

# Taming the (wire)Shark wireshark Hands on Lab



Matthias Burkhard  
mburkhar@de.ibm.com  
IBM Germany



: mreede

Twitter

August 8. 2012 4:30 PM – 5:30 PM  
11342 Orange County Salon 2/3



IP Wizards

ip.wizards@groups.facebook.com

# Session Contents

## Taming the (wire)Shark – Hands on Lab

Learn how to configure the wireshark trace tool to better suit your needs

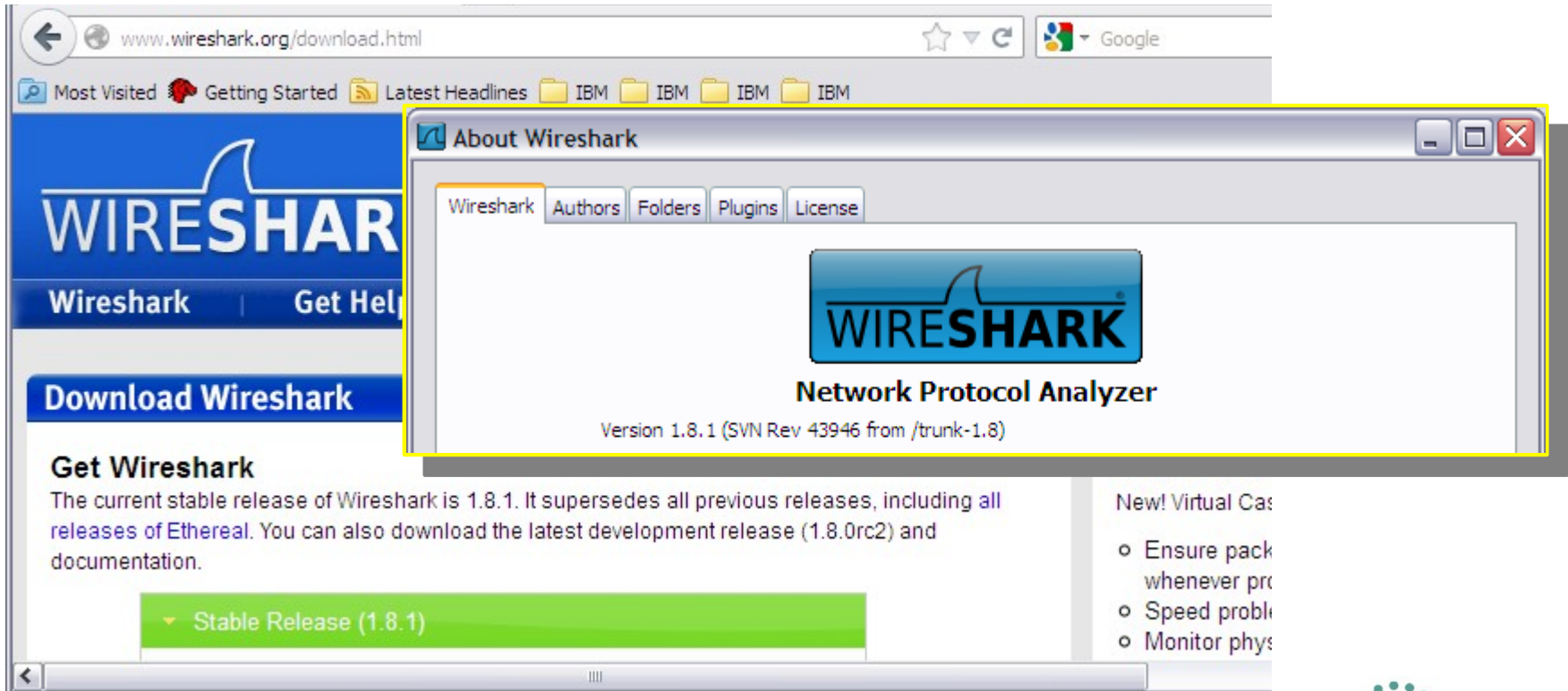
Change the Default Profile

Create a profile for CICS Transaction Gateway Protocol problems

# Download wireshark

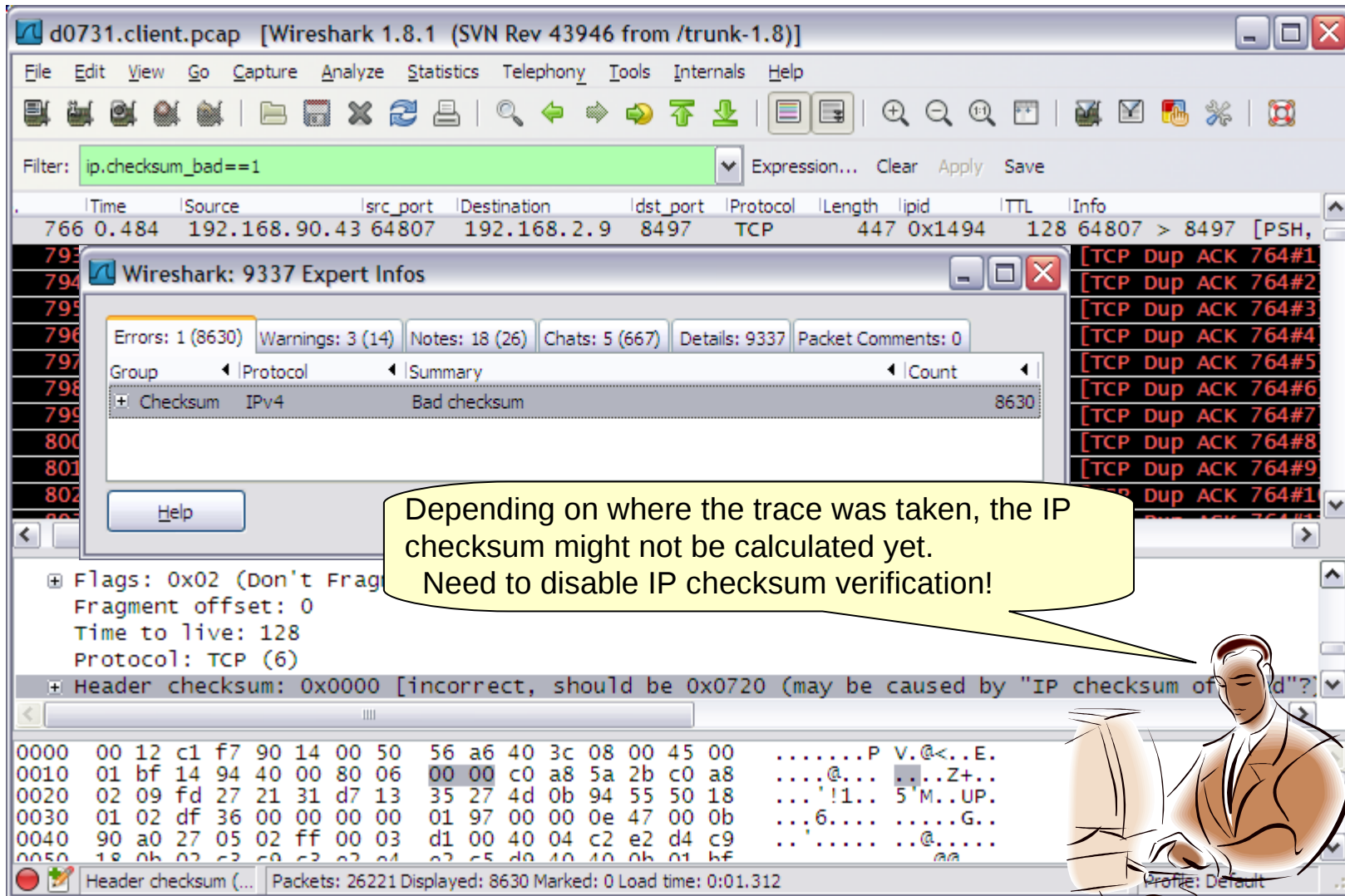
<http://www.wireshark.org/>

Wireshark is constantly improved and updated so check out the website regularly  
As of August 2012, the latest stable release is 1.8.1  
Help → About Wireshark will tell you what's installed.



The screenshot shows a web browser window at [www.wireshark.org/download.html](http://www.wireshark.org/download.html). The page features the Wireshark logo and a prominent blue button labeled "Download Wireshark". Below this, a section titled "Get Wireshark" states: "The current stable release of Wireshark is 1.8.1. It supersedes all previous releases, including all releases of Ethereal. You can also download the latest development release (1.8.0rc2) and documentation." A green button labeled "Stable Release (1.8.1)" is visible. An "About Wireshark" dialog box is overlaid on the page, showing the Wireshark logo and the text "Network Protocol Analyzer" and "Version 1.8.1 (SVN Rev 43946 from /trunk-1.8)". The dialog box has tabs for "Wireshark", "Authors", "Folders", "Plugins", and "License".

# Default Configuration: Not to everyone's taste



Wireshark: 9337 Expert Infos

Errors: 1 (8630) Warnings: 3 (14) Notes: 18 (26) Chats: 5 (667) Details: 9337 Packet Comments: 0

Group	Protocol	Summary	Count
+	Checksum	IPv4 Bad checksum	8630

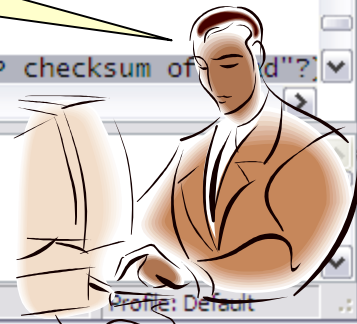
Help

Flags: 0x02 (Don't Fragment)  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (6)

Header checksum: 0x0000 [incorrect, should be 0x0720 (may be caused by "IP checksum of ...")]

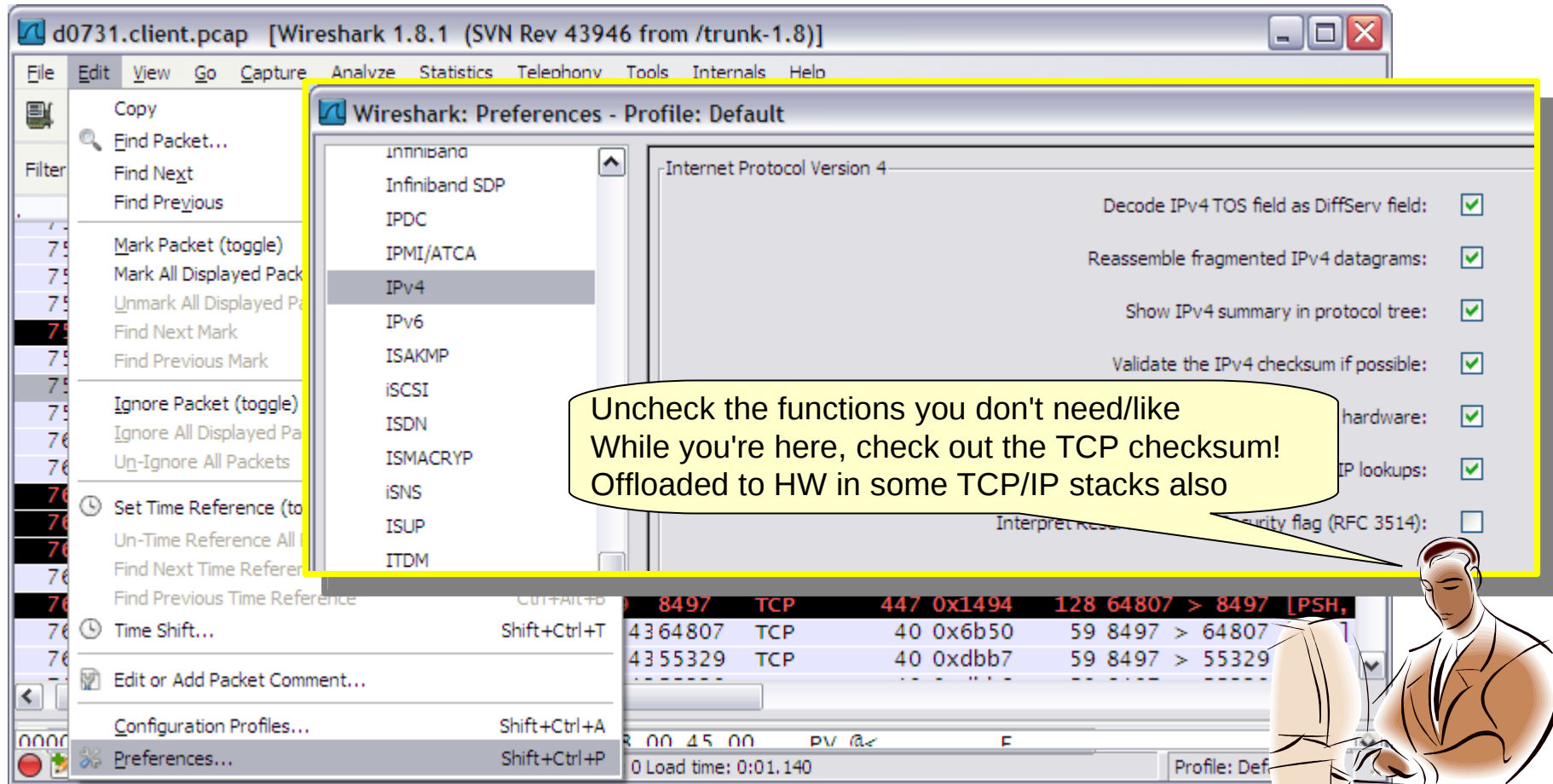
0000 00 12 c1 f7 90 14 00 50 56 a6 40 3c 08 00 45 00 .....P V.@<...E.  
 0010 01 bf 14 94 40 00 80 06 00 00 c0 a8 5a 2b c0 a8 .....@... ..Z+..  
 0020 02 09 fd 27 21 31 d7 13 35 27 4d 0b 94 55 50 18 ...!1.. 5'M..UP.  
 0030 01 02 df 36 00 00 00 00 01 97 00 00 0e 47 00 0b ...6.....G..  
 0040 90 a0 27 05 02 ff 00 03 d1 00 40 04 c2 e2 d4 c9 .....@...@..  
 0050 18 0b 02 c2 c0 c2 c2 c4 c2 c5 d0 40 40 0b 01 bf .....@..@..

Header checksum (... Packets: 26221 Displayed: 8630 Marked: 0 Load time: 0:01.312



# Default Configuration: Edit - Preferences

Change the configuration for IPV4 and TCP traffic



**Wireshark: Preferences - Profile: Default**

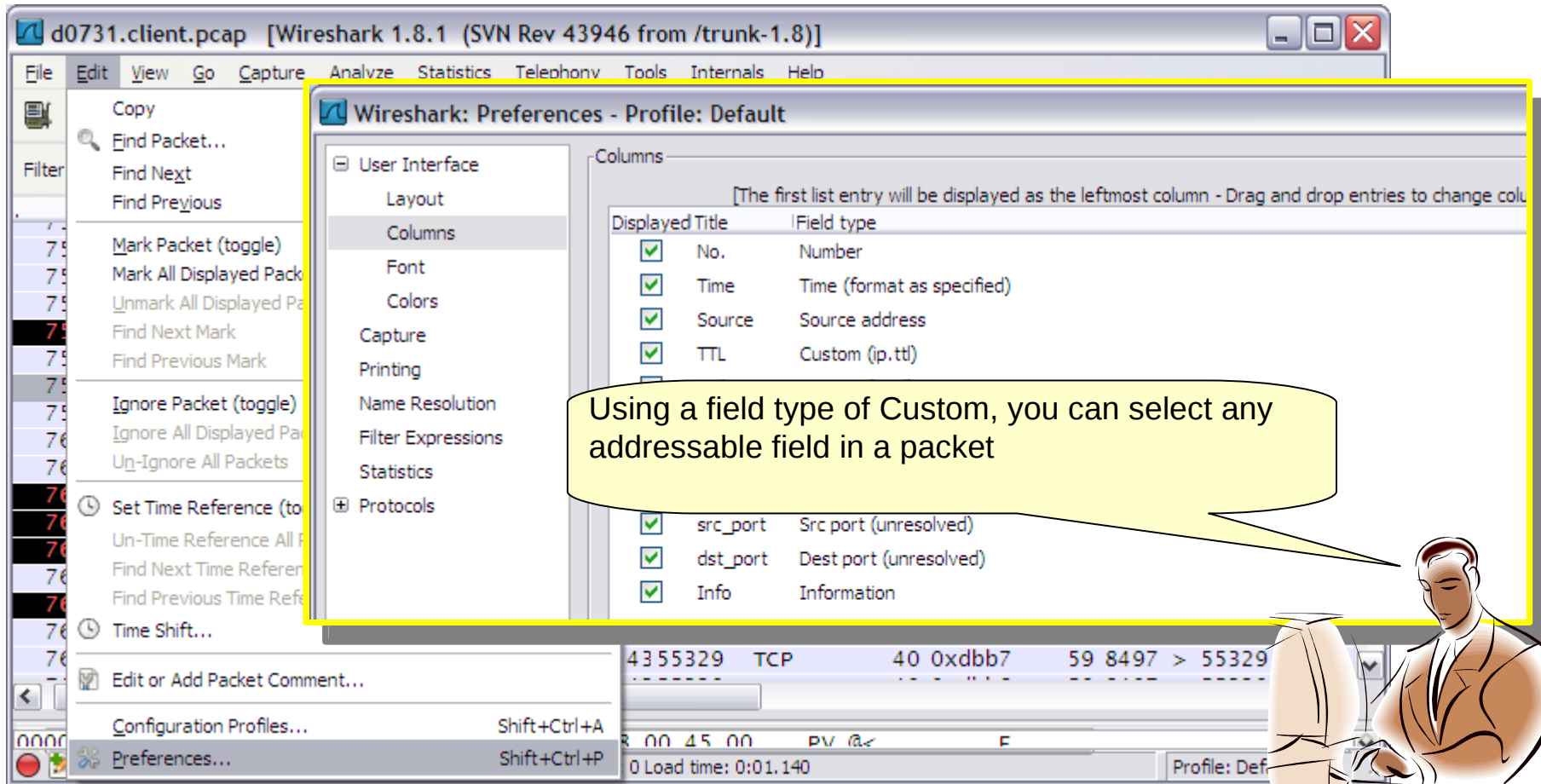
- Decode IPv4 TOS field as DiffServ field:
- Reassemble fragmented IPv4 datagrams:
- Show IPv4 summary in protocol tree:
- Validate the IPv4 checksum if possible:

Uncheck the functions you don't need/like  
While you're here, check out the TCP checksum!  
Offloaded to HW in some TCP/IP stacks also

No.	Time	Source	Destination	Protocol	Length	Info
75	0.000000	192.168.1.100	192.168.1.1	TCP	60	8497 → 8497 [PSH, Seq=4364807, Win=0, Len=0]
76	0.000000	192.168.1.1	192.168.1.100	TCP	60	8497 → 8497 [ACK, Seq=4364807, Win=0, Len=0]
77	0.000000	192.168.1.100	192.168.1.1	TCP	60	55329 → 55329 [PSH, Seq=4355329, Win=0, Len=0]
78	0.000000	192.168.1.1	192.168.1.100	TCP	60	55329 → 55329 [ACK, Seq=4355329, Win=0, Len=0]

# Default Configuration: Edit - Preferences

Add additional columns to the packet list window



The screenshot shows the Wireshark interface with the 'Preferences - Profile: Default' dialog box open. The 'Columns' section is selected in the left sidebar. The 'Columns' table is as follows:

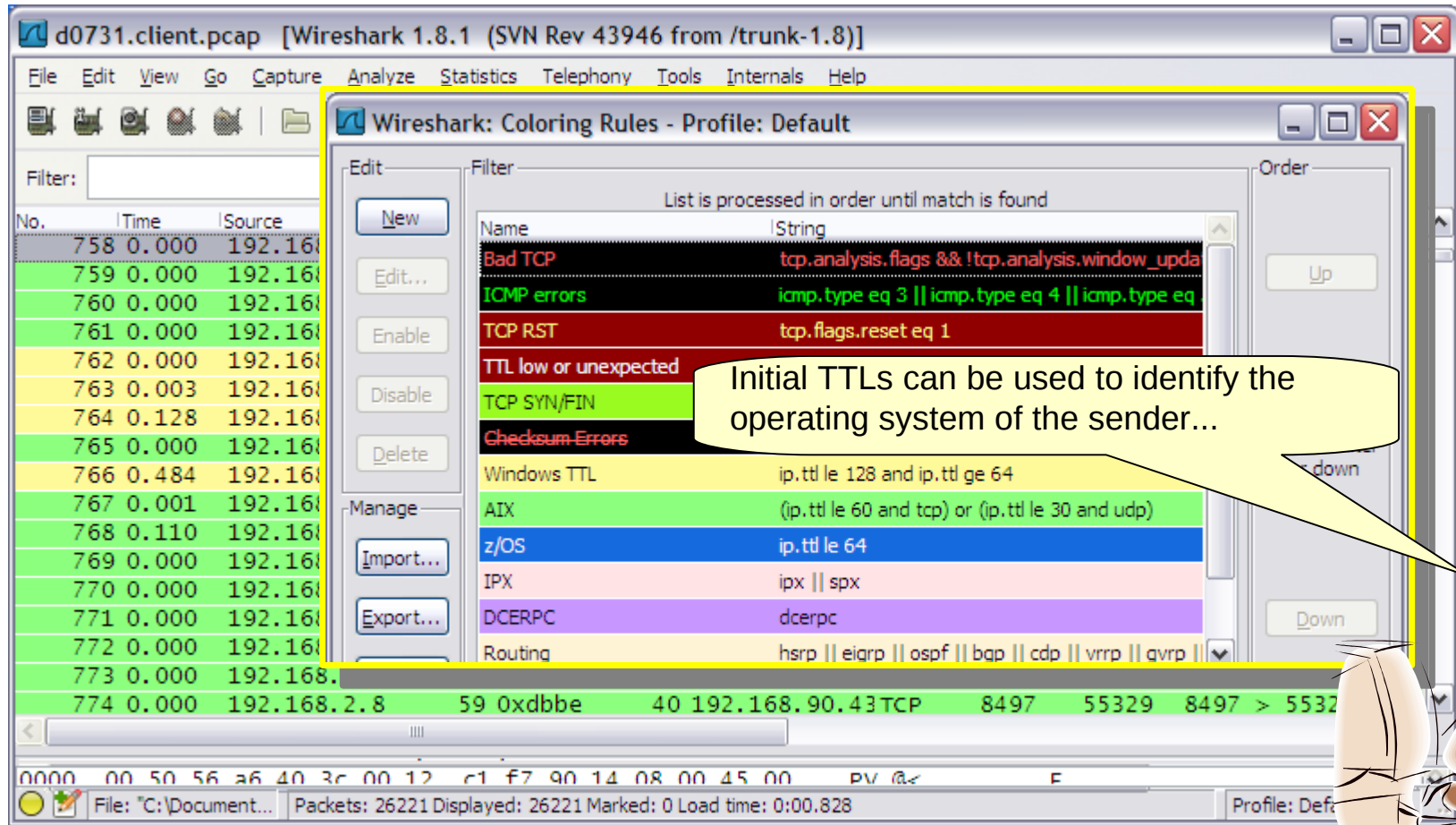
Displayed Title	Field type
<input checked="" type="checkbox"/> No.	Number
<input checked="" type="checkbox"/> Time	Time (format as specified)
<input checked="" type="checkbox"/> Source	Source address
<input checked="" type="checkbox"/> TTL	Custom (ip.ttl)
<input checked="" type="checkbox"/> src_port	Src port (unresolved)
<input checked="" type="checkbox"/> dst_port	Dest port (unresolved)
<input checked="" type="checkbox"/> Info	Information

A yellow callout box contains the text: "Using a field type of Custom, you can select any addressable field in a packet".



# Default Configuration: Coloring Rules

Assign different colors based on direction of traffic



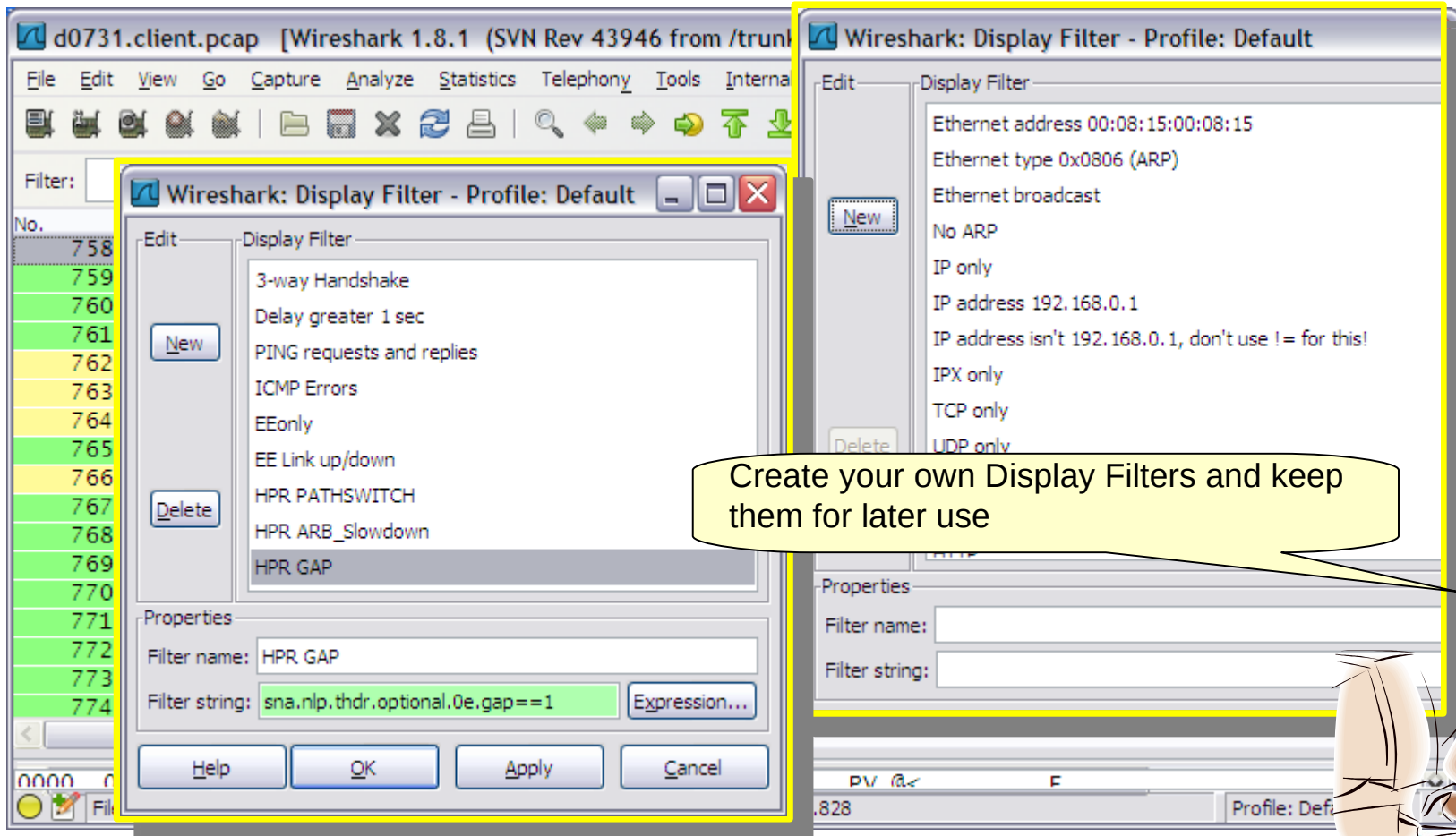
Initial TTLs can be used to identify the operating system of the sender...

Name	String
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_upda
ICMP errors	icmp.type eq 3    icmp.type eq 4    icmp.type eq
TCP RST	tcp.flags.reset eq 1
TTL low or unexpected	
TCP SYN/FIN	
Checksum Errors	
Windows TTL	ip.ttl le 128 and ip.ttl ge 64
AIX	(ip.ttl le 60 and tcp) or (ip.ttl le 30 and udp)
z/OS	ip.ttl le 64
IPX	ipx    spx
DCERPC	dcerpc
Routing	hsrp    eigrp    ospf    bgp    cdp    vrrp    qvrrp



# Default Configuration: Display Filters

## Change the pre-defined Display Filters



Wireshark: Display Filter - Profile: Default

Display Filter

- 3-way Handshake
- Delay greater 1 sec
- PING requests and replies
- ICMP Errors
- EEonly
- EE Link up/down
- HPR PATHSWITCH
- HPR ARB\_Slowdown
- HPR GAP

Properties

Filter name: HPR GAP

Filter string: `sna.nlp.thdr.optional.0e.gap==1` Expression...

Buttons: Help, OK, Apply, Cancel

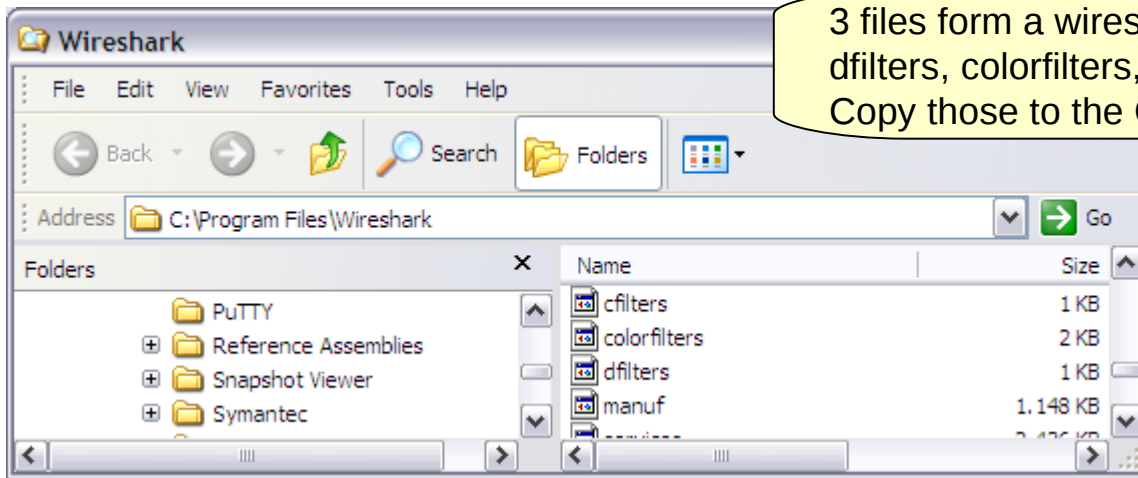
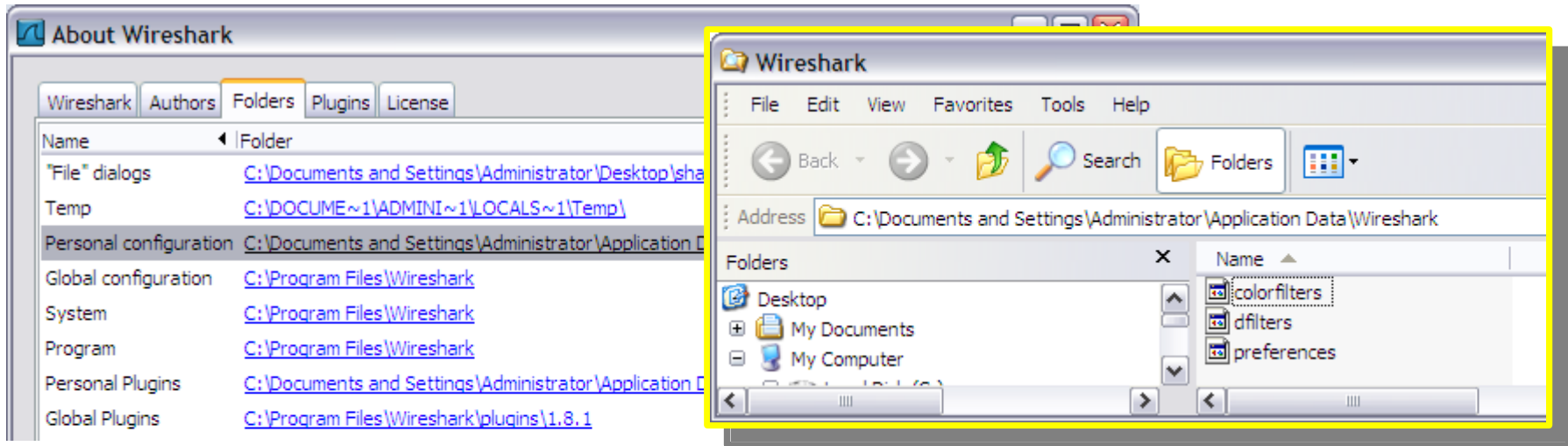
Callout: Create your own Display Filters and keep them for later use





# Default Configuration: Where is it kept?

Help → About Wireshark → Folders



3 files form a wireshark 'Profile'  
dfilters, colorfilters, preferences  
Copy those to the Global configuration



# New Profile: Create a Profile for ctg problems

Configuration for CICS Transaction Gateway problems

Some Background on CICS Transaction Gateway flows

- CTG was using SNA LU6.2 (APPC) protocol originally
- Native TCP Socket support came later
- Inside the TCP segment there are still LU6.2 structures to be found
  - SNA Sequence Numbers
  - SNA RH (Request Response Headers)
  - SNA FMH5 (0x0502FF) to start (ATTACH) a Transaction Program
  - SNA GDS Variables (0x12FF,0x12F2)
  - SNA FMH7 to report SNA Sense Codes

# Background: CICS Transaction Gateway

## 'SNA LU62' protocol within TCP

```

----- 2cIP - TRACE ANALYSIS PANEL -----
Command ==>
MAC Eth II IP_V4 TCP CTG RH_REQ FM FMH_05 LU62 GD_12F2
NA 192.168.2.8(8497) <- 192.168.90.43(55329) CTG AP ReQ FMH-5 ATTACH(BSMI) UCD RU()FMD
--RECORD 4(FILTERED) Len 498 Time 2012/07/31-15:22:57.885933 Capt SNIFFER
-----
MAC Eth II      MAC Ethernet II
0000 0012C1F7 90140050 56A6403C 0800      EBC:<  A7  & w      > ASC:<      PV @<      >
IP_V4          IP_V4 Header
0000 450001BC 14CD4000 80060000 C0A85A2B      EBC:<      {y!      > ASC:< E      @      Z+      >
0010 C0A80208      EBC:< {y      > ASC:<      >
TCP          TCP Header
0000 D8212131 2F7527A5 6E7693C0 501800FD      EBC:< Q.. . .v> l{&      > ASC:< !!1/u' nv P      >
0010 DF320000      EBC:< .      > ASC:< 2      >
CTG          CTG CICS Transaction Gateway
0000 00000194 00000E49 00      EBC:< m      > ASC:<      I      >
RH_REQ        Request Header
0000 0B90A0      EBC:<      > ASC:<      >
FM FMH_05 LU62  FM Header 5: Attach (LU 6.2)
0000 270502FF 0003D100 4004C2E2 D4C9180B      EBC:< .      J BSMI      > ASC:< '      @      >
0010 02C3C9C3 E2E4E2C5 D940400B 01BF0000      EBC:< CICSUSER      > ASC:<      @@      >
0020 00000000 000000      EBC:<      > ASC:<      >
GD_12F2      User Control Data (X'12F2') GDS Variable
0000 016112F2 0A850202 01020000 01040E43      EBC:< / 2 e      > ASC:< a      C      >
0010 0E020000 07E10000 00800100 000A02E4      EBC:<      U      > ASC:<      >
0020 E7C7E4C9 C3E30007 08C2E2D4 C9000504      EBC:< XGUICT BSMI      > ASC:<      >
0030 012C012F 06303030 38534553 53494F4E      EBC:< .      .      |+      > ASC:< , / 0008SESSION      >
0040 20202020 20202020 20202020 20202020      EBC:< .....      > ASC:<      >
0050 20202020 20202050 494E4720 20202020      EBC:< .....& + .....      > ASC:<      PING      >
0060 20202020 20202020 20202020 20202020      EBC:< .....      > ASC:<      >
0070 20202020 20474554 56414C55 45202020      EBC:< ..... < ...      > ASC:<      GETVALUE      >
0080 20202020 20202020 20202020 20202020      EBC:< .....      > ASC:<      >

```

2cIP <http://www.ansynova.com>

# AIX (CTG) closes the connection

Why? Who is at fault?

No. .	whazzin	Time	TTL	ip.id	Source	tcp_len	tcp.seq	data
131	ctg_big_data	0.00220	59	0xdc51	192.168.2.8	1300	1853275232	38303738303835202020304452422B5347454C30303
132	tcp_delay_ack	0.20219	128	0x151e	192.168.90.4	0	796208225	
133	ctg_big_data	0.00071	59	0xdc5e	192.168.2.8	1300	1853276532	2030303130303330303630313530323130323230323
134	tcp_delay_ack	0.20042	128	0x1523	192.168.90.4	0	796208225	
135	ctg_big_data	0.00144	59	0xdc72	192.168.2.8	1300	1853277832	20A7393920A73633204444A73035534C53534C53534
136	ctg_heartbeat	0.17204	128	0x1526	192.168.90.4	404	796208225	0000019400000E50000B90A0270502FF0003D100400
137	ctg_big_data	0.00098	59	0xdcc2	192.168.2.8	1300	1853279132	30303434333430323847454C46454747454C3030383
138	ctg_heartbeat	0.00779	59	0xdccc	192.168.2.8	1300	1853284368	0000014600000E4900039001013A12F207430E02000
139	tcp_ack	0.00002	128	0x1527	192.168.90.4	0	796208629	
140	ctg_big_data	0.00076	59	0xdcd0	192.168.2.8	1300	1853280432	36303236303333303339303635A7323720304452422
141	tcp_ack	0.00003	128	0x1528	192.168.90.4	0	796208629	
142	ctg_big_data	0.00076	59	0xdcd1	192.168.2.8	1300	1853281732	A7393920A73633204444A73035534C53534C53534B5
143	tcp_ack	0.00001	128	0x1529	192.168.90.4	0	796208629	
144	ctg_big_data	0.00108	59	0xdcd2	192.168.2.8	1300	1853283032	3830373830373830373830373830373830373830373830383
145	tcp_ack	0.00001	128	0x152a	192.168.90.4	0	796208629	
146	ctg_heartbeat	0.00097	59	0xdcd3	192.168.2.8	1300	1853284332	A73036304E312C3232373635A73035303631322C303
147	tcp_ack	0.00004	128	0x152b	192.168.90.4	0	796208629	
148	ctg_big_data	0.00080	59	0xdcd4	192.168.2.8	4	1853285668	2D2D2D23
149	FMH7	0.12260	128	0x1548	192.168.90.4	19	796208629	0000001300000E46000B900107070864000000
150	tcp_ack	0.00051	59	0xdcd5	192.168.2.8	0	1853285672	
151	FMH7	0.01838	128	0x154d	192.168.90.4	19	796208648	0000001300000E49000B900107070864000000
152	tcp_ack	0.00112	59	0xdcd6	192.168.2.8	0	1853285672	
153	FMH7	0.00005	59	0xdcd7	192.168.2.8	19	1853285672	0000001300000E46000B900107071008600B00
154	FIN	0.00000	59	0xdcd8	192.168.2.8	0	1853285691	
155	tcp_ack	0.00001	128	0x154e	192.168.90.4	0	796208667	
156	FMH7	0.01749	128	0x1556	192.168.90.4	19	796208667	0000001300000E4A000B900107070864000000
157	RST AIX	0.00104	59	0xdcdf	192.168.2.8	0	1853285692	

# Windows CICS Client ABENDs the transaction

... sends FMH7 with SNA sense 08640000

Filter: `data.data[6:2] eq 0e46` Expression... Clear Apply

No. .	whazzin	Time	TTL	ip.id	Source	tcp_len	tcp.seq	data
50	ctg_start_tx	0.55268	128	0x1490	192.168.90.4	821	796206192	0000033500000E46000B90A0270502FF0003D10
95	ctg_reply	0.59758	59	0xdbd3	192.168.2.8	1300	1853253132	00007A0400000E460003900179F812F207430E0
149	FMH7	3.86227	128	0x1548	192.168.90.4	19	796208629	0000001300000E46000B900107070864000000
153	FMH7	0.02007	59	0xdcd7	192.168.2.8	19	1853285672	0000001300000E46000B900107071008600B00

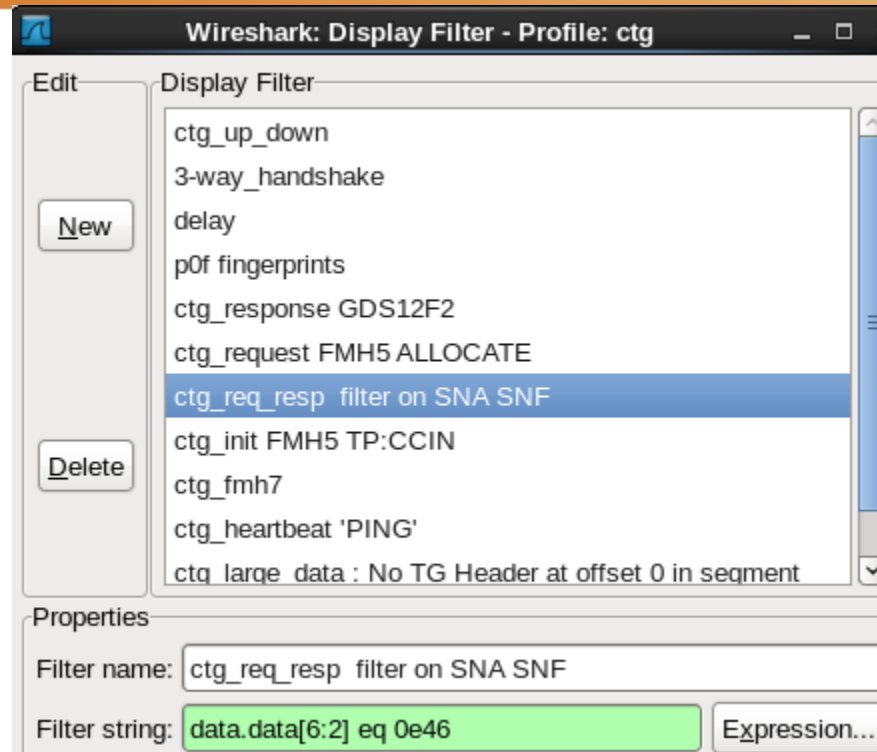
Frame 95 (1354 bytes on wire, 1354 bytes captured)  
 Ethernet II, Src: CheckPoi\_f7:90:14 (00:12:c1:f7:90:14), Dst: Vmware\_a6:40:3c (00:50:56:a6:40:3c)  
 Internet Protocol, Src: 192.168.2.8 (192.168.2.8), Dst: 192.168.90.43 (192.168.90.43)  
 Transmission Control Protocol, Src Port: 8497 (8497), Dst Port: 55329 (55329), Seq: 1853253132, Ack: 796207013  
 Data (1300 bytes)  
 Data: 00007A0400000E460003900179F812F207430E0200000079...  
 [Length: 1300]

```

0030  80 39 7f 05 00 00 00 00 7a 04 00 00 0e 46 00 03  .9.... z....F..
0040  90 01 79 f8 12 f2 07 43 0e 02 00 00 00 79 ed 06  ..y....C .....y..
0050  30 30 30 31 50 4f 53 20 20 20 20 20 20 20 20  0001POS
0060  20 20 20 4c 45 53 45 4e 20 20 20 20 20 20 20  LESEN
0070  20 20 47 45 54 2d 44 45 41 4c 44 41 54 41 20  GET-DE ALDATA
0080  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0090  47 45 54 4e 45 58 54 20 20 20 20 20 20 20 20  GETNEXT
00a0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 31  10
  
```

Data (data.data), 1300 by... Packets: 157 Displayed: 4 Marked: 0 Profile: ctg

# ctg profile dfilters



```
"ctg_up_down" tcp.flags.syn==1 or tcp.flags.fin==1 or tcp.flags.reset==1 or data.data contains 0b:9001:0707 or (data.data[13:3] eq 05:02:ff and data.data[22:4] eq c3c3:c9d5 ) or data.data[12:4] eq 0034:12ff
"3-way_handshake" tcp.flags.syn==1 or (tcp.ack==1 and tcp.seq==1 and tcp.len==0 and !tcp.analysis.window_update)
"delay" frame.time_delta gt 0.02
"p0f fingerprints" tcp.flags.syn==1 or tcp.flags.reset==1
"ctg_response GDS12F2 " data.data contains 12f2 and !data.data contains 0502:ff
"ctg_request FMH5 ALLOCATE" data.data contains 0b:90:a0 and data.data contains 0502:ff
"ctg_req_resp filter on SNA SNF " data.data[6:2] eq 0e46
"ctg_init FMH5 TP:CCIN" (data.data[13:3] eq 05:02:ff and data.data[22:4] eq c3c3:c9d5 ) or data.data[12:4] eq 0034:12ff
"ctg_fmh7" data.data contains 0b:9001:0707
"ctg_heartbeat 'PING'" (data.data contains 013a:12f2 or data.data contains 0502:ff) && data.data contains 2020:5049:4e47
"ctg_large_data : No TG at offs 0 in segment" tcp.len gt 0 and !data.data[0:2] eq 0000 and !data.data[4:2] eq 0000
"ctg_req_rsp" data.data contains 0b:90a0 or data.data contains 03:9001 or data.data contains 0b:9001
```

# ctg profile

## colorfilters

Wireshark: Coloring Rules - Profile: ctg

List is processed in order until match is found

Name	String
SYN zOS	tcp.flags.syn == 1 and ip.ttl le 64 and tcp.window_size eq 65535
SYN WinXp	tcp.flags.syn == 1 and ip.ttl gt 64 and ip.ttl le 128 and tcp.window_size eq 65535
SYN Win7+	tcp.flags.syn == 1 and ip.ttl gt 64 and ip.ttl le 128 and tcp.window_size eq 8192 and tcp.options contains (
SYN Solaris	tcp.flags.syn == 1 and ip.ttl le 64 and tcp.window_size eq 49232
TCP RST	tcp.flags.reset eq 1
ctg_CCIN	(data.data[13:3] eq 05:02:ff and data.data[22:4] eq c3c3:c9d5 ) or data.data[12:4] eq 0034:12ff
FMH7	data.data contains 000b:9001:0707
ctg_heartbeat	(data.data contains 013a:12f2 or data.data contains 0502:ff) and data.data contains 2020:5049:4e47
ctg_reply	data.data[8:4] eq 0003:9001
ctg_start_tx	data.data contains 0b:90:a0 and data.data contains 0502:ff
SSL Handshake	data.data[0:3] eq 16:03:01 or ssl.handshake or data.data[0:3] eq 14:03:01 or data.data[0:3] eq 80:1f:01
ctg_big_data	tcp.len gt 0 and !data.data[0:2] eq 0000 and !data.data[4:2] eq 0000
<del>delay_20_ms-</del>	<del>frame.time_delta gt 0.02</del>
3-way-HS	tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0)
FIN	tcp.flags.fin==1 and ip.ttl <= 60
FIN Win	tcp.flags.fin==1 and ip.ttl > 100 and ip.ttl<=128

Order

Up

Move selected filter up or down

Down

Apply Cancel OK

# ctg profile preferences

