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

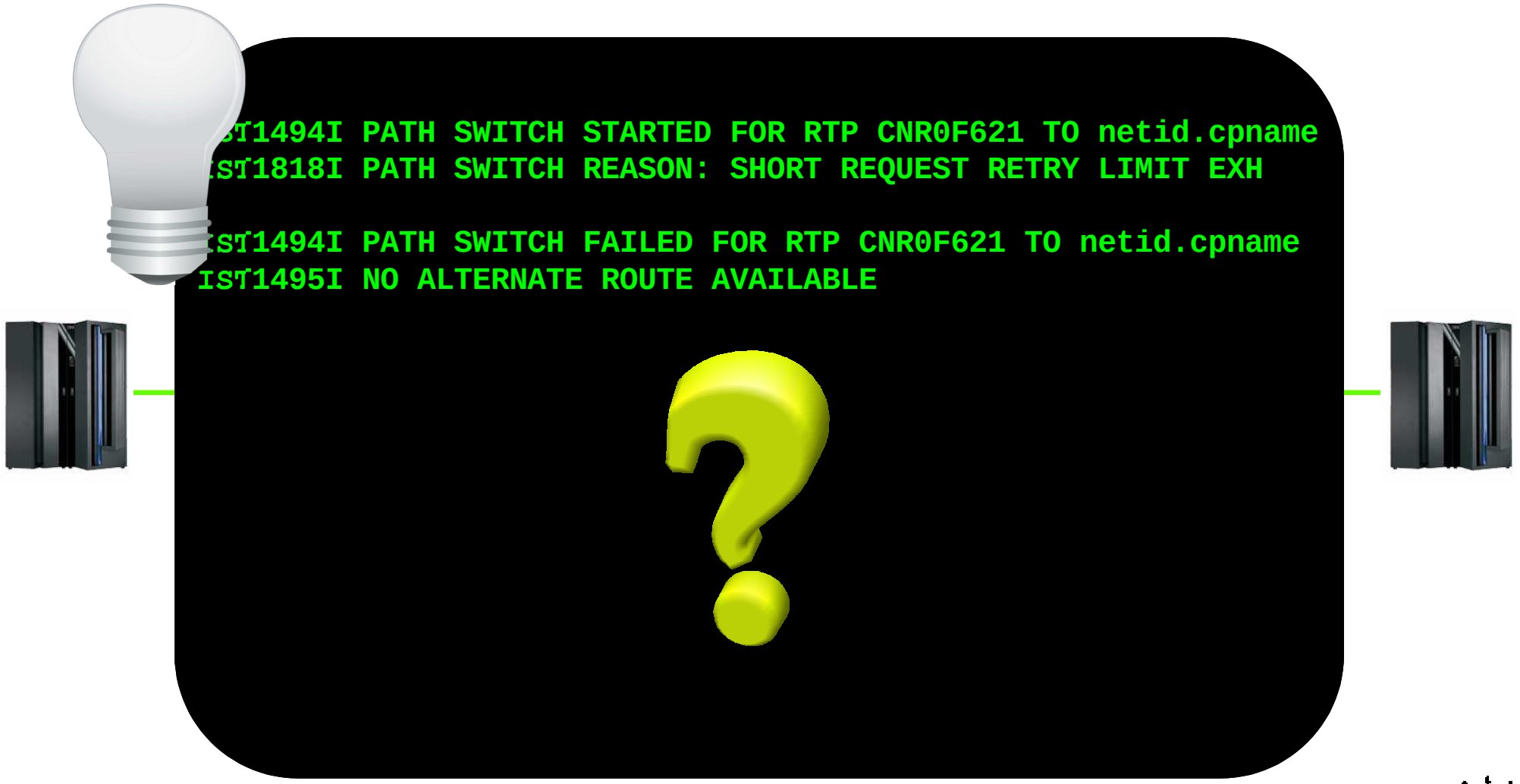
Now that you know the various layers of Enterprise Extender packets and the external symptoms of HPR problems it is time to look at some real examples of network flows.

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

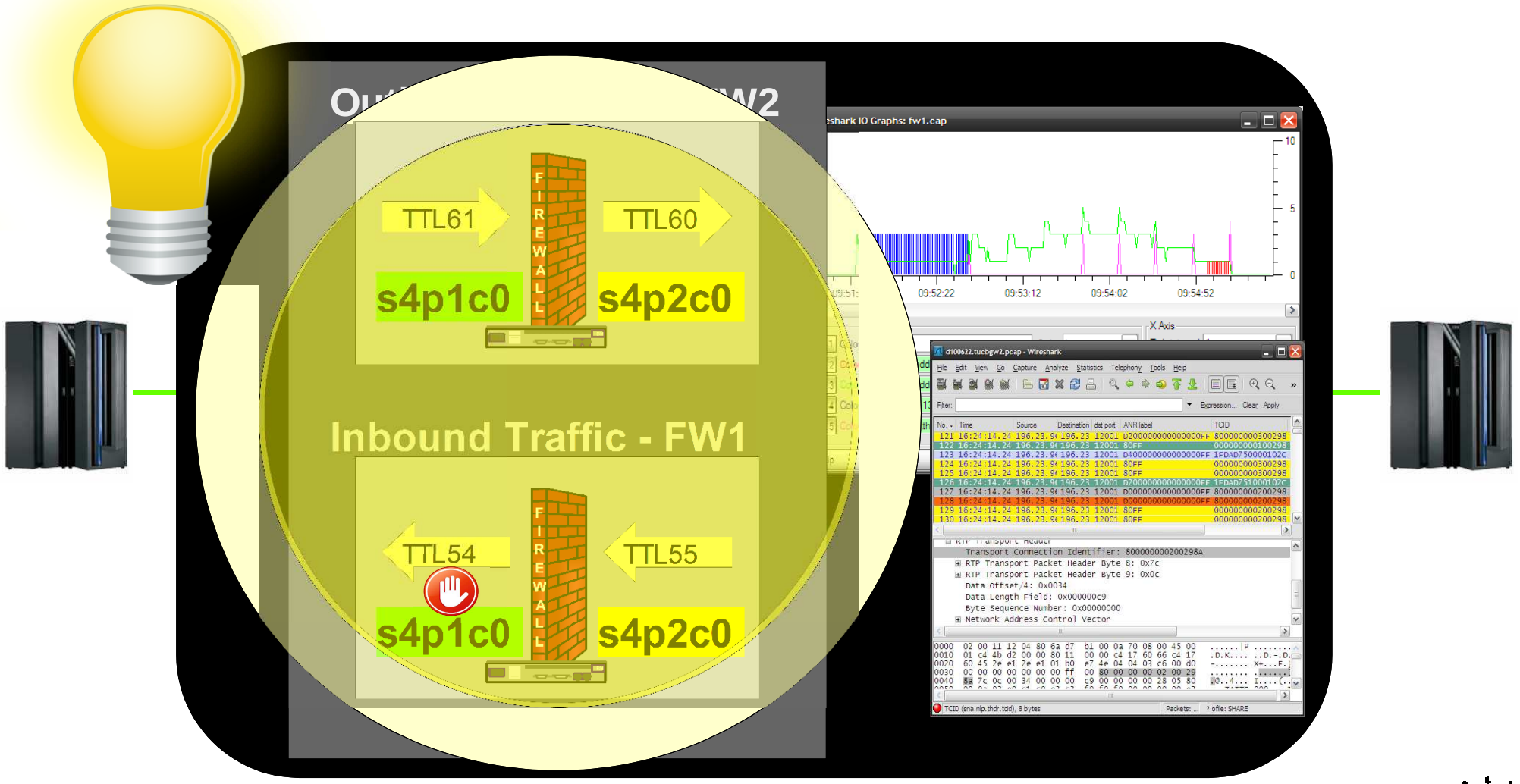
See how applying intelligent filters to an IP trace can speed up problem source identification and resolution of EE problems.

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

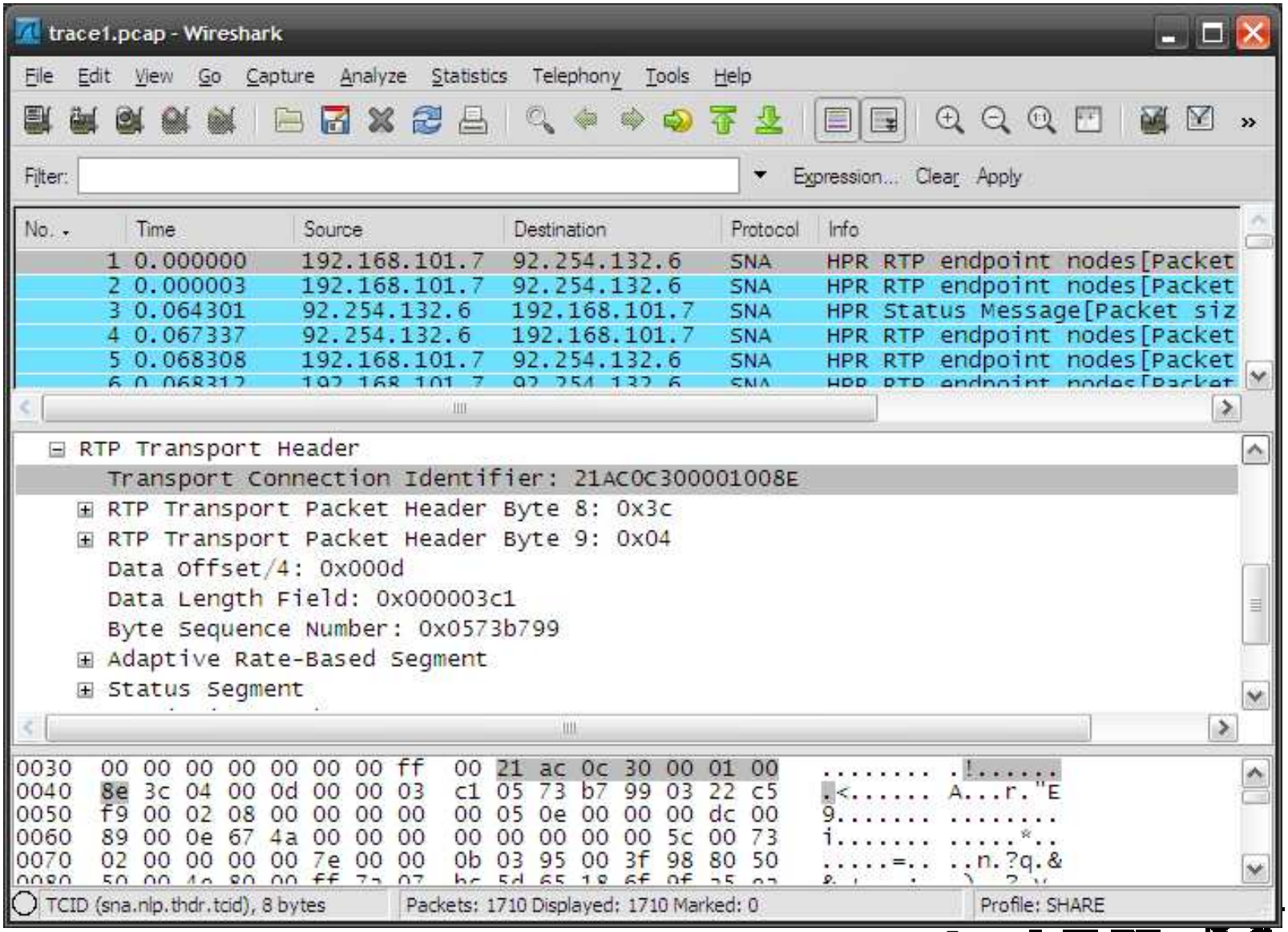


Turn on the light with wireshark



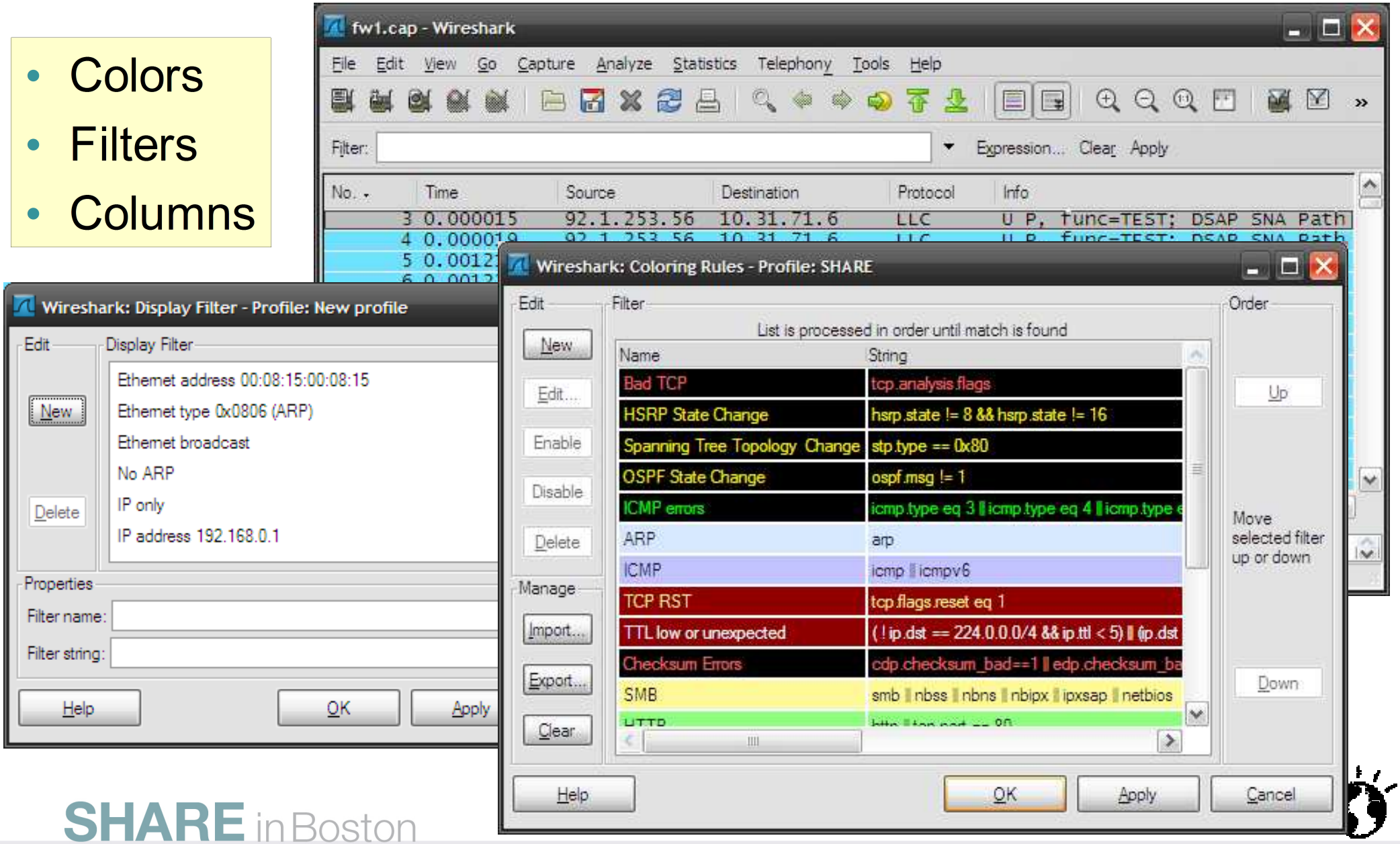
Wireshark default configuration

- Packet List
- Dissection
- Hex Detail



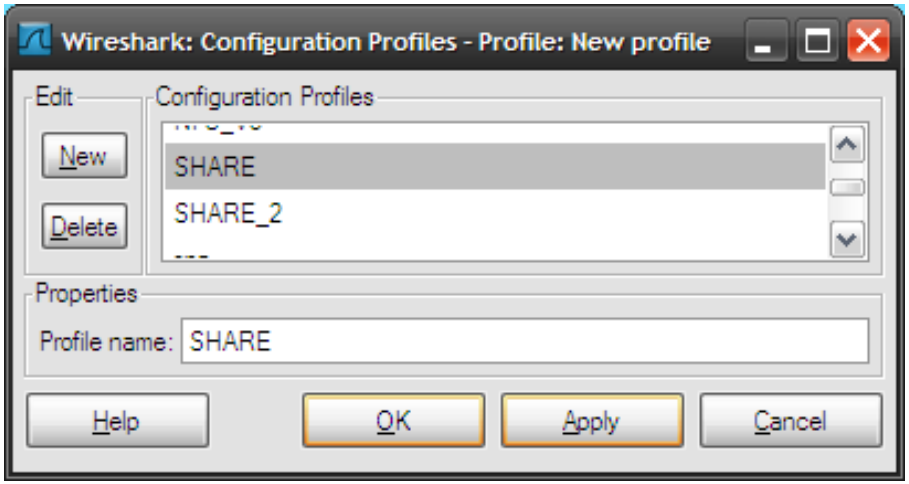
Wireshark default profile

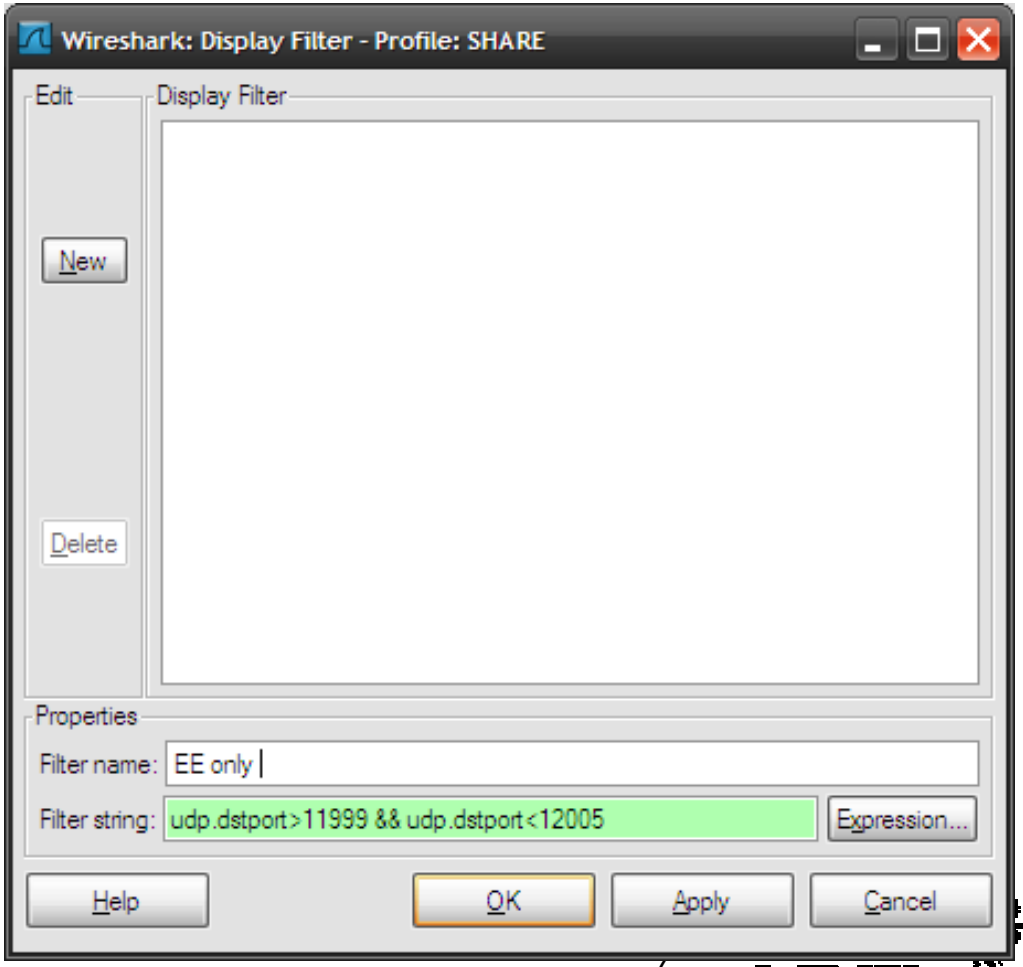
- Colors
- Filters
- Columns



Wireshark new SHARE profile

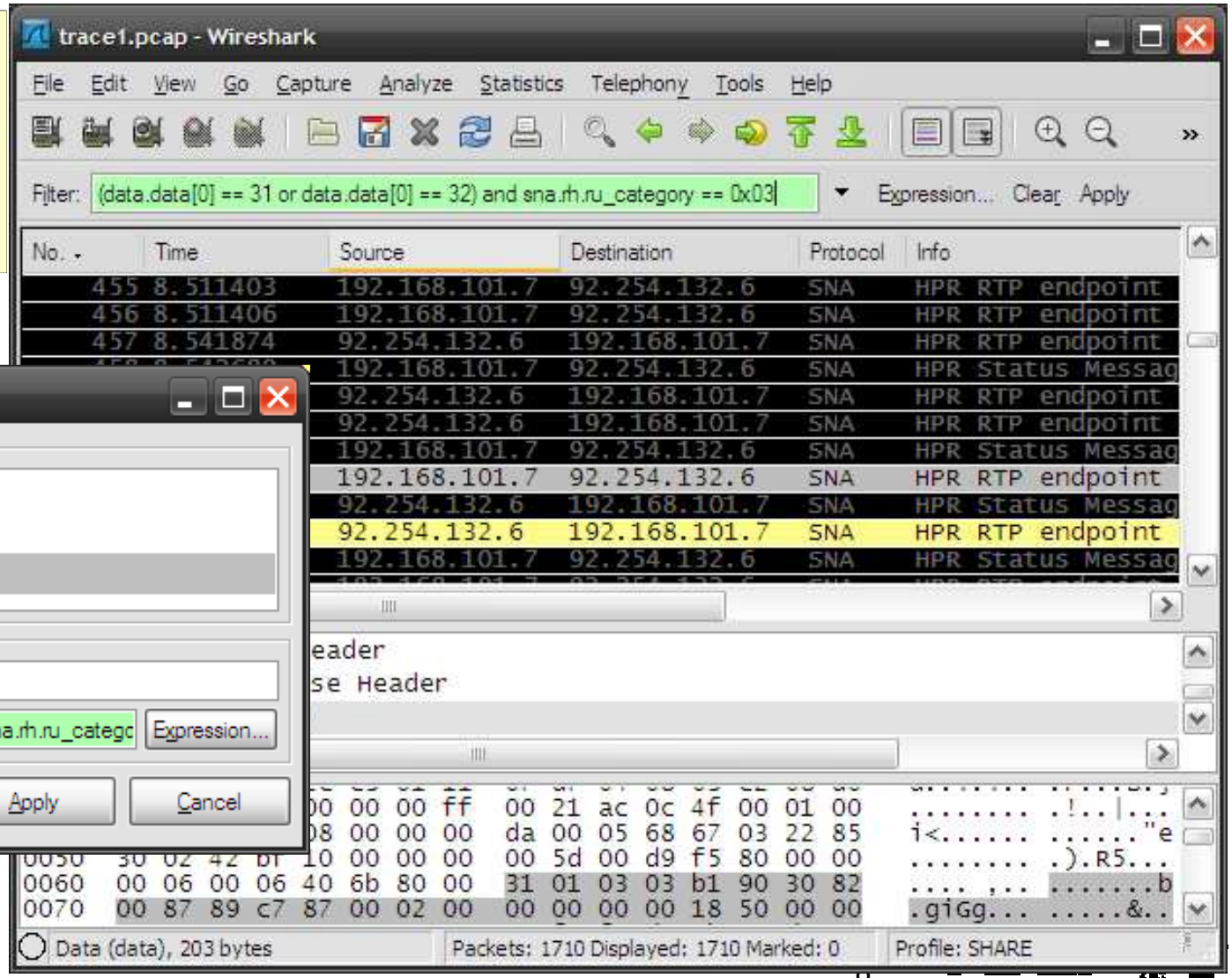
- SHIFT + CTRL + A
  - Clear filters
  - Create new filters



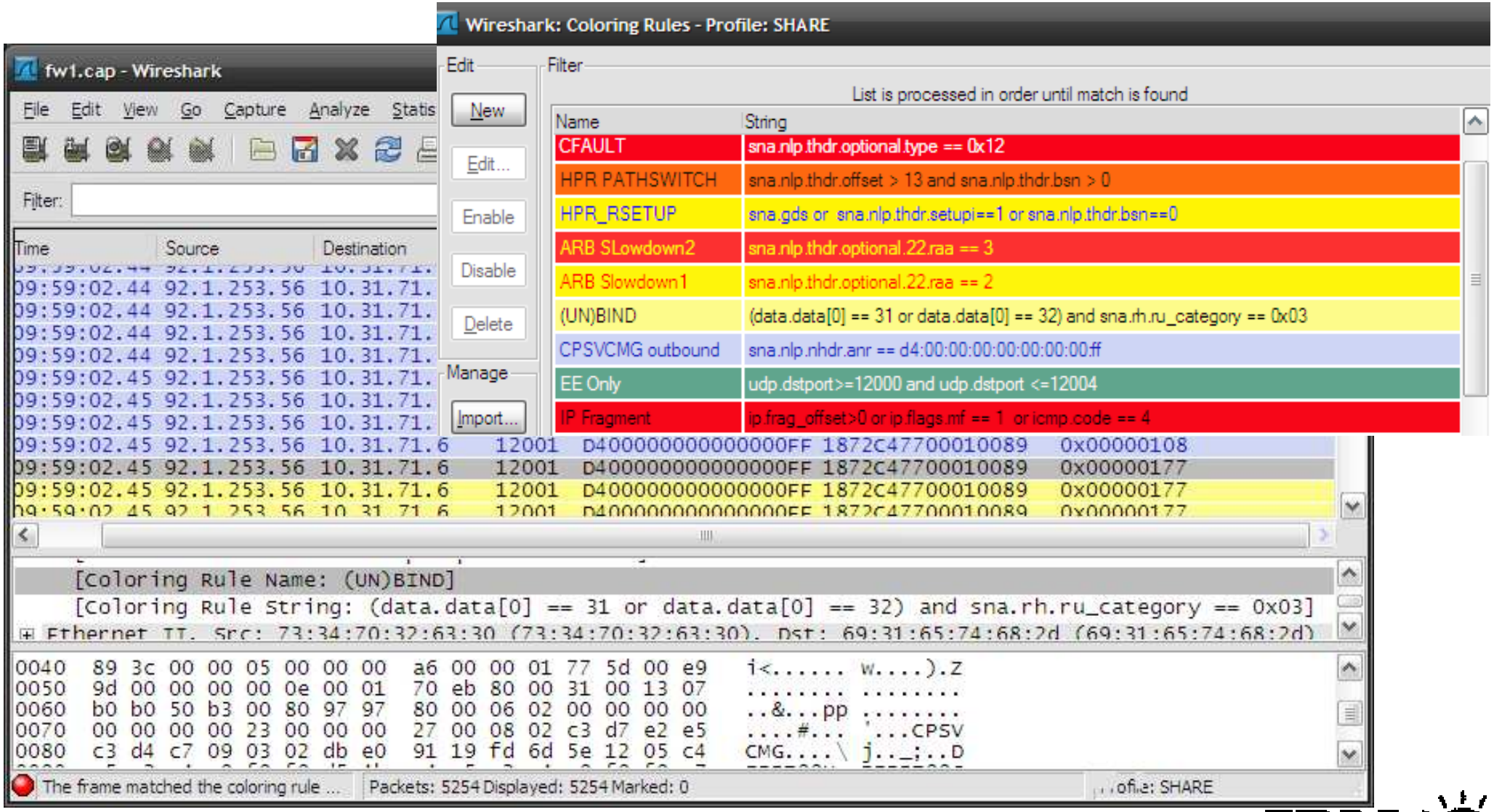


Wireshark SHARE Filters: BIND/UNBIND

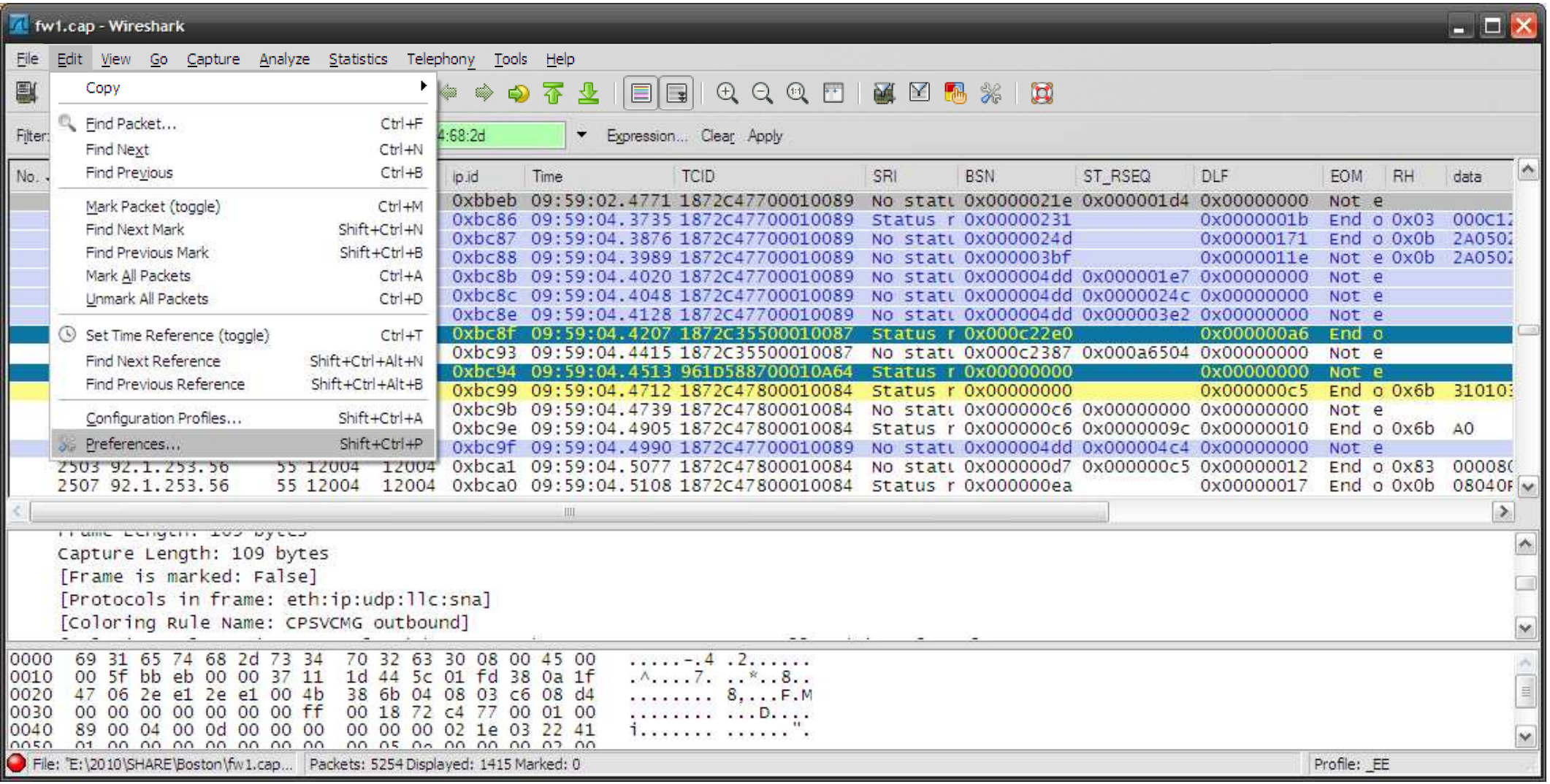
- SNA RUs
  - BIND RU:31
  - UNBIND RU: 32



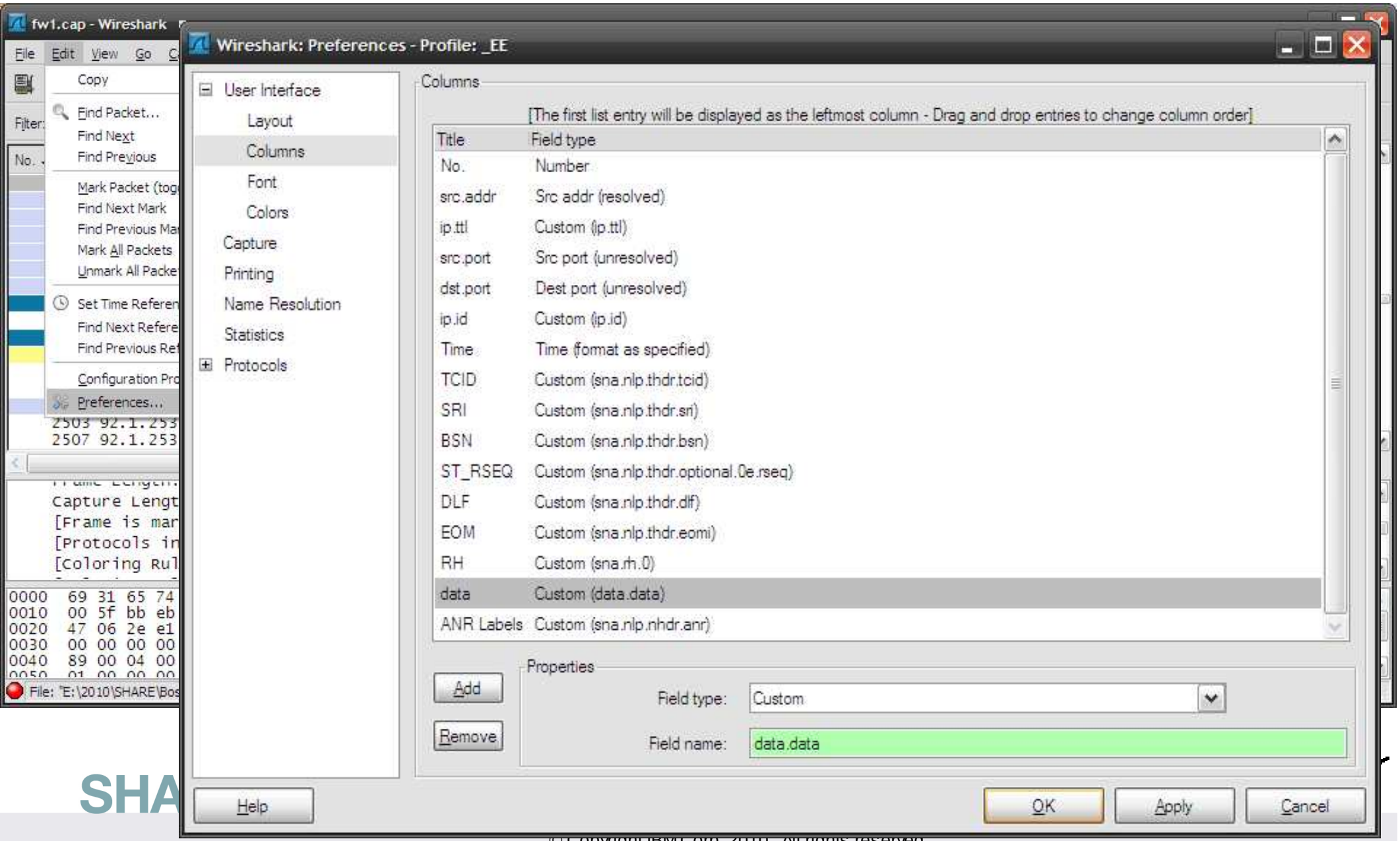
Wireshark SHARE : Coloring Rules



Wireshark SHARE Preferences: Columns

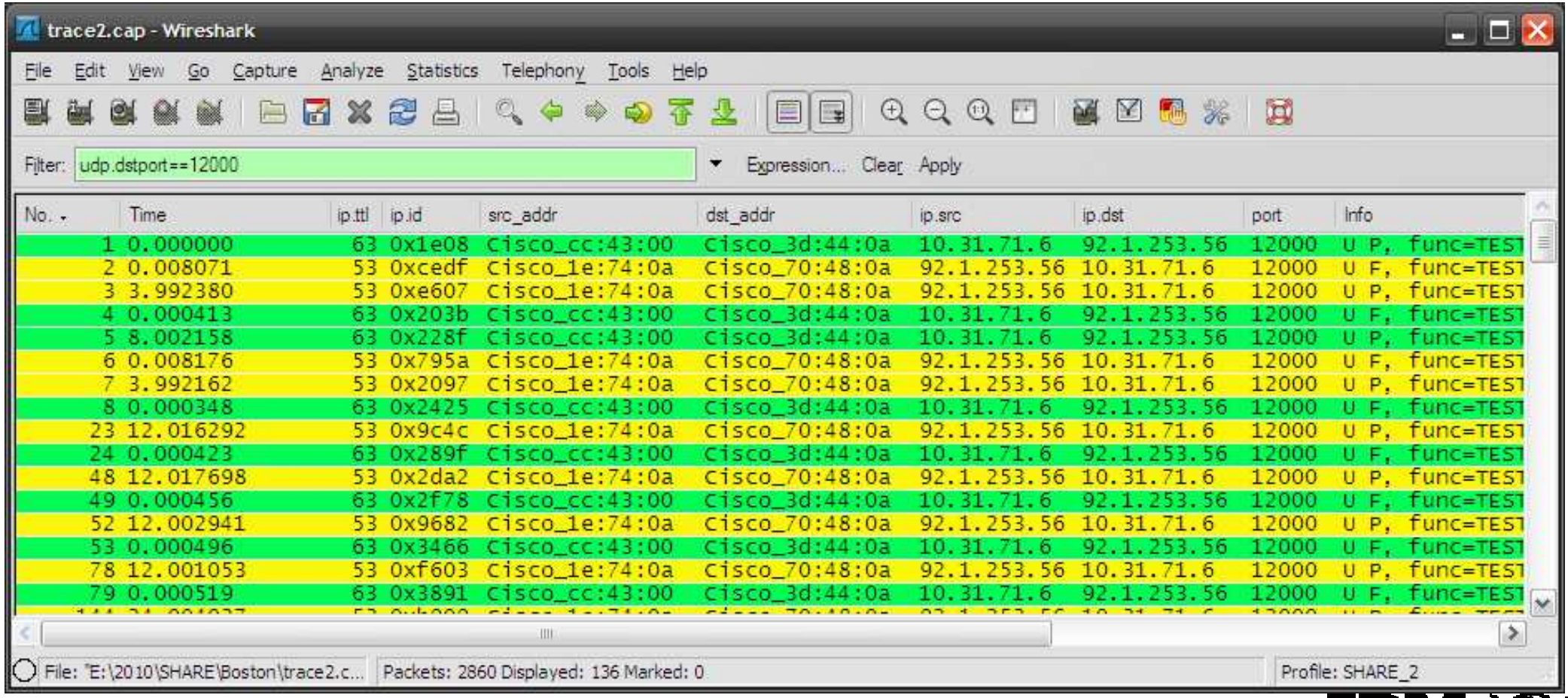


Wireshark SHARE Preferences: Columns



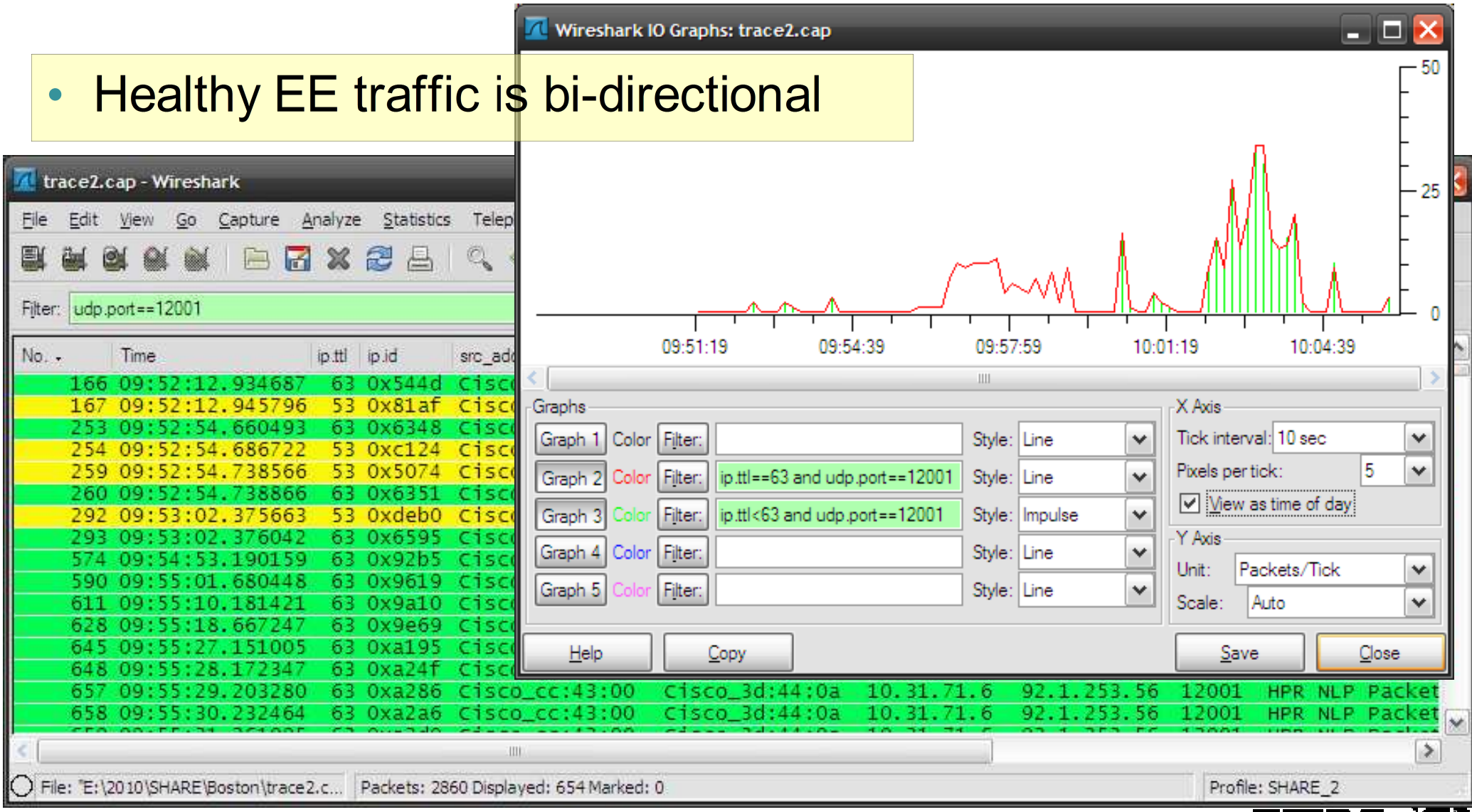
Wireshark SHARE profiles: IP Profile

- TTL as indicator of inbound/outbound

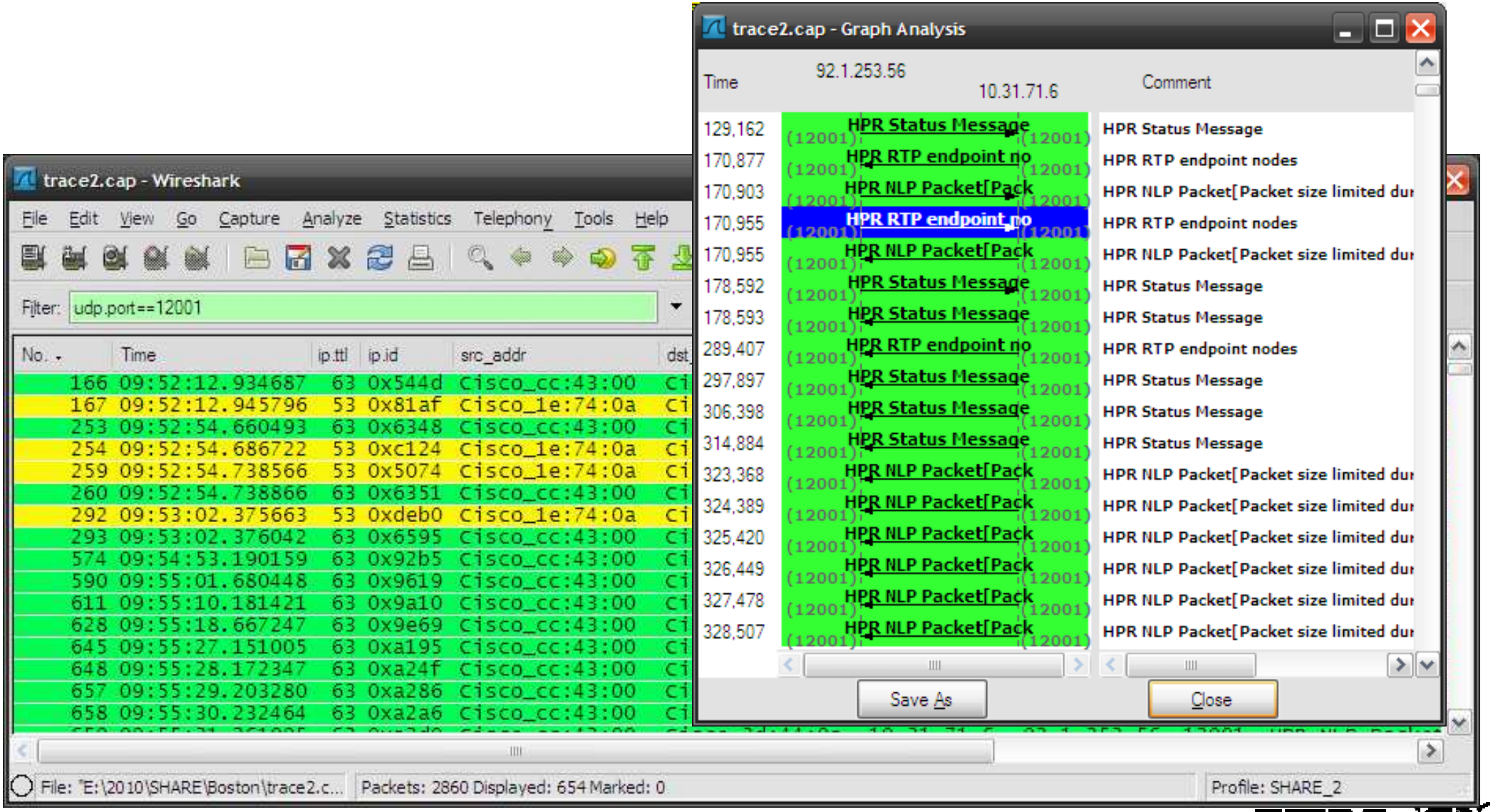


Wireshark SHARE profiles: IO Graph

- Healthy EE traffic is bi-directional



Wireshark SHARE profiles: Flow Graph

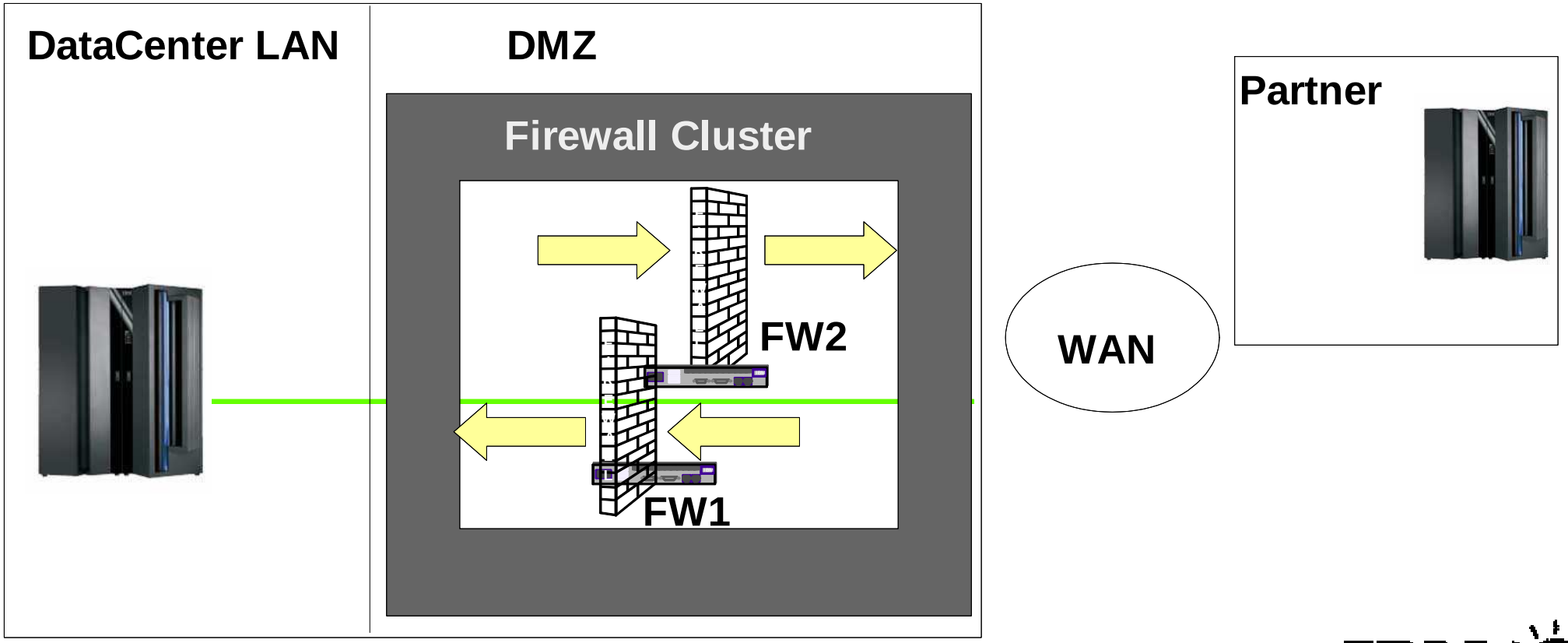


“Tell me and I'll forget;
show me and I may remember;
involve me and I'll understand.”
Part II: Hands-on experience

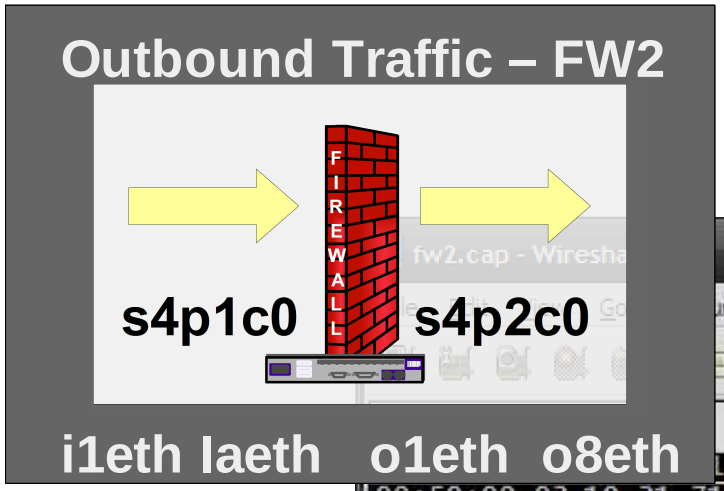
Get involved in a real EE Pathswitch problem

The Topology

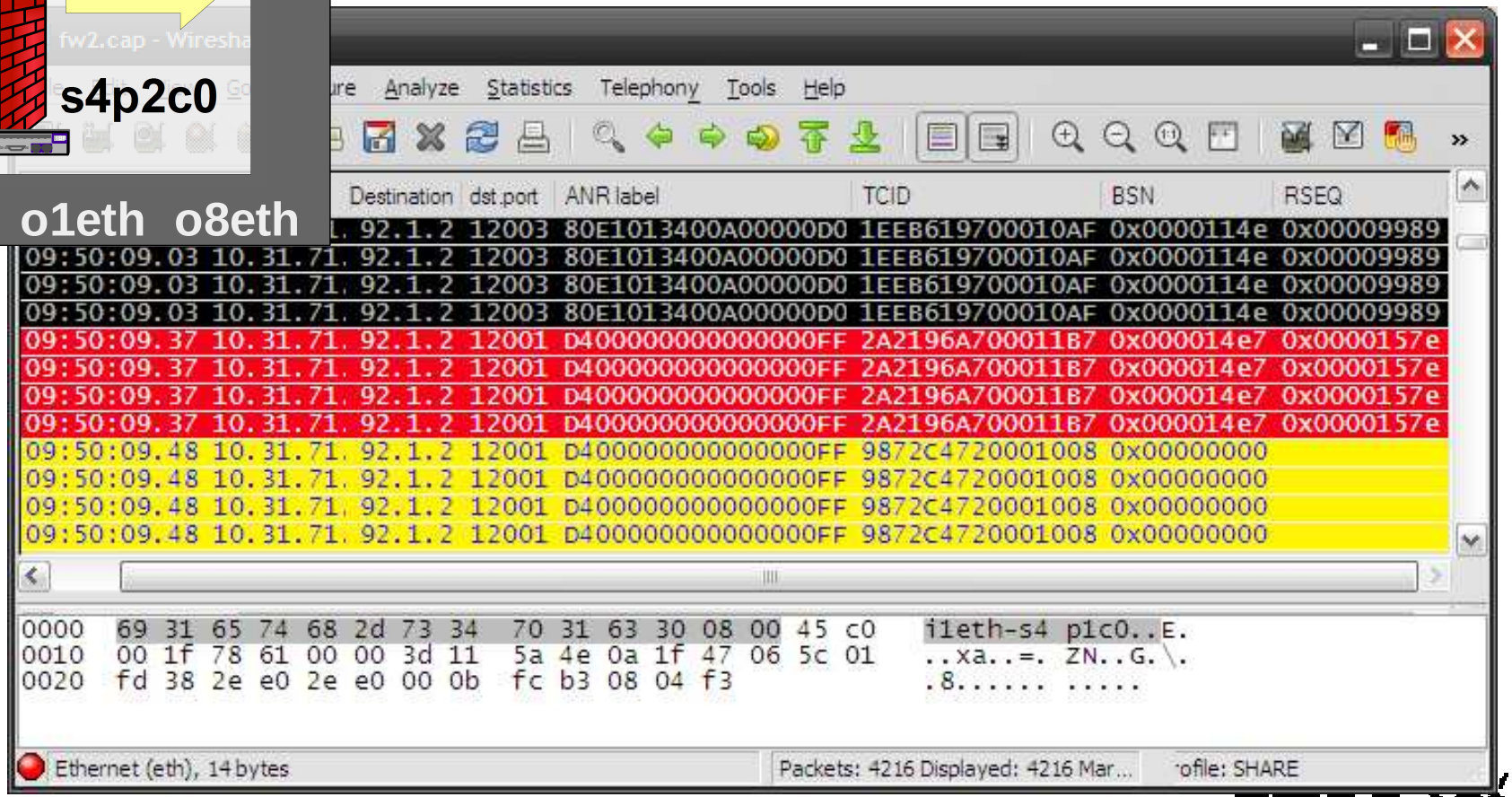
- Traces were taken in the FW cluster
- FW1 handles inbound , FW2 handles outbound traffic



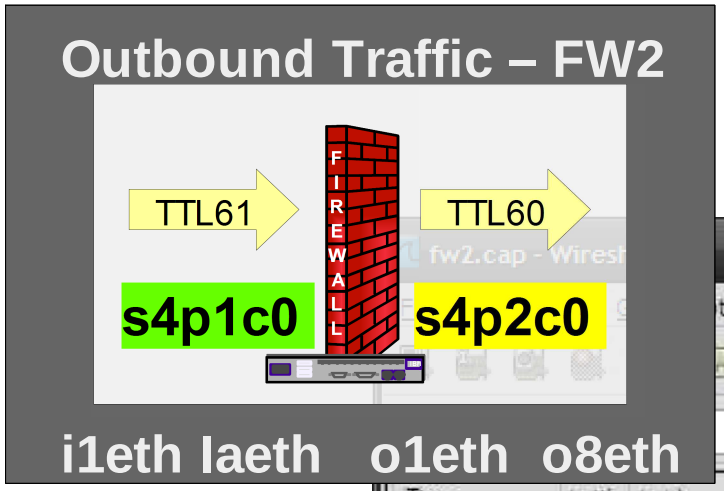
Outbound Traffic - fw2.cap



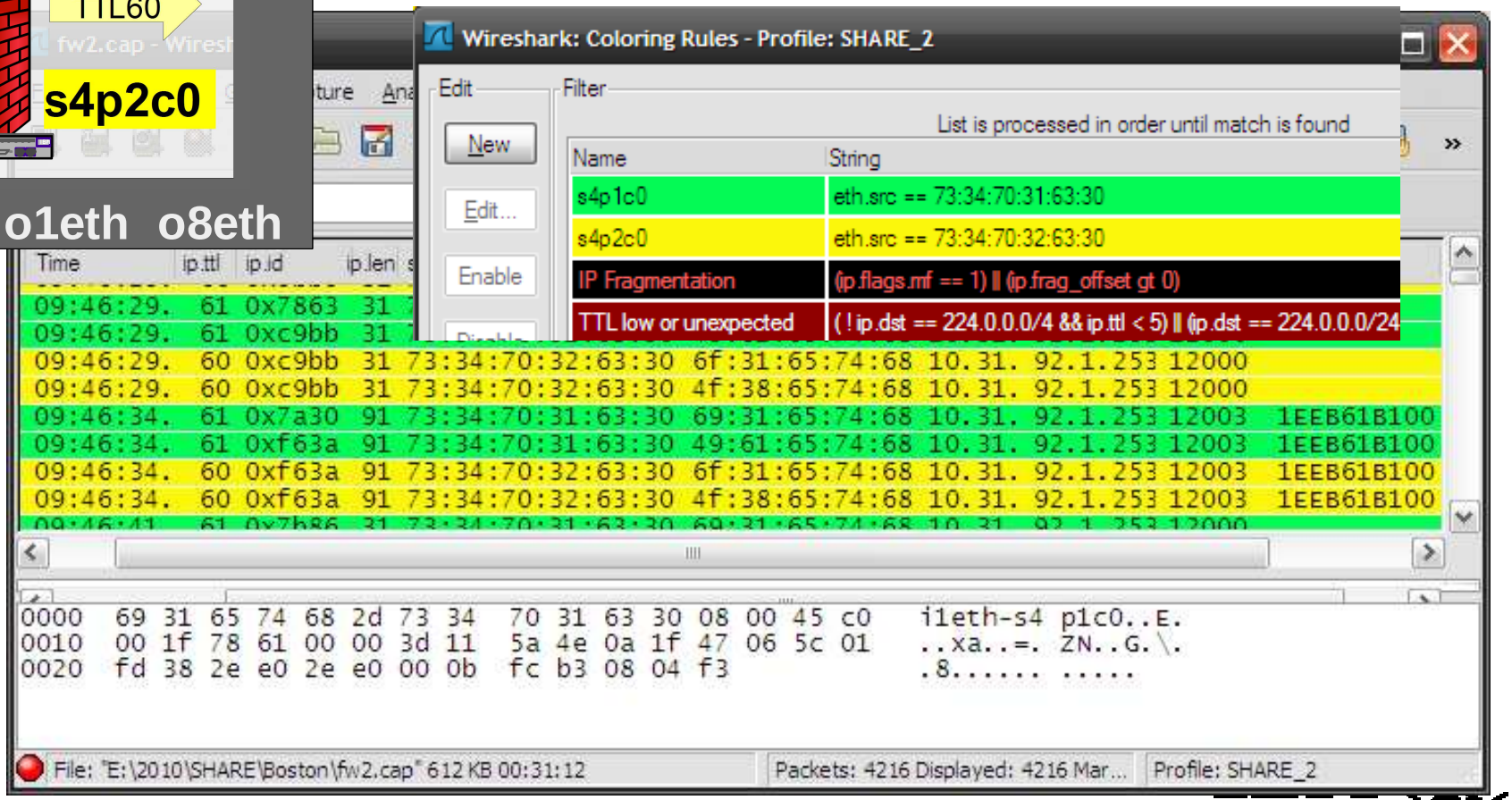
Every packet is traced 4 times as it flows through the FW Cluster
The Ethernet addresses change



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

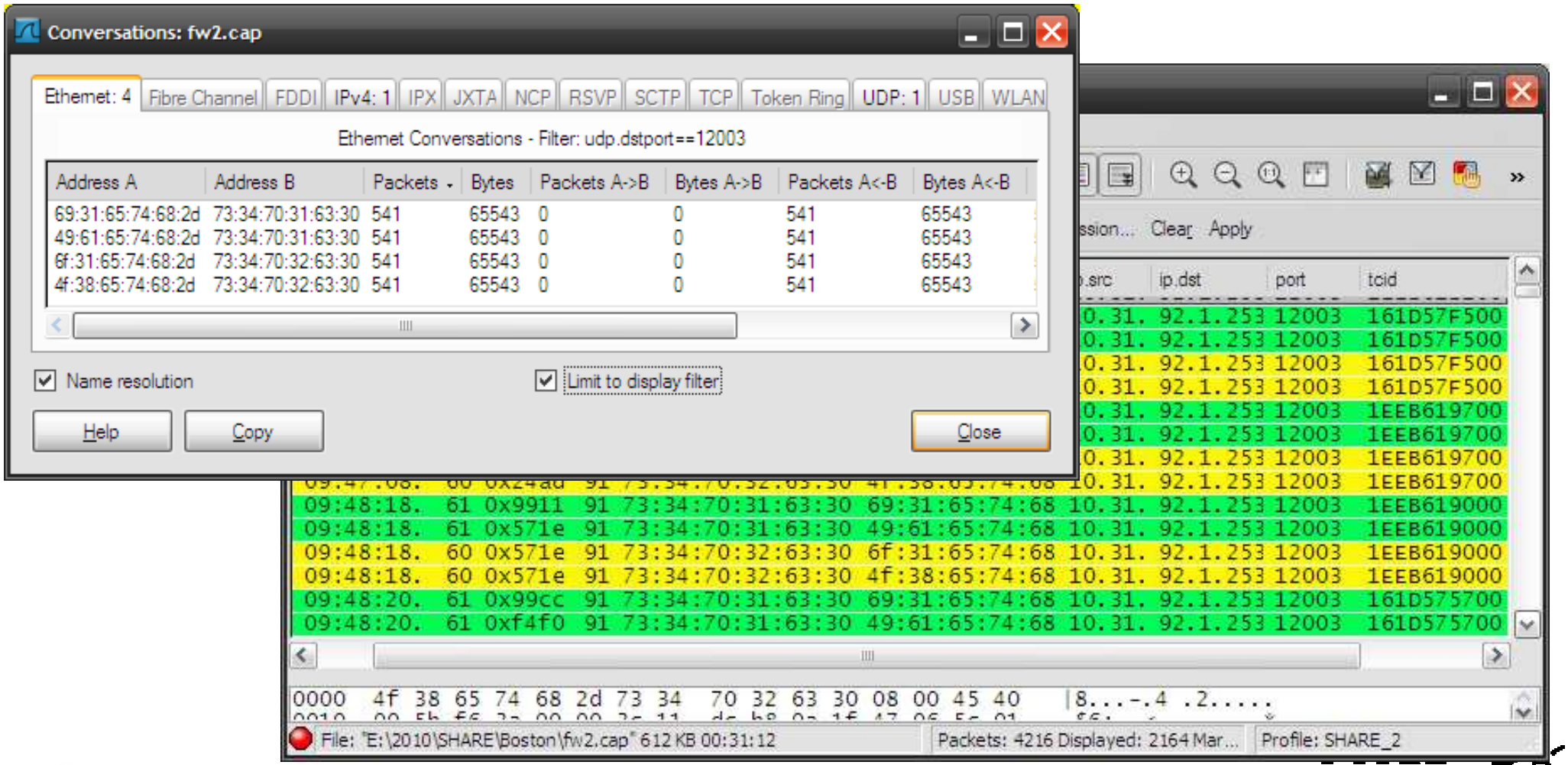


2 trace points in 's4p1c0' – TTL = 61
2 trace points in 's4p2c0' – TTL = 60



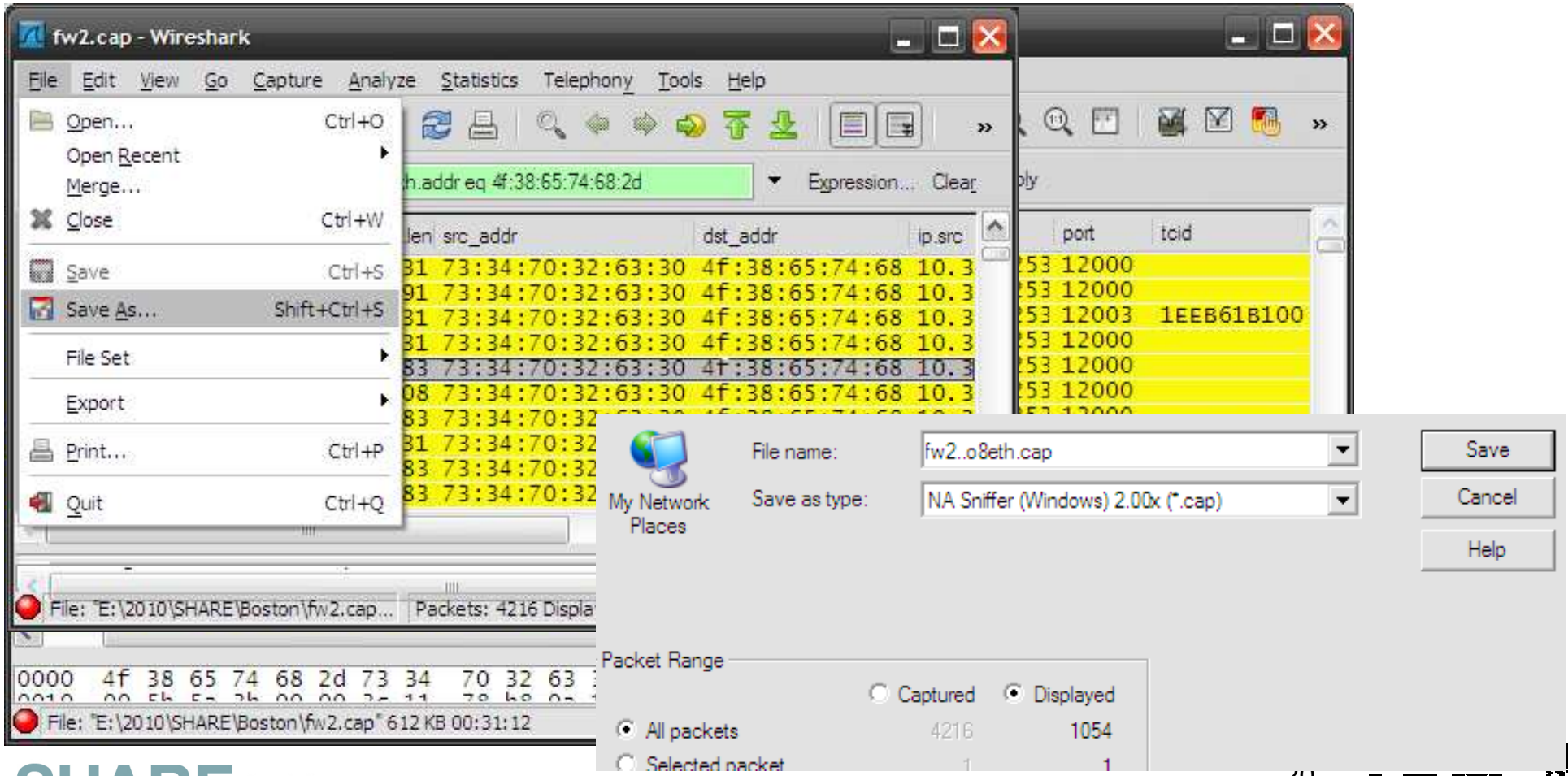
Wireshark Statistics: conversations 12003

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



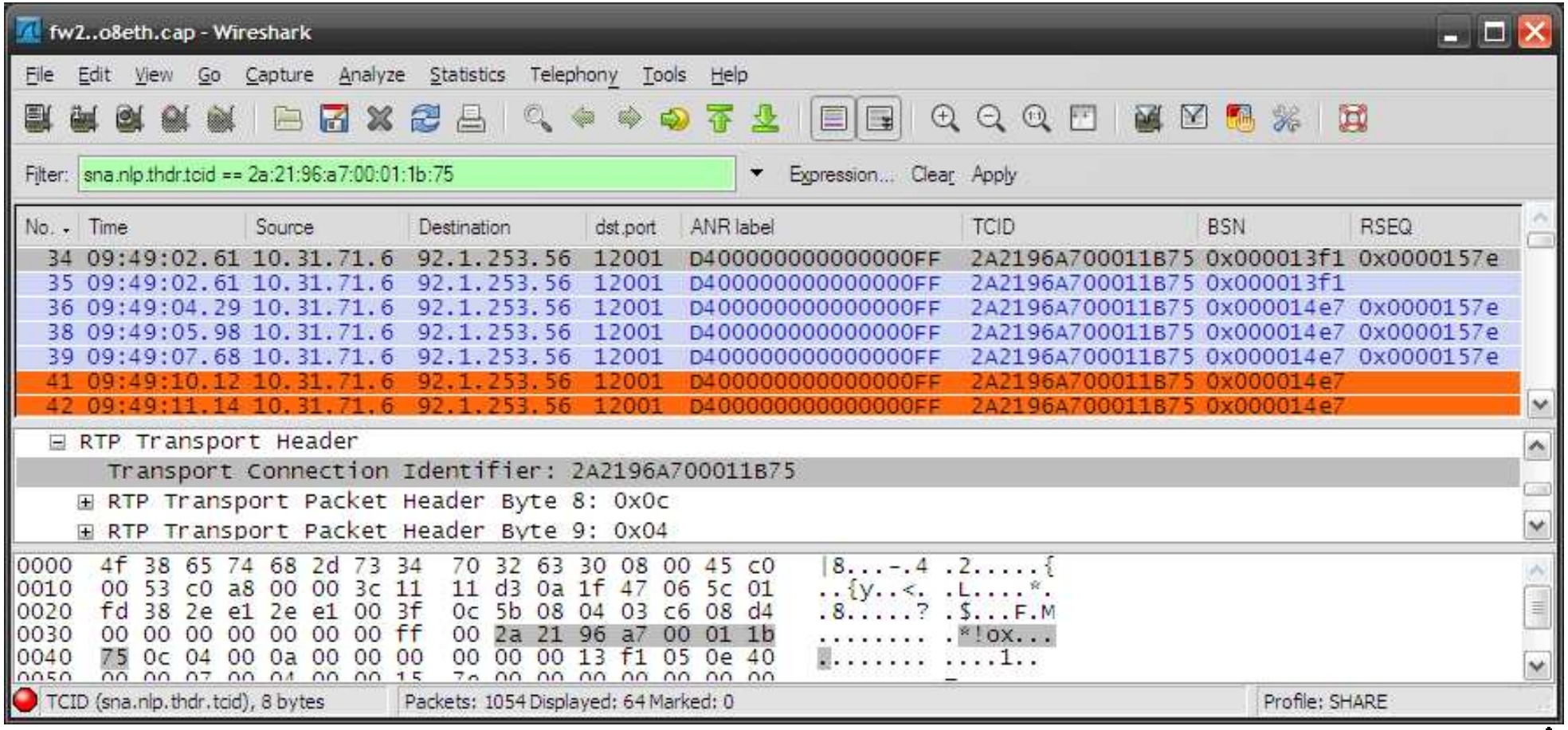
fw2.cap – saving filtered packets

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



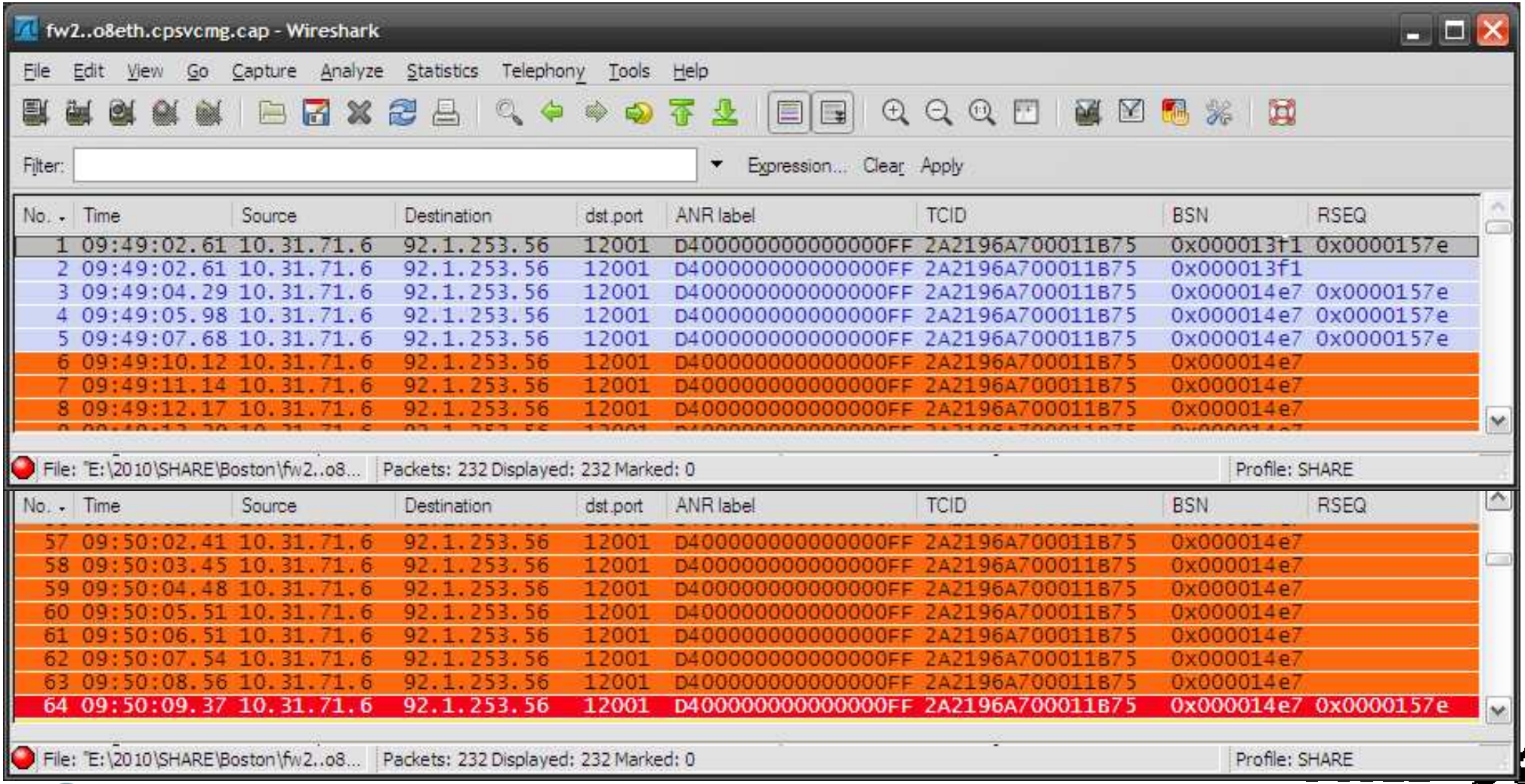
fw2.cap – TCID filter
CPSVCMG PATHSWITCH

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



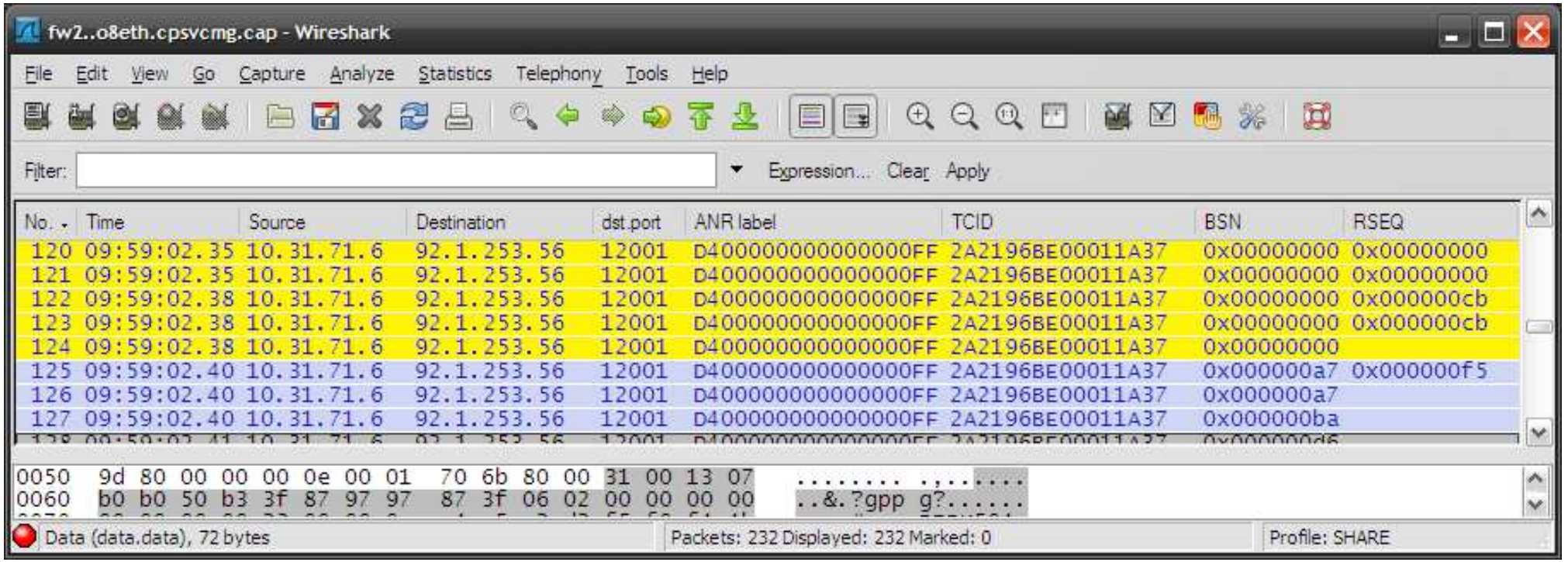
fw2.o8eth.cpsvcmg.cap PATHSWITCH,CFAULT

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



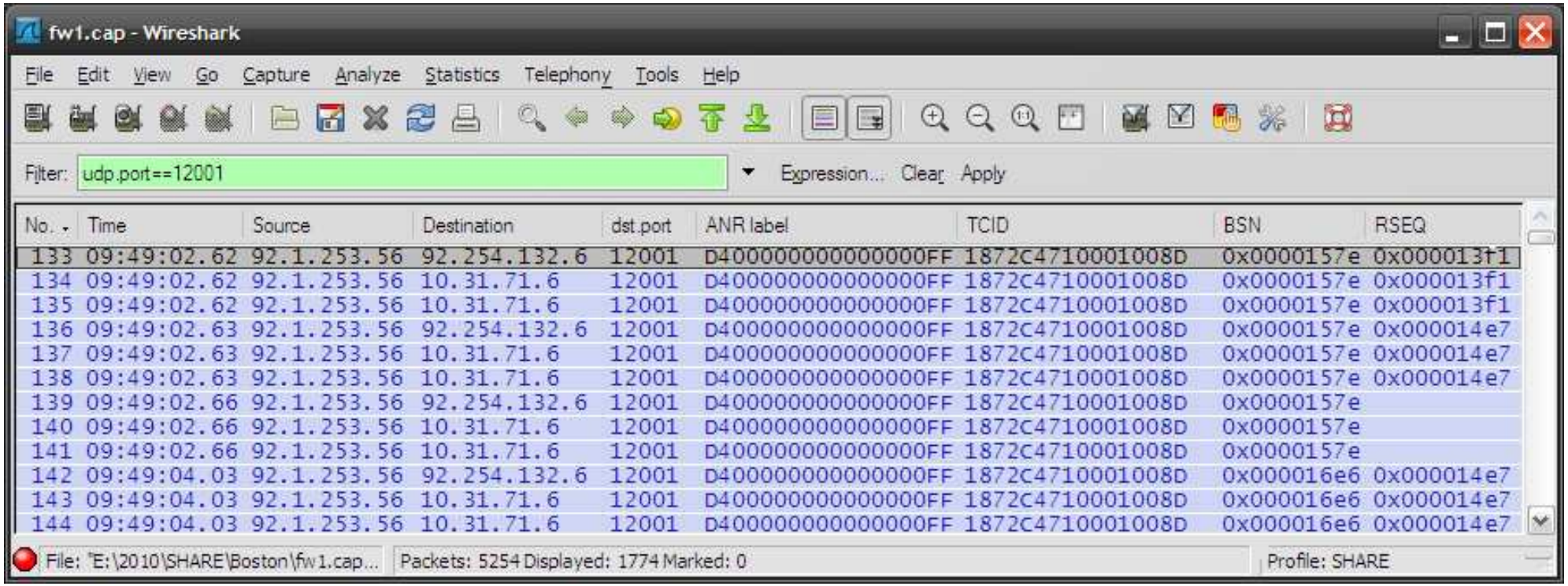
fw2.o8eth.cap
SETUP CPSVCMG

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



fw1.cap
UDP 12001

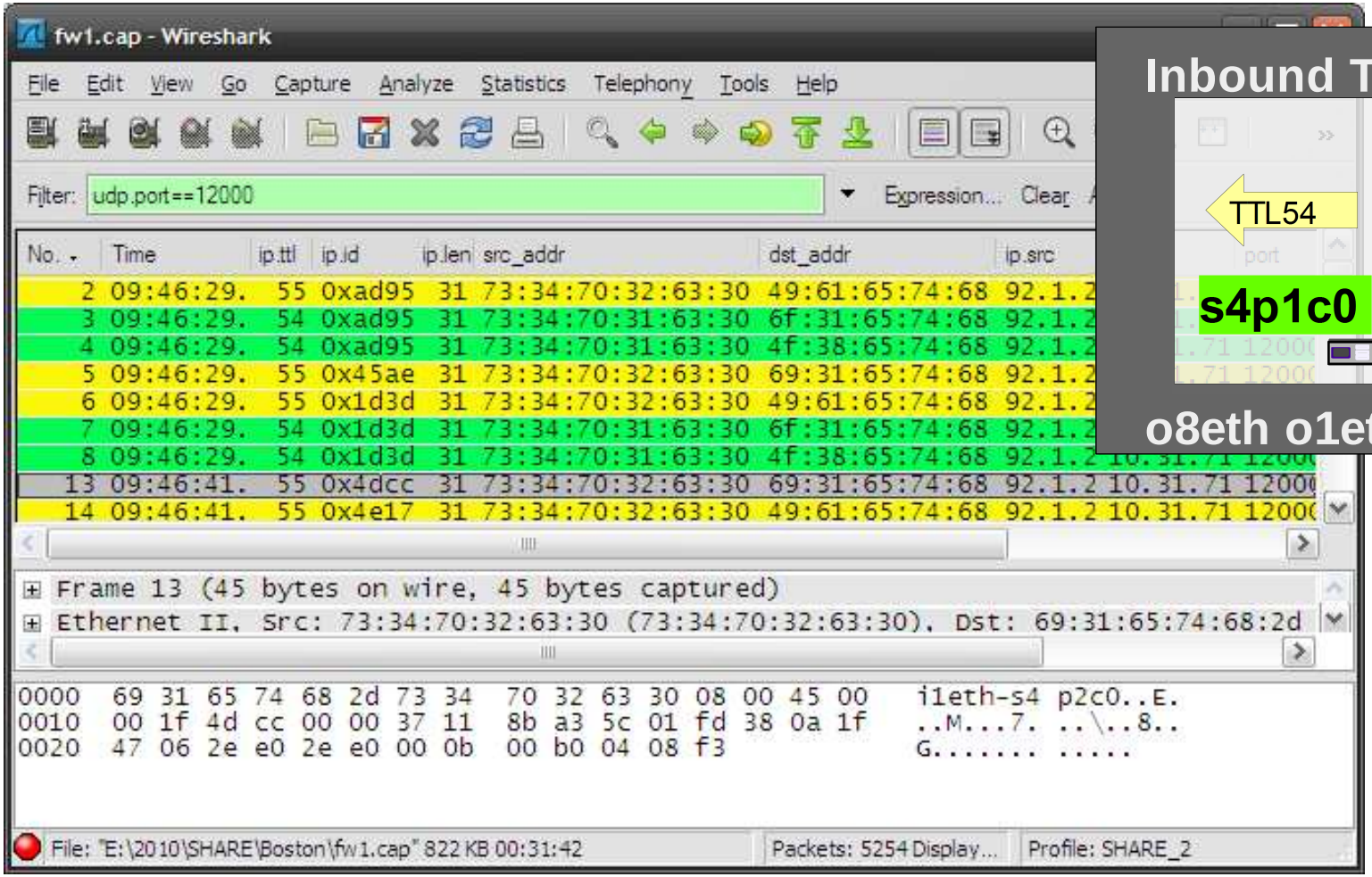
Existing CPSVCMG pipe with incrementing BSN and RSEQ
Every packet is traced 3 times
Destination IP address changes between packet1 and packet 2



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	D4000000000000000FF	1872C4710001008D	0x0000157e	0x000013f1
134	09:49:02.62	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	0x000013f1
135	09:49:02.62	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	0x000013f1
136	09:49:02.63	92.1.253.56	92.254.132.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	0x000014e7
137	09:49:02.63	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	0x000014e7
138	09:49:02.63	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	0x000014e7
139	09:49:02.66	92.1.253.56	92.254.132.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	
140	09:49:02.66	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	
141	09:49:02.66	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x0000157e	
142	09:49:04.03	92.1.253.56	92.254.132.6	12001	D4000000000000000FF	1872C4710001008D	0x000016e6	0x000014e7
143	09:49:04.03	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x000016e6	0x000014e7
144	09:49:04.03	92.1.253.56	10.31.71.6	12001	D4000000000000000FF	1872C4710001008D	0x000016e6	0x000014e7

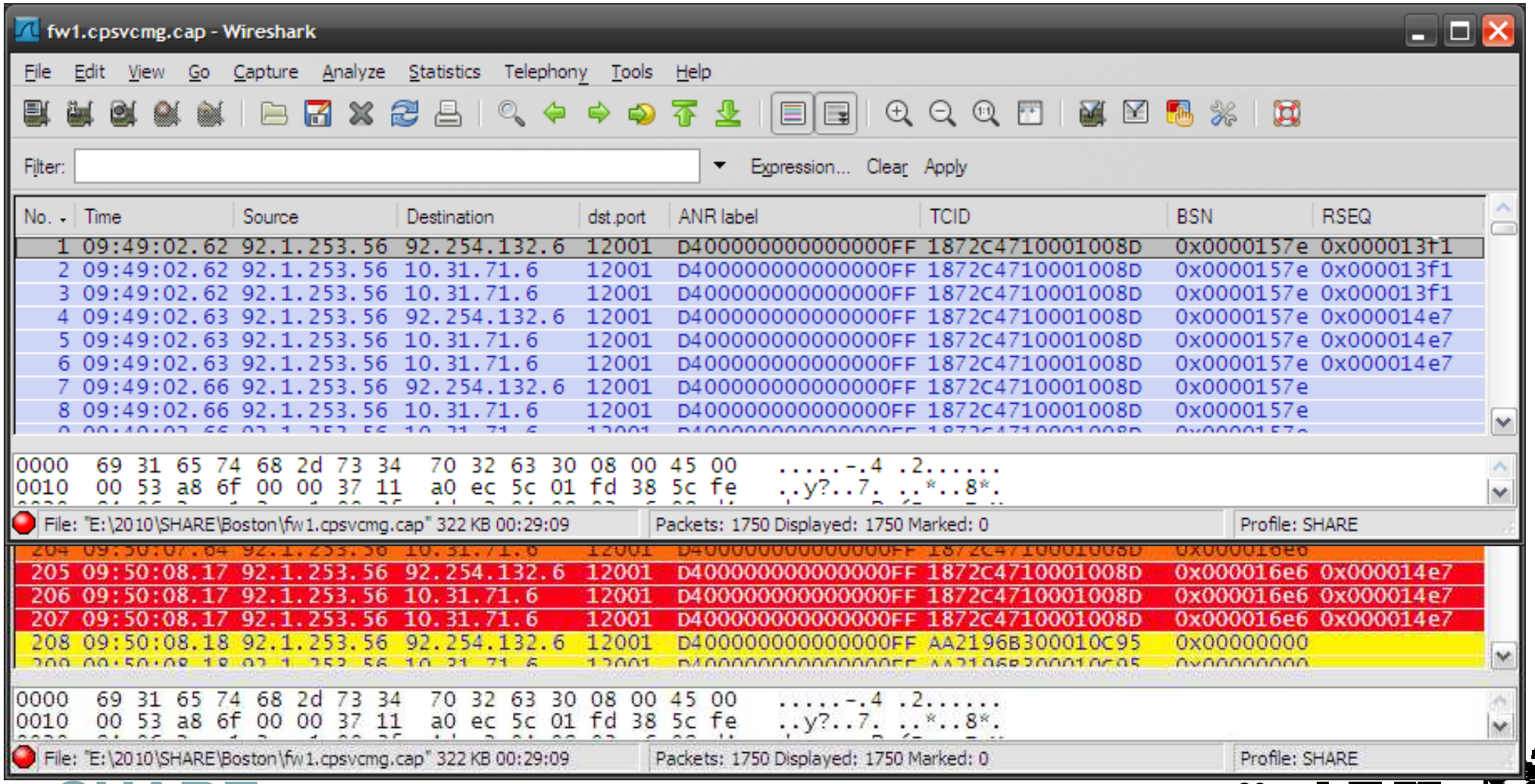
fw1.cap
UDP 12000

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



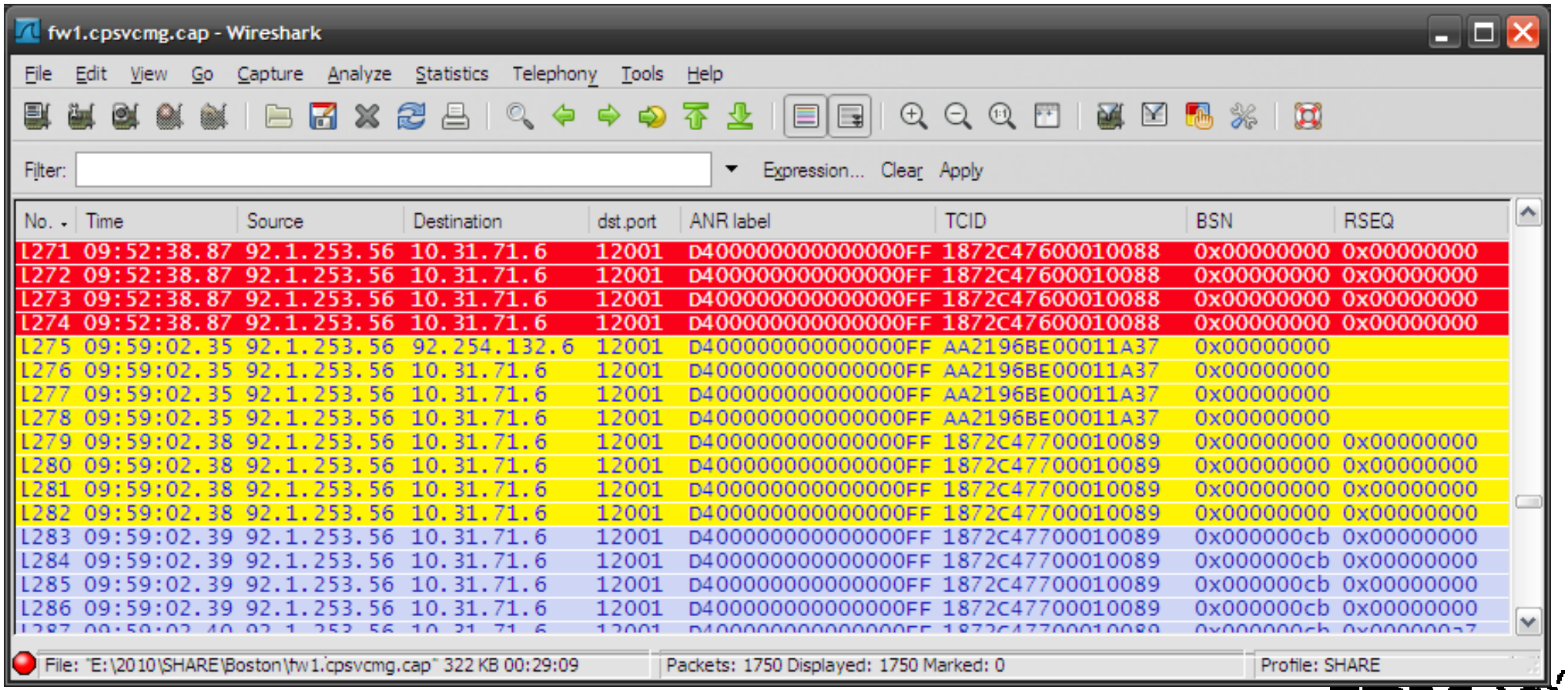
fw1.cpsvcmg.cap

Existing CPSVCMG pathswitching and failing



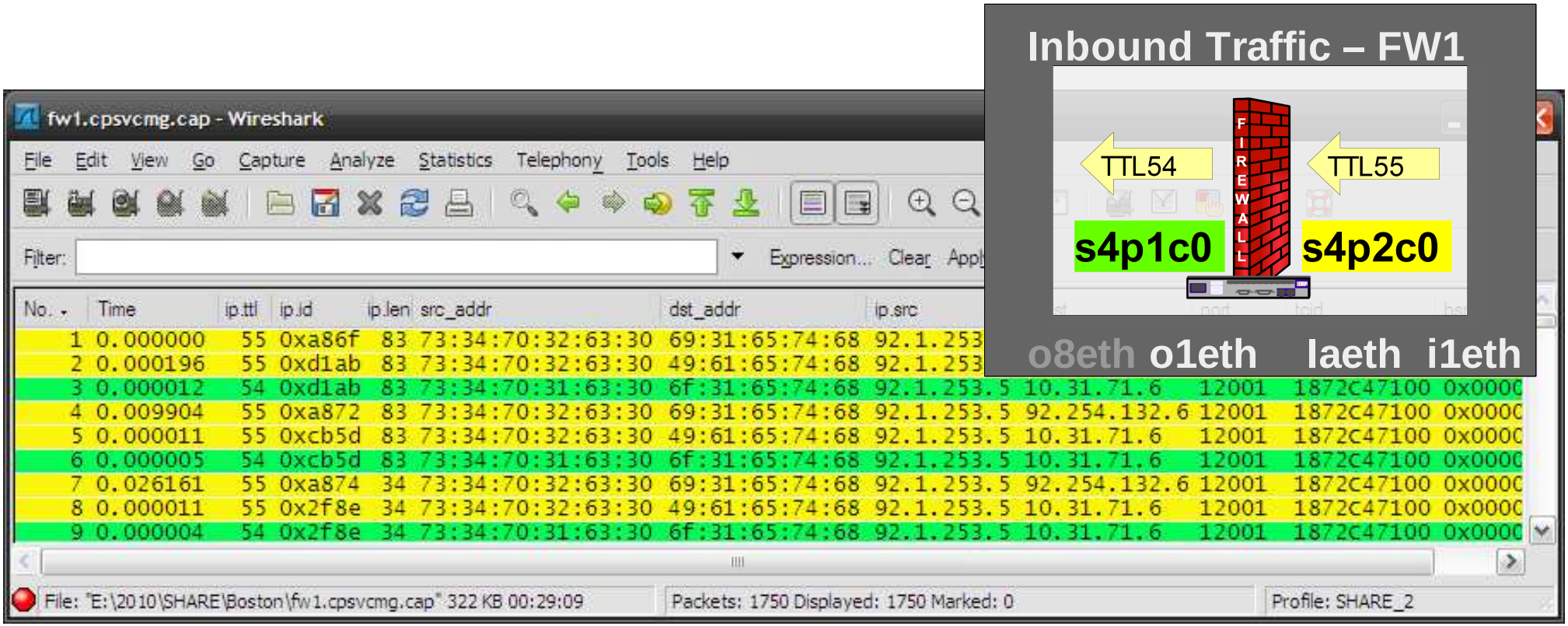
fw1.cpsvcmg.cap

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



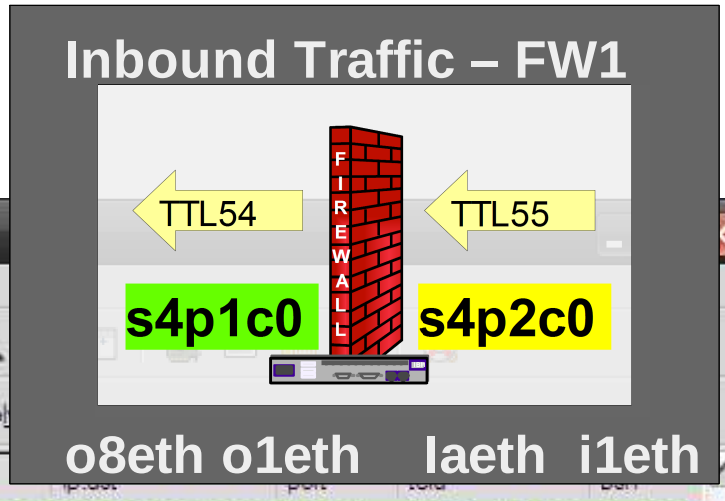
fw1.cpsvcmg.cap

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



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

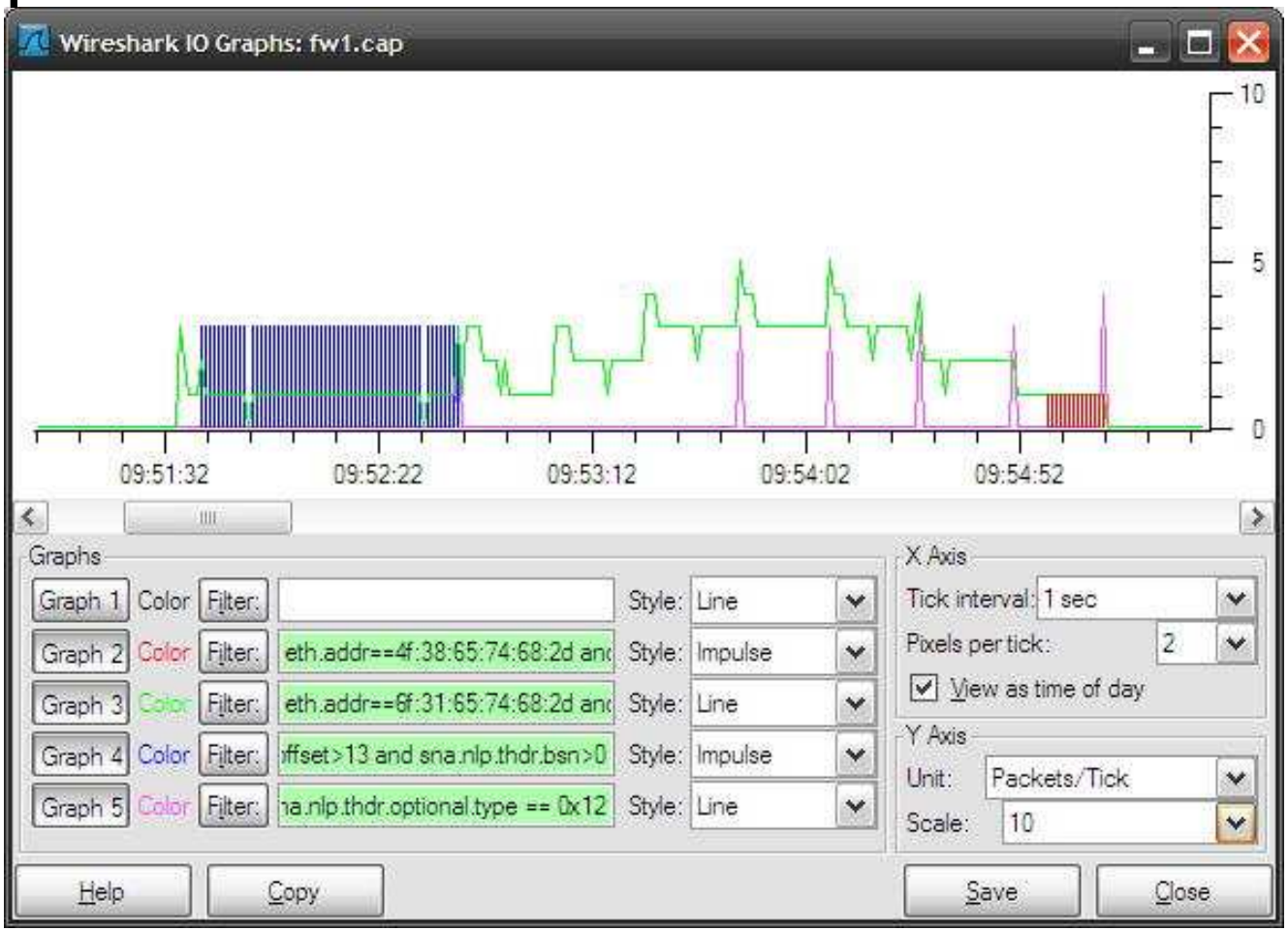
Filter: Expression... Clear Appl

No.	Time	ip.ttl	ip.id	ip.len	src_addr	dst_addr	ip.src				
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

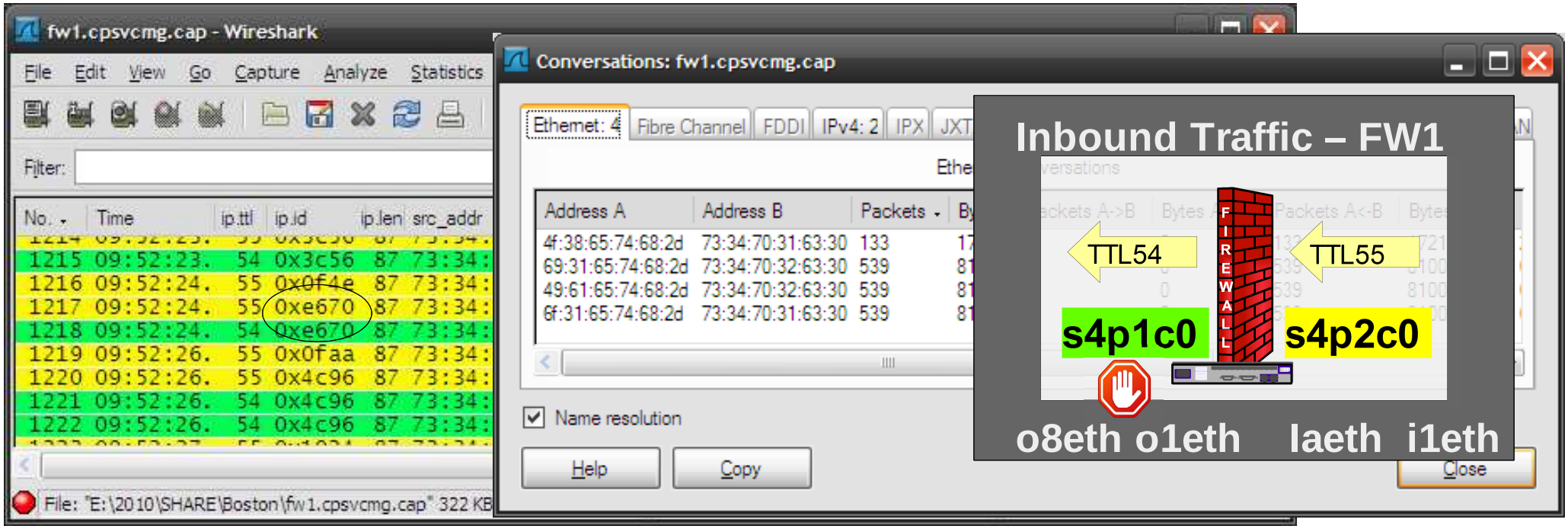
File: "E:\2010\SHARE\Boston\fw1.cpsvcmg.cap" 322 KB 00:29:09 | Packets: 1750 Displayed: 1750 Marked: 0 | Profile: SHARE_2

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



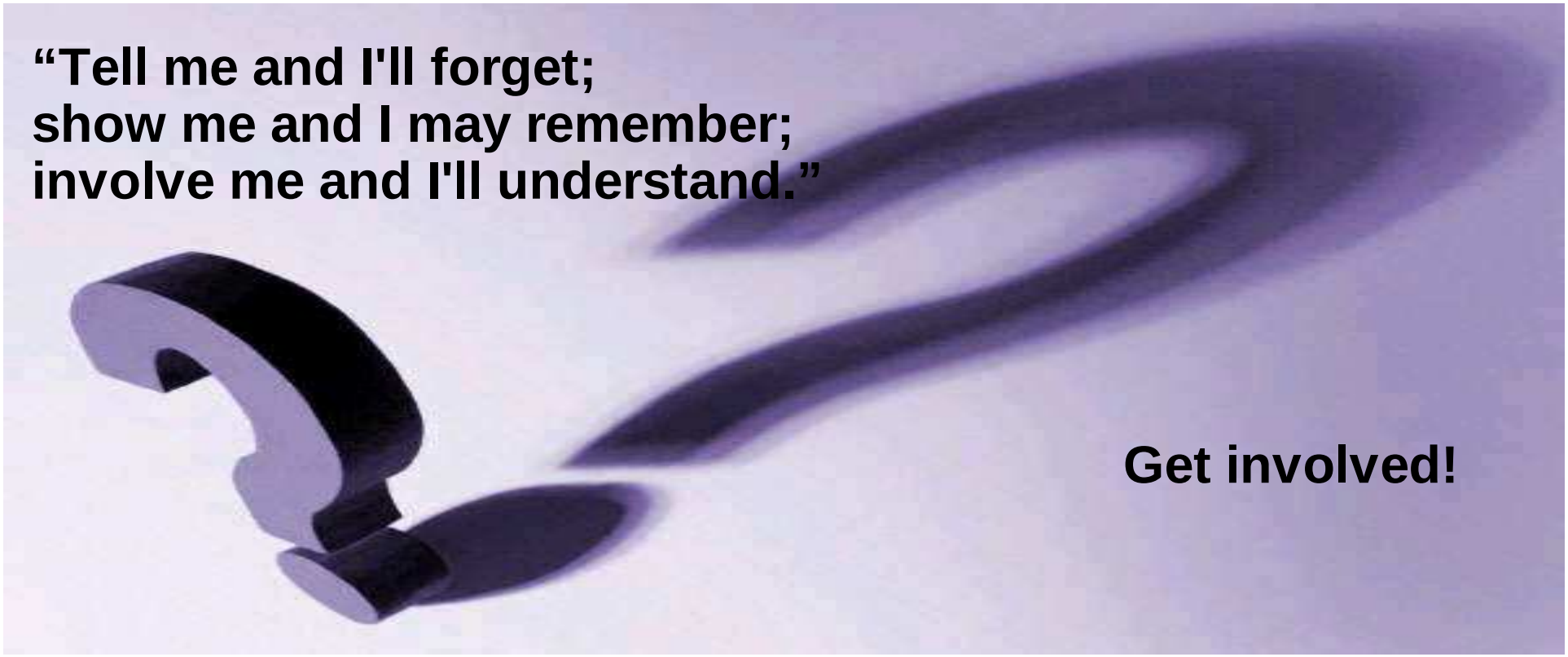
fw1.cpsvcmg.cap
Wireshark Statistics: conversations



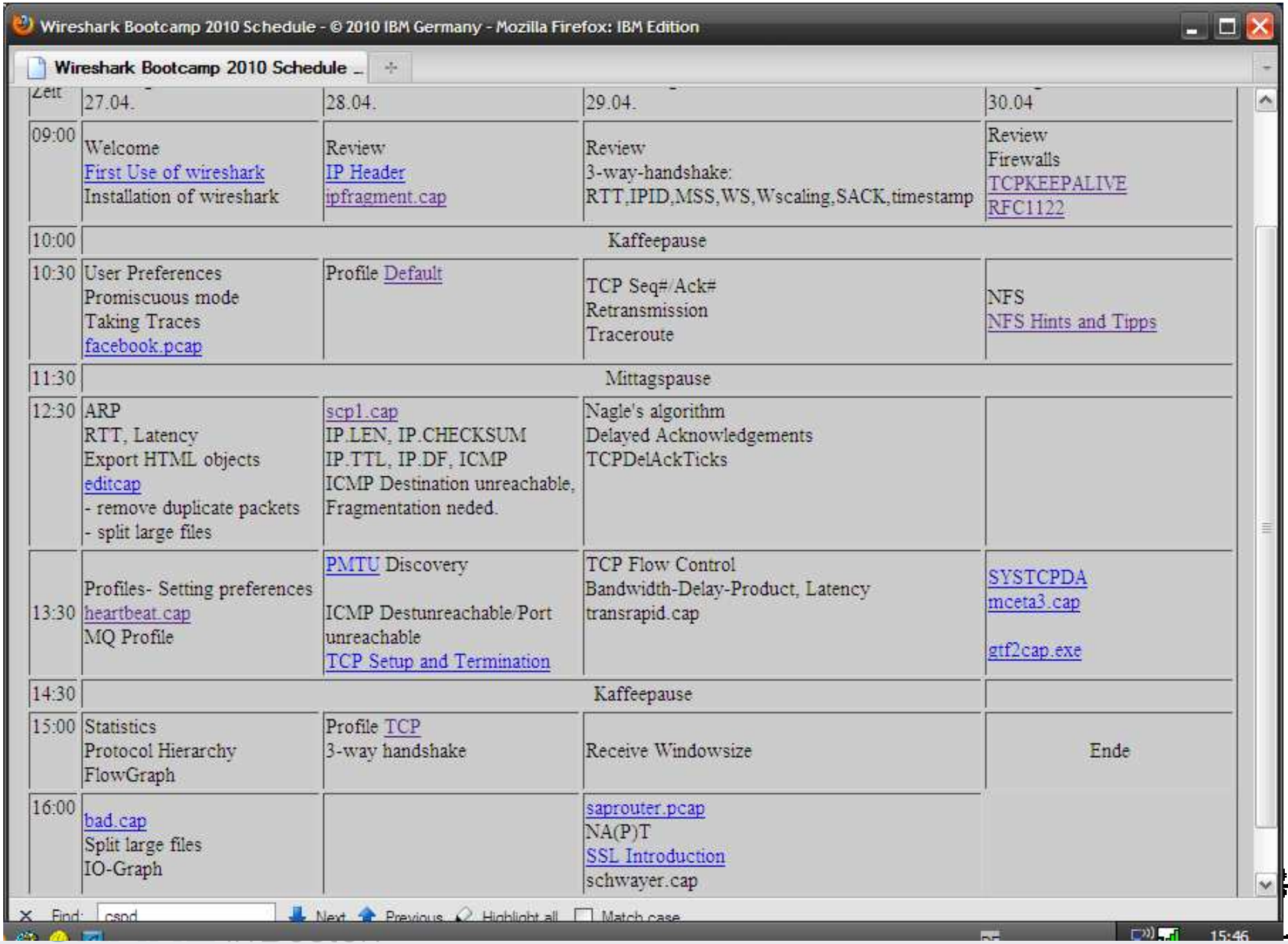
- The inbound firewall is dropping 12001 packets on its last leg (s4p1c0) towards the datacenter.
- IPID E670 was not sent out of the firewall
  - After IPID 4C96 was sent succesfully, the problem went away

Questions

- Need more? Come to Wireshark Bootcamp 2010



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



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	scp1.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 Windowsize	Ende
16:00	bad.cap Split large files IO-Graph		saprouter.pcap NA(P)T SSL Introduction schwayer.cap	