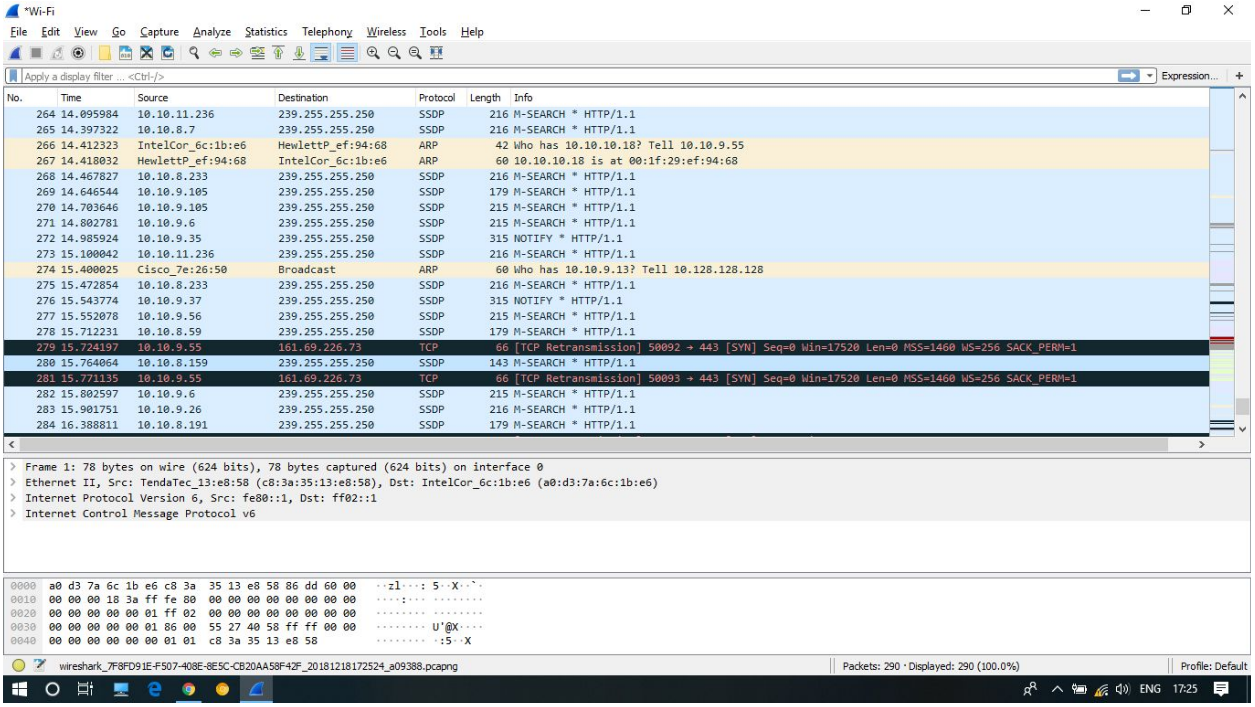
1. Scenario 1: capture all data.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

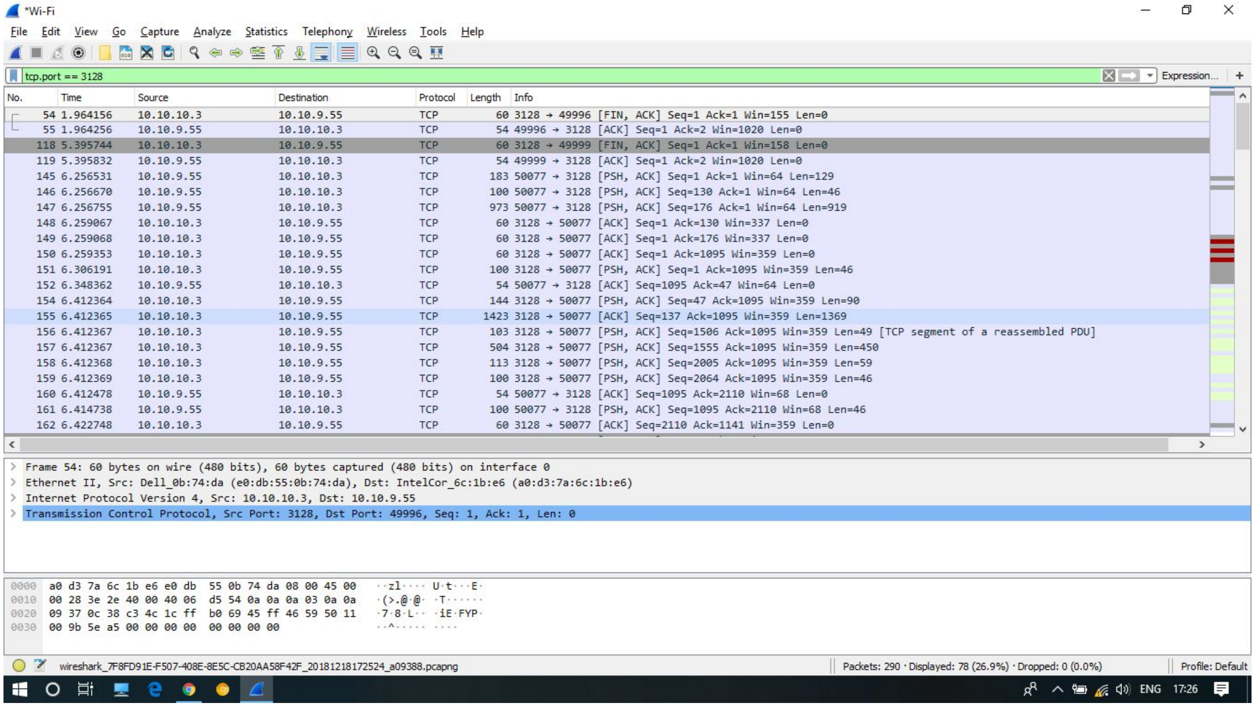
```
No.     Time       Source             Destination        Protocol  Length  Info
    264 14.095984  10.10.11.236       239.255.255.250    SSDP       216 M-SEARCH * HTTP/1.1
    265 14.397322  10.10.8.7          239.255.255.250    SSDP       216 M-SEARCH * HTTP/1.1
    266 14.412323  IntelCor_6c:1b:e6  HewlettP_ef:94:68  ARP         42 Who has 10.10.10.18? Tell 10.10.9.55
    267 14.418032  HewlettP_ef:94:68  IntelCor_6c:1b:e6  ARP         60 10.10.10.18 is at 00:1f:29:ef:94:68
    268 14.467827  10.10.8.233        239.255.255.250    SSDP       216 M-SEARCH * HTTP/1.1
    269 14.646544  10.10.9.105        239.255.255.250    SSDP       179 M-SEARCH * HTTP/1.1
    270 14.703646  10.10.9.105        239.255.255.250    SSDP       215 M-SEARCH * HTTP/1.1
    271 14.802781  10.10.9.6          239.255.255.250    SSDP       215 M-SEARCH * HTTP/1.1
    272 14.985924  10.10.9.35         239.255.255.250    SSDP       315 NOTIFY * HTTP/1.1
    273 15.100042  10.10.11.236       239.255.255.250    SSDP       216 M-SEARCH * HTTP/1.1
    274 15.400025  Cisco_7e:26:50     Broadcast          ARP         60 Who has 10.10.9.13? Tell 10.128.128.128
    275 15.472854  10.10.8.233        239.255.255.250    SSDP       216 M-SEARCH * HTTP/1.1
    276 15.543774  10.10.9.37         239.255.255.250    SSDP       315 NOTIFY * HTTP/1.1
    277 15.552078  10.10.9.56         239.255.255.250    SSDP       215 M-SEARCH * HTTP/1.1
    278 15.712231  10.10.8.59         239.255.255.250    SSDP       179 M-SEARCH * HTTP/1.1
    279 15.724197  10.10.9.55         161.69.226.73      TCP         66 [TCP Retransmission] 50092 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
    280 15.764064  10.10.8.159        239.255.255.250    SSDP       143 M-SEARCH * HTTP/1.1
    281 15.771135  10.10.9.55         161.69.226.73      TCP         66 [TCP Retransmission] 50093 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
    282 15.802597  10.10.9.6          239.255.255.250    SSDP       215 M-SEARCH * HTTP/1.1
    283 15.901751  10.10.9.26         239.255.255.250    SSDP       216 M-SEARCH * HTTP/1.1
    284 16.388811  10.10.8.191        239.255.255.250    SSDP       179 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: TendaTec_13:e8:58 (c8:3a:35:13:e8:58), Dst: IntelCor_6c:1b:e6 (a0:d3:7a:6c:1b:e6)
> Internet Protocol Version 6, Src: fe80::1, Dst: ff02::1
> Internet Control Message Protocol v6
```

```
0000  a0 d3 7a 6c 1b e6 c8 3a  35 13 e8 58 86 dd 60 00   ··zl···: 5··X··`·
0010  00 00 00 18 3a ff fe 80  00 00 00 00 00 00 00 00   ····:··· ········
0020  00 00 00 00 00 01 ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 86 00  55 27 40 58 ff ff 00 00   ········ U'@X····
0040  00 00 00 00 00 00 01 01  c8 3a 35 13 e8 58         ········ ·:5··X
```

wireshark_7F8FD91E-F507-408E-8E5C-CB20AA58F42F_20181218172524_a09388.pcapng | Packets: 290 · Displayed: 290 (100.0%) | Profile: Default

2. Scenario 2: use filters to capture all data on port 3128.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

tcp.port == 3128

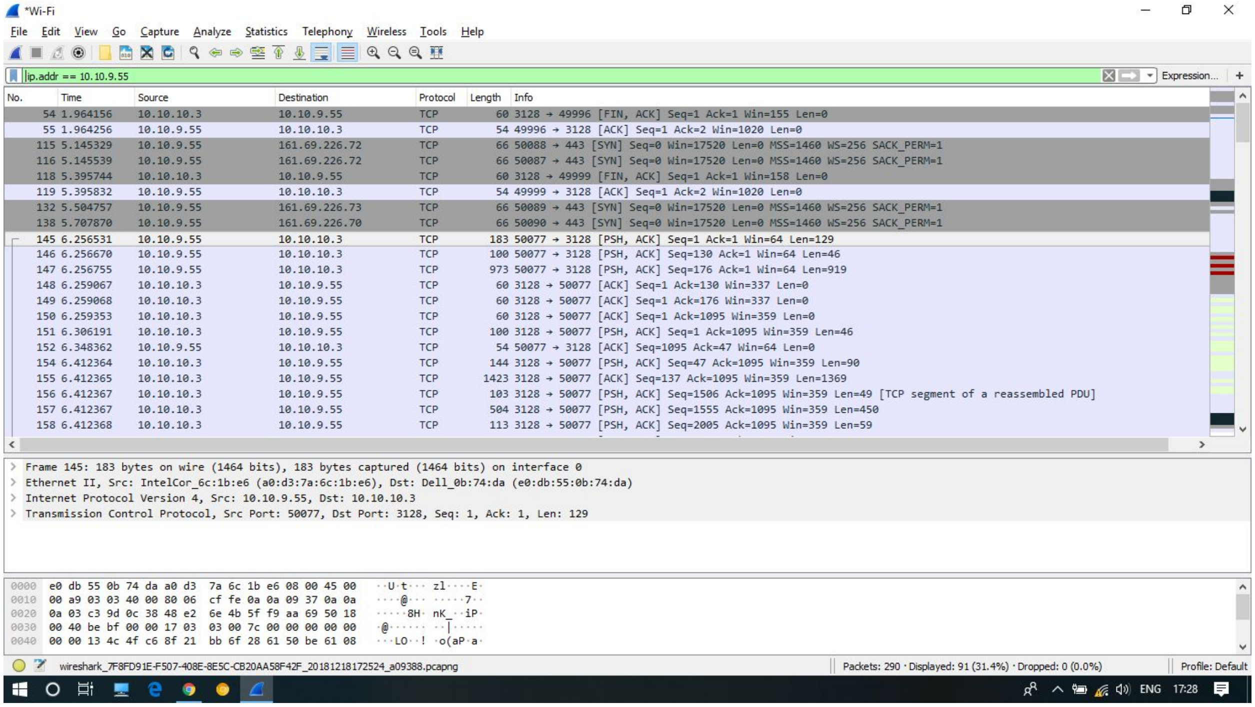
```
No.     Time       Source        Destination   Protocol  Length  Info
     54 1.964156   10.10.10.3    10.10.9.55    TCP         60 3128 → 49996 [FIN, ACK] Seq=1 Ack=1 Win=155 Len=0
     55 1.964256   10.10.9.55    10.10.10.3    TCP         54 49996 → 3128 [ACK] Seq=1 Ack=2 Win=1020 Len=0
    118 5.395744   10.10.10.3    10.10.9.55    TCP         60 3128 → 49999 [FIN, ACK] Seq=1 Ack=1 Win=158 Len=0
    119 5.395832   10.10.9.55    10.10.10.3    TCP         54 49999 → 3128 [ACK] Seq=1 Ack=2 Win=1020 Len=0
    145 6.256531   10.10.9.55    10.10.10.3    TCP        183 50077 → 3128 [PSH, ACK] Seq=1 Ack=1 Win=64 Len=129
    146 6.256670   10.10.9.55    10.10.10.3    TCP        100 50077 → 3128 [PSH, ACK] Seq=130 Ack=1 Win=64 Len=46
    147 6.256755   10.10.9.55    10.10.10.3    TCP        973 50077 → 3128 [PSH, ACK] Seq=176 Ack=1 Win=64 Len=919
    148 6.259067   10.10.10.3    10.10.9.55    TCP         60 3128 → 50077 [ACK] Seq=1 Ack=130 Win=337 Len=0
    149 6.259068   10.10.10.3    10.10.9.55    TCP         60 3128 → 50077 [ACK] Seq=1 Ack=176 Win=337 Len=0
    150 6.259353   10.10.10.3    10.10.9.55    TCP         60 3128 → 50077 [ACK] Seq=1 Ack=1095 Win=359 Len=0
    151 6.306191   10.10.10.3    10.10.9.55    TCP        100 3128 → 50077 [PSH, ACK] Seq=1 Ack=1095 Win=359 Len=46
    152 6.348362   10.10.9.55    10.10.10.3    TCP         54 50077 → 3128 [ACK] Seq=1095 Ack=47 Win=64 Len=0
    154 6.412364   10.10.10.3    10.10.9.55    TCP        144 3128 → 50077 [PSH, ACK] Seq=47 Ack=1095 Win=359 Len=90
    155 6.412365   10.10.10.3    10.10.9.55    TCP       1423 3128 → 50077 [ACK] Seq=137 Ack=1095 Win=359 Len=1369
    156 6.412367   10.10.10.3    10.10.9.55    TCP        103 3128 → 50077 [PSH, ACK] Seq=1506 Ack=1095 Win=359 Len=49 [TCP segment of a reassembled PDU]
    157 6.412367   10.10.10.3    10.10.9.55    TCP        504 3128 → 50077 [PSH, ACK] Seq=1555 Ack=1095 Win=359 Len=450
    158 6.412368   10.10.10.3    10.10.9.55    TCP        113 3128 → 50077 [PSH, ACK] Seq=2005 Ack=1095 Win=359 Len=59
    159 6.412369   10.10.10.3    10.10.9.55    TCP        100 3128 → 50077 [PSH, ACK] Seq=2064 Ack=1095 Win=359 Len=46
    160 6.412478   10.10.9.55    10.10.10.3    TCP         54 50077 → 3128 [ACK] Seq=1095 Ack=2110 Win=68 Len=0
    161 6.414738   10.10.9.55    10.10.10.3    TCP        100 50077 → 3128 [PSH, ACK] Seq=1095 Ack=2110 Win=68 Len=46
    162 6.422748   10.10.10.3    10.10.9.55    TCP         60 3128 → 50077 [ACK] Seq=2110 Ack=1141 Win=359 Len=0
```

```
> Frame 54: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Dell_0b:74:da (e0:db:55:0b:74:da), Dst: IntelCor_6c:1b:e6 (a0:d3:7a:6c:1b:e6)
> Internet Protocol Version 4, Src: 10.10.10.3, Dst: 10.10.9.55
> Transmission Control Protocol, Src Port: 3128, Dst Port: 49996, Seq: 1, Ack: 1, Len: 0
```

```
0000  a0 d3 7a 6c 1b e6 e0 db  55 0b 74 da 08 00 45 00   ··zl···· U·t···E·
0010  00 28 3e 2e 40 00 40 06  d5 54 0a 0a 0a 03 0a 0a   ·(>.@·@· ·T······
0020  09 37 0c 38 c3 4c 1c ff  b0 69 45 ff 46 59 50 11   ·7·8·L·· ·iE·FYP·
0030  00 9b 5e a5 00 00 00 00  00 00 00 00               ··^····· ····
```

wireshark_7F8FD91E-F507-408E-8E5C-CB20AA58F42F_20181218172524_a09388.pcapng | Packets: 290 · Displayed: 78 (26.9%) · Dropped: 0 (0.0%) | Profile: Default

3. Scenario 3: use filters to capture data originated/destined to known IP address (like google IP, your friends IP, LMS, proxy server IP)



```
ip.addr == 10.10.9.55
```

```
No.   Time        Source         Destination     Protocol Length Info
   54 1.964156    10.10.10.3     10.10.9.55      TCP        60 3128 → 49996 [FIN, ACK] Seq=1 Ack=1 Win=155 Len=0
   55 1.964256    10.10.9.55     10.10.10.3      TCP        54 49996 → 3128 [ACK] Seq=1 Ack=2 Win=1020 Len=0
  115 5.145329    10.10.9.55     161.69.226.72   TCP        66 50088 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
  116 5.145539    10.10.9.55     161.69.226.72   TCP        66 50087 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
  118 5.395744    10.10.10.3     10.10.9.55      TCP        60 3128 → 49999 [FIN, ACK] Seq=1 Ack=1 Win=158 Len=0
  119 5.395832    10.10.9.55     10.10.10.3      TCP        54 49999 → 3128 [ACK] Seq=1 Ack=2 Win=1020 Len=0
  132 5.504757    10.10.9.55     161.69.226.73   TCP        66 50089 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
  138 5.707870    10.10.9.55     161.69.226.70   TCP        66 50090 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
  145 6.256531    10.10.9.55     10.10.10.3      TCP       183 50077 → 3128 [PSH, ACK] Seq=1 Ack=1 Win=64 Len=129
  146 6.256670    10.10.9.55     10.10.10.3      TCP       100 50077 → 3128 [PSH, ACK] Seq=130 Ack=1 Win=64 Len=46
  147 6.256755    10.10.9.55     10.10.10.3      TCP       973 50077 → 3128 [PSH, ACK] Seq=176 Ack=1 Win=64 Len=919
  148 6.259067    10.10.10.3     10.10.9.55      TCP        60 3128 → 50077 [ACK] Seq=1 Ack=130 Win=337 Len=0
  149 6.259068    10.10.10.3     10.10.9.55      TCP        60 3128 → 50077 [ACK] Seq=1 Ack=176 Win=337 Len=0
  150 6.259353    10.10.10.3     10.10.9.55      TCP        60 3128 → 50077 [ACK] Seq=1 Ack=1095 Win=359 Len=0
  151 6.306191    10.10.10.3     10.10.9.55      TCP       100 3128 → 50077 [PSH, ACK] Seq=1 Ack=1095 Win=359 Len=46
  152 6.348362    10.10.9.55     10.10.10.3      TCP        54 50077 → 3128 [ACK] Seq=1095 Ack=47 Win=64 Len=0
  154 6.412364    10.10.10.3     10.10.9.55      TCP       144 3128 → 50077 [PSH, ACK] Seq=47 Ack=1095 Win=359 Len=90
  155 6.412365    10.10.10.3     10.10.9.55      TCP      1423 3128 → 50077 [ACK] Seq=137 Ack=1095 Win=359 Len=1369
  156 6.412367    10.10.10.3     10.10.9.55      TCP       103 3128 → 50077 [PSH, ACK] Seq=1506 Ack=1095 Win=359 Len=49 [TCP segment of a reassembled PDU]
  157 6.412367    10.10.10.3     10.10.9.55      TCP       504 3128 → 50077 [PSH, ACK] Seq=1555 Ack=1095 Win=359 Len=450
  158 6.412368    10.10.10.3     10.10.9.55      TCP       113 3128 → 50077 [PSH, ACK] Seq=2005 Ack=1095 Win=359 Len=59
```

```
> Frame 145: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 0
> Ethernet II, Src: IntelCor_6c:1b:e6 (a0:d3:7a:6c:1b:e6), Dst: Dell_0b:74:da (e0:db:55:0b:74:da)
> Internet Protocol Version 4, Src: 10.10.9.55, Dst: 10.10.10.3
> Transmission Control Protocol, Src Port: 50077, Dst Port: 3128, Seq: 1, Ack: 1, Len: 129
```

```
0000  e0 db 55 0b 74 da a0 d3  7a 6c 1b e6 08 00 45 00   ··U·t···  zl····E·
0010  00 a9 03 03 40 00 80 06  cf fe 0a 0a 09 37 0a 0a   ····@···  ·····7··
0020  0a 03 c3 9d 0c 38 48 e2  6e 4b 5f f9 aa 69 50 18   ·····8H·  nK_··iP·
0030  00 40 be bf 00 00 17 03  03 00 7c 00 00 00 00 00   ·@······  ··|·····
0040  00 00 13 4c 4f c6 8f 21  bb 6f 28 61 50 be 61 08   ···LO··!  ·o(aP·a·
```

```
wireshark_7F8FD91E-F507-408E-8E5C-CB20AA58F42F_20181218172524_a09388.pcapng    Packets: 290 · Displayed: 91 (31.4%) · Dropped: 0 (0.0%)    Profile: Default
```