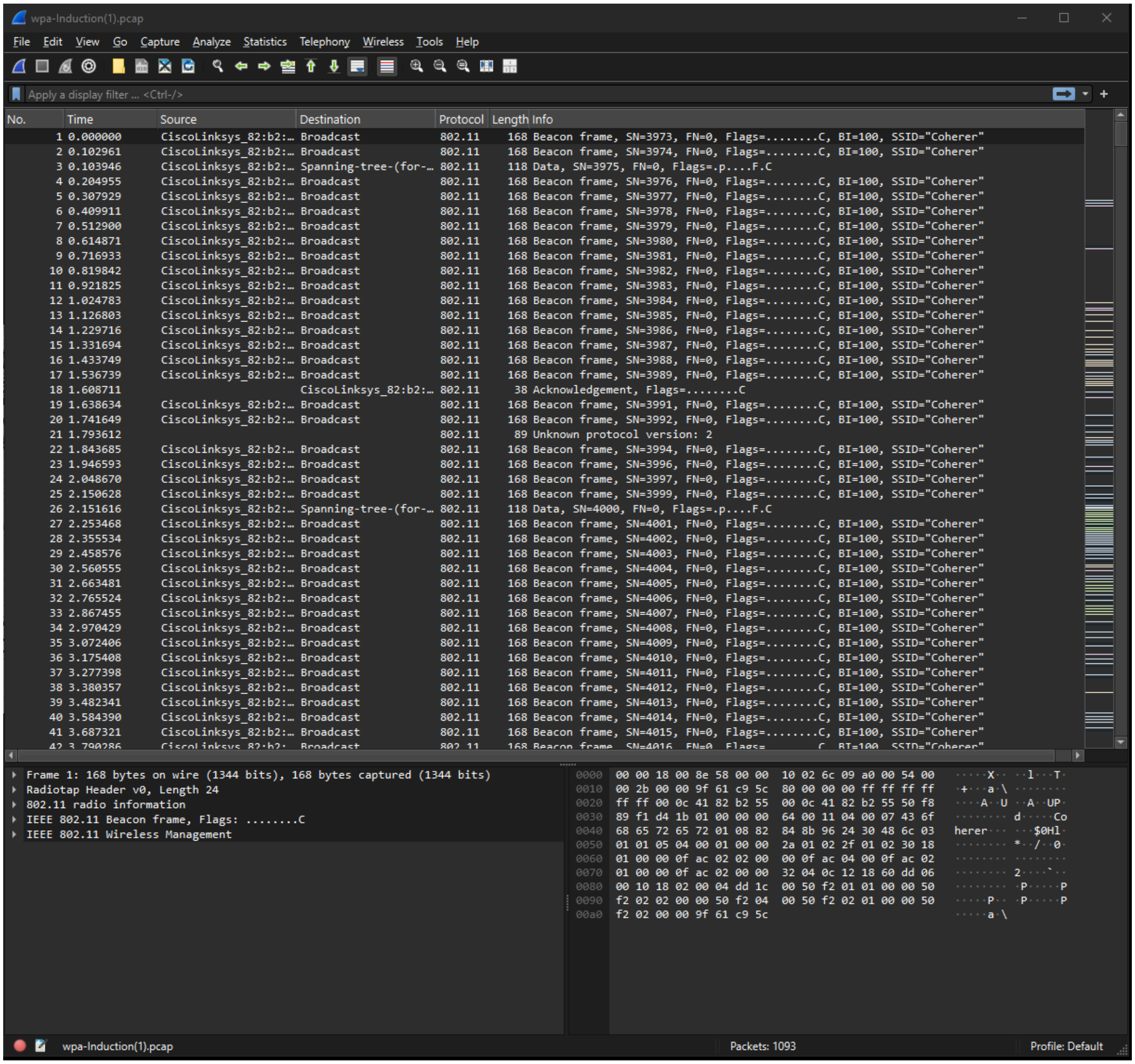
Samantha Jackson
CSCI4406_Lab
10-15-2024

Lab 6 - Traffic Analysis Using Wireshark

Opening “wpa-Induction(1).pcap” in Wireshark

Observations/Issues: None. File downloaded and opened in Wireshark without issue.


wpa-Induction(1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                 Destination            Protocol Length Info
    1 0.000000   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3973, FN=0, Flags=........C, BI=100, SSID="Coherer"
    2 0.102961   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3974, FN=0, Flags=........C, BI=100, SSID="Coherer"
    3 0.103946   CiscoLinksys_82:b2:…   Spanning-tree-(for-…   802.11   118 Data, SN=3975, FN=0, Flags=.p....F.C
    4 0.204955   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3976, FN=0, Flags=........C, BI=100, SSID="Coherer"
    5 0.307929   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3977, FN=0, Flags=........C, BI=100, SSID="Coherer"
    6 0.409911   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3978, FN=0, Flags=........C, BI=100, SSID="Coherer"
    7 0.512900   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3979, FN=0, Flags=........C, BI=100, SSID="Coherer"
    8 0.614871   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3980, FN=0, Flags=........C, BI=100, SSID="Coherer"
    9 0.716933   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3981, FN=0, Flags=........C, BI=100, SSID="Coherer"
   10 0.819842   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3982, FN=0, Flags=........C, BI=100, SSID="Coherer"
   11 0.921825   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3983, FN=0, Flags=........C, BI=100, SSID="Coherer"
   12 1.024783   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3984, FN=0, Flags=........C, BI=100, SSID="Coherer"
   13 1.126803   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3985, FN=0, Flags=........C, BI=100, SSID="Coherer"
   14 1.229716   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3986, FN=0, Flags=........C, BI=100, SSID="Coherer"
   15 1.331694   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3987, FN=0, Flags=........C, BI=100, SSID="Coherer"
   16 1.433749   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3988, FN=0, Flags=........C, BI=100, SSID="Coherer"
   17 1.536739   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3989, FN=0, Flags=........C, BI=100, SSID="Coherer"
   18 1.608711                          CiscoLinksys_82:b2:…   802.11    38 Acknowledgement, Flags=........C
   19 1.638634   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3991, FN=0, Flags=........C, BI=100, SSID="Coherer"
   20 1.741649   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3992, FN=0, Flags=........C, BI=100, SSID="Coherer"
   21 1.793612                                                 802.11    89 Unknown protocol version: 2
   22 1.843685   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3994, FN=0, Flags=........C, BI=100, SSID="Coherer"
   23 1.946593   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3996, FN=0, Flags=........C, BI=100, SSID="Coherer"
   24 2.048670   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3997, FN=0, Flags=........C, BI=100, SSID="Coherer"
   25 2.150628   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=3999, FN=0, Flags=........C, BI=100, SSID="Coherer"
   26 2.151616   CiscoLinksys_82:b2:…   Spanning-tree-(for-…   802.11   118 Data, SN=4000, FN=0, Flags=.p....F.C
   27 2.253468   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4001, FN=0, Flags=........C, BI=100, SSID="Coherer"
   28 2.355534   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4002, FN=0, Flags=........C, BI=100, SSID="Coherer"
   29 2.458576   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4003, FN=0, Flags=........C, BI=100, SSID="Coherer"
   30 2.560555   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4004, FN=0, Flags=........C, BI=100, SSID="Coherer"
   31 2.663481   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4005, FN=0, Flags=........C, BI=100, SSID="Coherer"
   32 2.765524   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4006, FN=0, Flags=........C, BI=100, SSID="Coherer"
   33 2.867455   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4007, FN=0, Flags=........C, BI=100, SSID="Coherer"
   34 2.970429   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4008, FN=0, Flags=........C, BI=100, SSID="Coherer"
   35 3.072406   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4009, FN=0, Flags=........C, BI=100, SSID="Coherer"
   36 3.175408   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4010, FN=0, Flags=........C, BI=100, SSID="Coherer"
   37 3.277398   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4011, FN=0, Flags=........C, BI=100, SSID="Coherer"
   38 3.380357   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4012, FN=0, Flags=........C, BI=100, SSID="Coherer"
   39 3.482341   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4013, FN=0, Flags=........C, BI=100, SSID="Coherer"
   40 3.584390   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4014, FN=0, Flags=........C, BI=100, SSID="Coherer"
   41 3.687321   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4015, FN=0, Flags=........C, BI=100, SSID="Coherer"
   42 3.790286   CiscoLinksys_82:b2:…   Broadcast              802.11   168 Beacon frame, SN=4016, FN=0, Flags=........C, BI=100, SSID="Coherer"
```

```
▸ Frame 1: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▸ IEEE 802.11 Wireless Management
```

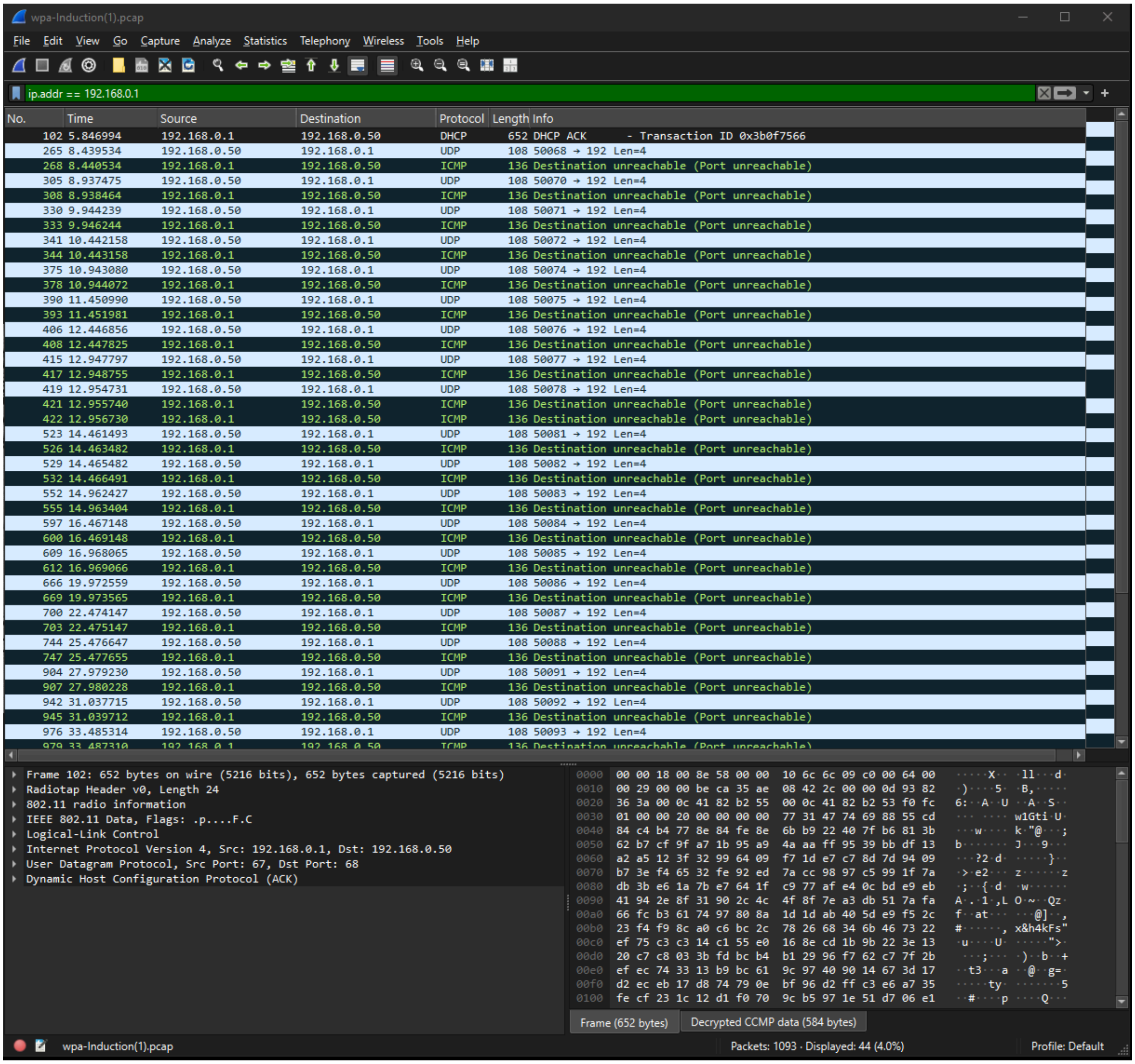
```
0000  00 00 18 00 8e 58 00 00  10 02 6c 09 a0 00 54 00   ·····X·· ··l···T·
0010  00 2b 00 00 9f 61 c9 5c  80 00 00 00 ff ff ff ff   ·+···a·\ ········
0020  ff ff 00 0c 41 82 b2 55  00 0c 41 82 b2 55 50 f8   ····A··U ··A··UP·
0030  89 f1 d4 1b 01 00 00 00  64 00 11 04 00 07 43 6f   ········ d·····Co
0040  68 65 72 65 72 01 08 82  84 8b 96 24 30 48 6c 03   herer··· ···$0Hl·
0050  01 01 05 04 00 01 00 00  2a 01 02 2f 01 02 30 18   ········ *··/··0·
0060  01 00 00 0f ac 02 02 00  00 0f ac 04 00 0f ac 02   ········ ········
0070  01 00 00 0f ac 02 00 00  32 04 0c 12 18 60 dd 06   ········ 2····`··
0080  00 10 18 02 00 04 dd 1c  00 50 f2 01 01 00 00 50   ········ ·P·····P
0090  f2 02 02 00 00 50 f2 04  00 50 f2 02 01 00 00 50   ·····P·· ·P·····P
00a0  f2 02 00 00 9f 61 c9 5c                            ·····a·\
```

wpa-Induction(1).pcap   Packets: 1093   Profile: Default

Filtering traffic using display filters

Applying display filter to filter by IP address – Filtered using ip.addr == 192.168.0.1

Observations/Issues: Filtering by IP address is straightforward. You simply enter the filter into the “Apply a display filter …” search bar. You can enter the filter like “ip.addr == 192.168.0.1”.



wpa-Induction(1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.1

```
No.   Time       Source        Destination   Protocol Length Info
  102 5.846994   192.168.0.1   192.168.0.50  DHCP     652 DHCP ACK      - Transaction ID 0x3b0f7566
  265 8.439534   192.168.0.50  192.168.0.1   UDP      108 50068 → 192 Len=4
  268 8.440534   192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  305 8.937475   192.168.0.50  192.168.0.1   UDP      108 50070 → 192 Len=4
  308 8.938464   192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  330 9.944239   192.168.0.50  192.168.0.1   UDP      108 50071 → 192 Len=4
  333 9.946244   192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  341 10.442158  192.168.0.50  192.168.0.1   UDP      108 50072 → 192 Len=4
  344 10.443158  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  375 10.943080  192.168.0.50  192.168.0.1   UDP      108 50074 → 192 Len=4
  378 10.944072  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  390 11.450990  192.168.0.50  192.168.0.1   UDP      108 50075 → 192 Len=4
  393 11.451981  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  406 12.446856  192.168.0.50  192.168.0.1   UDP      108 50076 → 192 Len=4
  408 12.447825  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  415 12.947797  192.168.0.50  192.168.0.1   UDP      108 50077 → 192 Len=4
  417 12.948755  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  419 12.954731  192.168.0.50  192.168.0.1   UDP      108 50078 → 192 Len=4
  421 12.955740  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  422 12.956730  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  523 14.461493  192.168.0.50  192.168.0.1   UDP      108 50081 → 192 Len=4
  526 14.463482  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  529 14.465482  192.168.0.50  192.168.0.1   UDP      108 50082 → 192 Len=4
  532 14.466491  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  552 14.962427  192.168.0.50  192.168.0.1   UDP      108 50083 → 192 Len=4
  555 14.963404  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  597 16.467148  192.168.0.50  192.168.0.1   UDP      108 50084 → 192 Len=4
  600 16.469148  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  609 16.968065  192.168.0.50  192.168.0.1   UDP      108 50085 → 192 Len=4
  612 16.969066  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  666 19.972559  192.168.0.50  192.168.0.1   UDP      108 50086 → 192 Len=4
  669 19.973565  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  700 22.474147  192.168.0.50  192.168.0.1   UDP      108 50087 → 192 Len=4
  703 22.475147  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  744 25.476647  192.168.0.50  192.168.0.1   UDP      108 50088 → 192 Len=4
  747 25.477655  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  904 27.979230  192.168.0.50  192.168.0.1   UDP      108 50091 → 192 Len=4
  907 27.980228  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  942 31.037715  192.168.0.50  192.168.0.1   UDP      108 50092 → 192 Len=4
  945 31.039712  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
  976 33.485314  192.168.0.50  192.168.0.1   UDP      108 50093 → 192 Len=4
  979 33.487310  192.168.0.1   192.168.0.50  ICMP     136 Destination unreachable (Port unreachable)
```

```
▸ Frame 102: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▸ IEEE 802.11 Data, Flags: .p....F.C
▸ Logical-Link Control
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.50
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▸ Dynamic Host Configuration Protocol (ACK)
```

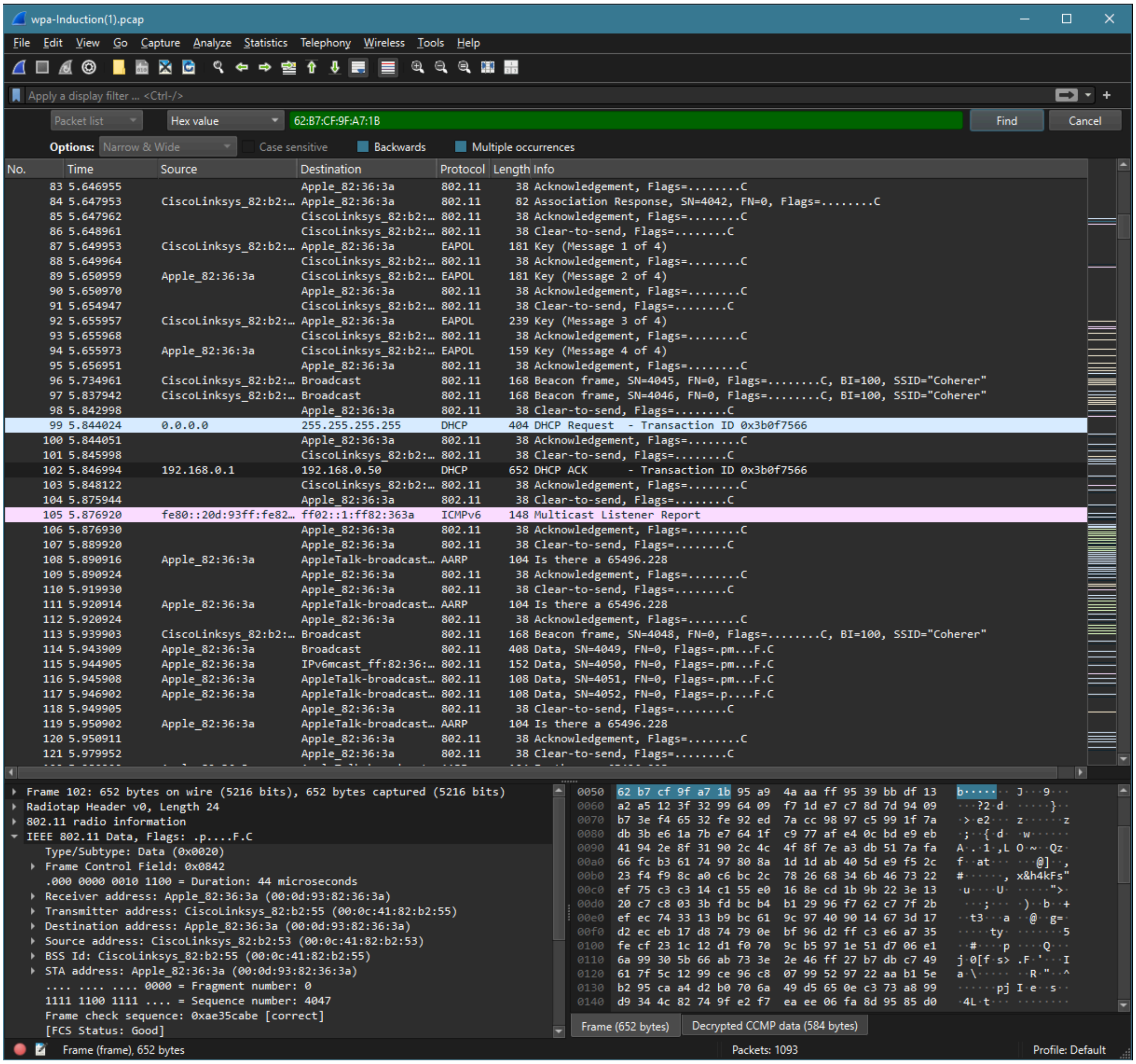
```
0000  00 00 18 00 8e 58 00 00  10 6c 6c 09 c0 00 64 00   ·····X·· ·ll···d·
0010  00 29 00 00 be ca 35 ae  08 42 2c 00 00 0d 93 82   ·)····5· ·B,·····
0020  36 3a 00 0c 41 82 b2 55  00 0c 41 82 b2 53 f0 fc   6:··A··U ··A··S··
0030  01 00 00 20 00 00 00 00  77 31 47 74 69 88 55 cd   ··· ···· w1Gti·U·
0040  84 c4 b4 77 8e 84 fe 8e  6b b9 22 40 7f b6 81 3b   ···w···· k·"@···;
0050  62 b7 cf 9f a7 1b 95 a9  4a aa ff 95 39 bb df 13   b······· J···9···
0060  a2 a5 12 3f 32 99 64 09  f7 1d e7 c7 8d 7d 94 09   ···?2·d· ·····}··
0070  b7 3e f4 65 32 fe 92 ed  7a cc 98 97 c5 99 1f 7a   ·>·e2··· z······z
0080  db 3b e6 1a 7b e7 64 1f  c9 77 af e4 0c bd e9 eb   ·;··{·d· ·w······
0090  41 94 2e 8f 31 90 2c 4c  4f 8f 7e a3 db 51 7a fa   A·.·1·,L O·~··Qz·
00a0  66 fc b3 61 74 97 80 8a  1d 1d ab 40 5d e9 f5 2c   f··at··· ···@]··,
00b0  23 f4 f9 8c a0 c6 bc 2c  78 26 68 34 6b 46 73 22   #······, x&h4kFs"
00c0  ef 75 c3 c3 14 c1 55 e0  16 8e cd 1b 9b 22 3e 13   ·u····U· ·····">·
00d0  20 c7 c8 03 3b fd bc b4  b1 29 96 f7 62 c7 7f 2b    ···;··· ·)··b··+
00e0  ef ec 74 33 13 b9 bc 61  9c 97 40 90 14 67 3d 17   ··t3···a ··@··g=·
00f0  d2 ec eb 17 d8 74 79 0e  bf 96 d2 ff c3 e6 a7 35   ·····ty· ·······5
0100  fe cf 23 1c 12 d1 f0 70  9c b5 97 1e 51 d7 06 e1   ··#····p ····Q···
```

Packets: 1093 · Displayed: 44 (4.0%)

Profile: Default

Applying display filter to filter by Hex value – Filtered using 62:B7:CF:9F:A7:1B

Observations/Issues: Filtering by Hex value isn’t as straightforward as filtering by IP. In order to filter by Hex value you need to use the “Find packet” function in Wireshark > Edit > Find packet. In order to find all applicable results you need to repeatedly hit the “Find” button.



wpa-Induction(1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Find
Cancel

Packet list | Hex value | 62:B7:CF:9F:A7:1B

Options: Narrow & Wide | □ Case sensitive | ☑ Backwards | ☑ Multiple occurrences

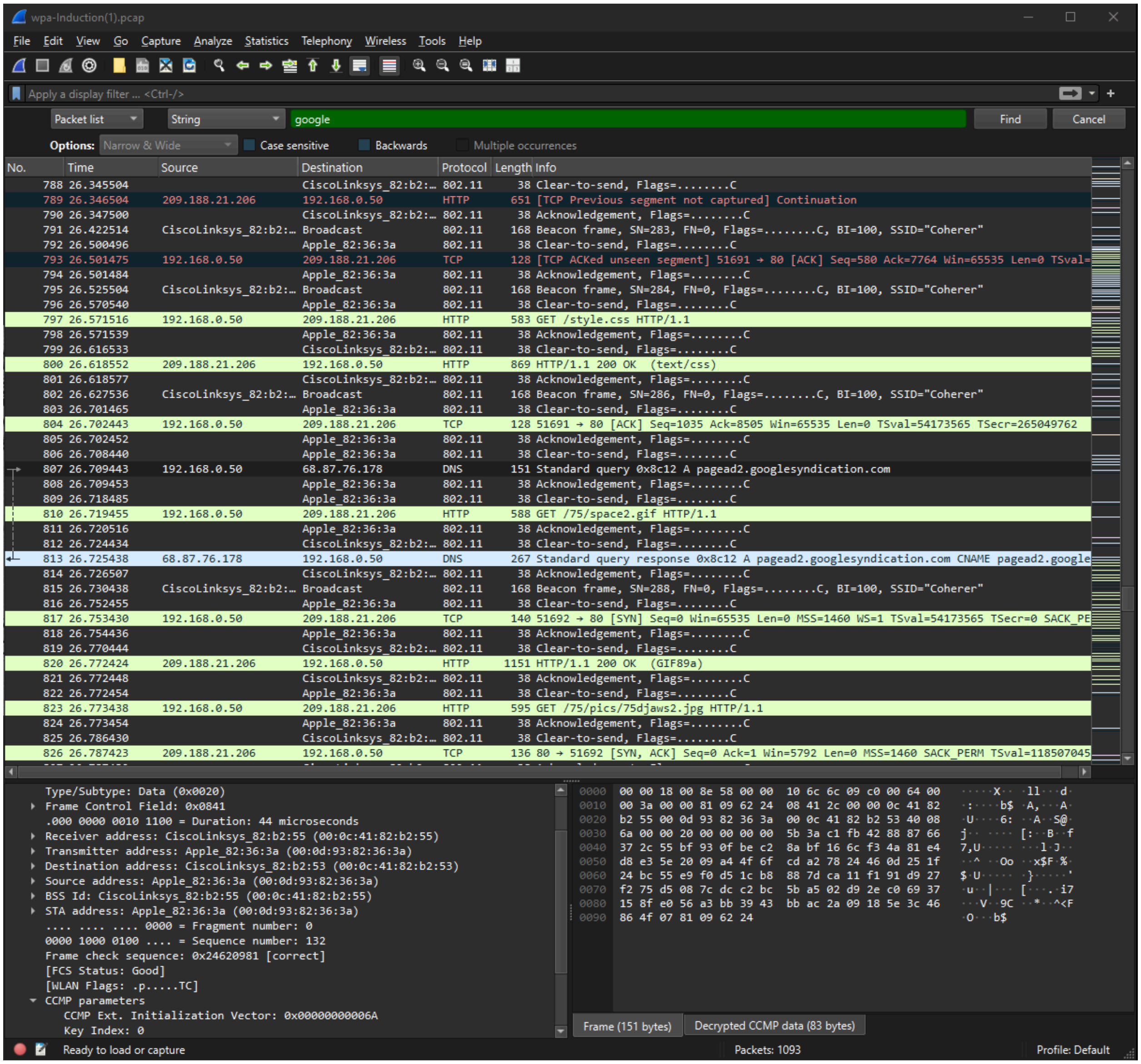
```
No.  Time     Source                 Destination            Protocol Length Info
  83 5.646955                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
  84 5.647953 CiscoLinksys_82:b2:… Apple_82:36:3a         802.11     82 Association Response, SN=4042, FN=0, Flags=........C
  85 5.647962                        CiscoLinksys_82:b2:… 802.11     38 Acknowledgement, Flags=........C
  86 5.648961                        CiscoLinksys_82:b2:… 802.11     38 Clear-to-send, Flags=........C
  87 5.649953 CiscoLinksys_82:b2:… Apple_82:36:3a         EAPOL     181 Key (Message 1 of 4)
  88 5.649964                        CiscoLinksys_82:b2:… 802.11     38 Acknowledgement, Flags=........C
  89 5.650959 Apple_82:36:3a         CiscoLinksys_82:b2:… EAPOL     181 Key (Message 2 of 4)
  90 5.650970                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
  91 5.654947                        CiscoLinksys_82:b2:… 802.11     38 Clear-to-send, Flags=........C
  92 5.655957 CiscoLinksys_82:b2:… Apple_82:36:3a         EAPOL     239 Key (Message 3 of 4)
  93 5.655968                        CiscoLinksys_82:b2:… 802.11     38 Acknowledgement, Flags=........C
  94 5.655973 Apple_82:36:3a         CiscoLinksys_82:b2:… EAPOL     159 Key (Message 4 of 4)
  95 5.656951                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
  96 5.734961 CiscoLinksys_82:b2:… Broadcast              802.11    168 Beacon frame, SN=4045, FN=0, Flags=........C, BI=100, SSID="Coherer"
  97 5.837942 CiscoLinksys_82:b2:… Broadcast              802.11    168 Beacon frame, SN=4046, FN=0, Flags=........C, BI=100, SSID="Coherer"
  98 5.842998                        Apple_82:36:3a         802.11     38 Clear-to-send, Flags=........C
  99 5.844024 0.0.0.0                255.255.255.255        DHCP      404 DHCP Request  - Transaction ID 0x3b0f7566
 100 5.844051                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
 101 5.845998                        CiscoLinksys_82:b2:… 802.11     38 Clear-to-send, Flags=........C
 102 5.846994 192.168.0.1            192.168.0.50           DHCP      652 DHCP ACK      - Transaction ID 0x3b0f7566
 103 5.848122                        CiscoLinksys_82:b2:… 802.11     38 Acknowledgement, Flags=........C
 104 5.875944                        Apple_82:36:3a         802.11     38 Clear-to-send, Flags=........C
 105 5.876920 fe80::20d:93ff:fe82… ff02::1:ff82:363a      ICMPv6    148 Multicast Listener Report
 106 5.876930                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
 107 5.889920                        Apple_82:36:3a         802.11     38 Clear-to-send, Flags=........C
 108 5.890916 Apple_82:36:3a         AppleTalk-broadcast… AARP      104 Is there a 65496.228
 109 5.890924                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
 110 5.919930                        Apple_82:36:3a         802.11     38 Clear-to-send, Flags=........C
 111 5.920914 Apple_82:36:3a         AppleTalk-broadcast… AARP      104 Is there a 65496.228
 112 5.920924                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
 113 5.939903 CiscoLinksys_82:b2:… Broadcast              802.11    168 Beacon frame, SN=4048, FN=0, Flags=........C, BI=100, SSID="Coherer"
 114 5.943909 Apple_82:36:3a         Broadcast              802.11    408 Data, SN=4049, FN=0, Flags=.pm...F.C
 115 5.944905 Apple_82:36:3a         IPv6mcast_ff:82:36:… 802.11    152 Data, SN=4050, FN=0, Flags=.pm...F.C
 116 5.945908 Apple_82:36:3a         AppleTalk-broadcast… 802.11    108 Data, SN=4051, FN=0, Flags=.pm...F.C
 117 5.946902 Apple_82:36:3a         AppleTalk-broadcast… 802.11    108 Data, SN=4052, FN=0, Flags=.p....F.C
 118 5.949905                        Apple_82:36:3a         802.11     38 Clear-to-send, Flags=........C
 119 5.950902 Apple_82:36:3a         AppleTalk-broadcast… AARP      104 Is there a 65496.228
 120 5.950911                        Apple_82:36:3a         802.11     38 Acknowledgement, Flags=........C
 121 5.979952                        Apple_82:36:3a         802.11     38 Clear-to-send, Flags=........C
```

```
▸ Frame 102: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Data, Flags: .p....F.C
    Type/Subtype: Data (0x0020)
  ▸ Frame Control Field: 0x0842
    .000 0000 0010 1100 = Duration: 44 microseconds
  ▸ Receiver address: Apple_82:36:3a (00:0d:93:82:36:3a)
  ▸ Transmitter address: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
  ▸ Destination address: Apple_82:36:3a (00:0d:93:82:36:3a)
  ▸ Source address: CiscoLinksys_82:b2:53 (00:0c:41:82:b2:53)
  ▸ BSS Id: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
  ▸ STA address: Apple_82:36:3a (00:0d:93:82:36:3a)
    .... .... .... 0000 = Fragment number: 0
    1111 1100 1111 .... = Sequence number: 4047
    Frame check sequence: 0xae35cabe [correct]
    [FCS Status: Good]
```

```
0050  62 b7 cf 9f a7 1b 95 a9  4a aa ff 95 39 bb df 13   b······· J···9···
0060  a2 a5 12 3f 32 99 64 09  f7 1d e7 c7 8d 7d 94 09   ···?2·d· ·····}··
0070  b7 3e f4 65 32 fe 92 ed  7a cc 98 97 c5 99 1f 7a   ·>·e2··· z······z
0080  db 3b e6 1a 7b e7 64 1f  c9 77 af e4 0c bd e9 eb   ·;··{·d· ·w······
0090  41 94 2e 8f 31 90 2c 4c  4f 8f 7e a3 db 51 7a fa   A·.·1·,L O·~··Qz·
00a0  66 fc b3 61 74 97 80 8a  1d 1d ab 40 5d e9 f5 2c   f··at··· ···@]··,
00b0  23 f4 f9 8c a0 c6 bc 2c  78 26 68 34 6b 46 73 22   #······, x&h4kFs"
00c0  ef 75 c3 c3 14 c1 55 e0  16 8e cd 1b 9b 22 3e 13   ·u····U· ·····">·
00d0  20 c7 c8 03 3b fd bc b4  b1 29 96 f7 62 c7 7f 2b    ···;··· ·)··b··+
00e0  ef ec 74 33 13 b9 bc 61  9c 97 40 90 14 67 3d 17   ··t3···a ··@··g=·
00f0  d2 ec eb 17 d8 74 79 0e  bf 96 d2 ff c3 e6 a7 35   ·····ty· ·······5
0100  fe cf 23 1c 12 d1 f0 70  9c b5 97 1e 51 d7 06 e1   ··#····p ····Q···
0110  6a 99 30 5b 66 ab 73 3e  2e 46 ff 27 b7 db c7 49   j·0[f·s> .F·'···I
0120  61 7f 5c 12 99 ce 96 c8  07 99 52 97 22 aa b1 5e   a·\····· ··R·"··^
0130  b2 95 ca a4 d2 b0 70 6a  49 d5 65 0e c3 73 a8 99   ······pj I·e··s··
0140  d9 34 4c 82 74 9f e2 f7  ea ee 06 fa 8d 95 85 d0   ·4L·t··· ········
```

Applying display filter to filter by string – Filtered using google

Observations/Issues: Filtering by string uses the same function (Wireshark > Edit > Find) as filtering by Hex you just change the search term to String. In order to find all applicable results you need to repeatedly hit the “Find” button.


wpa-Induction(1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Find
Cancel
Frame (151 bytes)
Decrypted CCMP data (83 bytes)

Packet list | String | google

Options: Narrow & Wide □ Case sensitive □ Backwards □ Multiple occurrences

```
No.  Time      Source               Destination          Protocol Length Info
 788 26.345504                      CiscoLinksys_82:b2:… 802.11    38 Clear-to-send, Flags=........C
 789 26.346504 209.188.21.206       192.168.0.50         HTTP     651 [TCP Previous segment not captured] Continuation
 790 26.347500                      CiscoLinksys_82:b2:… 802.11    38 Acknowledgement, Flags=........C
 791 26.422514 CiscoLinksys_82:b2:… Broadcast            802.11   168 Beacon frame, SN=283, FN=0, Flags=........C, BI=100, SSID="Coherer"
 792 26.500496                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 793 26.501475 192.168.0.50         209.188.21.206       TCP      128 [TCP ACKed unseen segment] 51691 → 80 [ACK] Seq=580 Ack=7764 Win=65535 Len=0 TSval=
 794 26.501484                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 795 26.525504 CiscoLinksys_82:b2:… Broadcast            802.11   168 Beacon frame, SN=284, FN=0, Flags=........C, BI=100, SSID="Coherer"
 796 26.570540                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 797 26.571516 192.168.0.50         209.188.21.206       HTTP     583 GET /style.css HTTP/1.1
 798 26.571539                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 799 26.616533                      CiscoLinksys_82:b2:… 802.11    38 Clear-to-send, Flags=........C
 800 26.618552 209.188.21.206       192.168.0.50         HTTP     869 HTTP/1.1 200 OK  (text/css)
 801 26.618577                      CiscoLinksys_82:b2:… 802.11    38 Acknowledgement, Flags=........C
 802 26.627536 CiscoLinksys_82:b2:… Broadcast            802.11   168 Beacon frame, SN=286, FN=0, Flags=........C, BI=100, SSID="Coherer"
 803 26.701465                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 804 26.702443 192.168.0.50         209.188.21.206       TCP      128 51691 → 80 [ACK] Seq=1035 Ack=8505 Win=65535 Len=0 TSval=54173565 TSecr=265049762
 805 26.702452                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 806 26.708440                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 807 26.709443 192.168.0.50         68.87.76.178         DNS      151 Standard query 0x8c12 A pagead2.googlesyndication.com
 808 26.709453                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 809 26.718485                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 810 26.719455 192.168.0.50         209.188.21.206       HTTP     588 GET /75/space2.gif HTTP/1.1
 811 26.720516                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 812 26.724434                      CiscoLinksys_82:b2:… 802.11    38 Clear-to-send, Flags=........C
 813 26.725438 68.87.76.178         192.168.0.50         DNS      267 Standard query response 0x8c12 A pagead2.googlesyndication.com CNAME pagead2.google
 814 26.726507                      CiscoLinksys_82:b2:… 802.11    38 Acknowledgement, Flags=........C
 815 26.730438 CiscoLinksys_82:b2:… Broadcast            802.11   168 Beacon frame, SN=288, FN=0, Flags=........C, BI=100, SSID="Coherer"
 816 26.752455                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 817 26.753430 192.168.0.50         209.188.21.206       TCP      140 51692 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSval=54173565 TSecr=0 SACK_PE
 818 26.754436                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 819 26.770444                      CiscoLinksys_82:b2:… 802.11    38 Clear-to-send, Flags=........C
 820 26.772424 209.188.21.206       192.168.0.50         HTTP    1151 HTTP/1.1 200 OK  (GIF89a)
 821 26.772448                      CiscoLinksys_82:b2:… 802.11    38 Acknowledgement, Flags=........C
 822 26.772454                      Apple_82:36:3a       802.11    38 Clear-to-send, Flags=........C
 823 26.773438 192.168.0.50         209.188.21.206       HTTP     595 GET /75/pics/75djaws2.jpg HTTP/1.1
 824 26.773454                      Apple_82:36:3a       802.11    38 Acknowledgement, Flags=........C
 825 26.786430                      CiscoLinksys_82:b2:… 802.11    38 Clear-to-send, Flags=........C
 826 26.787423 209.188.21.206       192.168.0.50         TCP      136 80 → 51692 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=118507045
```

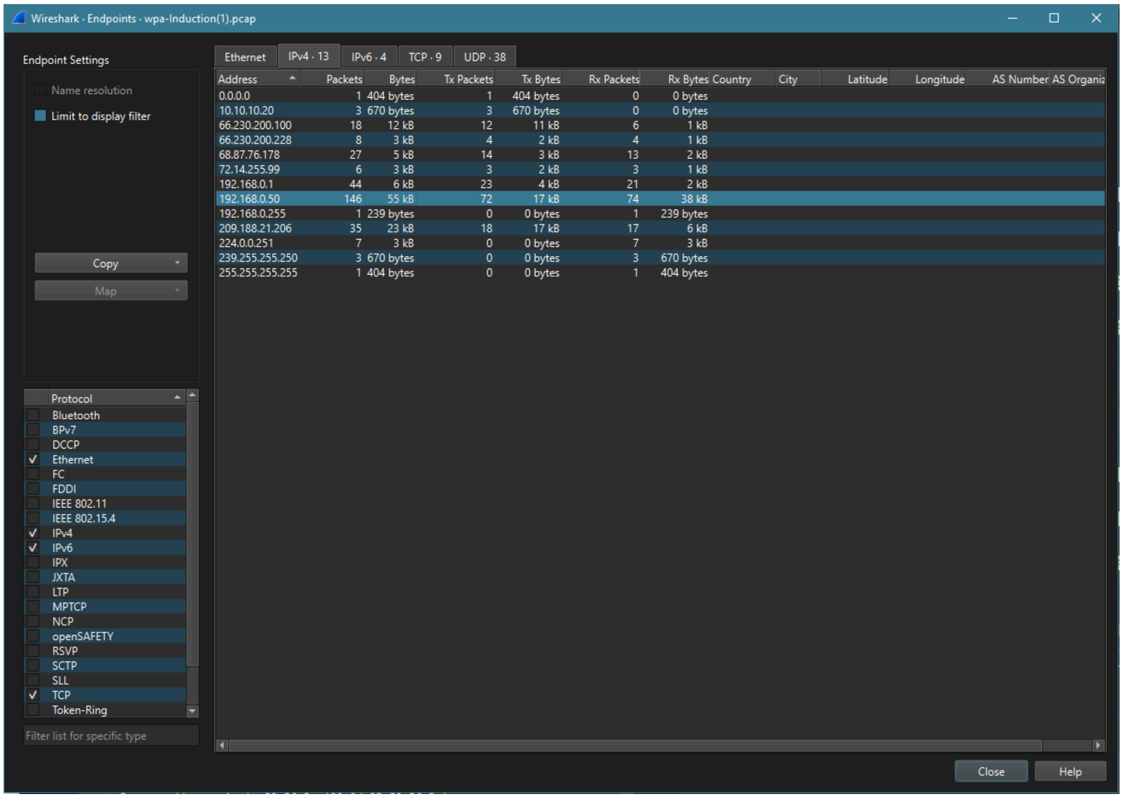
```
    Type/Subtype: Data (0x0020)
  ▸ Frame Control Field: 0x0841
    .000 0000 0010 1100 = Duration: 44 microseconds
  ▸ Receiver address: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
  ▸ Transmitter address: Apple_82:36:3a (00:0d:93:82:36:3a)
  ▸ Destination address: CiscoLinksys_82:b2:53 (00:0c:41:82:b2:53)
  ▸ Source address: Apple_82:36:3a (00:0d:93:82:36:3a)
  ▸ BSS Id: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
  ▸ STA address: Apple_82:36:3a (00:0d:93:82:36:3a)
    .... .... .... 0000 = Fragment number: 0
    0000 1000 0100 .... = Sequence number: 132
    Frame check sequence: 0x24620981 [correct]
    [FCS Status: Good]
    [WLAN Flags: .p.....TC]
  ▾ CCMP parameters
      CCMP Ext. Initialization Vector: 0x00000000006A
      Key Index: 0
```

```
0000  00 00 18 00 8e 58 00 00  10 6c 6c 09 c0 00 64 00   ·····X·· ·ll···d·
0010  00 3a 00 00 81 09 62 24  08 41 2c 00 00 0c 41 82   ·:····b$ ·A,···A·
0020  b2 55 00 0d 93 82 36 3a  00 0c 41 82 b2 53 40 08   ·U····6: ··A··S@·
0030  6a 00 00 20 00 00 00 00  5b 3a c1 fb 42 88 87 66   j·· ···· [:··B··f
0040  37 2c 55 bf 93 0f be c2  8a bf 16 6c f3 4a 81 e4   7,U····· ···l·J··
0050  d8 e3 5e 20 09 a4 4f 6f  cd a2 78 24 46 0d 25 1f   ··^ ··Oo ··x$F·%·
0060  24 bc 55 e9 f0 d5 1c b8  88 7d ca 11 f1 91 d9 27   $·U····· ·}·····'
0070  f2 75 d5 08 7c dc c2 bc  5b a5 02 d9 2e c0 69 37   ·u··|··· [···.·i7
0080  15 8f e0 56 a3 bb 39 43  bb ac 2a 09 18 5e 3c 46   ···V··9C ··*··^<F
0090  86 4f 07 81 09 62 24                               ·O···b$
```

Ready to load or capture | Packets: 1093 | Profile: Default

Analyzing endpoints

Observations/Issues: I selected TCP package #773 under the IPv4 tab end point 192.168.0.50 had the most packets at 146. IPv6 had significantly less traffic with the most intensive endpoint being 9 packets at address fe80::20d:93ff:fe82:363a


Wireshark · Endpoints · wpa-Induction(1).pcap
Copy
Map
Close
Help
Filter list for specific type

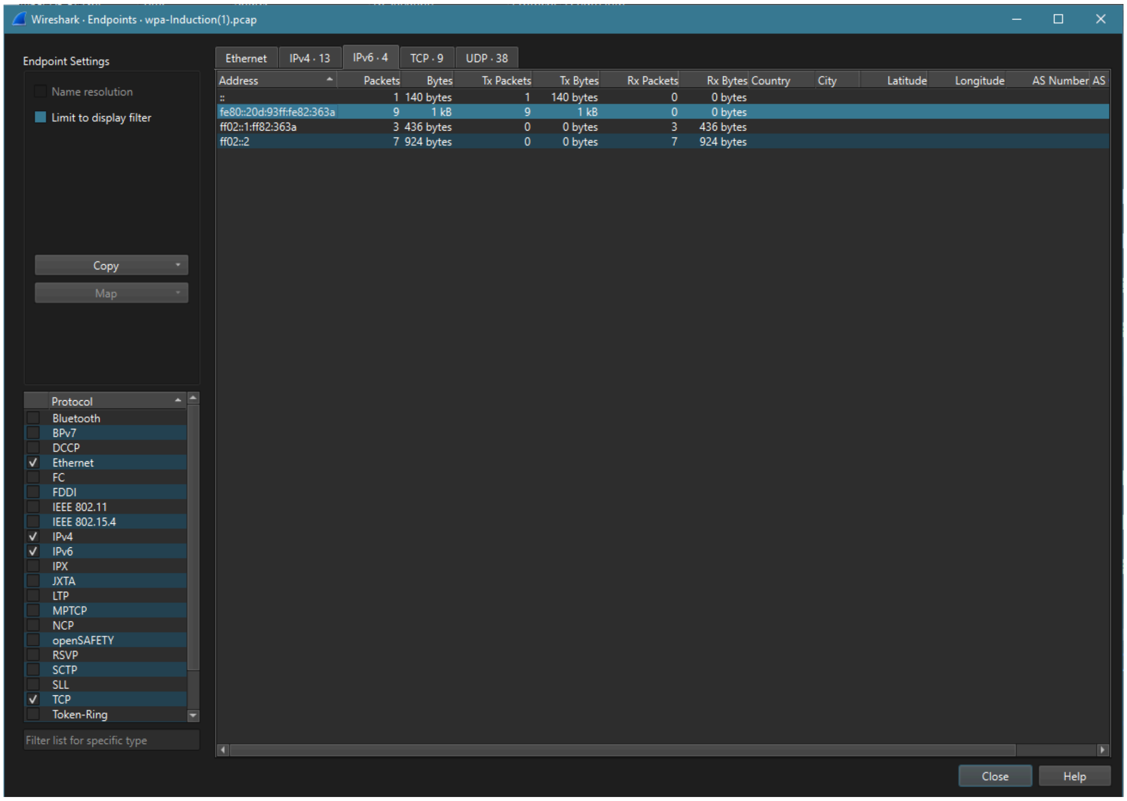
Endpoint Settings

☐ Name resolution
☑ Limit to display filter

	Protocol
☐	Bluetooth
☐	BPv7
☐	DCCP
✓	Ethernet
☐	FC
☐	FDDI
☐	IEEE 802.11
☐	IEEE 802.15.4
✓	IPv4
✓	IPv6
☐	IPX
☐	JXTA
☐	LTP
☐	MPTCP
☐	NCP
☐	openSAFETY
☐	RSVP
☐	SCTP
☐	SLL
✓	TCP
☐	Token-Ring

Ethernet | IPv4 · 13 | IPv6 · 4 | TCP · 9 | UDP · 38

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organiz
0.0.0.0	1	404 bytes	1	404 bytes	0	0 bytes						
10.10.10.20	3	670 bytes	3	670 bytes	0	0 bytes						
66.230.200.100	18	12 kB	12	11 kB	6	1 kB						
66.230.200.228	8	3 kB	4	2 kB	4	1 kB						
68.87.76.178	27	5 kB	14	3 kB	13	2 kB						
72.14.255.99	6	3 kB	3	2 kB	3	1 kB						
192.168.0.1	44	6 kB	23	4 kB	21	2 kB						
192.168.0.50	146	55 kB	72	17 kB	74	38 kB						
192.168.0.255	1	239 bytes	0	0 bytes	1	239 bytes						
209.188.21.206	35	23 kB	18	17 kB	17	6 kB						
224.0.0.251	7	3 kB	0	0 bytes	7	3 kB						
239.255.255.250	3	670 bytes	0	0 bytes	3	670 bytes						
255.255.255.255	1	404 bytes	0	0 bytes	1	404 bytes						


Wireshark · Endpoints · wpa-Induction(1).pcap
Copy
Map
Close
Help
Filter list for specific type

Endpoint Settings

☐ Name resolution
☑ Limit to display filter

	Protocol
☐	Bluetooth
☐	BPv7
☐	DCCP
✓	Ethernet
☐	FC
☐	FDDI
☐	IEEE 802.11
☐	IEEE 802.15.4
✓	IPv4
✓	IPv6
☐	IPX
☐	JXTA
☐	LTP
☐	MPTCP
☐	NCP
☐	openSAFETY
☐	RSVP
☐	SCTP
☐	SLL
✓	TCP
☐	Token-Ring

Ethernet | IPv4 · 13 | IPv6 · 4 | TCP · 9 | UDP · 38

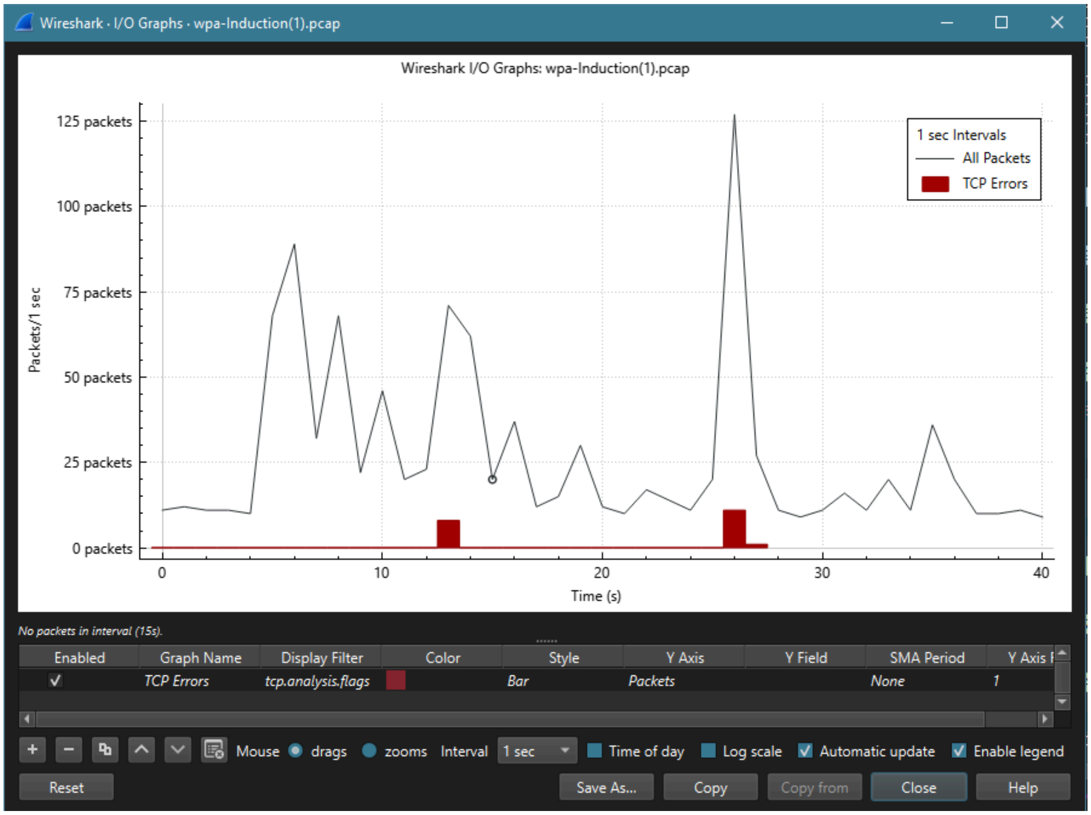
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS
::	1	140 bytes	1	140 bytes	0	0 bytes						
fe80::20d:93ff:fe82:363a	9	1 kB	9	1 kB	0	0 bytes						
ff02::1:ff82:363a	3	436 bytes	0	0 bytes	3	436 bytes						
ff02::2	7	924 bytes	0	0 bytes	7	924 bytes						

Analyzing graphs for traffic

IO Graphs

Observations/Issues: No issues. There are multiple filters for I/O Graphs that could make it useful for network analysis under many different circumstances.

No filter

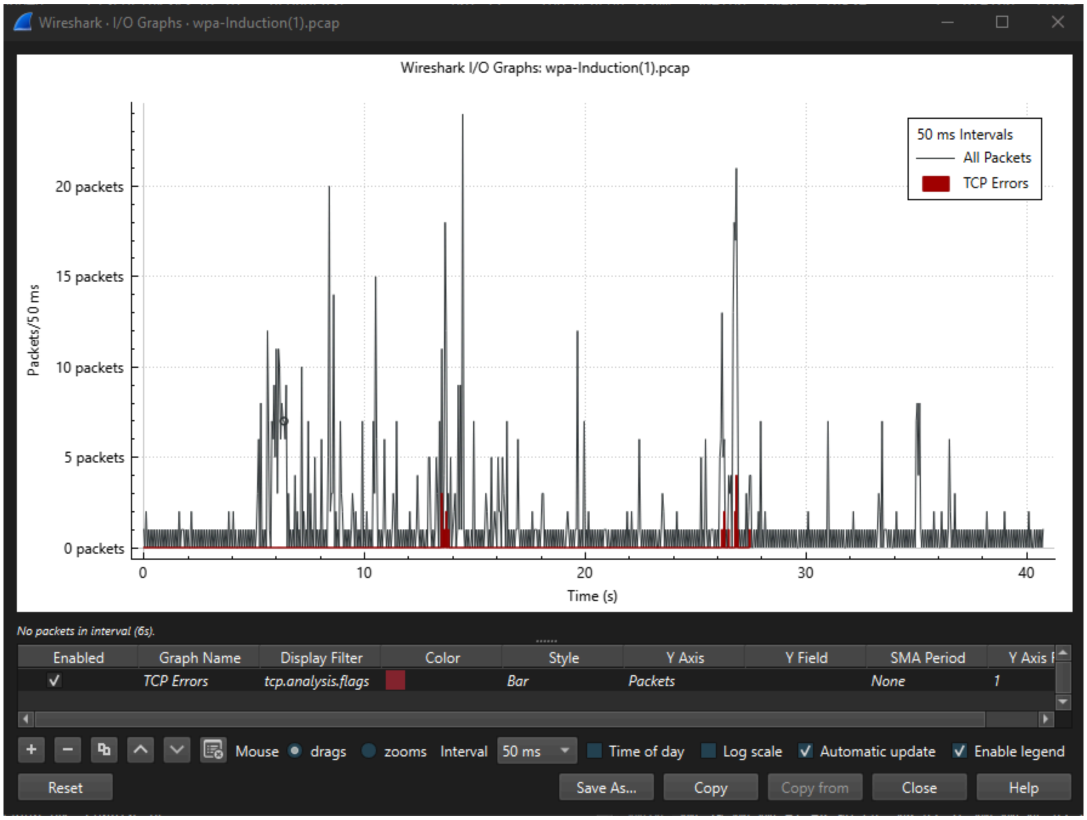


No packets in interval (15s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis F
✓	*TCP Errors*	*tcp.analysis.flags*	🟥	*Bar*	*Packets*		*None*	*1*

Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

Interval: 50 ms

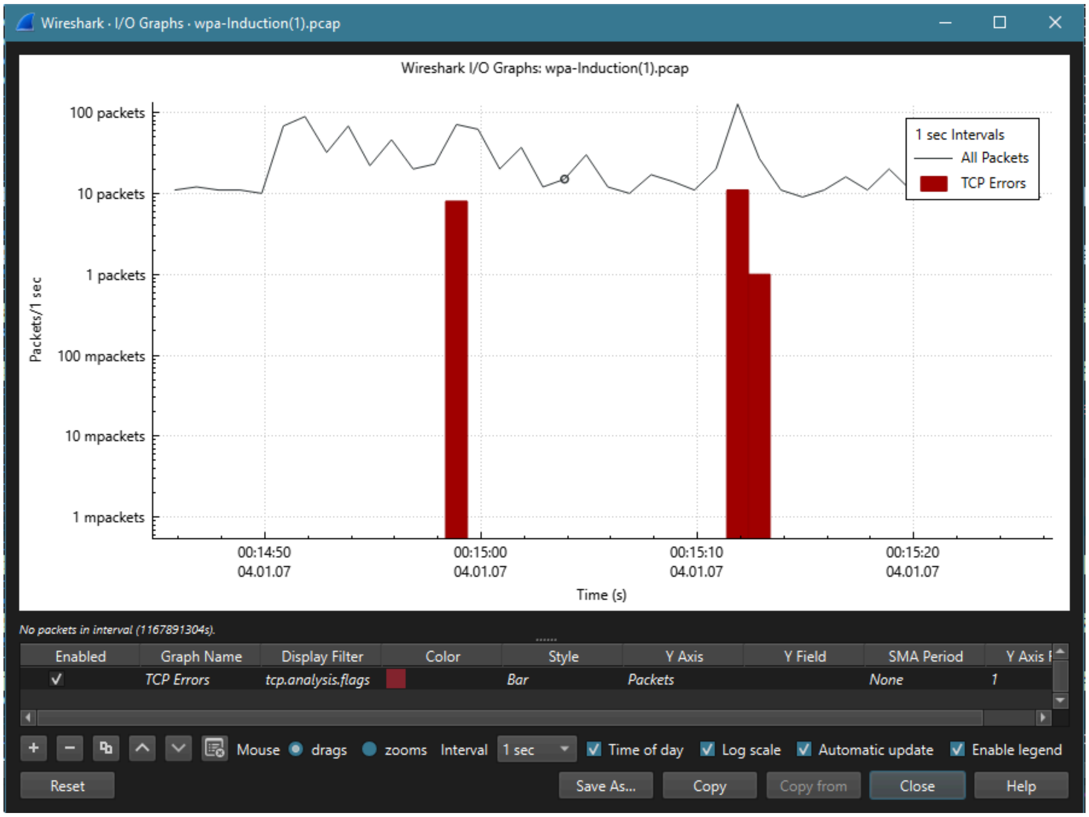


No packets in interval (6s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis I
✓	*TCP Errors*	*tcp.analysis.flags*	🟥	*Bar*	*Packets*		*None*	*1*

Mouse ● drags ○ zooms Interval 50 ms □ Time of day □ Log scale ☑ Automatic update ☑ Enable legend

Interval: 1 sec, Time of day, Log scale



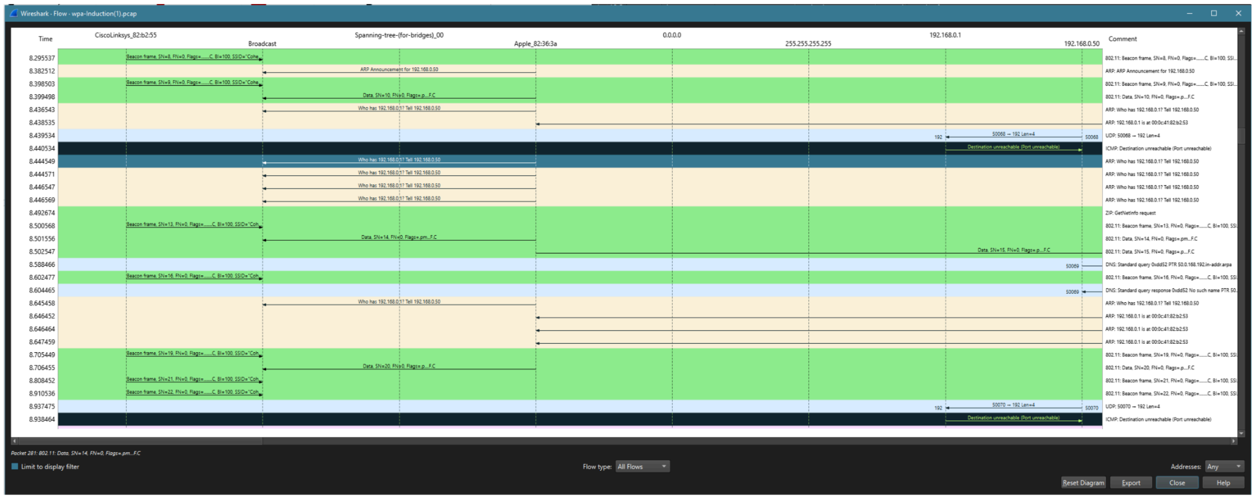
No packets in interval (1167891304s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis I
✓	*TCP Errors*	*tcp.analysis.flags*	🟥	*Bar*	*Packets*		*None*	*1*

Mouse ● drags ○ zooms Interval 1 sec ☑ Time of day ☑ Log scale ☑ Automatic update ☑ Enable legend

Flow Graphs

Observations/Issues: No issues. This Flow Graph is pretty interesting in the context of network analysis. It allows you to see a variety of things but most valuable is probably unreachable ports which give a time stamp and any surrounding comments.



Wireshark · Flow · wpa-Induction(1).pcap

CiscoLinksys_82:b2:55
Broadcast
Spanning-tree-(for-bridges)_00
Apple_82:36:3a
0.0.0.0
255.255.255.255
192.168.0.1
192.168.0.50
Beacon frame, SN=8, FN=0, Flags=........C, BI=100, SSID="Cohe...
ARP Announcement for 192.168.0.50
Data, SN=10, FN=0, Flags=.p....F.C
Who has 192.168.0.1? Tell 192.168.0.50
192
50068 → 192 Len=4
50068
Destination unreachable (Port unreachable)
Data, SN=14, FN=0, Flags=.pm...F.C
Data, SN=15, FN=0, Flags=.p....F.C
50069
Data, SN=20, FN=0, Flags=.p....F.C
50070 → 192 Len=4
50070

```
Time       Comment
8.295537   802.11: Beacon frame, SN=8, FN=0, Flags=........C, BI=100, SSI...
8.382512   ARP: ARP Announcement for 192.168.0.50
8.398503   802.11: Beacon frame, SN=9, FN=0, Flags=........C, BI=100, SSI...
8.399498   802.11: Data, SN=10, FN=0, Flags=.p....F.C
8.436543   ARP: Who has 192.168.0.1? Tell 192.168.0.50
8.438535   ARP: 192.168.0.1 is at 00:0c:41:82:b2:53
8.439534   UDP: 50068 → 192 Len=4
8.440534   ICMP: Destination unreachable (Port unreachable)
8.444549   ARP: Who has 192.168.0.1? Tell 192.168.0.50
8.444571   ARP: Who has 192.168.0.1? Tell 192.168.0.50
8.446547   ARP: Who has 192.168.0.1? Tell 192.168.0.50
8.446569   ARP: Who has 192.168.0.1? Tell 192.168.0.50
8.492674   ZIP: GetNetInfo request
8.500568   802.11: Beacon frame, SN=13, FN=0, Flags=........C, BI=100, SSI
8.501556   802.11: Data, SN=14, FN=0, Flags=.pm...F.C
8.502547   802.11: Data, SN=15, FN=0, Flags=.p....F.C
8.588466   DNS: Standard query 0xdd52 PTR 50.0.168.192.in-addr.arpa
8.602477   802.11: Beacon frame, SN=16, FN=0, Flags=........C, BI=100, SSI
8.604465   DNS: Standard query response 0xdd52 No such name PTR 50...
8.645458   ARP: Who has 192.168.0.1? Tell 192.168.0.50
8.646452   ARP: 192.168.0.1 is at 00:0c:41:82:b2:53
8.646464   ARP: 192.168.0.1 is at 00:0c:41:82:b2:53
8.647459   ARP: 192.168.0.1 is at 00:0c:41:82:b2:53
8.705449   802.11: Beacon frame, SN=19, FN=0, Flags=........C, BI=100, SSI
8.706455   802.11: Data, SN=20, FN=0, Flags=.p....F.C
8.808452   802.11: Beacon frame, SN=21, FN=0, Flags=........C, BI=100, SSI
8.910536   802.11: Beacon frame, SN=22, FN=0, Flags=........C, BI=100, SSI
8.937475   UDP: 50070 → 192 Len=4
8.938464   ICMP: Destination unreachable (Port unreachable)
```

Packet 281: 802.11: Data, SN=14, FN=0, Flags=.pm...F.C

■ Limit to display filter

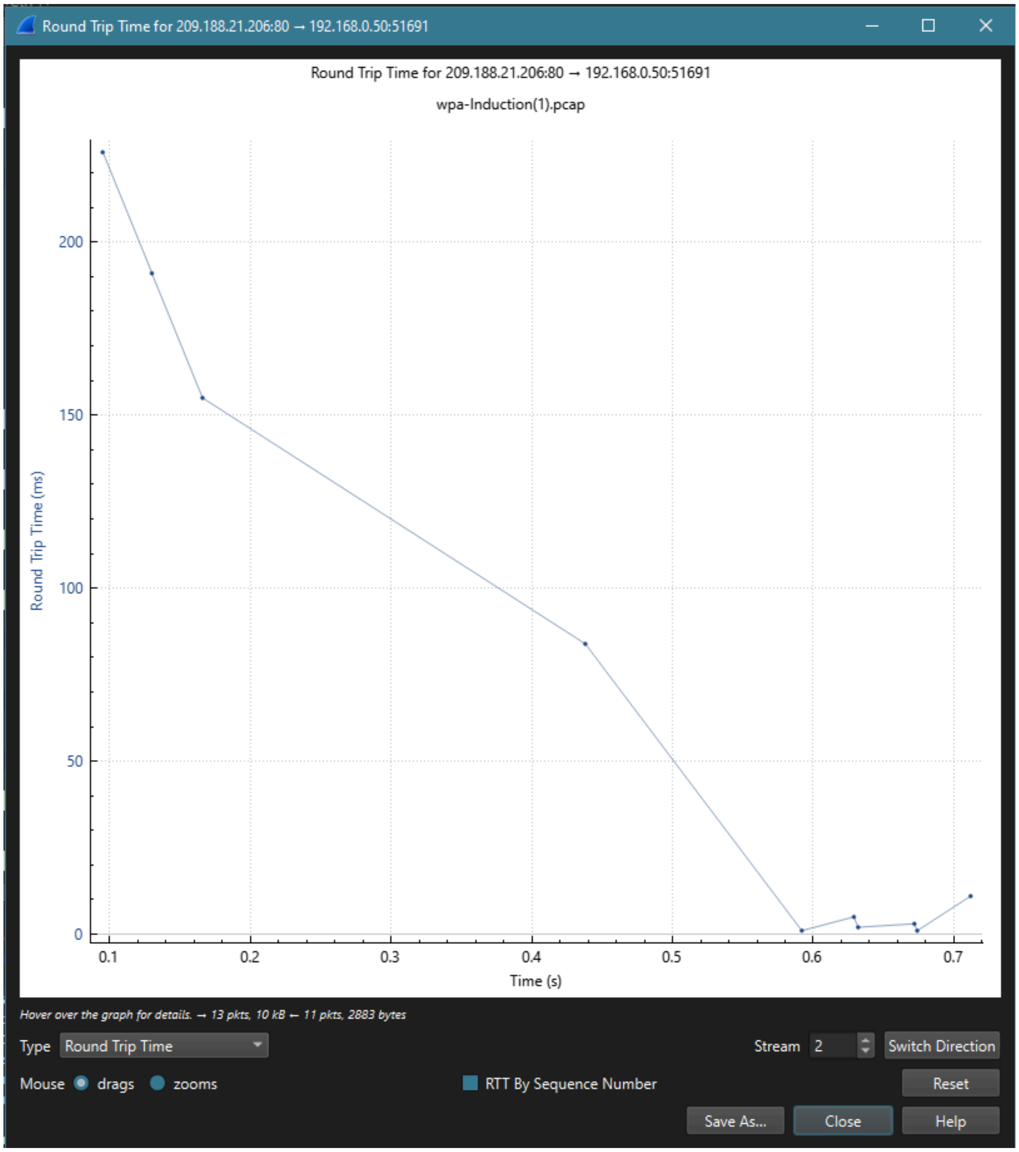
Flow type: All Flows

Addresses: Any

TCP Stream Graphs

Round-trip time graphs

Observations/Issues: No issues. I filtered the results using TCP packet #773. This packet shows a decrease in traffic not all the way down to zero but fairly close.



Round Trip Time for 209.188.21.206:80 → 192.168.0.50:51691

Round Trip Time for 209.188.21.206:80 → 192.168.0.50:51691

wpa-Induction(1).pcap

Hover over the graph for details. → 13 pkts, 10 kB ← 11 pkts, 2883 bytes

Type: Round Trip Time

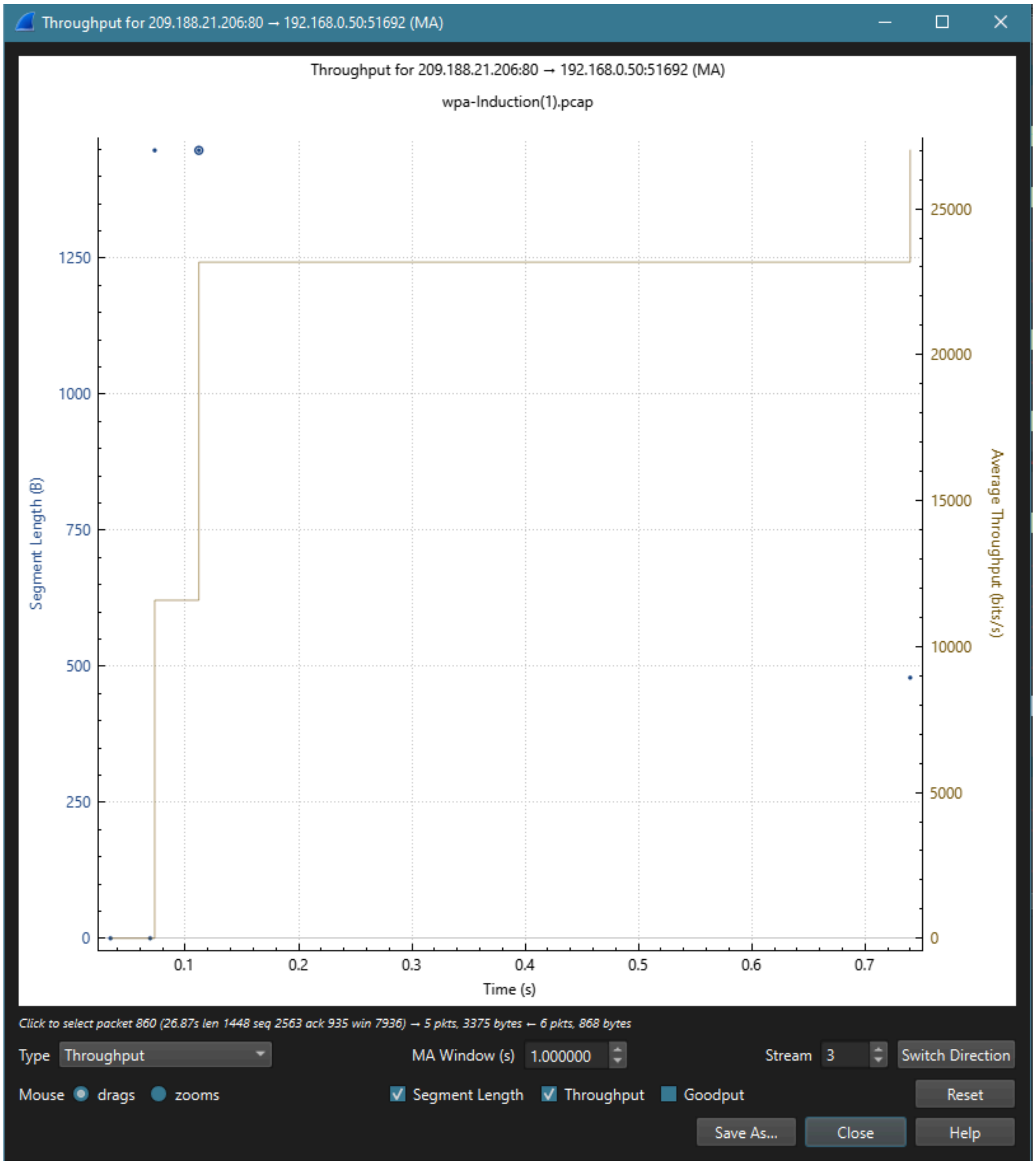
Stream: 2

Mouse: ● drags ○ zooms

□ RTT By Sequence Number

Throughput graphs (tcp trace)

Observations/Issues: No issues. Selected packet #773 this looks significantly different from the provided example but that’s probably because of the difference in files.



Click to select packet 860 (26.87s len 1448 seq 2563 ack 935 win 7936) → 5 pkts, 3375 bytes ← 6 pkts, 868 bytes

Type Throughput

MA Window (s) 1.000000

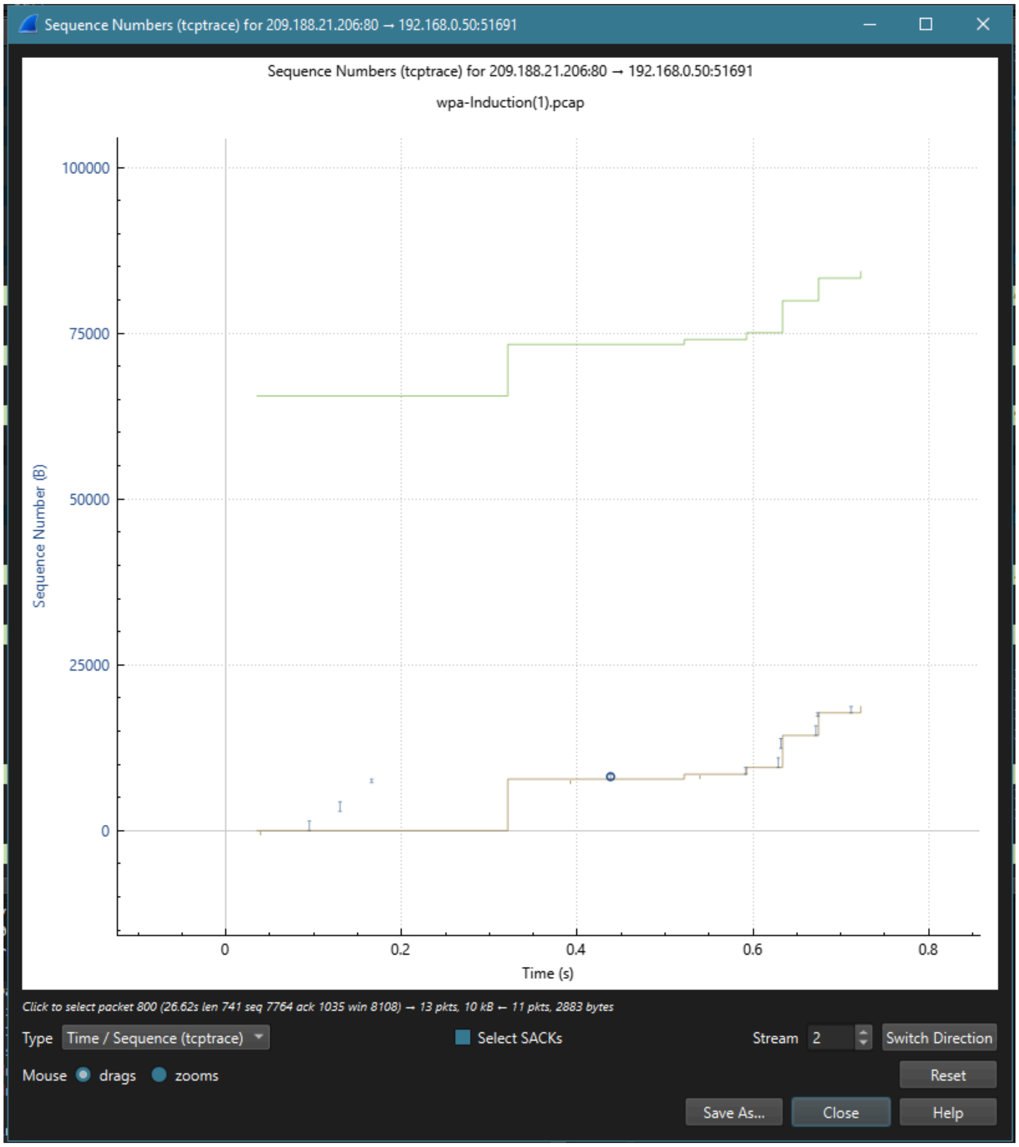
Stream 3

Mouse ● drags ○ zooms

☑ Segment Length ☑ Throughput □ Goodput

Time sequence graphs

Observations/Issues: No issues. Selected packet #773. This one looks similar to the provided example and mimics the previous throughput graph.



Sequence Numbers (tcptrace) for 209.188.21.206:80 → 192.168.0.50:51691

Sequence Numbers (tcptrace) for 209.188.21.206:80 → 192.168.0.50:51691

wpa-Induction(1).pcap

Click to select packet 800 (26.62s len 741 seq 7764 ack 1035 win 8108) → 13 pkts, 10 kB ← 11 pkts, 2883 bytes

Type Time / Sequence (tcptrace)

☑ Select SACKs

Stream 2

Mouse ● drags ○ zooms