: Unverified
Stream index: 0
Stream Packet Number: 91
Timestamps
Time since first frame: 0.274960000 seconds
Time since previous frame: 0.000071000 seconds
UDP payload (34 bytes)

Filter: tcp.port == 52886 || udp.port == 52886, port 52886

```
> Frame 408: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
  Ethernet II, Src: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2), Dst: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    Source: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  Internet Protocol Version 4, Src: 162.0.180.73, Dst: 192.168.1.99
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 54
    Identification: 0x8122 (33058)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 117
    Protocol: UDP (17)
    Header Checksum: 0xac3f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 162.0.180.73
    Destination Address: 192.168.1.99
    [Stream index: 4]
  User Datagram Protocol, Src Port: 443, Dst Port: 52886
    Source Port: 443
```

Ethernet Header:
Packet Size: 68
Destination MAC Address: 0e:83:01:0b:07:68
Source MAC Address: 80:cc:9c:11:e2:c2
Ethertype: 0x0800

IP Header:
Version: 4
Header Length: 20
Type of Service: 0x00
Total Length: 54
Identification: 0x8122
Flags: 0x00
Fragment Offset: 0
Time to Live: 117
Protocol: 17
Header Checksum: 0xac3f
Source IP Address: 162.0.180.73
Destination IP Address: 192.168.1.99

Layer UDP
:
Source Port: 443
Destination Port: 52886
Length: 34
Checksum: 0xe0ab [unverified]
Checksum Status: Unverified
Stream index: 2
Stream Packet Number: 295
Timestamps
Time since first frame: 0.059887000 seconds
Time since previous frame: 0.009942000 seconds
UDP payload (26 bytes)

```
> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2), Dst: 0e:83:01:0b:07:68
  > Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
  > Source: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  > Internet Protocol Version 4, Src: 104.16.80.73, Dst: 192.168.1.99
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x357b (13691)
    > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 55
    Protocol: TCP (6)
    Header Checksum: 0x93e4 [validation failed]
    [Header checksum status: Unverified]
    Source Address: 104.16.80.73
    Destination Address: 192.168.1.99
    [Stream index: 11]
  > Transmission Control Protocol, Src Port: 443, Dst Port: 49525, Seq: 1044110400
```

```

Layer TCP
:      Source Port: 443
      Destination Port: 49525
      Stream index: 3
      Conversation completeness: Incomplete (4)
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
      ....0 .... = Data: Absent
      ....1. .... = ACK: Present
      ....0. .... = SYN-ACK: Absent
      ....0. .... = SYN: Absent
      ....0. .... = EST: Absent

```

```
> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bit) on interface 0
  > Ethernet II, Src: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2), Dst: 0e:83:01:0b:07:68
    > Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
    > Source: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
      Type: IPv4 (0x0800)
      [Stream index: 0]
  > Internet Protocol Version 4, Src: 104.16.80.73, Dst: 192.168.1.99
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 52
      Identification: 0x357b (13691)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 55
      Protocol: TCP (6)
      Header Checksum: 0x93e4 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 104.16.80.73
      Destination Address: 192.168.1.99
      [Stream index: 11]
  > Transmission Control Protocol, Src Port: 443, Dst Port: 49525, Seq: 1111111111
```

```

Layer TCP
:      Source Port: 443
      Destination Port: 49525
      Stream index: 3
      Conversation completeness: Incomplete (4)
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
      ....0 .... = Data: Absent

```

Filter: tcp, -tcp

```
> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on 0
Ethernet II, Src: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2), Dst: 0e:83:01:0b:07:68
  Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
  Source: Netgear_11:e2:c2 (80:cc:9c:11:e2:c2)
  Type: IPv4 (0x0800)
  [Stream index: 0]
Internet Protocol Version 4, Src: 104.16.80.73, Dst: 192.168.1.99
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x357b (13691)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 55
  Protocol: TCP (6)
  Header Checksum: 0x93e4 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 104.16.80.73
  Destination Address: 192.168.1.99
  [Stream index: 11]
Transmission Control Protocol, Src Port: 443, Dst Port: 49525, Seq: 104168073
```

```
Ethernet Header:
  Packet Size: 66
  Destination MAC Address: 0e:83:01:0b:07:68
  Source MAC Address: 80:cc:9c:11:e2:c2
  Ethertype: 0x0800
IP Header:
  Version: 4
  Header Length: 20
  Type of Service: 0x00
  Total Length: 52
  Identification: 0x357b
  Flags: 0x02
  Fragment Offset: 0
  Time to Live: 55
  Protocol: 6
  Header Checksum: 0x93e4
  Source IP Address: 104.16.80.73
  Destination IP Address: 192.168.1.99
Layer TCP
:
  Source Port: 443
  Destination Port: 49525
  Stream index: 3
  Conversation completeness: Incomplete (4)
```

Filter udp, -udp

```
> Frame 464: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on 0
Ethernet II, Src: ASUS_TekCOMPU_f7:a2:86 (04:d9:f5:f7:a2:86), Dst: 33:33:00:00:00:fb
  Destination: IPv6mcast_fb (33:33:00:00:00:fb)
  Source: ASUS_TekCOMPU_f7:a2:86 (04:d9:f5:f7:a2:86)
  Type: IPv6 (0x86dd)
  [Stream index: 5]
Internet Protocol Version 6, Src: fe80::280e:c6ee:6a14:f3a0, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  Source Port: 5353
  Destination Port: 5353
  Length: 237
  Checksum: 0x95cb [unverified]
  [Checksum Status: Unverified]
  [Stream index: 8]
  [Stream Packet Number: 4]
  [Timestamps]
  UDP payload (229 bytes)
```

```
Ethernet Header:
  Packet Size: 291
  Destination MAC Address: 33:33:00:00:00:fb
  Source MAC Address: 04:d9:f5:f7:a2:86
  Ethertype: 0x86dd
IP Header:
  Version: 6
  Source IP Address: fe80::280e:c6ee:6a14:f3a0
  Destination IP Address: ff02::fb
Layer UDP
:
  Source Port: 5353
  Destination Port: 5353
  Length: 237
  Checksum: 0x95cb [unverified]
  Checksum Status: Unverified
  Stream index: 8
  Stream Packet Number: 4
  Timestamps
  Time since first frame: 0.002726000 seconds
  Time since previous frame: 0.001383000 seconds
  UDP payload (229 bytes)
```

Filter: icmp, -icmp

```
> Frame 448: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on 0
Ethernet II, Src: 06:b0:79:47:c8:7c (06:b0:79:47:c8:7c), Dst: 0e:83:01:0b:07:68
  Destination: 0e:83:01:0b:07:68 (0e:83:01:0b:07:68)
  Source: 06:b0:79:47:c8:7c (06:b0:79:47:c8:7c)
  Type: IPv6 (0x86dd)
  [Stream index: 1]
Internet Protocol Version 6, Src: fe80::101d:54d5:a0bf:1558, Dst: fe80::188d:c4be:bff:ba5
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0)
  .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 24
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  Source Address: fe80::101d:54d5:a0bf:1558
  Destination Address: fe80::188d:c4be:bff:ba5
  [Stream index: 0]
Internet Control Message Protocol v6
```

```
Ethernet Header:
  Packet Size: 78
  Destination MAC Address: 0e:83:01:0b:07:68
  Source MAC Address: 06:b0:79:47:c8:7c
  Ethertype: 0x86dd
IP Header:
  Version: 6
  Source IP Address: fe80::101d:54d5:a0bf:1558
  Destination IP Address: fe80::188d:c4be:bff:ba5
Layer ICMPv6
:
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0x1126 [correct]
  Checksum Status: Good
  Flags: 0x40000000, Solicited
  0... .. = Router: Not set
  .1. .... = Solicited: Set
  ..0. .... = Override: Not set
  ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
  Target Address: fe80::101d:54d5:a0bf:1558
```