

Summer 2010 - Session 6868

End the journey through the dark

Turn on the light with wireshark

Matthias Burkhard
mburkhar@de.ibm.com
IBM Germany

Thursday, August 5, 2010: 11:00 AM-12:30 PM
Hynes Convention Center, Room 109



SHARE in Boston



Session Content



Now that you know the various layers of Enterprise Extender packets and the external symptoms of HPR problems it is time to look at some real examples of network flows.

Learn how to configure the wireshark trace tool to identify HPR flows in an IP trace more easily.

See how applying intelligent filters to an IP trace can speed up problem source identification and resolution of EE problems.

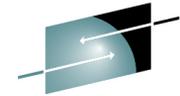
You're invited to bring your notebook with the latest version of the tracetool to gain some hands on experience during this session.

The journey through the dark



```
IST1494I PATH SWITCH STARTED FOR RTP CNR0F621 TO netid.cpname  
IST1818I PATH SWITCH REASON: SHORT REQUEST RETRY LIMIT EXH  
  
IST1494I PATH SWITCH FAILED FOR RTP CNR0F621 TO netid.cpname  
IST1495I NO ALTERNATE ROUTE AVAILABLE
```





Turn on the light with wireshark



Inbound Traffic - FW1

TTL61 → FIREWALL → TTL60

s4p1c0 s4p2c0

TTL54 ← FIREWALL ← TTL55

s4p1c0 s4p2c0

Wireshark IO Graphs: fw1.cap

d:\00622.tucbgw2.pcap - Wireshark

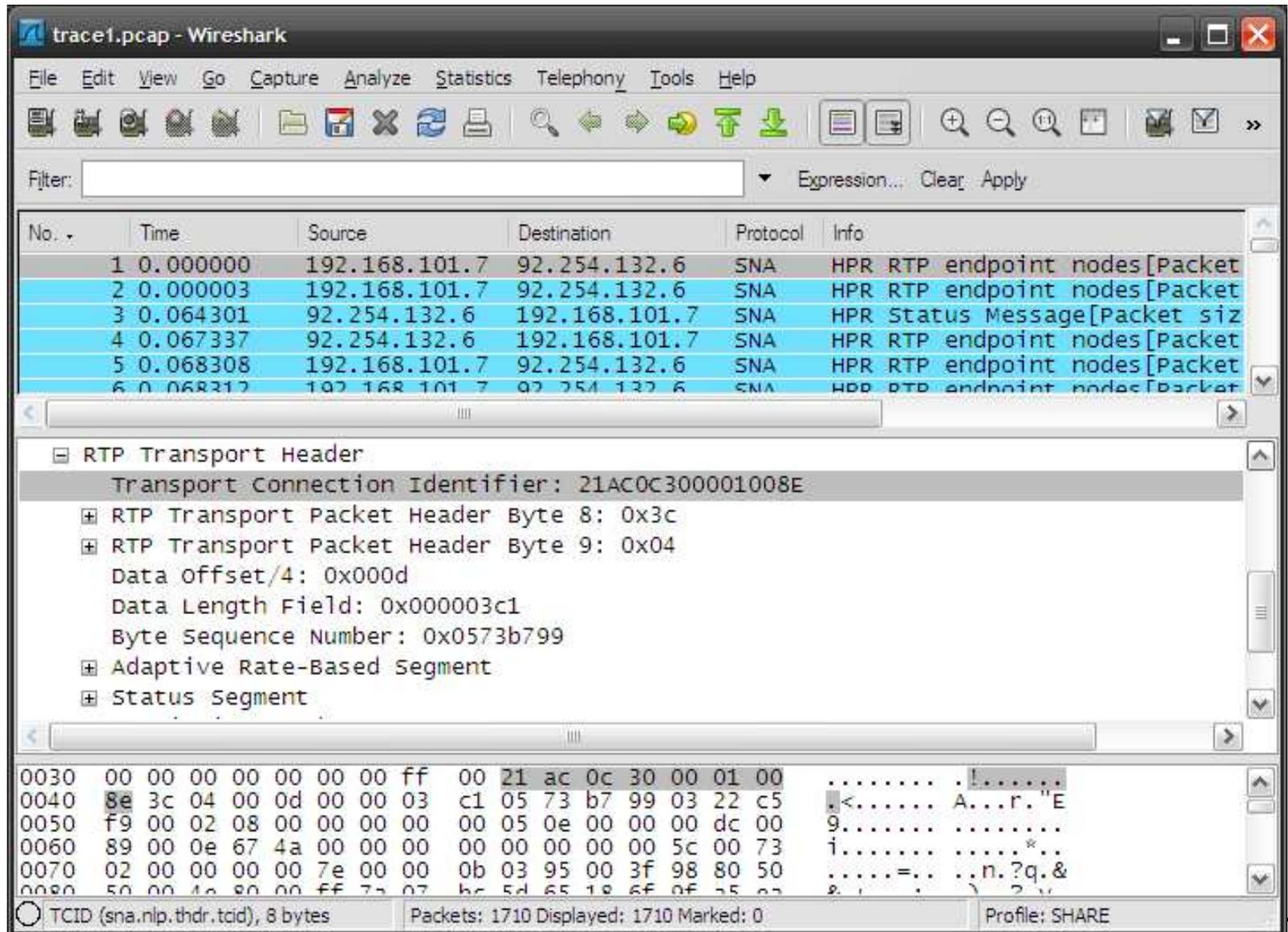
| No. | Time | Source | Destination | dst.port | ANR label | TCID |
|-----|-------------|-----------|-------------|----------|--------------------|------------------|
| 121 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 0200000000000000FF | 800000000300298 |
| 122 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 80FF | 00000000000298 |
| 123 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | D000000000000000FF | 1FDAD750000102c |
| 124 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 80FF | 00000000000298 |
| 125 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 80FF | 00000000000298 |
| 126 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | D200000000000000FF | 1FDAD751000102c |
| 127 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | D000000000000000FF | 800000000200298 |
| 128 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 0000000000000000FF | 80000000000298 |
| 129 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 80FF | 0000000000020298 |
| 130 | 16:24:14.24 | 196.23.91 | 196.23 | 12001 | 80FF | 0000000000020298 |

Filter:
 Transport Connection Identifier: 800000000200298A
 RTP Transport Packet Header Byte 8: 0x7c
 RTP Transport Packet Header Byte 9: 0x0c
 data offset/4: 0x0034
 data Length Field: 0x000000c9
 Byte sequence Number: 0x00000000
 Network Address Control Vector



Wireshark default configuration

- Packet List
- Dissection
- Hex Detail



The screenshot shows the Wireshark interface with the following components:

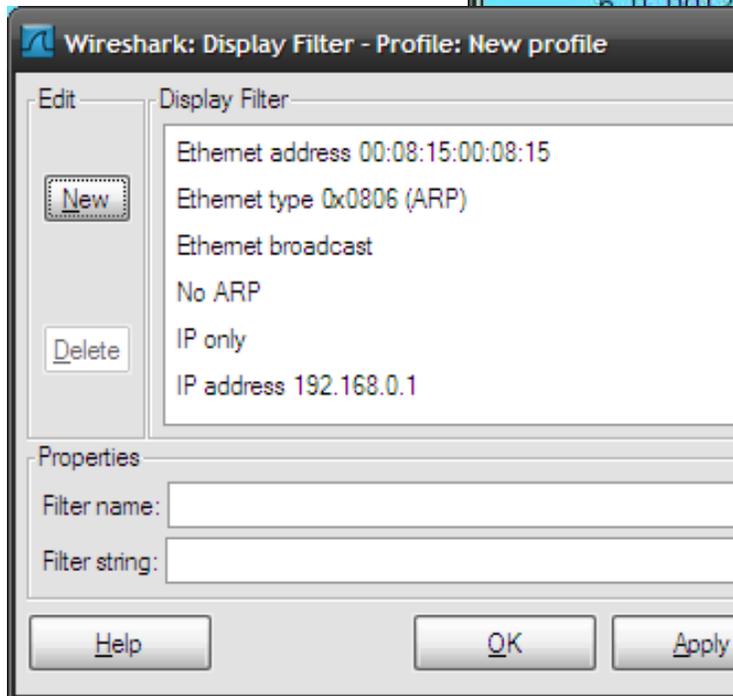
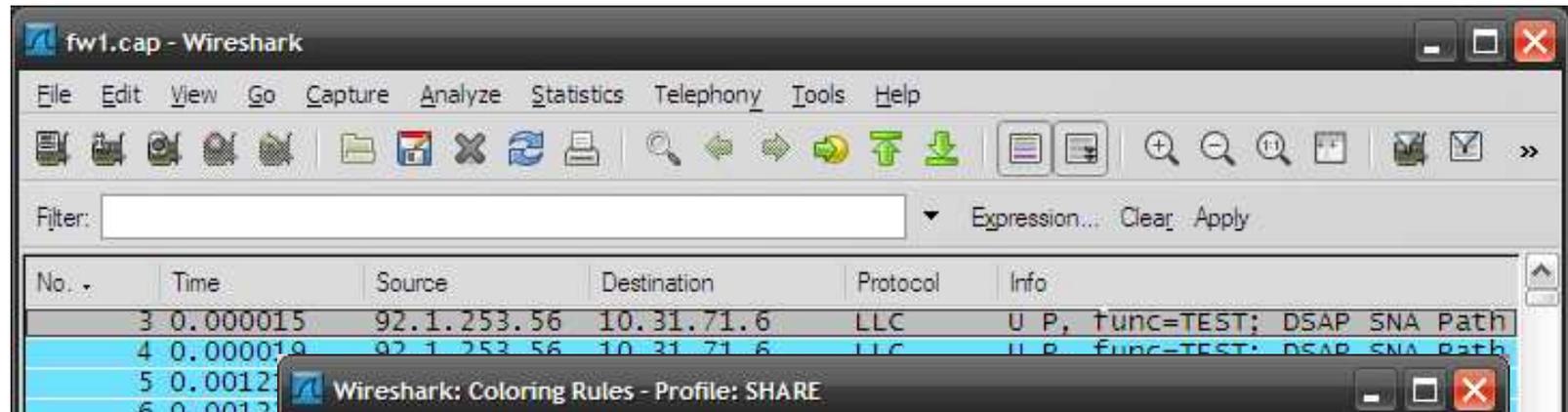
- Packet List:** A table with columns for No., Time, Source, Destination, Protocol, and Info. The first six packets are highlighted in blue.

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|---------------|---------------|----------|-------------------------------|
| 1 | 0.000000 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint nodes[Packet |
| 2 | 0.000003 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint nodes[Packet |
| 3 | 0.064301 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message[Packet siz |
| 4 | 0.067337 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint nodes[Packet |
| 5 | 0.068308 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint nodes[Packet |
| 6 | 0.068312 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint nodes[Packet |
- Dissection:** The 'RTP Transport Header' is expanded, showing fields such as:
 - Transport Connection Identifier: 21AC0C300001008E
 - RTP Transport Packet Header Byte 8: 0x3c
 - RTP Transport Packet Header Byte 9: 0x04
 - Data Offset/4: 0x000d
 - Data Length Field: 0x000003c1
 - Byte Sequence Number: 0x0573b799
 - Adaptive Rate-Based Segment
 - Status Segment
- Hex Detail:** The bottom pane shows the raw bytes of the selected packet in hexadecimal and ASCII.

| Offset | Hex | ASCII |
|--------|-------------------------|----------------|
| 0030 | 00 00 00 00 00 00 00 ff |! |
| 0040 | 8e 3c 04 00 0d 00 00 03 | <.....A...r."E |
| 0050 | f9 00 02 08 00 00 00 00 | 9..... |
| 0060 | 89 00 0e 67 4a 00 00 00 | i.....* |
| 0070 | 02 00 00 00 00 7e 00 00 | ...=..n.?q.& |
| 0080 | 50 00 4e 80 00 ff 72 07 | ...?..?.. |

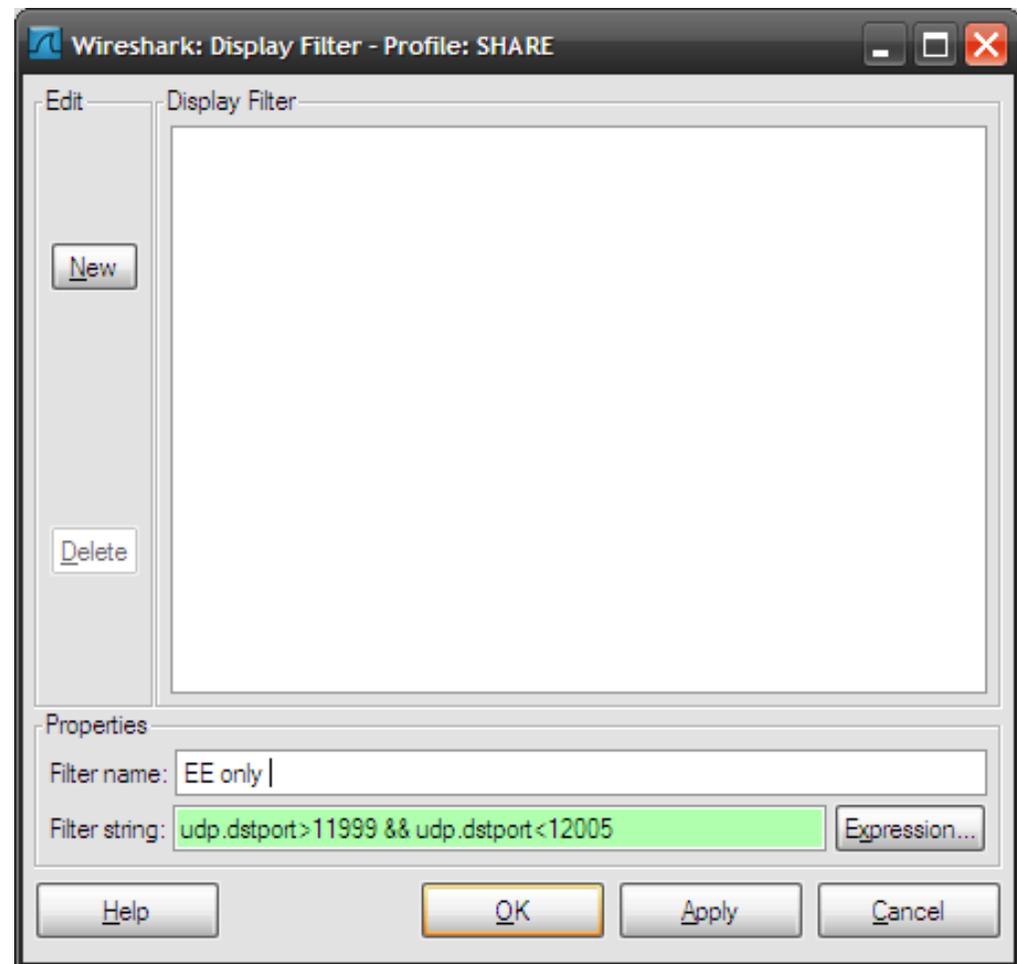
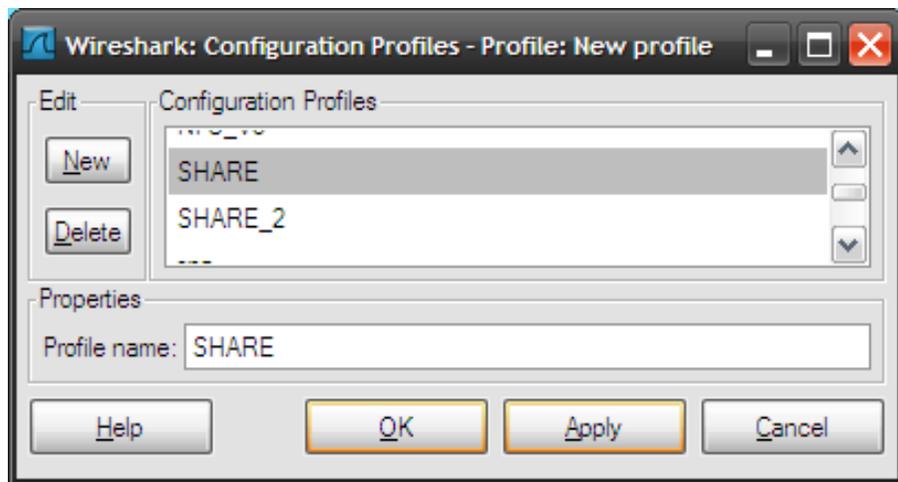
Wireshark default profile

- Colors
- Filters
- Columns



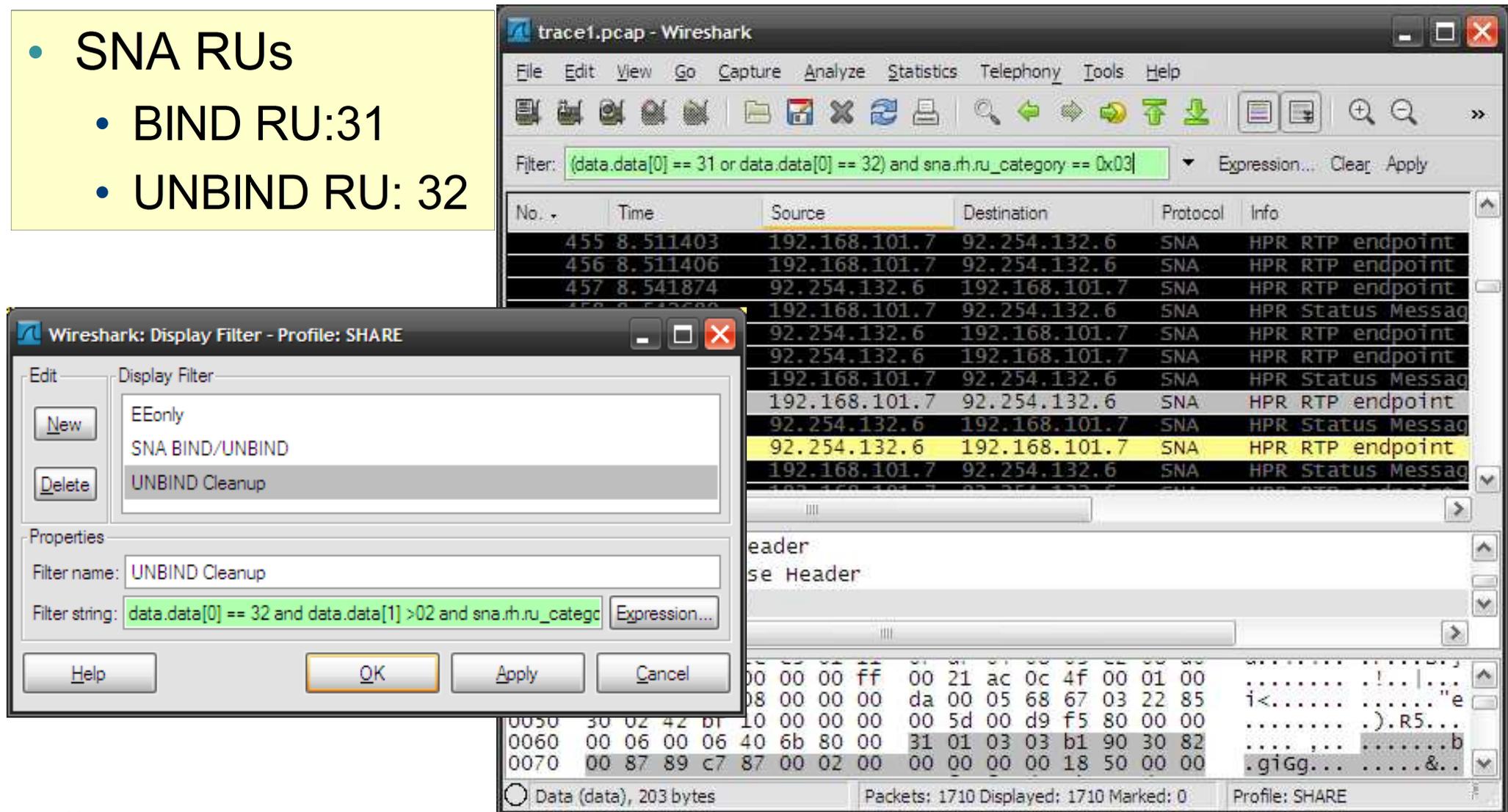
Wireshark new SHARE profile

- SHIFT + CTRL + A
 - Clear filters
 - Create new filters



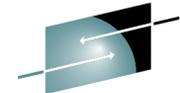
Wireshark SHARE Filters: BIND/UNBIND

- SNA RUs
 - BIND RU:31
 - UNBIND RU: 32



The screenshot shows the Wireshark interface with a packet capture named 'trace1.pcap'. The filter bar contains the expression: `(data.data[0] == 31 or data.data[0] == 32) and sna.rh.ru_category == 0x03`. The packet list shows several SNA HPR RTP endpoint and SNA HPR Status Message packets. A dialog box titled 'Wireshark: Display Filter - Profile: SHARE' is open, showing the 'UNBIND Cleanup' filter selected. The 'Filter string' field contains: `data.data[0] == 32 and data.data[1] >02 and sna.rh.ru_categ`.

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|---------------|---------------|----------|--------------------|
| 455 | 8.511403 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 456 | 8.511406 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 457 | 8.541874 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 458 | 8.542688 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 459 | 8.542700 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 460 | 8.542712 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 461 | 8.542724 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 462 | 8.542736 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 463 | 8.542748 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 464 | 8.542760 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 465 | 8.542772 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 466 | 8.542784 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 467 | 8.542796 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 468 | 8.542808 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 469 | 8.542820 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 470 | 8.542832 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 471 | 8.542844 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 472 | 8.542856 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 473 | 8.542868 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 474 | 8.542880 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 475 | 8.542892 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 476 | 8.542904 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 477 | 8.542916 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 478 | 8.542928 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 479 | 8.542940 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 480 | 8.542952 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 481 | 8.542964 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 482 | 8.542976 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 483 | 8.542988 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 484 | 8.542999 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 485 | 8.543010 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 486 | 8.543021 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 487 | 8.543032 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 488 | 8.543043 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 489 | 8.543054 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 490 | 8.543065 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 491 | 8.543076 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 492 | 8.543087 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 493 | 8.543098 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 494 | 8.543109 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 495 | 8.543120 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |
| 496 | 8.543131 | 92.254.132.6 | 192.168.101.7 | SNA | HPR RTP endpoint |
| 497 | 8.543142 | 192.168.101.7 | 92.254.132.6 | SNA | HPR Status Message |
| 498 | 8.543153 | 192.168.101.7 | 92.254.132.6 | SNA | HPR RTP endpoint |
| 499 | 8.543164 | 92.254.132.6 | 192.168.101.7 | SNA | HPR Status Message |



Wireshark SHARE : Coloring Rules

Wireshark: Coloring Rules - Profile: SHARE

List is processed in order until match is found

| Name | String |
|------------------|---|
| CFAULT | sna.nlp.thdr.optional.type == 0x12 |
| HPR PATHSWITCH | sna.nlp.thdr.offset > 13 and sna.nlp.thdr.bsn > 0 |
| HPR_RSETUP | sna.gds or sna.nlp.thdr.setupi == 1 or sna.nlp.thdr.bsn == 0 |
| ARB Slowdown2 | sna.nlp.thdr.optional.22.raa == 3 |
| ARB Slowdown1 | sna.nlp.thdr.optional.22.raa == 2 |
| (UN)BIND | (data.data[0] == 31 or data.data[0] == 32) and sna.rh.ru_category == 0x03 |
| CPSVCMG outbound | sna.nlp.nhdr.anr == d4:00:00:00:00:00:00:00:ff |
| EE Only | udp.dstport >= 12000 and udp.dstport <= 12004 |
| IP Fragment | ip frag_offset > 0 or ip flags.mf == 1 or icmp.code == 4 |

[Coloring Rule Name: (UN)BIND]
[Coloring Rule String: (data.data[0] == 31 or data.data[0] == 32) and sna.rh.ru_category == 0x03]

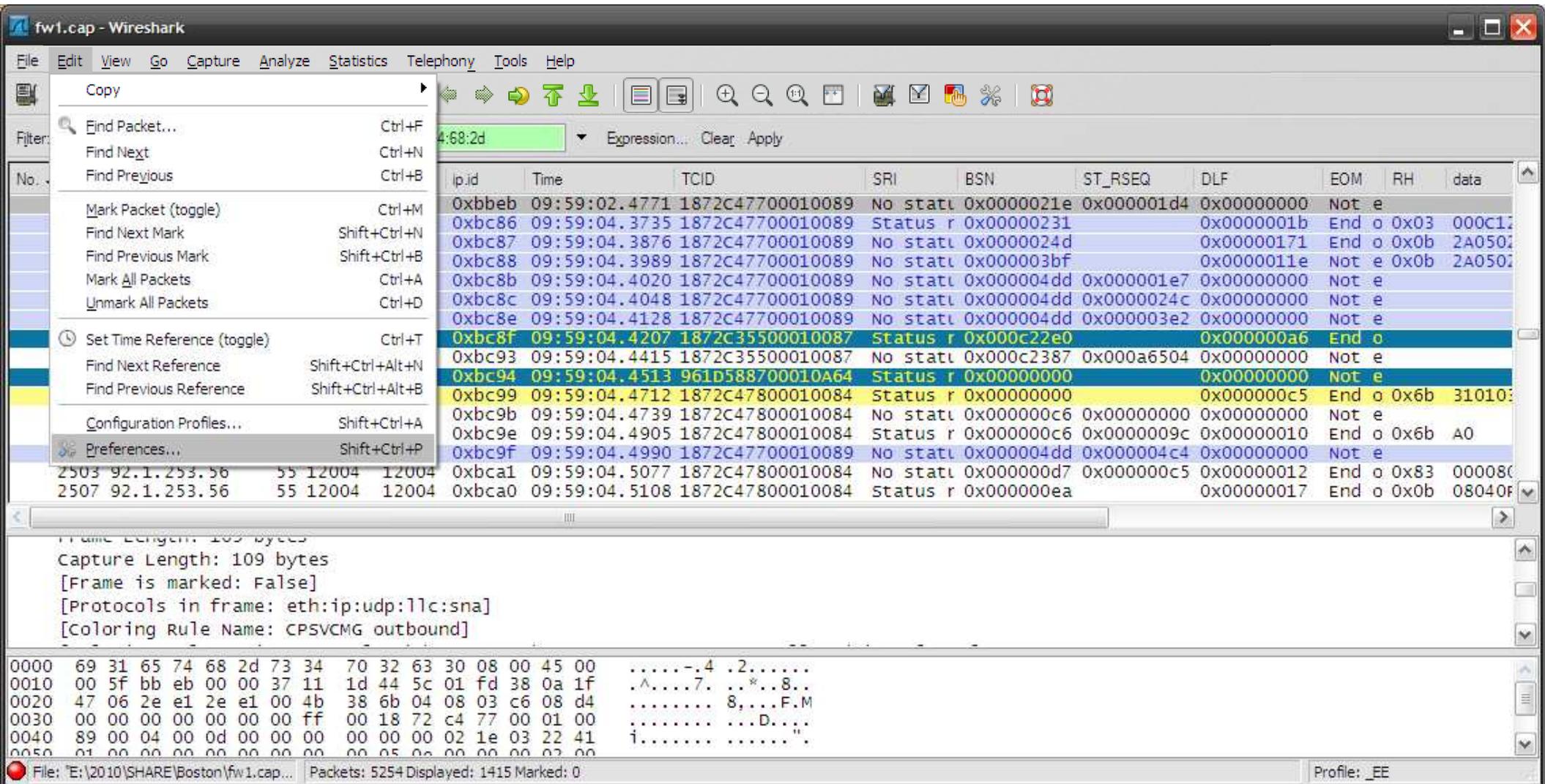
Ethernet II, Src: 73:34:70:32:63:30 (73:34:70:32:63:30), Dst: 69:31:65:74:68:2d (69:31:65:74:68:2d)

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0040 | 89 3c 00 00 05 00 00 00 | a6 00 00 01 77 5d 00 e9 | i<..... w....).Z |
| 0050 | 9d 00 00 00 00 0e 00 01 | 70 eb 80 00 31 00 13 07 | |
| 0060 | b0 b0 50 b3 00 80 97 97 | 80 00 06 02 00 00 00 00 | ..&...pp |
| 0070 | 00 00 00 00 23 00 00 00 | 27 00 08 02 c3 d7 e2 e5 |#... '...CPSV |
| 0080 | c3 d4 c7 09 03 02 db e0 | 91 19 fd 6d 5e 12 05 c4 | CMG.... \ j...;.D |

The frame matched the coloring rule ... Packets: 5254 Displayed: 5254 Marked: 0 Profile: SHARE



Wireshark SHARE Preferences: Columns



The screenshot shows the Wireshark interface with the 'Columns' menu open. The menu options include: Copy, Find Packet..., Find Next, Find Previous, Mark Packet (toggle), Find Next Mark, Find Previous Mark, Mark All Packets, Unmark All Packets, Set Time Reference (toggle), Find Next Reference, Find Previous Reference, Configuration Profiles..., and Preferences... (highlighted).

The packet list table below the menu shows the following columns: No., ip.id, Time, TCID, SRI, BSN, ST_RSEQ, DLF, EOM, RH, data.

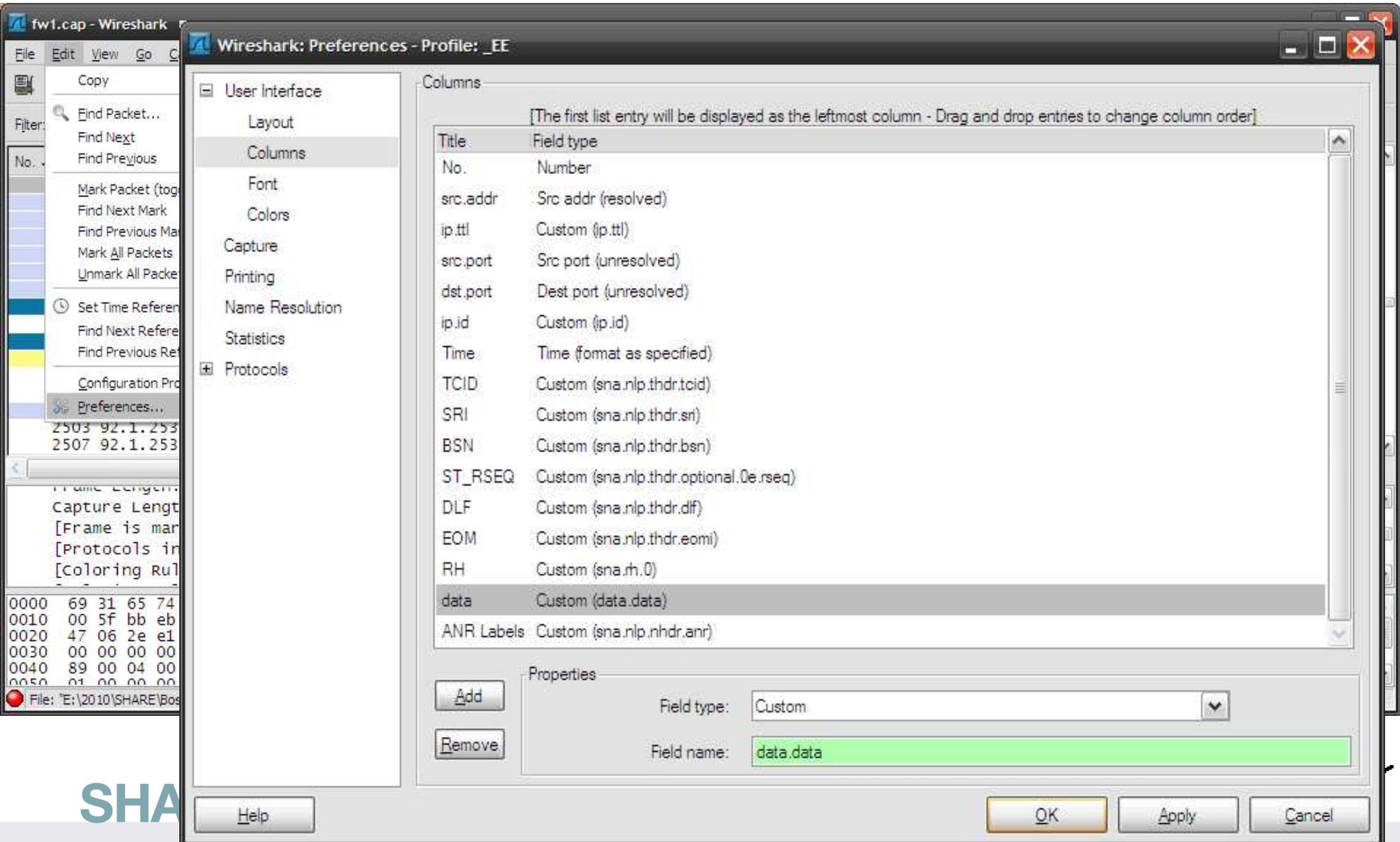
| No. | ip.id | Time | TCID | SRI | BSN | ST_RSEQ | DLF | EOM | RH | data |
|--------|---------------|------------------|----------|-------------|------------|------------|-------|------|--------|------|
| 0xbbeb | 09:59:02.4771 | 1872C47700010089 | No statl | 0x0000021e | 0x000001d4 | 0x00000000 | Not e | | | |
| 0xbc86 | 09:59:04.3735 | 1872C47700010089 | Status r | 0x00000231 | | 0x0000001b | End o | 0x03 | 000C17 | |
| 0xbc87 | 09:59:04.3876 | 1872C47700010089 | No statl | 0x0000024d | | 0x00000171 | End o | 0x0b | 2A0501 | |
| 0xbc88 | 09:59:04.3989 | 1872C47700010089 | No statl | 0x000003bf | | 0x0000011e | Not e | 0x0b | 2A0501 | |
| 0xbc8b | 09:59:04.4020 | 1872C47700010089 | No statl | 0x000004dd | 0x000001e7 | 0x00000000 | Not e | | | |
| 0xbc8c | 09:59:04.4048 | 1872C47700010089 | No statl | 0x000004dd | 0x0000024c | 0x00000000 | Not e | | | |
| 0xbc8e | 09:59:04.4128 | 1872C47700010089 | No statl | 0x000004dd | 0x000003e2 | 0x00000000 | Not e | | | |
| 0xbc8f | 09:59:04.4207 | 1872C35500010087 | Status r | 0x0000c22e0 | | 0x000000a6 | End o | | | |
| 0xbc93 | 09:59:04.4415 | 1872C35500010087 | No statl | 0x000c2387 | 0x000a6504 | 0x00000000 | Not e | | | |
| 0xbc94 | 09:59:04.4513 | 961D588700010A64 | Status r | 0x00000000 | | 0x00000000 | Not e | | | |
| 0xbc99 | 09:59:04.4712 | 1872C47800010084 | Status r | 0x00000000 | | 0x000000c5 | End o | 0x6b | 310103 | |
| 0xbc9b | 09:59:04.4739 | 1872C47800010084 | No statl | 0x000000c6 | 0x00000000 | 0x00000000 | Not e | | | |
| 0xbc9e | 09:59:04.4905 | 1872C47800010084 | Status r | 0x000000c6 | 0x0000009c | 0x00000010 | End o | 0x6b | A0 | |
| 0xbc9f | 09:59:04.4990 | 1872C47700010089 | No statl | 0x000004dd | 0x000004c4 | 0x00000000 | Not e | | | |
| 0xbca1 | 09:59:04.5077 | 1872C47800010084 | No statl | 0x000000d7 | 0x000000c5 | 0x00000012 | End o | 0x83 | 00008C | |
| 0xbca0 | 09:59:04.5108 | 1872C47800010084 | Status r | 0x000000ea | | 0x00000017 | End o | 0x0b | 08040F | |

The bottom pane shows the packet details for the selected packet (No. 2507):

- Frame Length: 109 bytes
- Capture Length: 109 bytes
- [Frame is marked: False]
- [Protocols in frame: eth:ip:udp:llc:sna]
- [Coloring Rule Name: CPSVCMG outbound]

The bottom status bar shows: File: 'E:\2010\SHARE\Boston\fw1.cap...' Packets: 5254 Displayed: 1415 Marked: 0 Profile: _EE

Wireshark SHARE Preferences: Columns



The screenshot shows the Wireshark Preferences dialog box for the profile '_EE'. The 'Columns' tab is selected in the left sidebar. The main area displays a list of columns with their respective field types. The 'data' column is highlighted. Below the list, the 'Properties' section shows the field type set to 'Custom' and the field name set to 'data.data'.

| Title | Field type |
|------------|--|
| No. | Number |
| src.addr | Src addr (resolved) |
| ip.ttl | Custom (ip.ttl) |
| src.port | Src port (unresolved) |
| dst.port | Dest port (unresolved) |
| ip.id | Custom (ip.id) |
| Time | Time (format as specified) |
| TCID | Custom (sna.nlp.thdr.tcid) |
| SRI | Custom (sna.nlp.thdr.sr) |
| BSN | Custom (sna.nlp.thdr.bsn) |
| ST_RSEQ | Custom (sna.nlp.thdr.optional.0e.rseq) |
| DLF | Custom (sna.nlp.thdr.dlf) |
| EOM | Custom (sna.nlp.thdr.eomi) |
| RH | Custom (sna.rh.0) |
| data | Custom (data.data) |
| ANR Labels | Custom (sna.nlp.nhdr.anr) |

Properties:

Field type: Custom

Field name: data.data

Wireshark SHARE profiles: IP Profile

- TTL as indicator of inbound/outbound

trace2.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

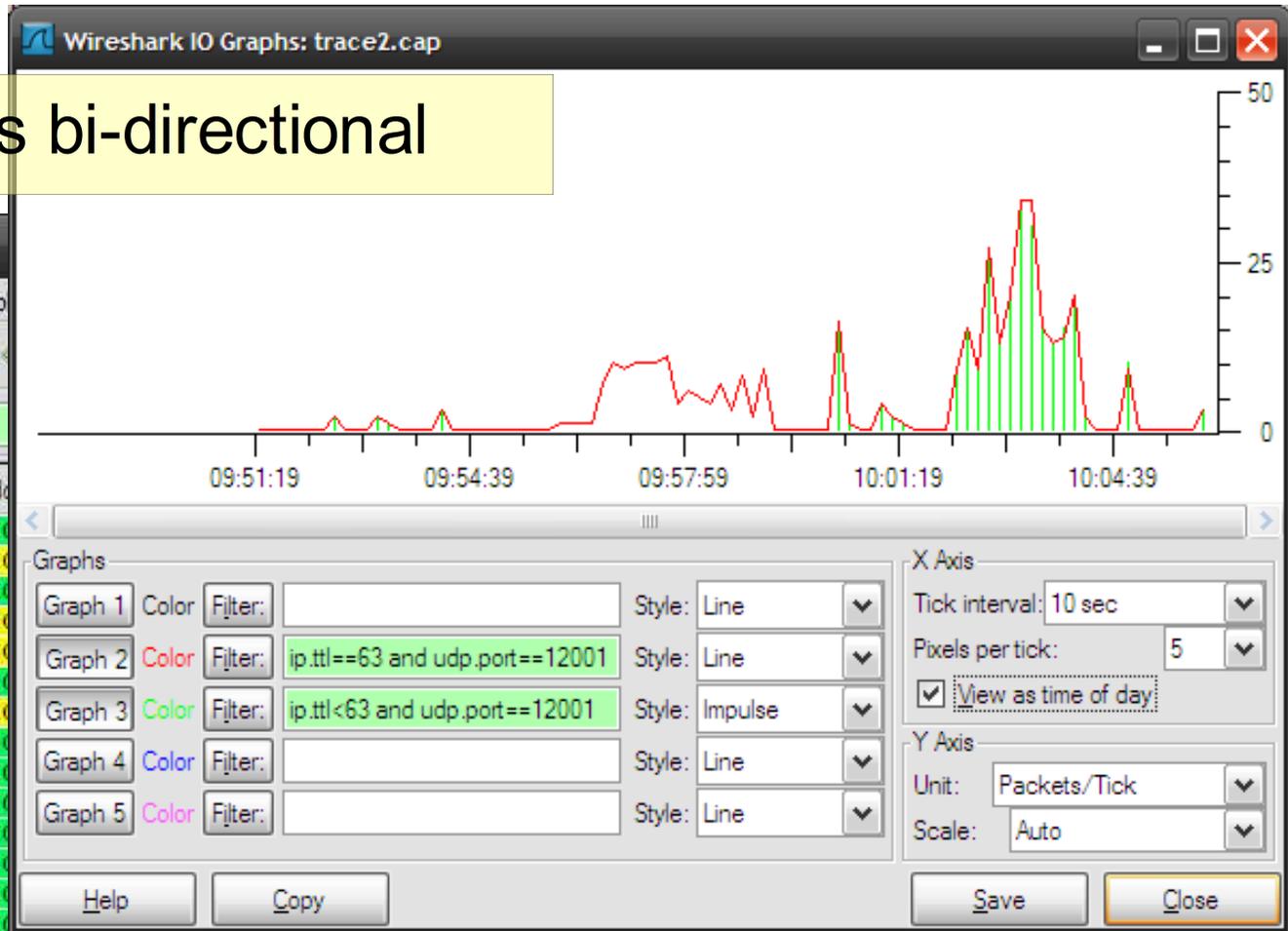
Filter: `udp.dstport==12000` Expression... Clear Apply

| No. | Time | ip.ttl | ip.id | src_addr | dst_addr | ip.src | ip.dst | port | Info |
|-----|-----------|--------|--------|----------------|----------------|-------------|-------------|-------|----------------|
| 1 | 0.000000 | 63 | 0x1e08 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U P, func=TEST |
| 2 | 0.008071 | 53 | 0xcdcf | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U F, func=TEST |
| 3 | 3.992380 | 53 | 0xe607 | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U P, func=TEST |
| 4 | 0.000413 | 63 | 0x203b | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U F, func=TEST |
| 5 | 8.002158 | 63 | 0x228f | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U P, func=TEST |
| 6 | 0.008176 | 53 | 0x795a | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U F, func=TEST |
| 7 | 3.992162 | 53 | 0x2097 | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U P, func=TEST |
| 8 | 0.000348 | 63 | 0x2425 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U F, func=TEST |
| 23 | 12.016292 | 53 | 0x9c4c | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U P, func=TEST |
| 24 | 0.000423 | 63 | 0x289f | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U F, func=TEST |
| 48 | 12.017698 | 53 | 0x2da2 | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U P, func=TEST |
| 49 | 0.000456 | 63 | 0x2f78 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U F, func=TEST |
| 52 | 12.002941 | 53 | 0x9682 | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U P, func=TEST |
| 53 | 0.000496 | 63 | 0x3466 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U F, func=TEST |
| 78 | 12.001053 | 53 | 0xf603 | Cisco_1e:74:0a | Cisco_70:48:0a | 92.1.253.56 | 10.31.71.6 | 12000 | U P, func=TEST |
| 79 | 0.000519 | 63 | 0x3891 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12000 | U F, func=TEST |

File: 'E:\2010\SHARE\Boston\trace2.c...' Packets: 2860 Displayed: 136 Marked: 0 Profile: SHARE_2

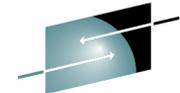
Wireshark SHARE profiles: IO Graph

- Healthy EE traffic is bi-directional



| No. - | Time | ip.ttl | ip.id | src_addr | dst_addr | protocol | length | info |
|-------|-----------------|--------|--------|----------------|----------------|------------|-------------|----------------------|
| 166 | 09:52:12.934687 | 63 | 0x544d | Cisco | | | | |
| 167 | 09:52:12.945796 | 53 | 0x81af | Cisco | | | | |
| 253 | 09:52:54.660493 | 63 | 0x6348 | Cisco | | | | |
| 254 | 09:52:54.686722 | 53 | 0xc124 | Cisco | | | | |
| 259 | 09:52:54.738566 | 53 | 0x5074 | Cisco | | | | |
| 260 | 09:52:54.738866 | 63 | 0x6351 | Cisco | | | | |
| 292 | 09:53:02.375663 | 53 | 0xdeb0 | Cisco | | | | |
| 293 | 09:53:02.376042 | 63 | 0x6595 | Cisco | | | | |
| 574 | 09:54:53.190159 | 63 | 0x92b5 | Cisco | | | | |
| 590 | 09:55:01.680448 | 63 | 0x9619 | Cisco | | | | |
| 611 | 09:55:10.181421 | 63 | 0x9a10 | Cisco | | | | |
| 628 | 09:55:18.667247 | 63 | 0x9e69 | Cisco | | | | |
| 645 | 09:55:27.151005 | 63 | 0xa195 | Cisco | | | | |
| 648 | 09:55:28.172347 | 63 | 0xa24f | Cisco | | | | |
| 657 | 09:55:29.203280 | 63 | 0xa286 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12001 HPR NLP Packet |
| 658 | 09:55:30.232464 | 63 | 0xa2a6 | Cisco_cc:43:00 | Cisco_3d:44:0a | 10.31.71.6 | 92.1.253.56 | 12001 HPR NLP Packet |

File: "E:\2010\SHARE\Boston\trace2.c..." Packets: 2860 Displayed: 654 Marked: 0 Profile: SHARE_2



SHARE
Technology · Connections · Results

Wireshark SHARE profiles: Flow Graph

The screenshot displays the Wireshark interface for a capture file named 'trace2.cap'. The main window shows a list of packets filtered by 'udp.port==12001'. The detailed view pane is open to the 'Graph Analysis' tab, showing a list of HPR RTP endpoint nodes. The nodes are listed with their time, IP addresses, and comments. The nodes are highlighted in green, and the selected node is highlighted in blue.

| Time | 92.1.253.56 | 10.31.71.6 | Comment |
|---------|-------------|------------|--|
| 129,162 | (12001) | (12001) | HPR Status Message |
| 170,877 | (12001) | (12001) | HPR RTP endpoint nodes |
| 170,903 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 170,955 | (12001) | (12001) | HPR RTP endpoint nodes |
| 170,955 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 178,592 | (12001) | (12001) | HPR Status Message |
| 178,593 | (12001) | (12001) | HPR Status Message |
| 289,407 | (12001) | (12001) | HPR RTP endpoint nodes |
| 297,897 | (12001) | (12001) | HPR Status Message |
| 306,398 | (12001) | (12001) | HPR Status Message |
| 314,884 | (12001) | (12001) | HPR Status Message |
| 323,368 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 324,389 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 325,420 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 326,449 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 327,478 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |
| 328,507 | (12001) | (12001) | HPR NLP Packet[Packet size limited dur |

File: "E:\2010\SHARE\Boston\trace2.c... Packets: 2860 Displayed: 654 Marked: 0 Profile: SHARE_2



**“Tell me and I'll forget;
show me and I may remember;
involve me and I'll understand.”**

Part II: Hands-on experience

Get involved in a real EE Pathswitch problem

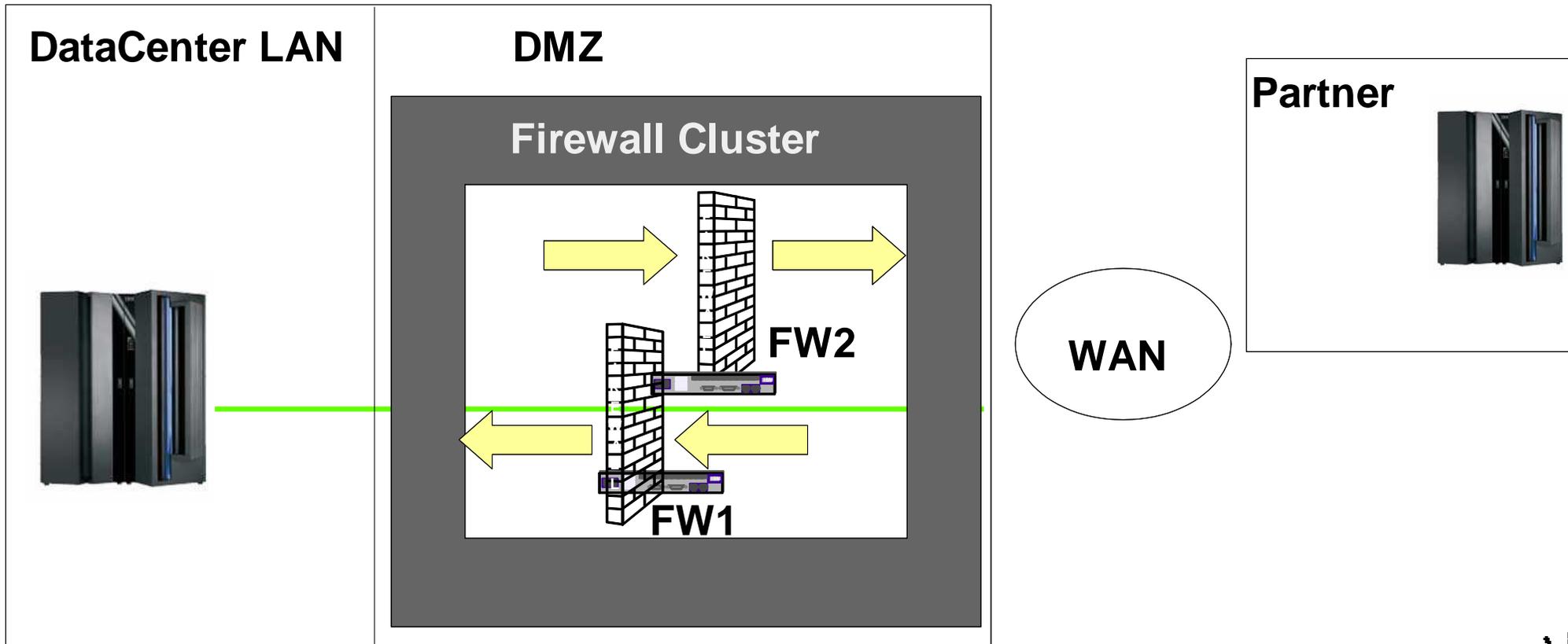


SHARE in Boston



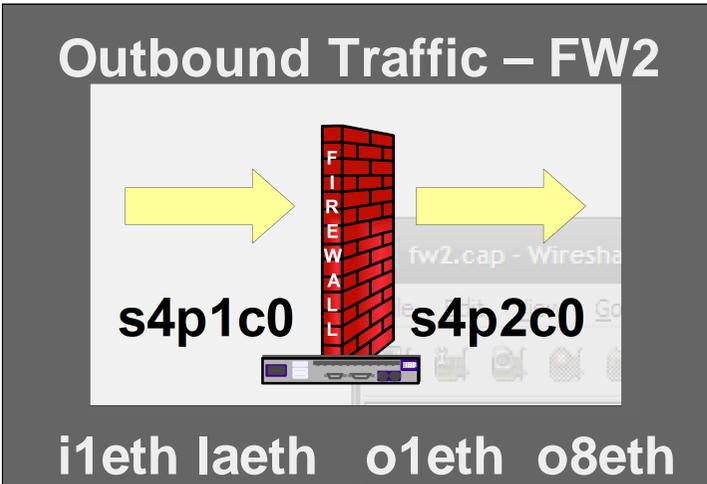
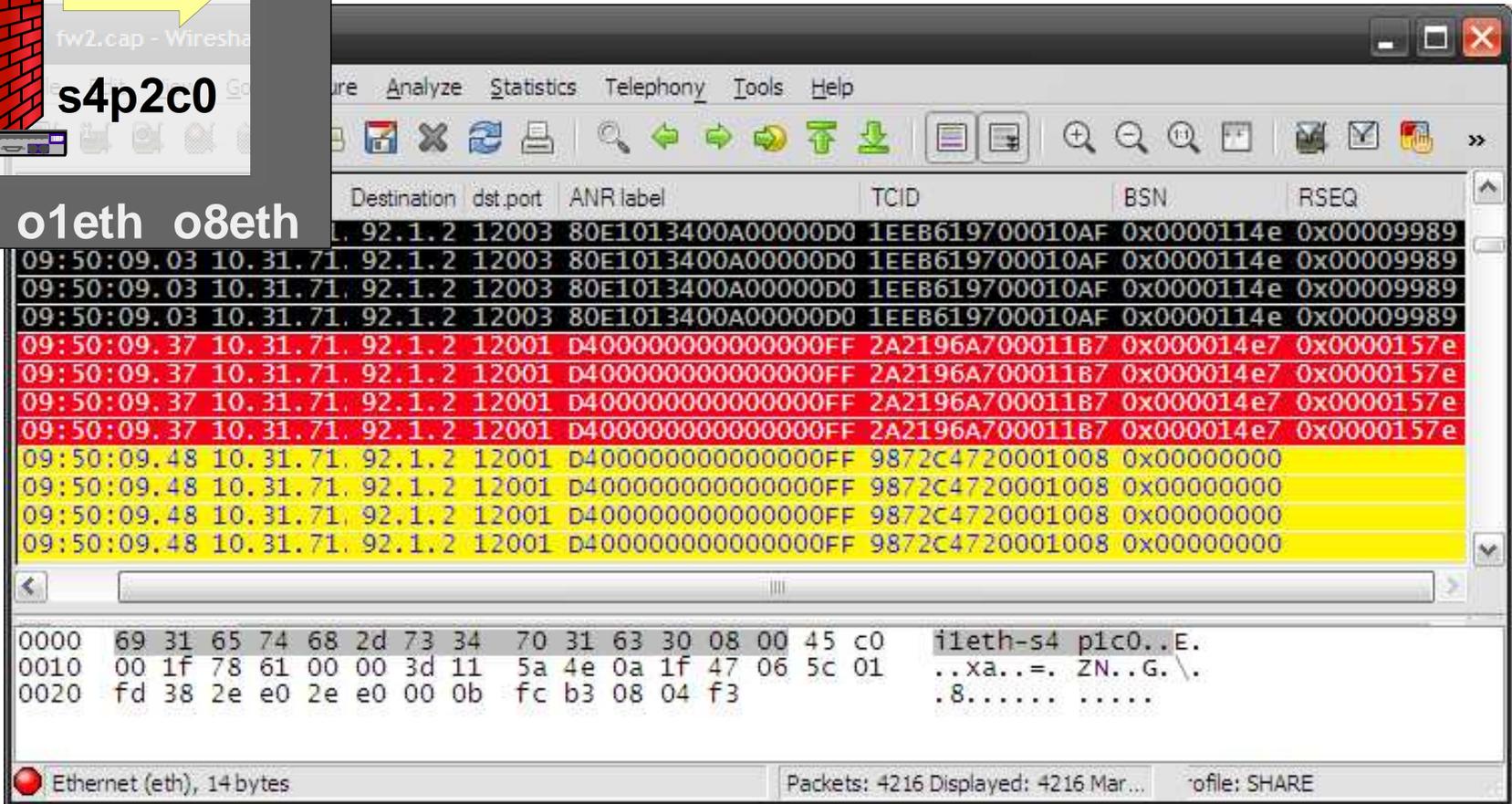
The Topology

- Traces were taken in the FW cluster
- FW1 handles inbound , FW2 handles outbound traffic



Outbound Traffic - fw2.cap

Every packet is traced 4 times as it flows through the FW Cluster
The Ethernet addresses change

| Time | Source IP | Destination IP | Port | Protocol | Length | Info |
|-------------|-----------|----------------|-------|--------------------|-----------------|-----------------------|
| 09:50:09.03 | 10.31.71 | 92.1.2 | 12003 | 80E1013400A00000D0 | 1EEB619700010AF | 0x0000114e 0x00009989 |
| 09:50:09.03 | 10.31.71 | 92.1.2 | 12003 | 80E1013400A00000D0 | 1EEB619700010AF | 0x0000114e 0x00009989 |
| 09:50:09.03 | 10.31.71 | 92.1.2 | 12003 | 80E1013400A00000D0 | 1EEB619700010AF | 0x0000114e 0x00009989 |
| 09:50:09.37 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 2A2196A700011B7 | 0x000014e7 0x0000157e |
| 09:50:09.37 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 2A2196A700011B7 | 0x000014e7 0x0000157e |
| 09:50:09.37 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 2A2196A700011B7 | 0x000014e7 0x0000157e |
| 09:50:09.37 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 2A2196A700011B7 | 0x000014e7 0x0000157e |
| 09:50:09.48 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 9872C4720001008 | 0x00000000 |
| 09:50:09.48 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 9872C4720001008 | 0x00000000 |
| 09:50:09.48 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 9872C4720001008 | 0x00000000 |
| 09:50:09.48 | 10.31.71 | 92.1.2 | 12001 | D400000000000000FF | 9872C4720001008 | 0x00000000 |

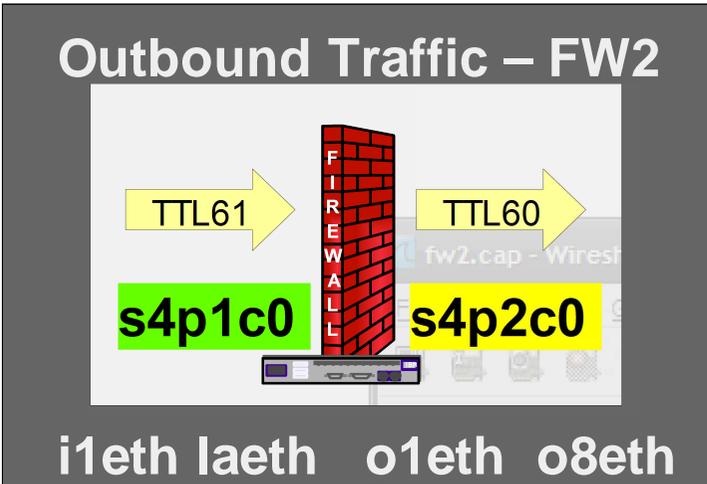
```

0000  69 31 65 74 68 2d 73 34 70 31 63 30 08 00 45 c0  i1eth-s4 p1c0..E.
0010  00 1f 78 61 00 00 3d 11 5a 4e 0a 1f 47 06 5c 01  ..xa..=. ZN..G.\.
0020  fd 38 2e e0 2e e0 00 0b fc b3 08 04 f3          .8.....
    
```

Ethernet (eth), 14 bytes Packets: 4216 Displayed: 4216 Mar... Profile: SHARE

fw2.cap - coloring rules <CTRL-V> + <C>

2 trace points in 's4p1c0' – TTL = 61
 2 trace points in 's4p2c0' – TTL = 60



Wireshark: Coloring Rules - Profile: SHARE_2

List is processed in order until match is found

| Name | String |
|-----------------------|---|
| s4p1c0 | eth.src == 73:34:70:31:63:30 |
| s4p2c0 | eth.src == 73:34:70:32:63:30 |
| IP Fragmentation | (ip.flags.mf == 1) (ip.frag_offset gt 0) |
| TTL low or unexpected | (!ip.dst == 224.0.0.0/4 && ip.ttl < 5) (ip.dst == 224.0.0.0/24 |

| Time | ip.ttl | ip.id | ip.len | ip.src | ip.dst | eth.src | eth.dst | eth.type | eth.len | eth.payload |
|-----------|--------|--------|--------|-------------------|----------------|----------------|---------|------------|---------|-------------|
| 09:46:29. | 61 | 0x7863 | 31 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 10.31.92.1.253 | 12000 | | | |
| 09:46:29. | 61 | 0xc9bb | 31 | 73:34:70:32:63:30 | 4f:38:65:74:68 | 10.31.92.1.253 | 12000 | | | |
| 09:46:29. | 60 | 0xc9bb | 31 | 73:34:70:32:63:30 | 4f:38:65:74:68 | 10.31.92.1.253 | 12000 | | | |
| 09:46:34. | 61 | 0x7a30 | 91 | 73:34:70:31:63:30 | 69:31:65:74:68 | 10.31.92.1.253 | 12003 | 1EEB61B100 | | |
| 09:46:34. | 61 | 0xf63a | 91 | 73:34:70:31:63:30 | 49:61:65:74:68 | 10.31.92.1.253 | 12003 | 1EEB61B100 | | |
| 09:46:34. | 60 | 0xf63a | 91 | 73:34:70:32:63:30 | 6f:31:65:74:68 | 10.31.92.1.253 | 12003 | 1EEB61B100 | | |
| 09:46:34. | 60 | 0xf63a | 91 | 73:34:70:32:63:30 | 4f:38:65:74:68 | 10.31.92.1.253 | 12003 | 1EEB61B100 | | |
| 09:46:41. | 61 | 0x7863 | 31 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 10.31.92.1.253 | 12000 | | | |

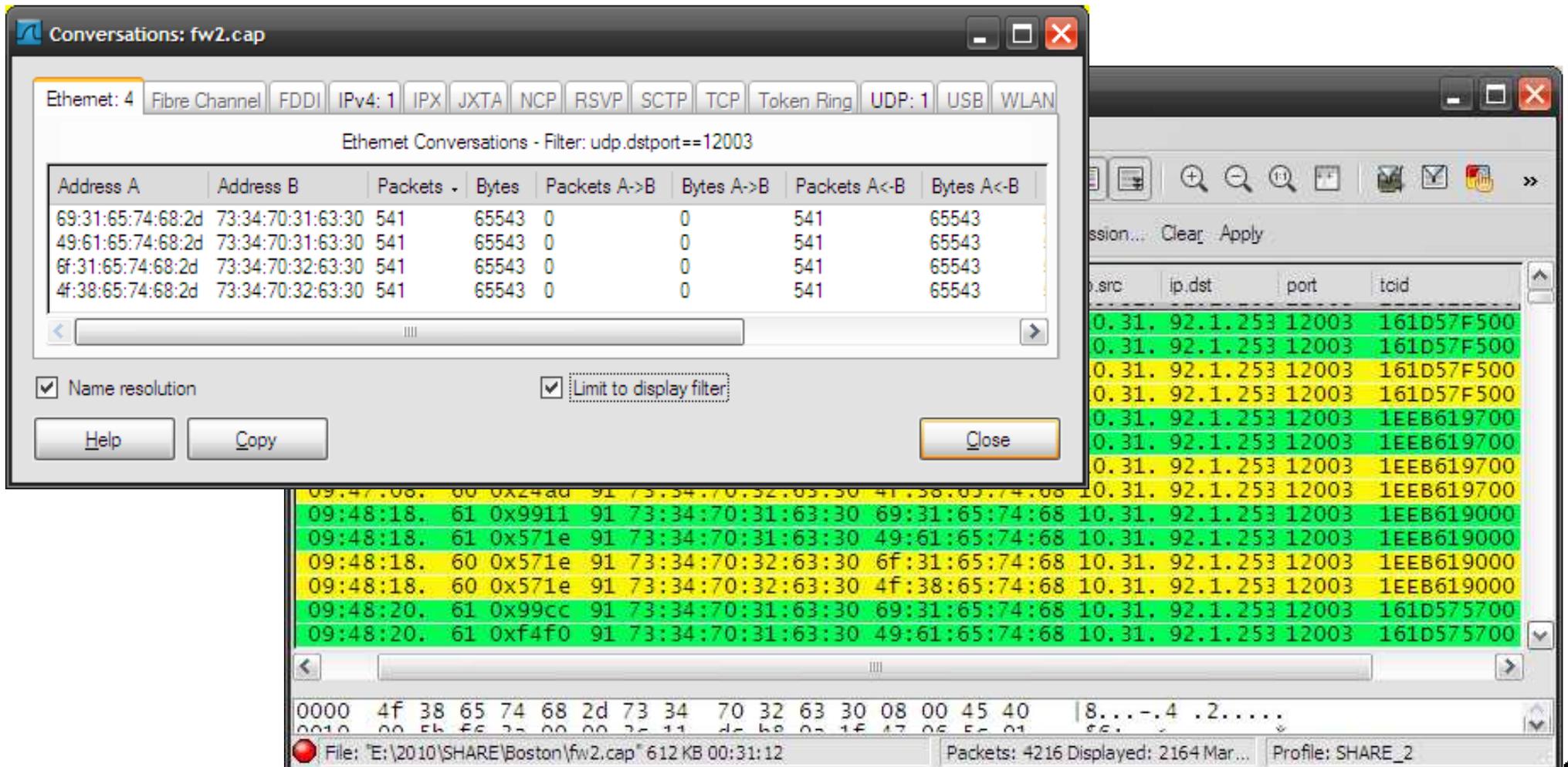
```

0000  69 31 65 74 68 2d 73 34 70 31 63 30 08 00 45 c0  i1eth-s4 p1c0..E.
0010  00 1f 78 61 00 00 3d 11 5a 4e 0a 1f 47 06 5c 01  ..xa..=. ZN..G.\.
0020  fd 38 2e e0 2e e0 00 0b fc b3 08 04 f3      .8.....
  
```

File: "E:\2010\SHARE\Boston\fw2.cap" 612 KB 00:31:12 Packets: 4216 Displayed: 4216 Mar... Profile: SHARE_2

Wireshark Statistics: conversations 12003

- Each packet is traced 4 times at different 'MAC addresses'



Conversations: fw2.cap

Ethernet: 4 | Fibre Channel | FDDI | IPv4: 1 | IPX | JXTA | NCP | RSVP | SCTP | TCP | Token Ring | UDP: 1 | USB | WLAN

Ethernet Conversations - Filter: udp.dstport==12003

| Address A | Address B | Packets | Bytes | Packets A->B | Bytes A->B | Packets A<-B | Bytes A<-B |
|-------------------|-------------------|---------|-------|--------------|------------|--------------|------------|
| 69:31:65:74:68:2d | 73:34:70:31:63:30 | 541 | 65543 | 0 | 0 | 541 | 65543 |
| 49:61:65:74:68:2d | 73:34:70:31:63:30 | 541 | 65543 | 0 | 0 | 541 | 65543 |
| 6f:31:65:74:68:2d | 73:34:70:32:63:30 | 541 | 65543 | 0 | 0 | 541 | 65543 |
| 4f:38:65:74:68:2d | 73:34:70:32:63:30 | 541 | 65543 | 0 | 0 | 541 | 65543 |

Name resolution Limit to display filter

Help Copy Close

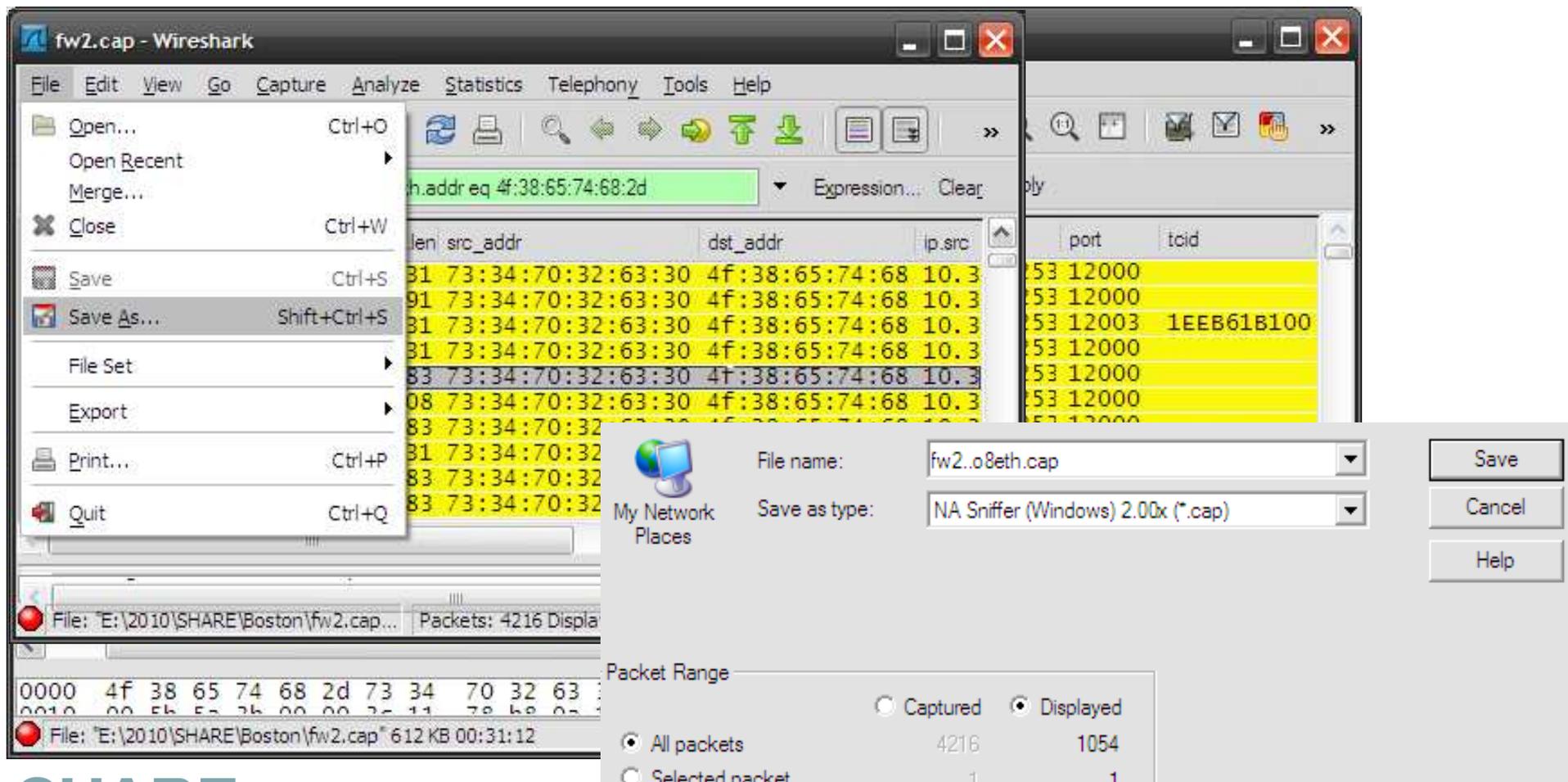
Packet list (visible):

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|-----------------|
| 0 | 0.000000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 1 | 0.001000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 2 | 0.002000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 3 | 0.003000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 4 | 0.004000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 5 | 0.005000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 6 | 0.006000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 7 | 0.007000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 8 | 0.008000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 9 | 0.009000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 10 | 0.010000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 11 | 0.011000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 12 | 0.012000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 13 | 0.013000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 14 | 0.014000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 15 | 0.015000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 16 | 0.016000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 17 | 0.017000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 18 | 0.018000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 19 | 0.019000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 20 | 0.020000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 21 | 0.021000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 22 | 0.022000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 23 | 0.023000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 24 | 0.024000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 25 | 0.025000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 26 | 0.026000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 27 | 0.027000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 28 | 0.028000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 29 | 0.029000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 30 | 0.030000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 31 | 0.031000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 32 | 0.032000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 33 | 0.033000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 34 | 0.034000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 35 | 0.035000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 36 | 0.036000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 37 | 0.037000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 38 | 0.038000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 39 | 0.039000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 40 | 0.040000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 41 | 0.041000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 42 | 0.042000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 43 | 0.043000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 44 | 0.044000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 45 | 0.045000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 46 | 0.046000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 47 | 0.047000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 48 | 0.048000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 49 | 0.049000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 50 | 0.050000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 51 | 0.051000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 52 | 0.052000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 53 | 0.053000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 54 | 0.054000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 55 | 0.055000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 56 | 0.056000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 57 | 0.057000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 58 | 0.058000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 59 | 0.059000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 60 | 0.060000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 61 | 0.061000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 62 | 0.062000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 63 | 0.063000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 64 | 0.064000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 65 | 0.065000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 66 | 0.066000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 67 | 0.067000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 68 | 0.068000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 69 | 0.069000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 70 | 0.070000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 71 | 0.071000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 72 | 0.072000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 73 | 0.073000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 74 | 0.074000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 75 | 0.075000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 76 | 0.076000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 77 | 0.077000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 78 | 0.078000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 79 | 0.079000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 80 | 0.080000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 81 | 0.081000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 82 | 0.082000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 83 | 0.083000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 84 | 0.084000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 85 | 0.085000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 86 | 0.086000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 87 | 0.087000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 88 | 0.088000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 89 | 0.089000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 90 | 0.090000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 91 | 0.091000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 92 | 0.092000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 93 | 0.093000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 94 | 0.094000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 95 | 0.095000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 96 | 0.096000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 97 | 0.097000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 98 | 0.098000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 99 | 0.099000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |
| 100 | 0.100000 | 10.31.92.1.253 | 10.31.92.1.253 | ICMP | 8 | 8...-.4 .2..... |

File: "E:\2010\SHARE\Boston\fw2.cap" 612 KB 00:31:12 Packets: 4216 Displayed: 2164 Mar... Profile: SHARE_2

fw2.cap – saving filtered packets

As every packet is traced 4 times as it flows through the FW Cluster, a filter on the 'last' ethernet address can be used to remove duplicate packets.



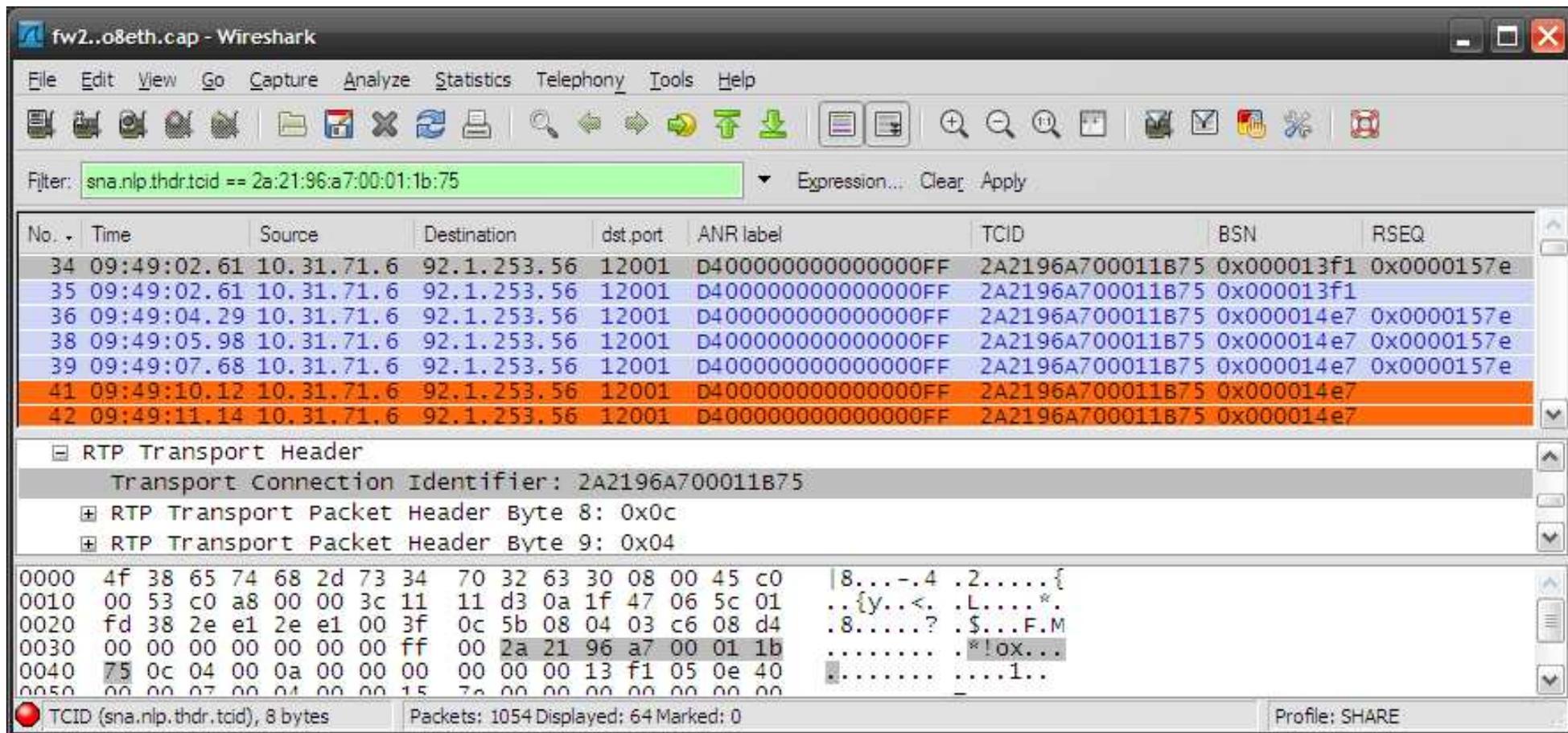
The screenshot shows the Wireshark interface with the file 'fw2.cap' open. A filter is applied to the packet list: 'eth.addr eq 4f:38:65:74:68:2d'. The packet list shows several entries with the following columns: len, src_addr, dst_addr, ip.src, port, and tcid. The 'Save As...' dialog box is open, showing the file name 'fw2.o8eth.cap' and the save type 'NA Sniffer (Windows) 2.00x (*.cap)'. The 'Packet Range' section shows 'All packets' selected, with 4216 captured packets and 1054 displayed packets.

| len | src_addr | dst_addr | ip.src | port | tcid |
|-----|-------------------|-------------------|--------|------|------------------|
| 81 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 91 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 81 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12003 1EEB61B100 |
| 81 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 83 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 08 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 83 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 81 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 83 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |
| 83 | 73:34:70:32:63:30 | 4f:38:65:74:68:2d | 10.3 | 53 | 12000 |



fw2.cap – TCID filter CPSVCMG PATHSWITCH

CPSVCMG pipe entering PATHSWITCH at 09:49:10
Current BSN:14E7, expected RSEQ: 157E



fw2..o8eth.cap - Wireshark

Filter: `sna.nlp.thdr.tcid == 2a:21:96:a7:00:01:1b:75`

| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|------------|-------------|----------|--------------------|------------------|------------|------------|
| 34 | 09:49:02.61 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000013f1 | 0x0000157e |
| 35 | 09:49:02.61 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000013f1 | |
| 36 | 09:49:04.29 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |
| 38 | 09:49:05.98 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |
| 39 | 09:49:07.68 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |
| 41 | 09:49:10.12 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 42 | 09:49:11.14 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |

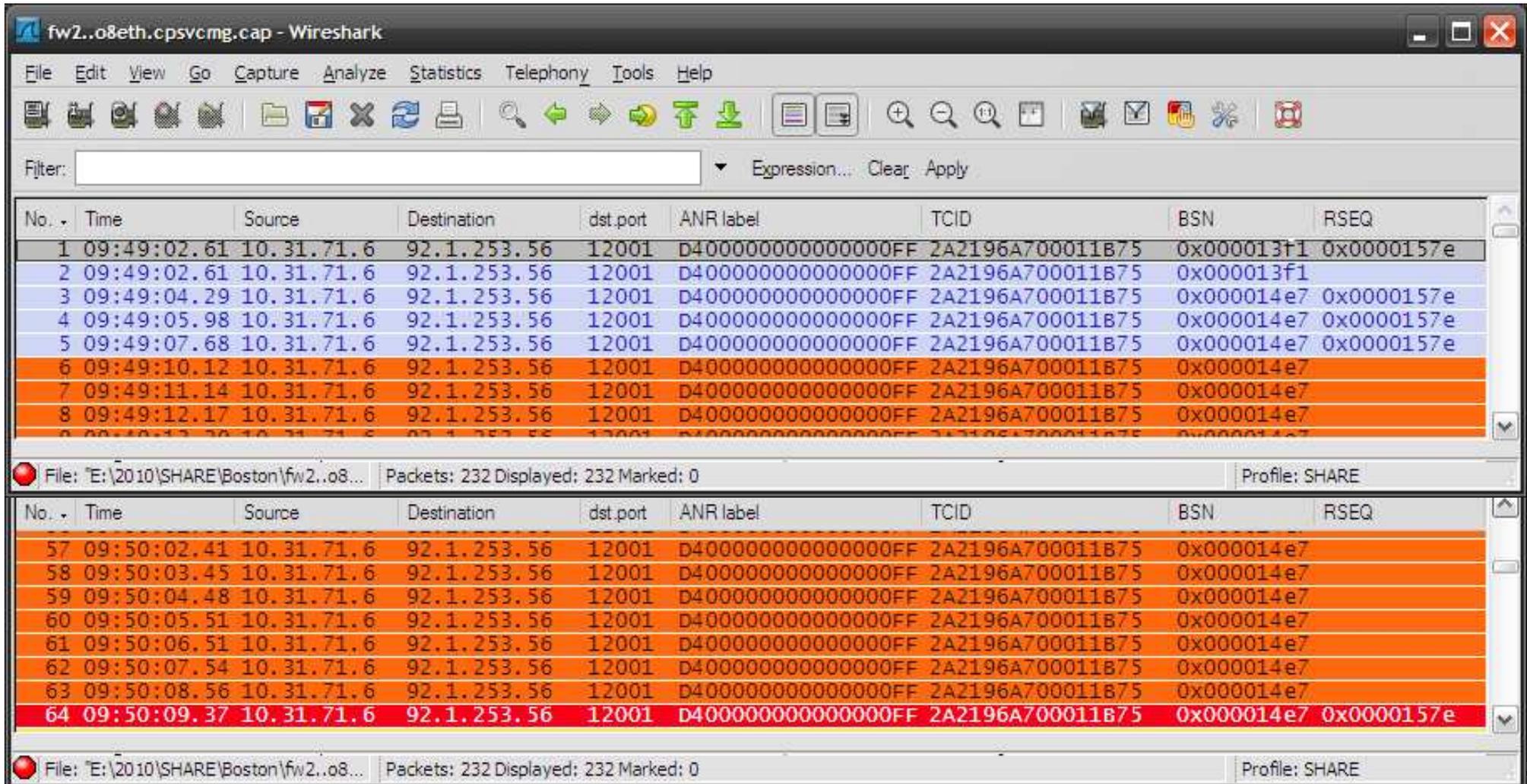
RTP Transport Header
 Transport Connection Identifier: 2A2196A700011B75
 RTP Transport Packet Header Byte 8: 0x0c
 RTP Transport Packet Header Byte 9: 0x04

| | | |
|------|---|---------------------|
| 0000 | 4f 38 65 74 68 2d 73 34 70 32 63 30 08 00 45 c0 | 8...-.4 .2.....{ |
| 0010 | 00 53 c0 a8 00 00 3c 11 11 d3 0a 1f 47 06 5c 01 | ..{y..<. .L.....* |
| 0020 | fd 38 2e e1 2e e1 00 3f 0c 5b 08 04 03 c6 08 d4 | .8.....? .\$....F.M |
| 0030 | 00 00 00 00 00 00 00 ff 00 2a 21 96 a7 00 01 1b | *!ox... |
| 0040 | 75 0c 04 00 0a 00 00 00 00 00 00 13 f1 05 0e 40 | 1.. |
| 0050 | 00 00 07 00 04 00 00 15 7e 00 00 00 00 00 00 | |

TCID (sna.nlp.thdr.tcid), 8 bytes Packets: 1054 Displayed; 64 Marked: 0 Profile: SHARE

fw2.o8eth.cpsvcmg.cap PATHSWITCH,CFAULT

PATHSWITCH failed at 09:50:09 BSN:14E7, RSEQ: 157E



fw2..o8eth.cpsvcmg.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|------------|-------------|----------|--------------------|------------------|------------|------------|
| 1 | 09:49:02.61 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000013f1 | 0x0000157e |
| 2 | 09:49:02.61 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000013f1 | |
| 3 | 09:49:04.29 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |
| 4 | 09:49:05.98 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |
| 5 | 09:49:07.68 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |
| 6 | 09:49:10.12 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 7 | 09:49:11.14 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 8 | 09:49:12.17 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |

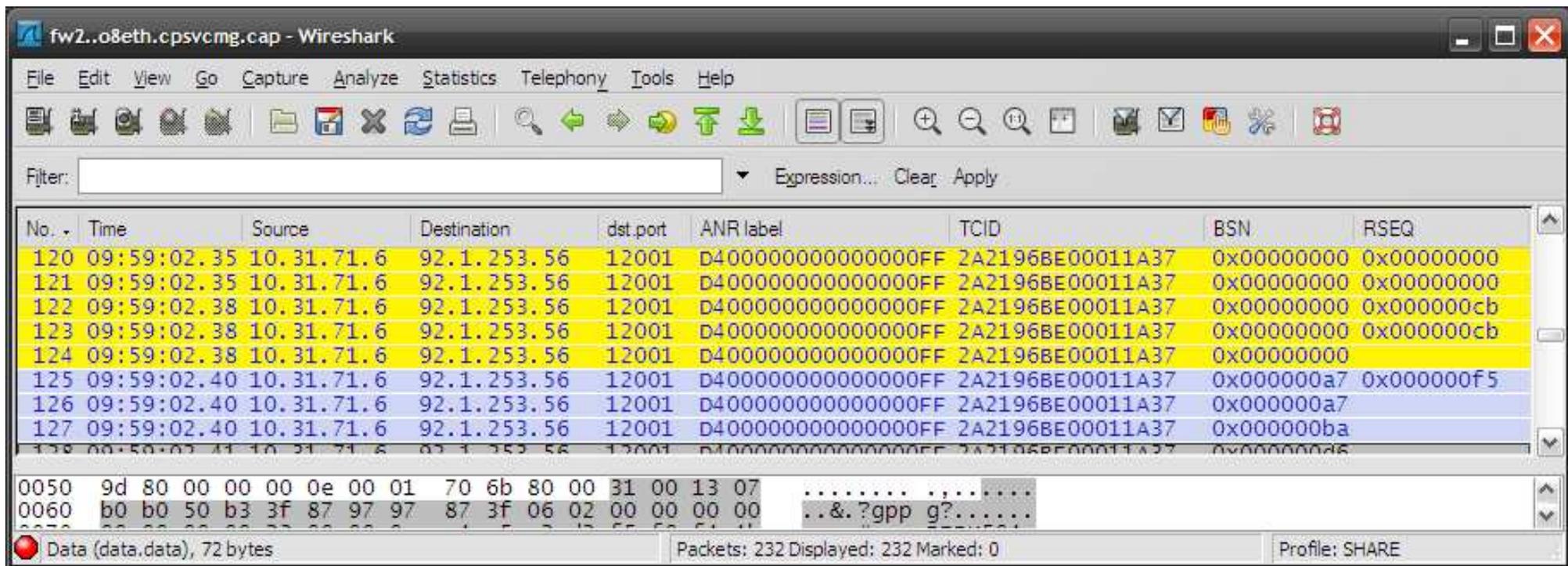
File: "E:\2010\SHARE\Boston\fw2..o8..." Packets: 232 Displayed: 232 Marked: 0 Profile: SHARE

| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|------------|-------------|----------|--------------------|------------------|------------|------------|
| 57 | 09:50:02.41 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 58 | 09:50:03.45 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 59 | 09:50:04.48 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 60 | 09:50:05.51 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 61 | 09:50:06.51 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 62 | 09:50:07.54 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 63 | 09:50:08.56 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | |
| 64 | 09:50:09.37 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196A700011B75 | 0x000014e7 | 0x0000157e |

File: "E:\2010\SHARE\Boston\fw2..o8..." Packets: 232 Displayed: 232 Marked: 0 Profile: SHARE

fw2.o8eth.cap SETUP CPSVCMG

New CPSVCMG pipe finally sets up at 09:59:02
CP-CP sessions are activated



The image shows a Wireshark capture window titled "fw2..o8eth.cpsvcmg.cap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help), a toolbar with various icons, and a filter field. The main display area shows a list of network packets. The first 127 packets are highlighted in yellow, indicating they are selected. The table below shows the details of these packets.

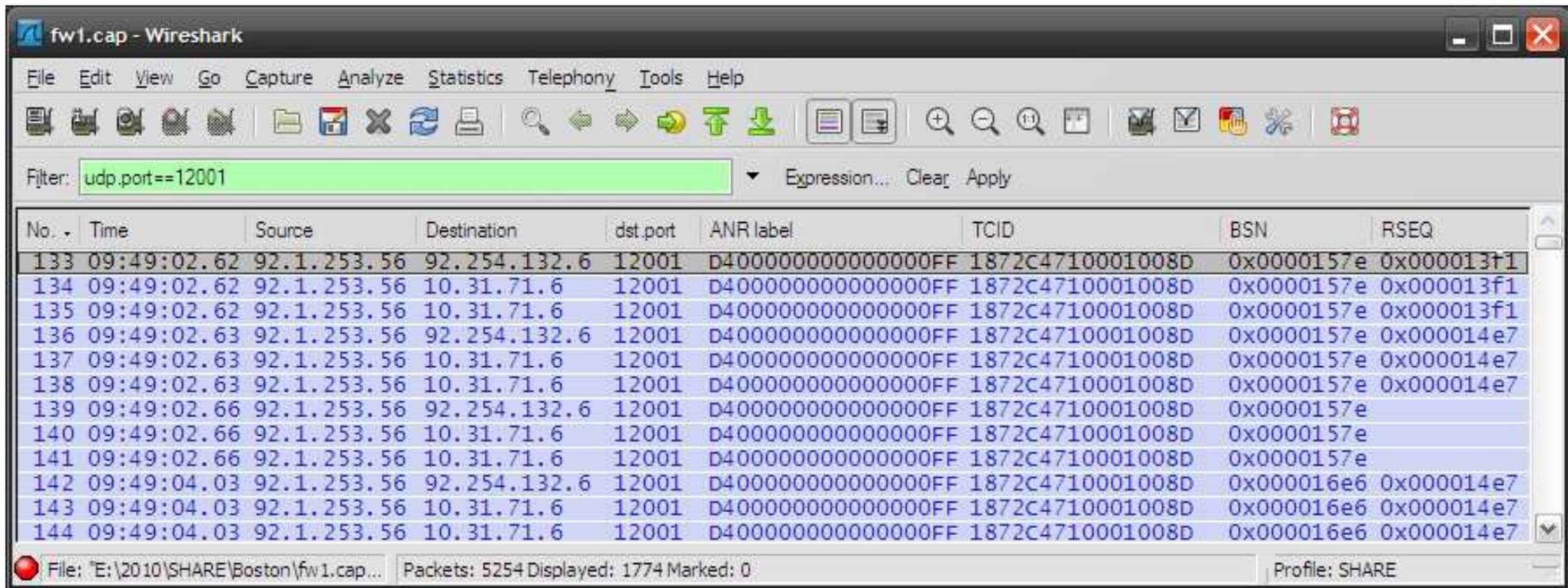
| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|------------|-------------|----------|--------------------|------------------|------------|------------|
| 120 | 09:59:02.35 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x00000000 | 0x00000000 |
| 121 | 09:59:02.35 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x00000000 | 0x00000000 |
| 122 | 09:59:02.38 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x00000000 | 0x000000cb |
| 123 | 09:59:02.38 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x00000000 | 0x000000cb |
| 124 | 09:59:02.38 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x00000000 | |
| 125 | 09:59:02.40 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x000000a7 | 0x000000f5 |
| 126 | 09:59:02.40 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x000000a7 | |
| 127 | 09:59:02.40 | 10.31.71.6 | 92.1.253.56 | 12001 | D400000000000000FF | 2A2196BE00011A37 | 0x000000ba | |

At the bottom of the capture, there is a packet details pane showing the structure of the selected packets. The first packet (No. 0050) is shown with its hex and ASCII representation. The second packet (No. 0060) is also shown with its hex and ASCII representation. The status bar at the bottom indicates "Data (data.data), 72 bytes", "Packets: 232 Displayed: 232 Marked: 0", and "Profile: SHARE".

fw1.cap

UDP 12001

Existing CPSVCMG pipe with incrementing BSN and RSEQ
Every packet is traced 3 times
Destination IP address changes between packet1 and packet 2

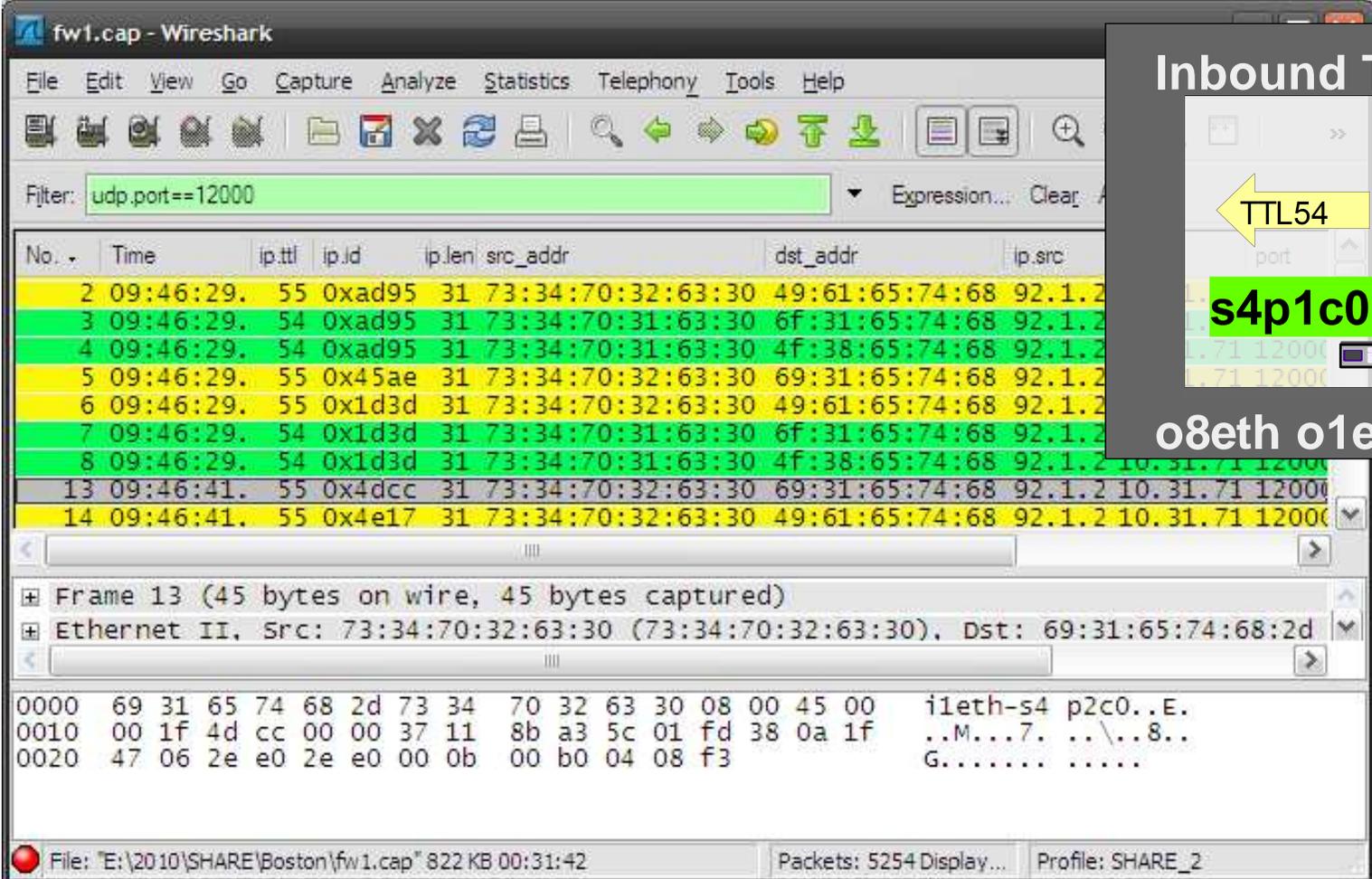


| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|-------------|--------------|----------|--------------------|------------------|------------|------------|
| 133 | 09:49:02.62 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000013f1 |
| 134 | 09:49:02.62 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000013f1 |
| 135 | 09:49:02.62 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000013f1 |
| 136 | 09:49:02.63 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000014e7 |
| 137 | 09:49:02.63 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000014e7 |
| 138 | 09:49:02.63 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000014e7 |
| 139 | 09:49:02.66 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | |
| 140 | 09:49:02.66 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | |
| 141 | 09:49:02.66 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | |
| 142 | 09:49:04.03 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | 0x000014e7 |
| 143 | 09:49:04.03 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | 0x000014e7 |
| 144 | 09:49:04.03 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | 0x000014e7 |

File: 'E:\2010\SHARE\Boston\fw1.cap...' Packets: 5254 Displayed: 1774 Marked: 0 Profile: SHARE

fw1.cap UDP 12000

Every packet is traced 4 times as it is routed through the FW



fw1.cap - Wireshark

Filter: `udp.port==12000`

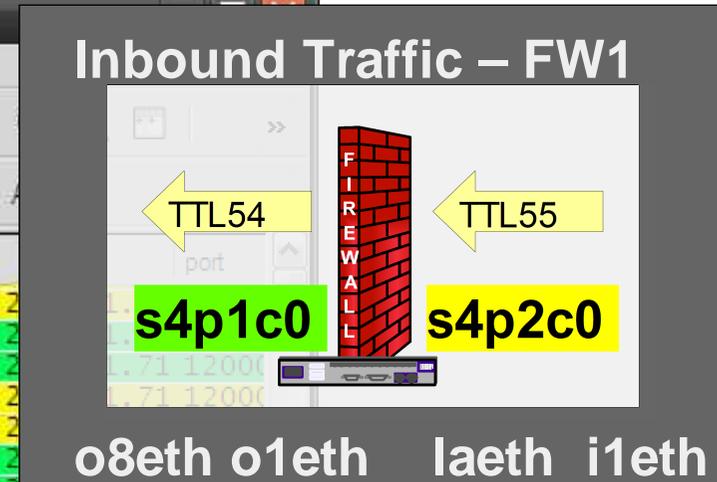
| No. | Time | ip.ttl | ip.id | ip.len | src_addr | dst_addr | ip.src |
|-----|-----------|--------|--------|--------|-------------------|----------------|-----------------------|
| 2 | 09:46:29. | 55 | 0xad95 | 31 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.2 |
| 3 | 09:46:29. | 54 | 0xad95 | 31 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.2 |
| 4 | 09:46:29. | 54 | 0xad95 | 31 | 73:34:70:31:63:30 | 4f:38:65:74:68 | 92.1.2 |
| 5 | 09:46:29. | 55 | 0x45ae | 31 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.2 |
| 6 | 09:46:29. | 55 | 0x1d3d | 31 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.2 |
| 7 | 09:46:29. | 54 | 0x1d3d | 31 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.2 |
| 8 | 09:46:29. | 54 | 0x1d3d | 31 | 73:34:70:31:63:30 | 4f:38:65:74:68 | 92.1.2 |
| 13 | 09:46:41. | 55 | 0x4dcc | 31 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.2 10.31.71 12000 |
| 14 | 09:46:41. | 55 | 0x4e17 | 31 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.2 10.31.71 12000 |

Frame 13 (45 bytes on wire, 45 bytes captured)

Ethernet II, Src: 73:34:70:32:63:30 (73:34:70:32:63:30), Dst: 69:31:65:74:68:2d

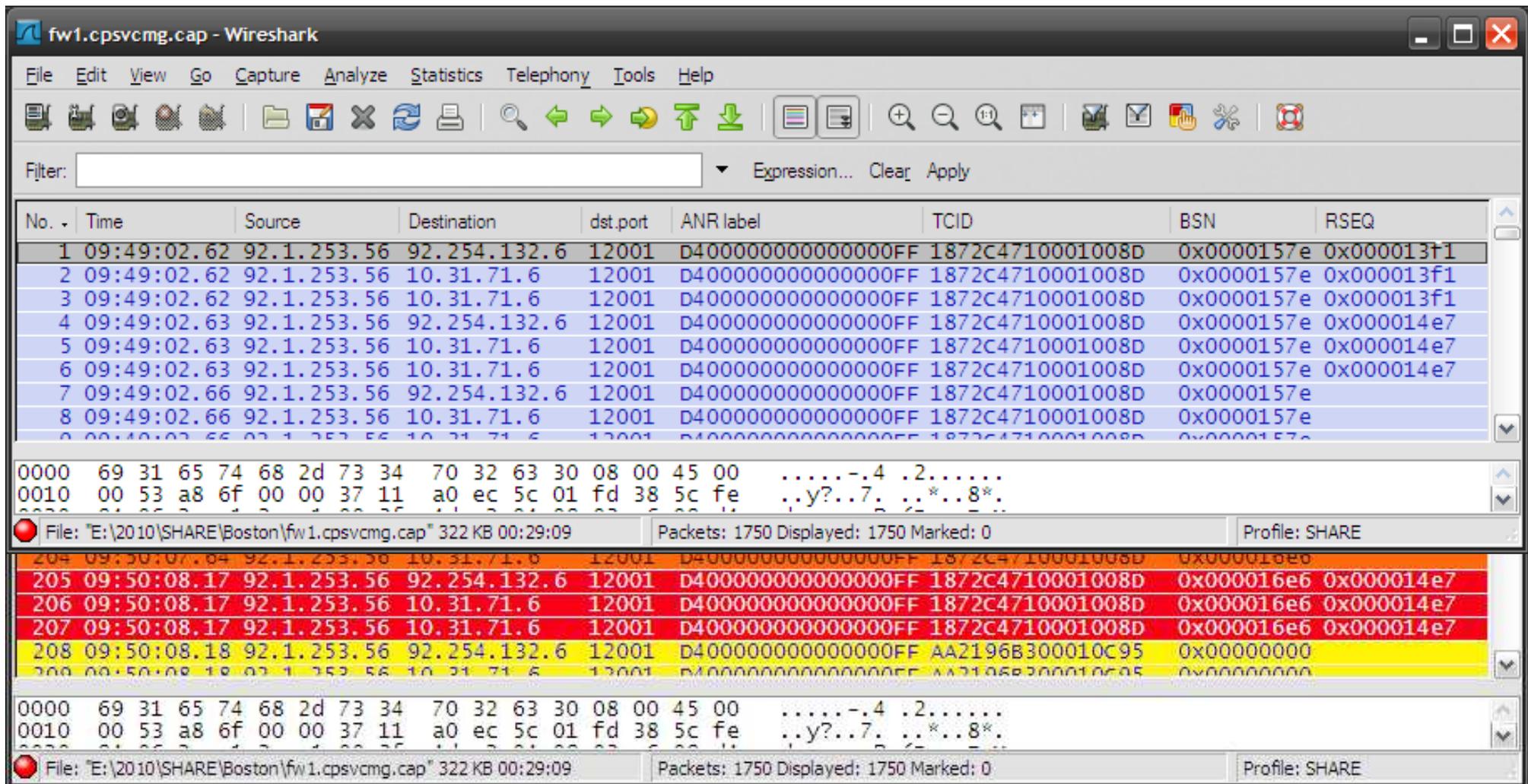
```
0000  69 31 65 74 68 2d 73 34 70 32 63 30 08 00 45 00  i1eth-s4 p2c0..E.
0010  00 1f 4d cc 00 00 37 11 8b a3 5c 01 fd 38 0a 1f  ..M...7.  ...8..
0020  47 06 2e e0 2e e0 00 0b 00 b0 04 08 f3          G.....
```

File: "E:\2010\SHARE\Boston\fw1.cap" 822 KB 00:31:42 Packets: 5254 Display... Profile: SHARE_2



fw1.cpsvcmg.cap

Existing CPSVCMG pathswitching and failing



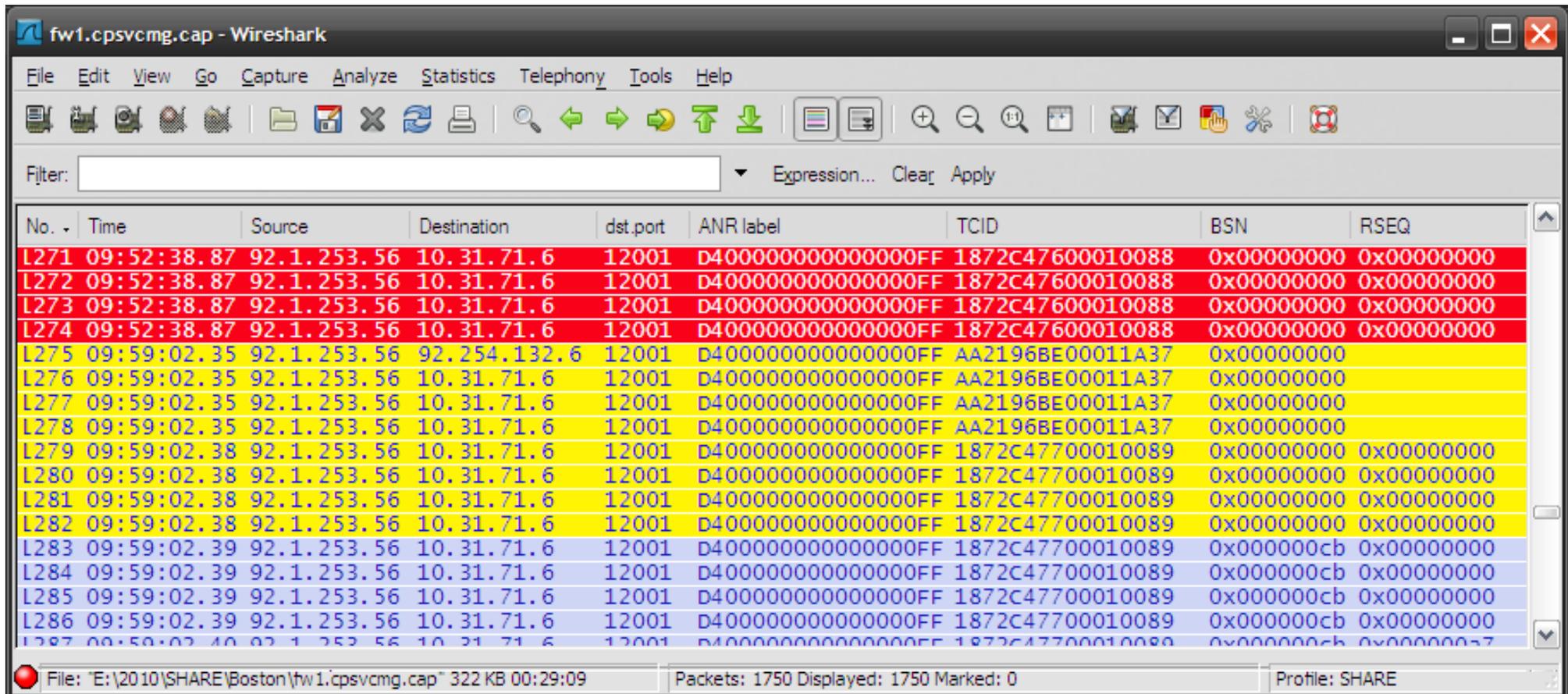
The image shows a Wireshark capture window titled "fw1.cpsvcmg.cap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help), a toolbar with various icons, and a filter field. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, dst.port, ANR label, TCID, BSN, and RSEQ. Below the list, there are two detailed views of packet data, each showing hexadecimal and ASCII representations. The status bar at the bottom of each view indicates "File: 'E:\2010\SHARE\Boston\fw1.cpsvcmg.cap' 322 KB 00:29:09", "Packets: 1750 Displayed: 1750 Marked: 0", and "Profile: SHARE".

| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|-------------|--------------|----------|--------------------|------------------|------------|------------|
| 1 | 09:49:02.62 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000013t1 |
| 2 | 09:49:02.62 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000013f1 |
| 3 | 09:49:02.62 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000013f1 |
| 4 | 09:49:02.63 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000014e7 |
| 5 | 09:49:02.63 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000014e7 |
| 6 | 09:49:02.63 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | 0x000014e7 |
| 7 | 09:49:02.66 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | |
| 8 | 09:49:02.66 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x0000157e | |

| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|-----|-------------|-------------|--------------|----------|--------------------|------------------|------------|------------|
| 204 | 09:50:07.84 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | |
| 205 | 09:50:08.17 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | 0x000014e7 |
| 206 | 09:50:08.17 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | 0x000014e7 |
| 207 | 09:50:08.17 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C4710001008D | 0x000016e6 | 0x000014e7 |
| 208 | 09:50:08.18 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | AA2196B300010C95 | 0x00000000 | |
| 209 | 09:50:08.18 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | AA2196B300010C95 | 0x00000000 | |

fw1.cpsvcmg.cap

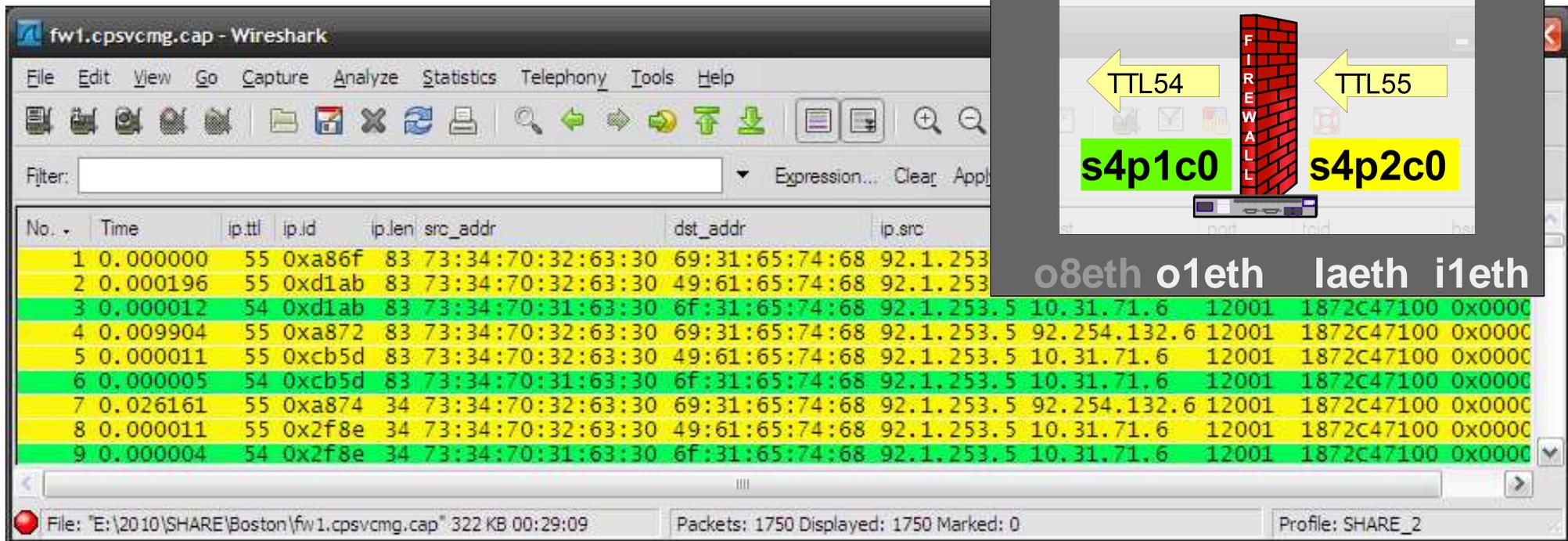
TCID 1872C476... fails at 09:52:38
More than 6 minutes later the pipe sets up
Every packet is – now - traced 4 times



| No. | Time | Source | Destination | dst.port | ANR label | TCID | BSN | RSEQ |
|------|-------------|-------------|--------------|----------|--------------------|------------------|------------|------------|
| 1271 | 09:52:38.87 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47600010088 | 0x00000000 | 0x00000000 |
| 1272 | 09:52:38.87 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47600010088 | 0x00000000 | 0x00000000 |
| 1273 | 09:52:38.87 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47600010088 | 0x00000000 | 0x00000000 |
| 1274 | 09:52:38.87 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47600010088 | 0x00000000 | 0x00000000 |
| 1275 | 09:59:02.35 | 92.1.253.56 | 92.254.132.6 | 12001 | D400000000000000FF | AA2196BE00011A37 | 0x00000000 | |
| 1276 | 09:59:02.35 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | AA2196BE00011A37 | 0x00000000 | |
| 1277 | 09:59:02.35 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | AA2196BE00011A37 | 0x00000000 | |
| 1278 | 09:59:02.35 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | AA2196BE00011A37 | 0x00000000 | |
| 1279 | 09:59:02.38 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x00000000 | 0x00000000 |
| 1280 | 09:59:02.38 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x00000000 | 0x00000000 |
| 1281 | 09:59:02.38 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x00000000 | 0x00000000 |
| 1282 | 09:59:02.38 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x00000000 | 0x00000000 |
| 1283 | 09:59:02.39 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x000000cb | 0x00000000 |
| 1284 | 09:59:02.39 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x000000cb | 0x00000000 |
| 1285 | 09:59:02.39 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x000000cb | 0x00000000 |
| 1286 | 09:59:02.39 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x000000cb | 0x00000000 |
| 1287 | 09:59:02.40 | 92.1.253.56 | 10.31.71.6 | 12001 | D400000000000000FF | 1872C47700010089 | 0x000000cb | 0x00000000 |

fw1.cpsvcmg.cap

In the beginning of the trace all packets are traced 3 times
twice with TTL=55 in s4p2c0, once with TTL=54 in s4p1c0



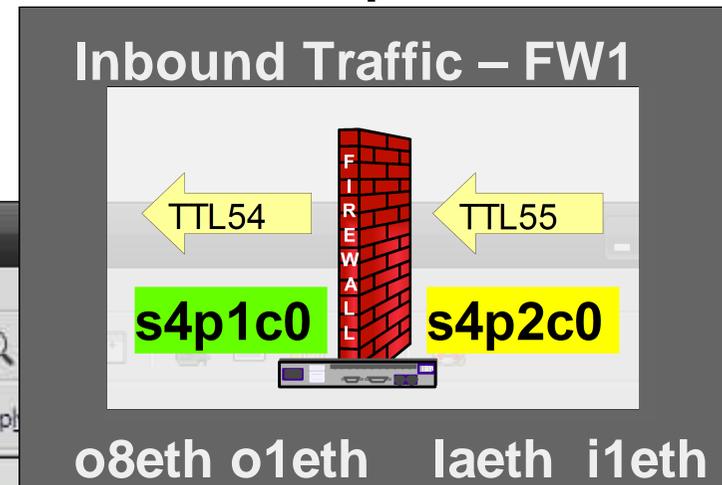
Inbound Traffic – FW1

| No. | Time | ip.ttl | ip.id | ip.len | src_addr | dst_addr | ip.src | ip.dst | eth.src | eth.dst |
|-----|----------|--------|--------|--------|-------------------|----------------|------------|--------------|---------|---------|
| 1 | 0.000000 | 55 | 0xa86f | 83 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.253.5 | 92.1.253.5 | o8eth | o1eth |
| 2 | 0.000196 | 55 | 0xd1ab | 83 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.253.5 | 92.1.253.5 | o8eth | o1eth |
| 3 | 0.000012 | 54 | 0xd1ab | 83 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.253.5 | 10.31.71.6 | laeth | i1eth |
| 4 | 0.009904 | 55 | 0xa872 | 83 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.253.5 | 92.254.132.6 | o8eth | o1eth |
| 5 | 0.000011 | 55 | 0xcb5d | 83 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.253.5 | 10.31.71.6 | o8eth | o1eth |
| 6 | 0.000005 | 54 | 0xcb5d | 83 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.253.5 | 10.31.71.6 | laeth | i1eth |
| 7 | 0.026161 | 55 | 0xa874 | 34 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.253.5 | 92.254.132.6 | o8eth | o1eth |
| 8 | 0.000011 | 55 | 0x2f8e | 34 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.253.5 | 10.31.71.6 | o8eth | o1eth |
| 9 | 0.000004 | 54 | 0x2f8e | 34 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.253.5 | 10.31.71.6 | laeth | i1eth |

File: "E:\2010\SHARE\Boston\fw1.cpsvcmg.cap" 322 KB 00:29:09 Packets: 1750 Displayed: 1750 Marked: 0 Profile: SHARE_2

fw1.cap

Starting 09:52:26h all packets are traced 4 times
twice with TTL=55 in s4p2c0, twice with TTL=54 in s4p1c0



fw1.cpsvcmg.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Appl

| No. | Time | ip.ttl | ip.id | ip.len | src_addr | dst_addr | ip.src | ip.dst | port | code | len | offset |
|------|-----------|--------|--------|--------|-------------------|----------------|------------|--------------|-------|------------|--------|--------|
| 1216 | 09:52:24. | 55 | 0x0f4e | 87 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.253.5 | 92.254.132.6 | 12001 | 1872c47600 | 0x0000 | |
| 1217 | 09:52:24. | 55 | 0xe670 | 87 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |
| 1218 | 09:52:24. | 54 | 0xe670 | 87 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |
| 1219 | 09:52:26. | 55 | 0x0faa | 87 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.253.5 | 92.254.132.6 | 12001 | 1872c47600 | 0x0000 | |
| 1220 | 09:52:26. | 55 | 0x4c96 | 87 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |
| 1221 | 09:52:26. | 54 | 0x4c96 | 87 | 73:34:70:31:63:30 | 6f:31:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |
| 1222 | 09:52:26. | 54 | 0x4c96 | 87 | 73:34:70:31:63:30 | 4f:38:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |
| 1223 | 09:52:27. | 55 | 0x1024 | 87 | 73:34:70:32:63:30 | 69:31:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |
| 1224 | 09:52:27. | 55 | 0x3969 | 87 | 73:34:70:32:63:30 | 49:61:65:74:68 | 92.1.253.5 | 10.31.71.6 | 12001 | 1872c47600 | 0x0000 | |

File: "E:\2010\SHARE\Boston\fw1.cpsvcmg.cap" 322 KB 00:29:09 Packets: 1750 Displayed: 1750 Marked: 0 Profile: SHARE_2

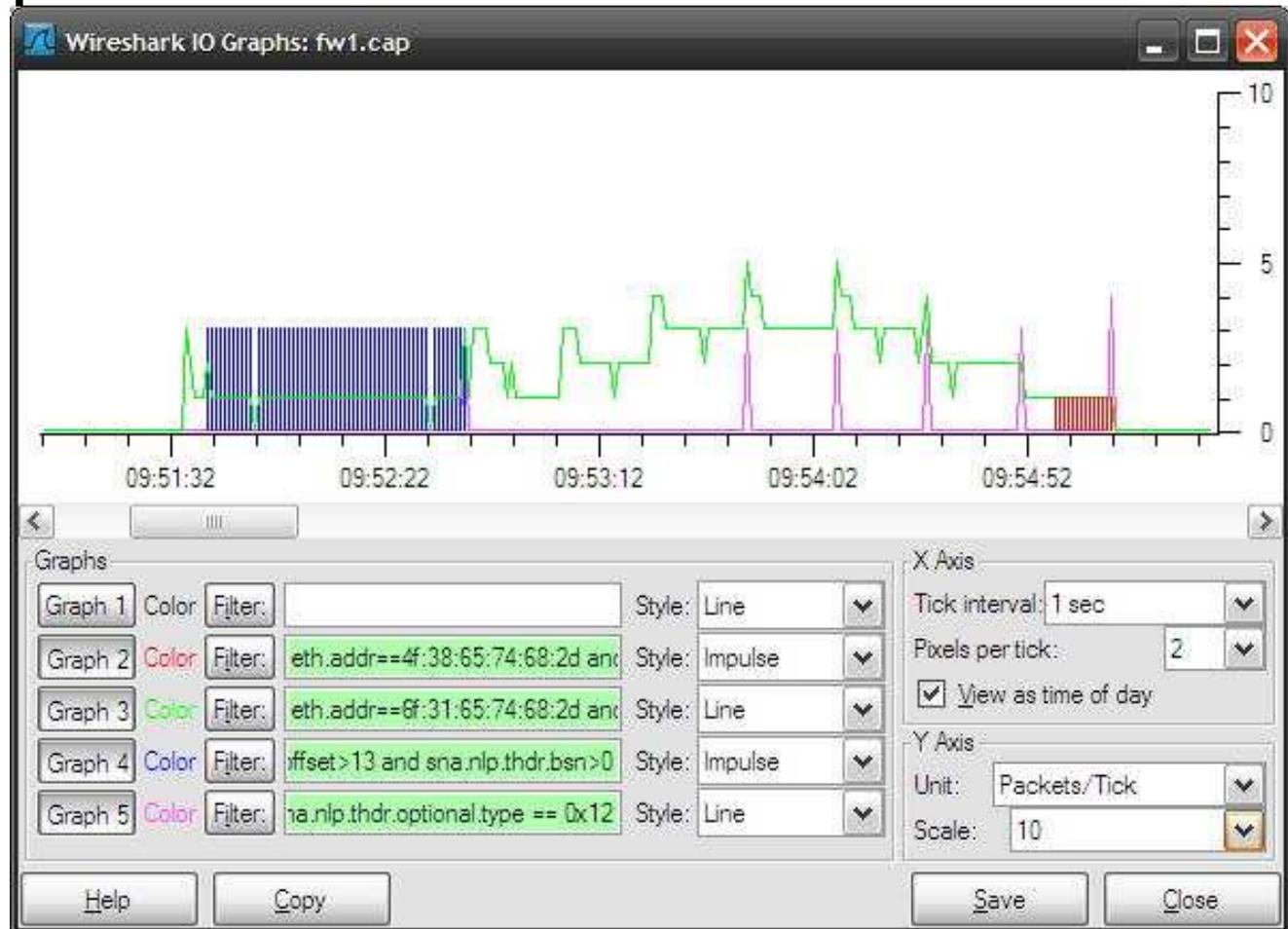
fw1.cap Statistics – IO Graph

Green line shows 12001 packets on o1eth

Red impulse shows 12001 packets on o8eth

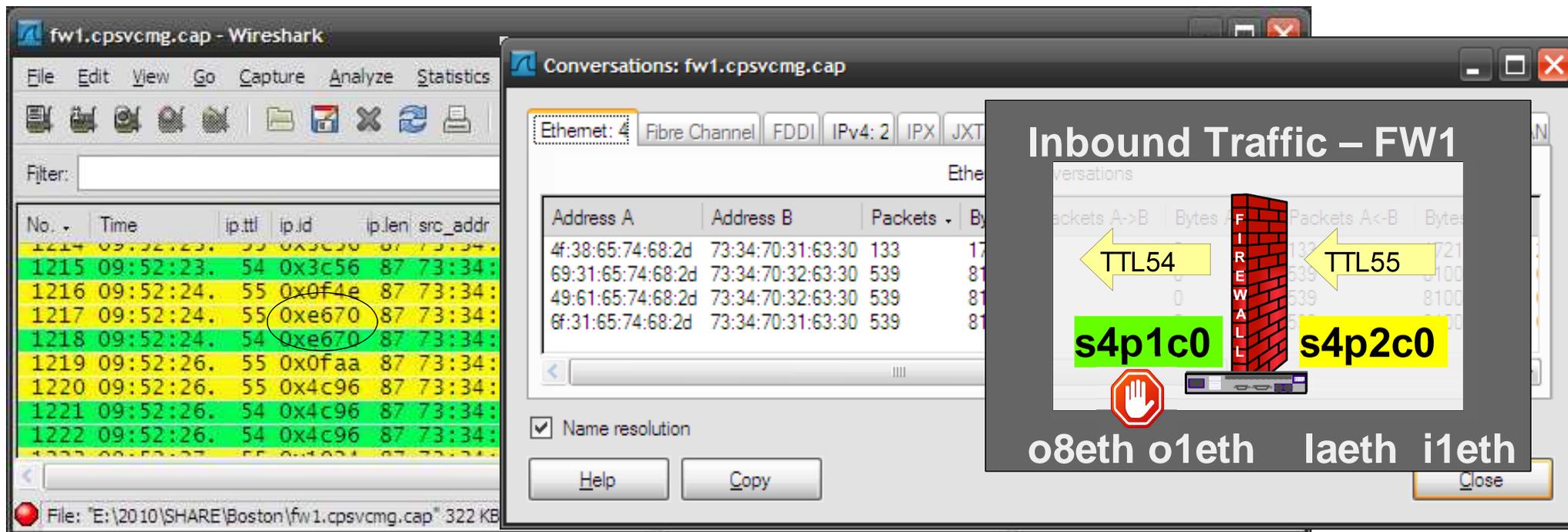
Blue - pipe pathswitching

Pink - Pipe terminating



fw1.cpsvcmg.cap

Wireshark Statistics: conversations



The image shows the Wireshark interface with two windows. The main window displays a list of captured packets with the following columns: No., Time, ip.ttl, ip.id, ip.len, src_addr. The packet list shows several packets with IP IDs 0x3c56, 0x0f4e, 0xe670, 0x0faa, 0x4c96, and 0x4c96. The IP ID 0xe670 is circled in red. The conversations window shows a table of conversations with columns: Address A, Address B, Packets, Bytes. The table shows four conversations between 4f:38:65:74:68:2d and 73:34:70:31:63:30, and 69:31:65:74:68:2d and 73:34:70:32:63:30. A diagram of a firewall is overlaid on the conversations window, showing inbound traffic from the left. The diagram includes a brick wall labeled 'FIREWALL', a stop sign, and labels for interfaces: o8eth, o1eth, laeth, and i1eth. The diagram also shows TTL values of 54 and 55, and packet counts s4p1c0 and s4p2c0.

- The inbound firewall is dropping 12001 packets on its last leg (s4p1c0) towards the datacenter.
- IPID E670 was not sent out of the firewall
 - After IPID 4C96 was sent successfully, the problem went away

Questions

- Need more? Come to Wireshark Bootcamp 2010

**“Tell me and I'll forget;
show me and I may remember;
involve me and I'll understand.”**



Get involved!

Berlin, DE Sep. 21-24: <http://tinyurl.com/ZOWIE0DE>
Markham, ON Nov. 9 – 12: <http://tinyurl.com/ZOWIE0CE>

SHARE in Boston

32



| Zeit | 27.04. | 28.04. | 29.04. | 30.04. |
|-------|--|---|--|---|
| 09:00 | Welcome First Use of wireshark Installation of wireshark | Review IP Header ipfragment.cap | Review 3-way-handshake: RTT,IPID,MSS,WS,Wscaling,SACK,timestamp | Review Firewalls TCPKEEPALIVE RFC1122 |
| 10:00 | Kaffeepause | | | |
| 10:30 | User Preferences Promiscuous mode Taking Traces facebook.pcap | Profile Default | TCP Seq#/Ack# Retransmission Traceroute | NFS NFS Hints and Tipps |
| 11:30 | Mittagspause | | | |
| 12:30 | ARP RTT, Latency Export HTML objects editcap - remove duplicate packets - split large files | scpl.cap IP.LEN, IP.CHECKSUM IP.TTL, IP.DF, ICMP ICMP Destination unreachable, Fragmentation neded. | Nagle's algorithm Delayed Acknowledgements TCPDelAckTicks | |
| 13:30 | Profiles- Setting preferences heartbeat.cap MQ Profile | PMTU Discovery ICMP Destunreachable/Port unreachable TCP Setup and Termination | TCP Flow Control Bandwidth-Delay-Product, Latency transrapid.cap | SYSTCPDA mceta3.cap gtf2cap.exe |
| 14:30 | Kaffeepause | | | |
| 15:00 | Statistics Protocol Hierarchy FlowGraph | Profile TCP 3-way handshake | Receive Window size | Ende |
| 16:00 | bad.cap Split large files IO-Graph | | saprouter.pcap NA(P)T SSL Introduction schwayer.cap | |