#SHAREorg

SHARE

Towards the OSA and beyond Using wireshark for FTP TLS Problem Analysis

Matthias Burkhard
IBM Germany

Thursday Aug. 15 2013
Session 13631

Twitter @mreede
Find us on Facebook at ip.wizards@groups.facebook.com
LinkedIn: de.linkedin.com/in/mreede/
IBM SmartCloud: Matthias Bu

SocialBusiness IBMSmartCloud

IBM Technical Support Services

SHARE in Boston

FTP from z/OS to ShopZ failed
TLS Security issue during SMP/E download

- The Problem
  - FTP to ShopZ failed with `secure_socket_init RC = 402`
    - It worked before (last successful download in January 2013)
    - Nothing changed at the z/OS V1R13 FTP client side
- The Evidence
  - Standard SYSTCPDA packet trace to external CTRACE writer
    - IPCS Trace Formatter shows server is closing the connection
    - AUTH TLS command got FTP-234 SSL OK message
- The Tool: wireshark with customized Profiles
  - Default Profile
    - More Custom Fields “Added as Column”
  - TCP Profile
    - New coloring rules assigned to highlight events

z/OS FTP Client Trace secure_socket_init fails with rc=402

```
EZA1554I Connecting to: dispby-117.boulder.ibm.com 170.225.15.117 port: 21.
220-IBM's internal systems must only be used for conducting IBM's
220-business or for purposes authorized by IBM management.
220-
220-Use is subject to audit at any time by IBM management.
220-
220 dhebpcb01 secure FTP server ready.
GU4945 ftpSetApplData: entered
FC0250 ftpAuth: security values: mech=TLS, tlsmech=FTP, sFTP=R, sCC=C, sDC=P
FC0297 ftpAuth: ........ cipherspecs =
FC0342 ftpAuth: environment_open()
FC0460 ftpAuth: environment_init()
FC0469 ftpAuth: environment initialization complete
EZA1701I >>> AUTH TLS
234 SSLv23/TLSv1
FC0919 authServer: secure_socket_open()
FC0986 authServer: secure_socket_init()
FC0999 authServer: secure_socket_init failed with rc = 402 (No SSL cipher
specifications)
FC1369 endSecureConn: entered
EZA2897I Authentication negotiation failed
FC1401 endSecureEnv: entered
EZA1534I *** Control connection with dispby-117.boulder.ibm.com dies.
SC3958 SETCEC code = 10
```

IPCS Trace Formatter – FTP 220
ctrace comp(systcpda) sub((tcpip)) full

```
    4 SYS1     PACKET   00000004 16:27:16.897019 Packet Trace
 From Interface    : OSAXF1LNK        Device: QDIO Ethernet    Full=107
 IpHeader: Version : 4                Header Length: 20
  Tos              : 00               QOS: Routine Normal Service
  Packet Length    : 107              ID Number: 3A59
  Fragment         :                  Offset: 0
  TTL              : 45               Protocol: TCP            CheckSum: 8DC4 FFFF
  Source           : 170.225.15.117
  Destination      : 10.9.1.17

 TCP
  Source Port      : 21    (ftp)      Destination Port: 13188 ()
  Sequence Number  : 933089570        Ack Number: 130121125
  Header Length    : 20               Flags: Ack Psh
  Window Size      : 65535            CheckSum: 7D25 FFFF Urgent Data Pointer: 0000
Data               : 67     Data Length: 67                    Offset: 28
220-IBM's internal systems must only be used for conducting IBM's
Ip Header          : 20               IP: 170.225.15.117, 10.9.1.17 Offset:  0
000000 4500006B 3A590000 2D068DC4 AAE10F75  0A090111
Protocol Header    : 20               Port: 21, 13188          Offset: 14
000000 00153384 379DD122 07C17DA5 5018FFFF  7D250000
Data               : 67     Data Length: 67                    Offset: 28
Data               : 67     Data Length: 67                    Offset: 28

000000 3232302D 49424D27 7320696E 7465726E  616C2073 79737465 6D73206D 75737420 |220-IBM's internal
000020 6F6E6C79 20626520 75736564 20666F72  20636F6E 64756374 696E6720 49424D27 |only be used for
000040 730D0A                                                                  |s..
```

IPCS Trace Formatter FTP ???
ctrace comp(systcpda) sub((tcpip)) full

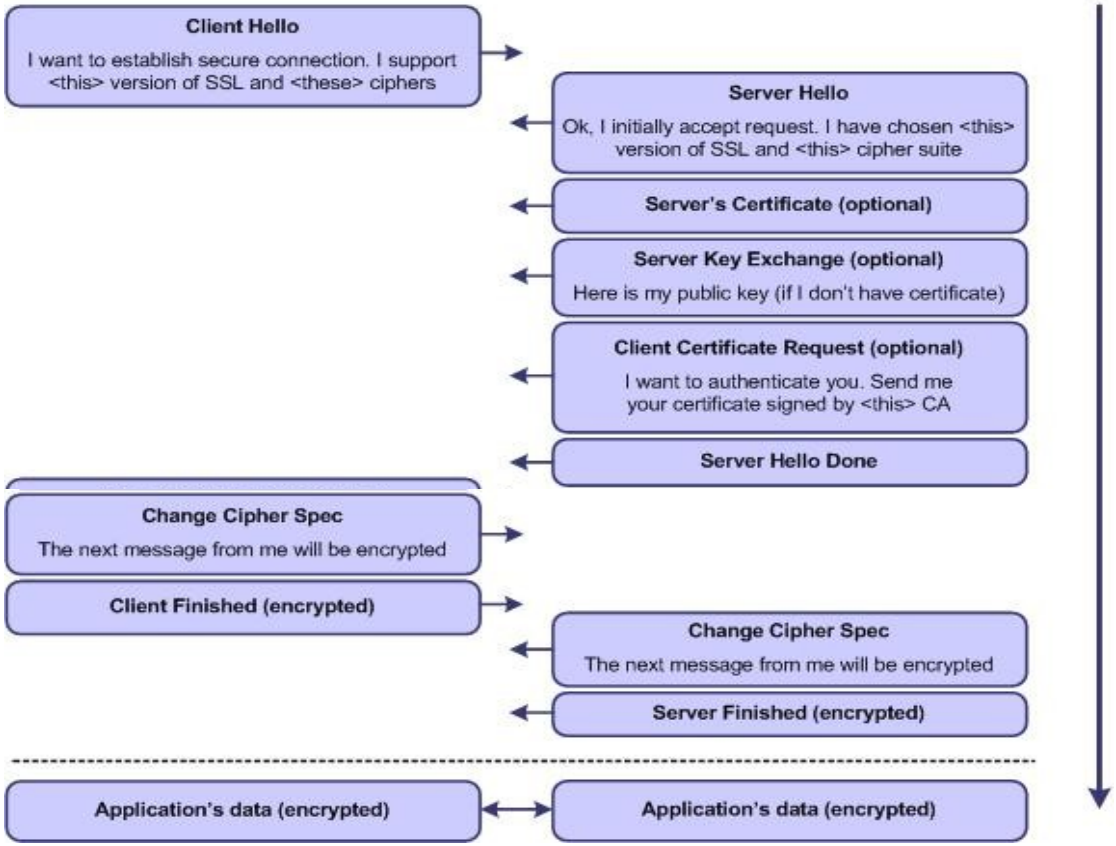
```
   11 SYS1     PACKET   00000004 16:27:17.393565 Packet Trace
 To Interface      : OSAXF0LNK        Device: QDIO Ethernet    Full=100
 IpHeader: Version : 4                Header Length: 20
  Tos              : 00               QOS: Routine Normal Service
  Packet Length    : 100              ID Number: 28B6
  Fragment         :                  Offset: 0
  TTL              : 64               Protocol: TCP            CheckSum: 0000 7391
  Source           : 10.9.1.17
  Destination      : 170.225.15.117
 TCP
  Source Port      : 13188 ()         Destination Port: 21    (ftp)
  Sequence Number  : 130121135        Ack Number: 933089827
  Header Length    : 20               Flags: Ack Psh
  Window Size      : 65535            CheckSum: 0000 05ED Urgent Data Pointer: 0000
Data               : 60     Data Length: 60                    Offset: 28
????7???3??R??E?C~{!I"b(?wws?$9@s??B2?1?S0'???????????????
Ip Header          : 20               IP: 10.9.1.17, 170.225.15.117 Offset:  0
000000 45000064 28B60000 40060000 0A090111  AAE10F75
Protocol Header    : 20               Port: 13188, 21          Offset: 14
000000 33840015 07C17DAF 379DD223 5018FFFF  00000000
Data               : 60     Data Length: 60                    Offset: 28
000000 16030100 37010000 33030152 0107C58B  43FE7B21 49A262A8 3F777773 1D24B940 |....7...3.
000020 73811742 32FFB189 53302700 000C00FF  00010002 00030006 00090100          |s..B2...S0
```

IPCS Trace Formatter FTP ???
ctrace comp(systcpda) sub((tcpip)) full

```
   12 SYS1     PACKET   00000004 16:27:17.539824 Packet Trace
 From Interface    : OSAXF1LNK        Device: QDIO Ethernet    Full=47
 IpHeader: Version : 4                Header Length: 20
  Tos              : 00               QOS: Routine Normal Service
  Packet Length    : 47               ID Number: 4102
  Fragment         :                  Offset: 0
  TTL              : 45               Protocol: TCP            CheckSum: 8757 FFFF
  Source           : 170.225.15.117
  Destination      : 10.9.1.17
 TCP
  Source Port      : 21    (ftp)      Destination Port: 13188 ()
  Sequence Number  : 933089827        Ack Number: 130121195
  Header Length    : 20               Flags: Ack Psh
  Window Size      : 65535            CheckSum: E749 FFFF Urgent Data Pointer: 0000
Data               : 7      Data Length: 7                     Offset: 28
??????(
Ip Header          : 20               IP: 170.225.15.117, 10.9.1.17 Offset:  0
000000 4500002F 41020000 2D068757 AAE10F75  0A090111
Protocol Header    : 20               Port: 21, 13188          Offset: 14
000000 00153384 379DD223 07C17DEB 5018FFFF  E7490000
Data               : 7      Data Length: 7                     Offset: 28
000000 15030100 020228                                                |......(
```

TLS Handshake Overview
The flows of a successful negotiation

14030....	Change Cipher Spec
15030....	TLS/SSL Alert
16030....	Handshake
17030....	Encrypted data



IPCS Trace Formatter FTP TLS Handshake The Client Hello

```
   11 SYS1     PACKET   00000004 16:27:17.393565 Packet Trace
 To Interface      : OSAXF0LNK        Device: QDIO Ethernet    Full=100
 IpHeader: Version : 4                Header Length: 20
  Tos              : 00               QOS: Routine Normal Service
  Packet Length    : 100              ID Number: 28B6
  Fragment         :                  Offset: 0
  TTL              : 64               Protocol: TCP            CheckSum: 0000 7391
  Source           : 10.9.1.17
  Destination      : 170.225.15.117
 TCP
  Source Port      : 13188 ()         Destination Port: 21    (ftp)
  Sequence Number  : 130121135        Ack Number: 933089827
  Header Length    : 20               Flags: Ack Psh
  Window Size      : 65535            CheckSum: 0000 05ED Urgent Data Pointer: 0000
Data               : 60     Data Length: 60                    Offset: 28
????7???3??R??E?C~{!I"b(?wws?$9@s??B2?1?S0'???????????????
Ip Header          : 20               IP: 10.9.1.17, 170.225.15.117 Offset:  0
000000 45000064 28B60000 40060000 0A090111  AAE10F75
Protocol Header    : 20               Port: 13188, 21          Offset: 14
000000 33840015 07C17DAF 379DD223 5018FFFF  00000000
Data               : 60     Data Length: 60                    Offset: 28
000000 16030100 37010000 33030152 0107C58B  43FE7B21 49A262A8 3F777773 1D24B940 |....7...3.
000020 73811742 32FFB189 53302700 000C00FF  00010002 00030006 00090100          |s..B2...S0
```

16030.... Handshake

IPCS Trace Formatter FTP TLS ALERT ctrace comp(systcpda) sub((tcpip)) full

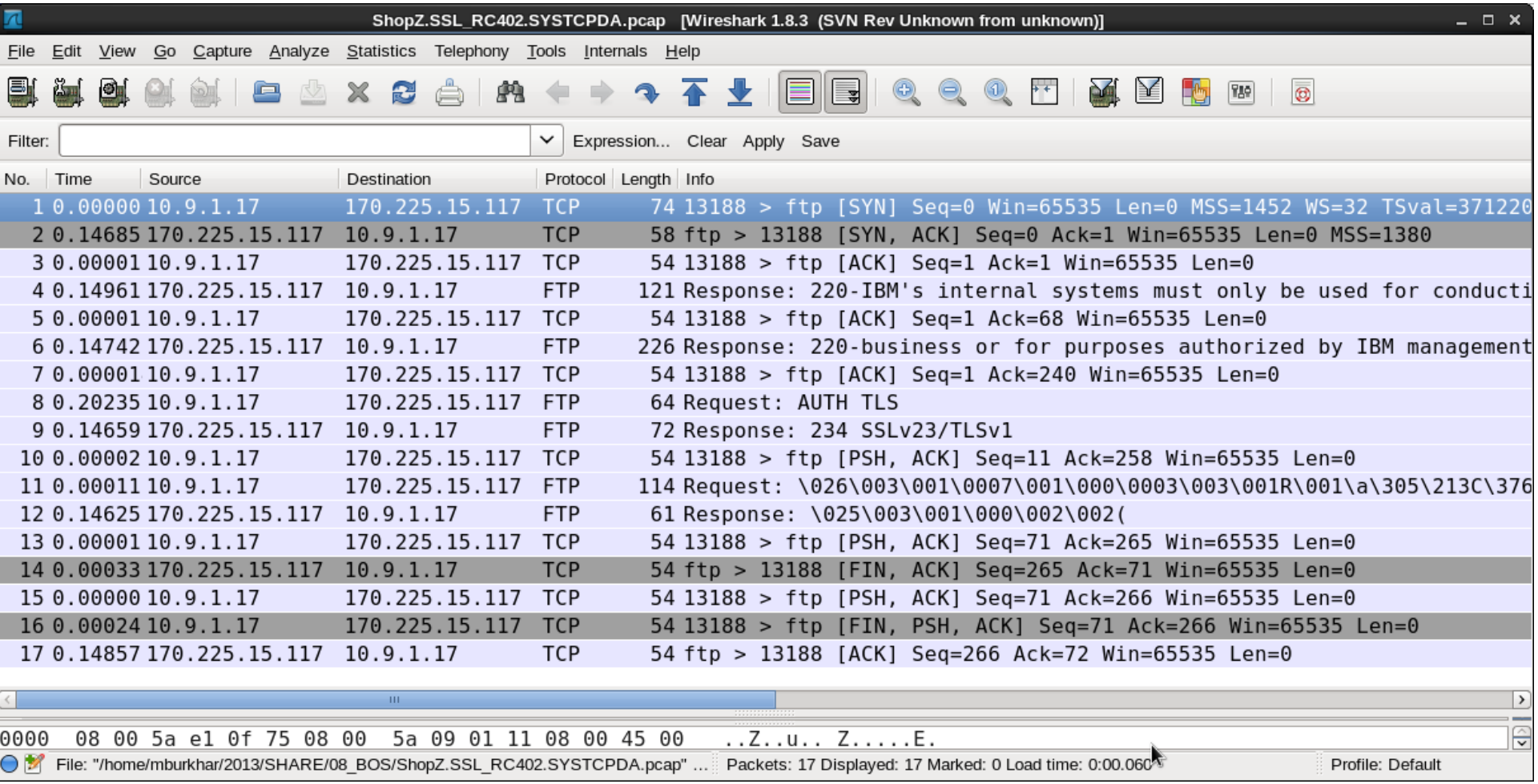
```
   12 SYS1     PACKET   00000004 16:27:17.539824 Packet Trace
 From Interface    : OSAXF1LNK        Device: QDIO Ethernet    Full=47
 IpHeader: Version : 4                Header Length: 20
  Tos              : 00               QOS: Routine Normal Service
  Packet Length    : 47               ID Number: 4102
  Fragment         :                  Offset: 0
  TTL              : 45               Protocol: TCP            CheckSum: 8757 FFFF
  Source           : 170.225.15.117
  Destination      : 10.9.1.17
 TCP
  Source Port      : 21    (ftp)      Destination Port: 13188 ()
  Sequence Number  : 933089827        Ack Number: 130121195
  Header Length    : 20               Flags: Ack Psh
  Window Size      : 65535            CheckSum: E749 FFFF Urgent Data Pointer: 0000
Data               : 7      Data Length: 7                     Offset: 28
??????(
Ip Header          : 20               IP: 170.225.15.117, 10.9.1.17 Offset:  0
000000 4500002F 41020000 2D068757 AAE10F75  0A090111
Protocol Header    : 20               Port: 21, 13188          Offset: 14
000000 00153384 379DD223 07C17DEB 5018FFFF  E7490000
Data               : 7      Data Length: 7                     Offset: 28
000000 15030100 020228                                                |......(
```

15030.... TLS/SSL Alert

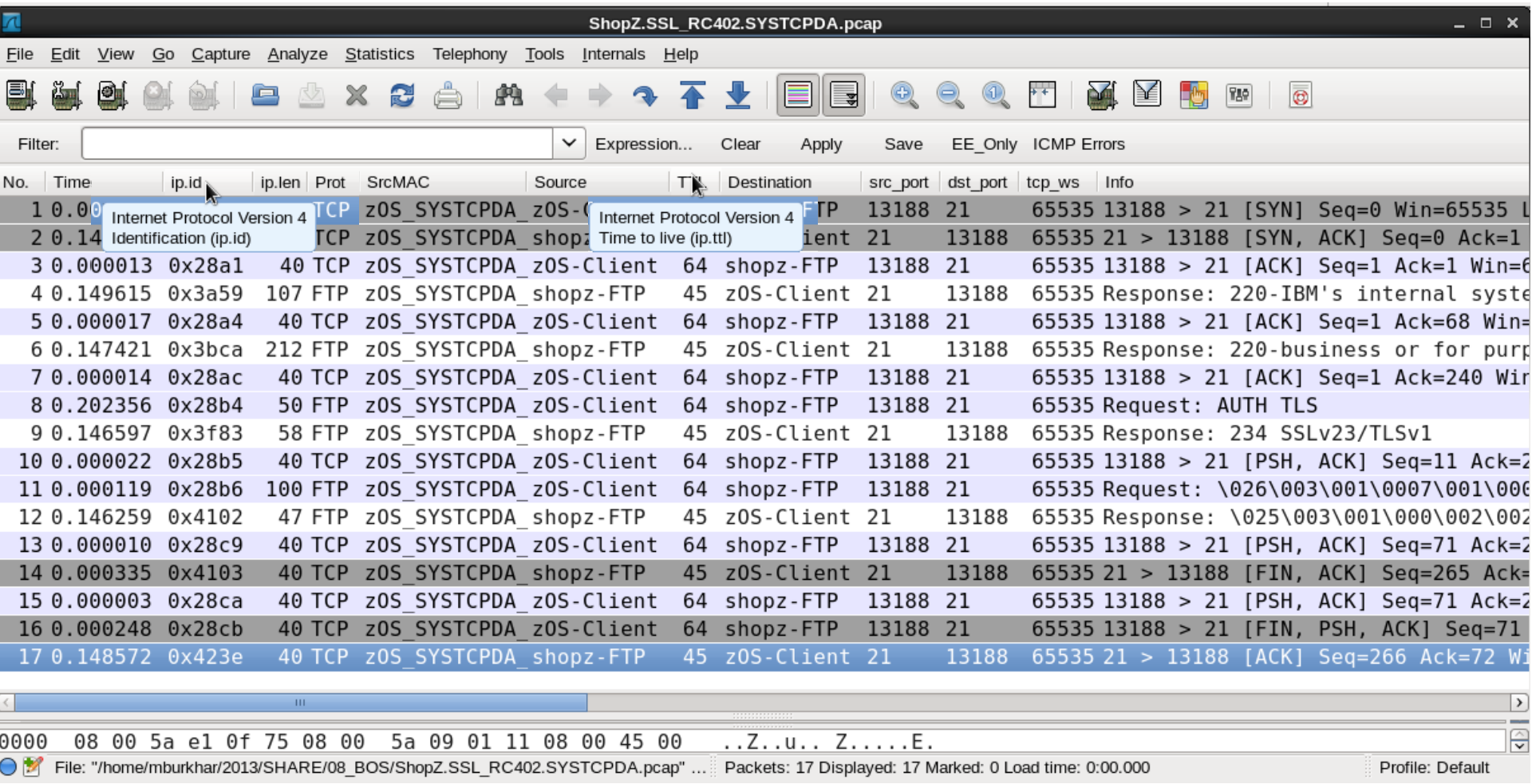
IPCS Trace Formatter Conversion
Convert SYSTCPDA to Sniffer

```
TSO ALLOC FI(SNIFFER) DSN('IP.WIZARDS.SYSTCPDA.PCAP') SHR REUSE
IP CTRACE COMP(SYSTCPDA) SUB((TCPIP)) OPTIONS((SNIFFER(1500 TCPDUMP)))
TSO FREE FI(SNIFFER)
 BROWSE    IP.WIZARDS.SYSTCPDA.PCAP
 Command ===>
****************************************************************************** Top of Data *****
~¥CM.....................
ê..D...P...¢...¢..!÷.Í..!.....á....q.. .ð©....i÷.Í.d...A'u....µ...í%.....Ð........../.....
ê..D..Å"..........!÷.Í..!.....á....£....±¿i÷.Í.......d.¸J..A'v-..........À
ê..D..Åð..........!÷.Í..!.....á....~.. .ð×....i÷.Í.d...A'v.¸J.&....v..
ê..D..®Û...`...`..!÷.Í..!.....á..,.ß....ýDi÷.Í.......d.¸J..A'v&...'.......ñâ(.Ë.Ñ>ÈÁÊ>/%.Ë`
ê..D..^...........!÷.Í..!.....á....u.. .ð¯....i÷.Í.d...A'v.¸JÁ&....Â..
ê..E..[z...O...S..!÷.Í..!.....á..M.-....»²i÷.Í.......d.¸JÁ.A'v&...«E......ÂÍËÑ>ÁËË.?Ê.Ã?Ê.ø
ê..E..[¼..........!÷.Í..!.....á....Ð.. .ð©....i÷.Í.d...A'v.¸K.&....¶..
ê..E..D.... ... ..!÷.Í..!.....á....©.. .ðs....i÷.Í.d...A'v.¸K.&....í.. íèç.è<ë..
ê..E...}...ç...ç..!÷.Í..!.....á....c....hôi÷.Í.......d.¸K..A'®&...0;......ëë<Î...è<ëÎ...
ê..E...W..........!÷.Í..!.....á....§.. .ð¿....i÷.Í.d...A'®.¸K.&....k..
ê..E...)...Ê...Ê..!÷.Í..!.....á..À.¶.. .ð>....i÷.Í.d...A'®.¸K.&...³.............ê..E»äÚ#.ñ
ê..E...^...........!÷.Í..!.....á... .....gïi÷.Í.......d.¸K..A'Ô&...Xñ.........
ê..E...Ý..........!÷.Í..!.....á....I.. .ðp....i÷.Í.d...A'Ô.¸K.&....|..
ê..E.............!÷.Í..!.....á... .....g)i÷.Í.......d.¸K..A'Ô&....î..
ê..E.............!÷.Í..!.....á....-.. .ðo....i÷.Í.d...A'Ô.¸K.&....+..
ê..E.............!÷.Í..!.....á....ô.. .ðn....i÷.Í.d...A'Ô.¸K.&....(..
ê..E..c-..........!÷.Í..!.....á...â.....f.i÷.Í.......d.¸K..A'Ö&....í..
****************************************************************************** Bottom of Data ***
```

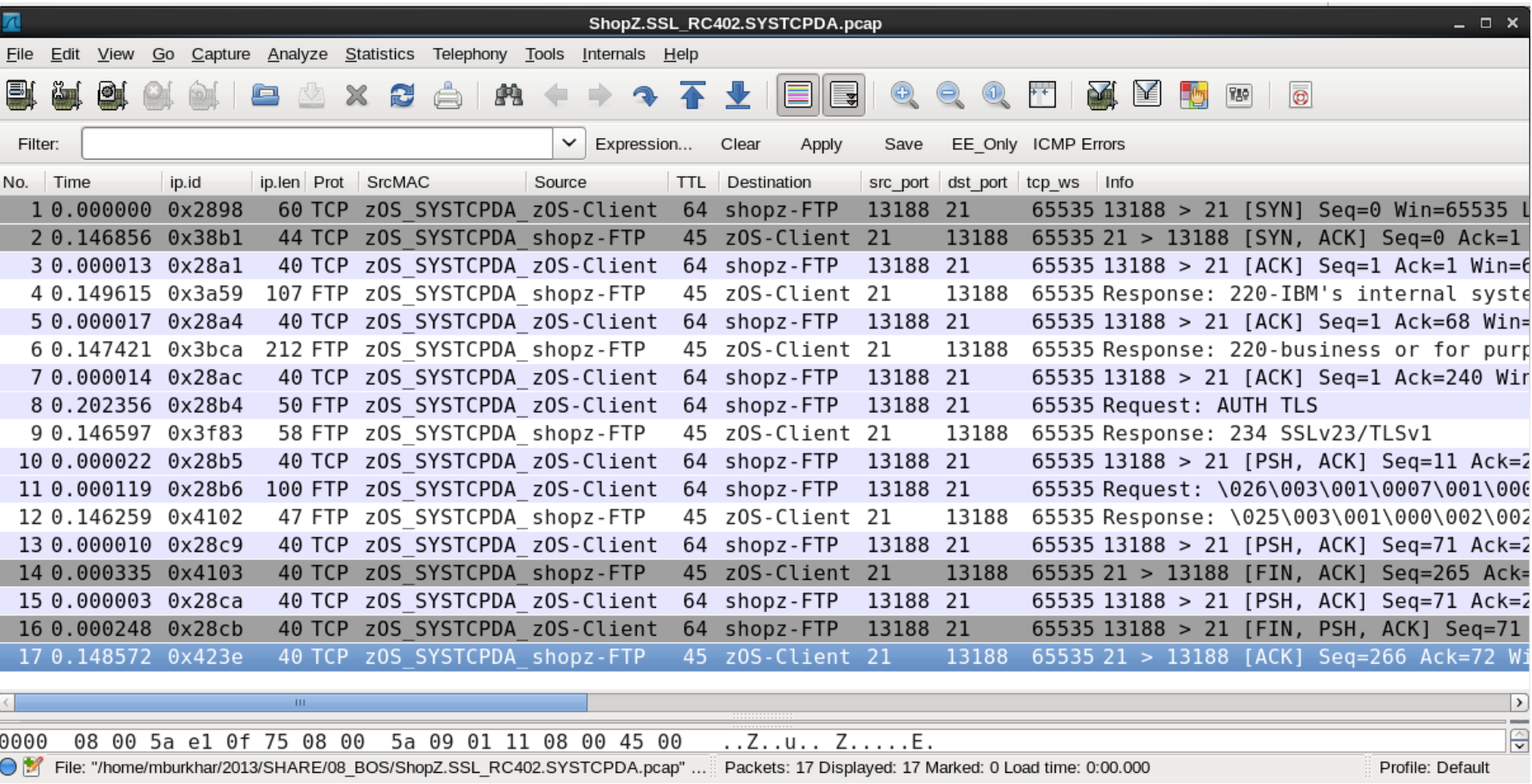
The Default Profile
Only basic information about each packet



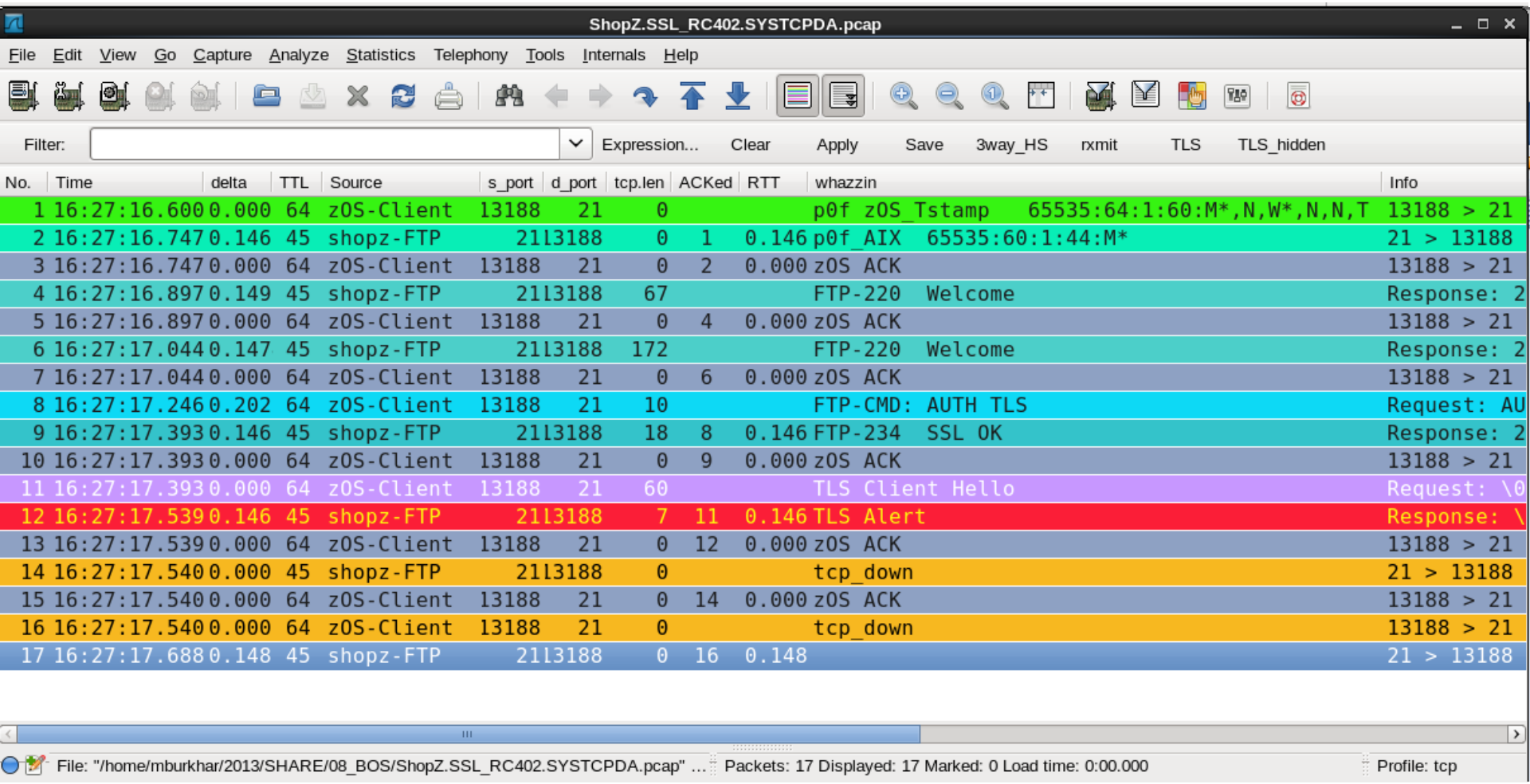
Default Profile
Adding columns to the packet list



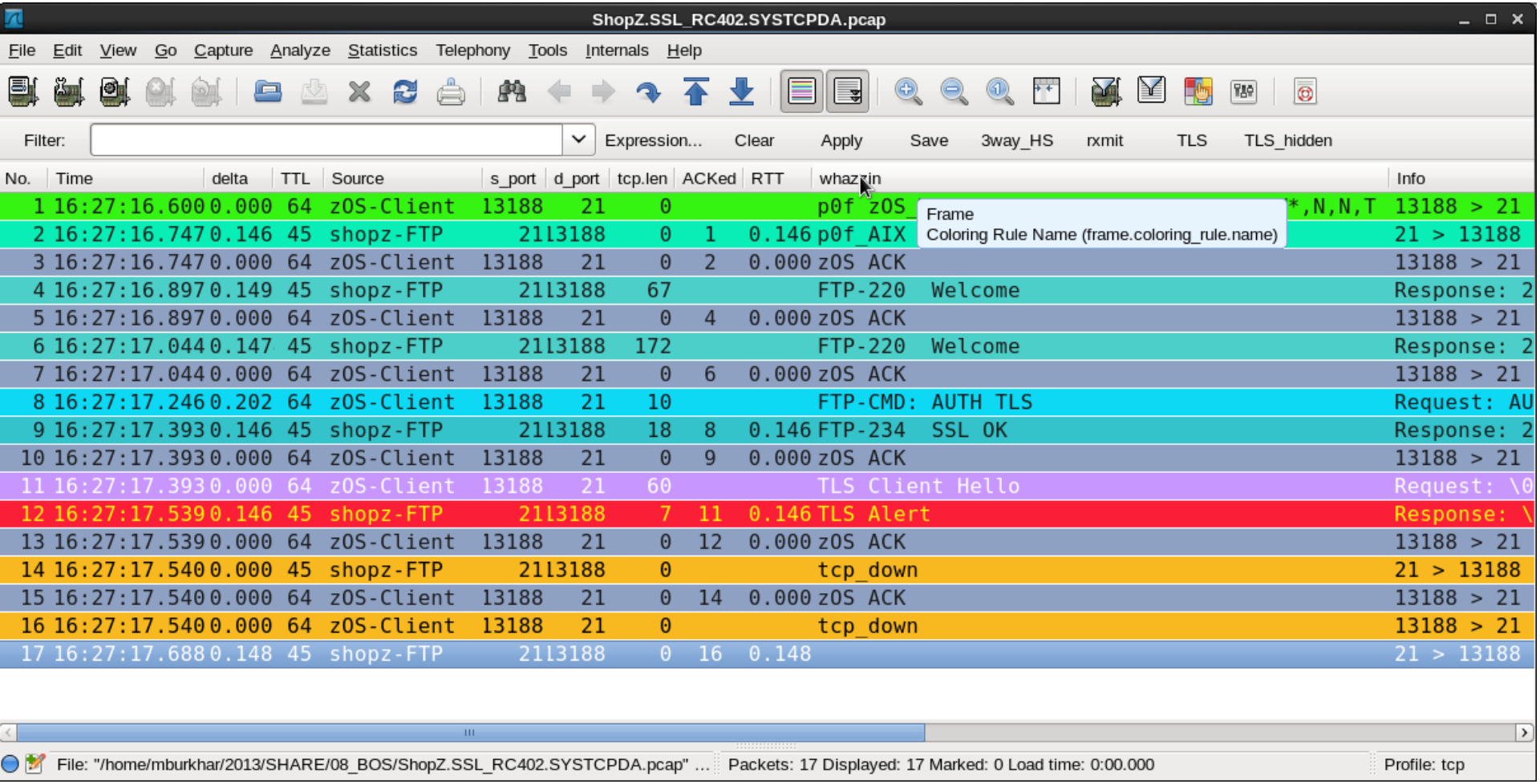
Why use different profiles?
A trace is a trace is a trace – isn't it?



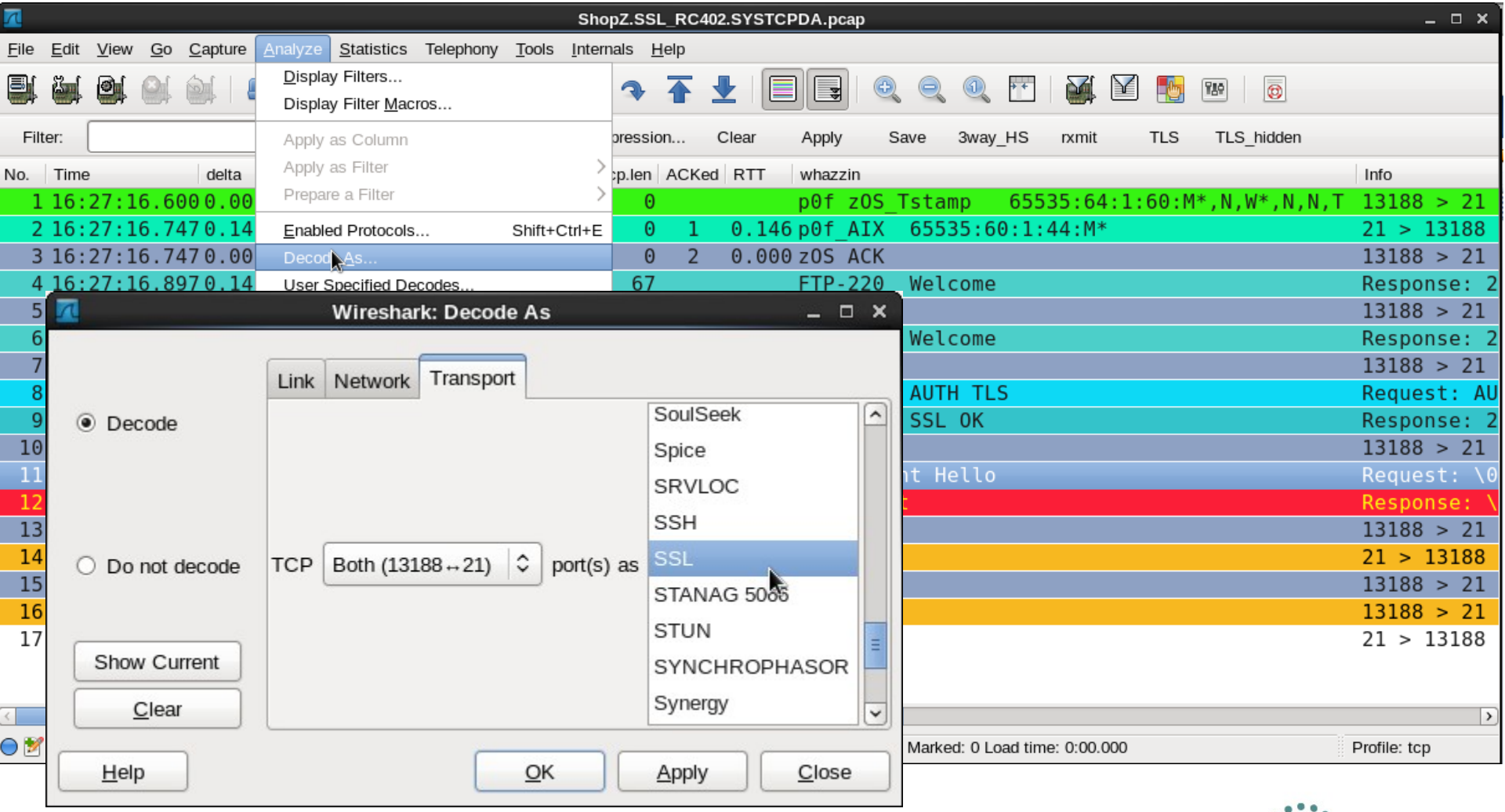
Why use different profiles?
A trace is a trace is a trace – isn't it?



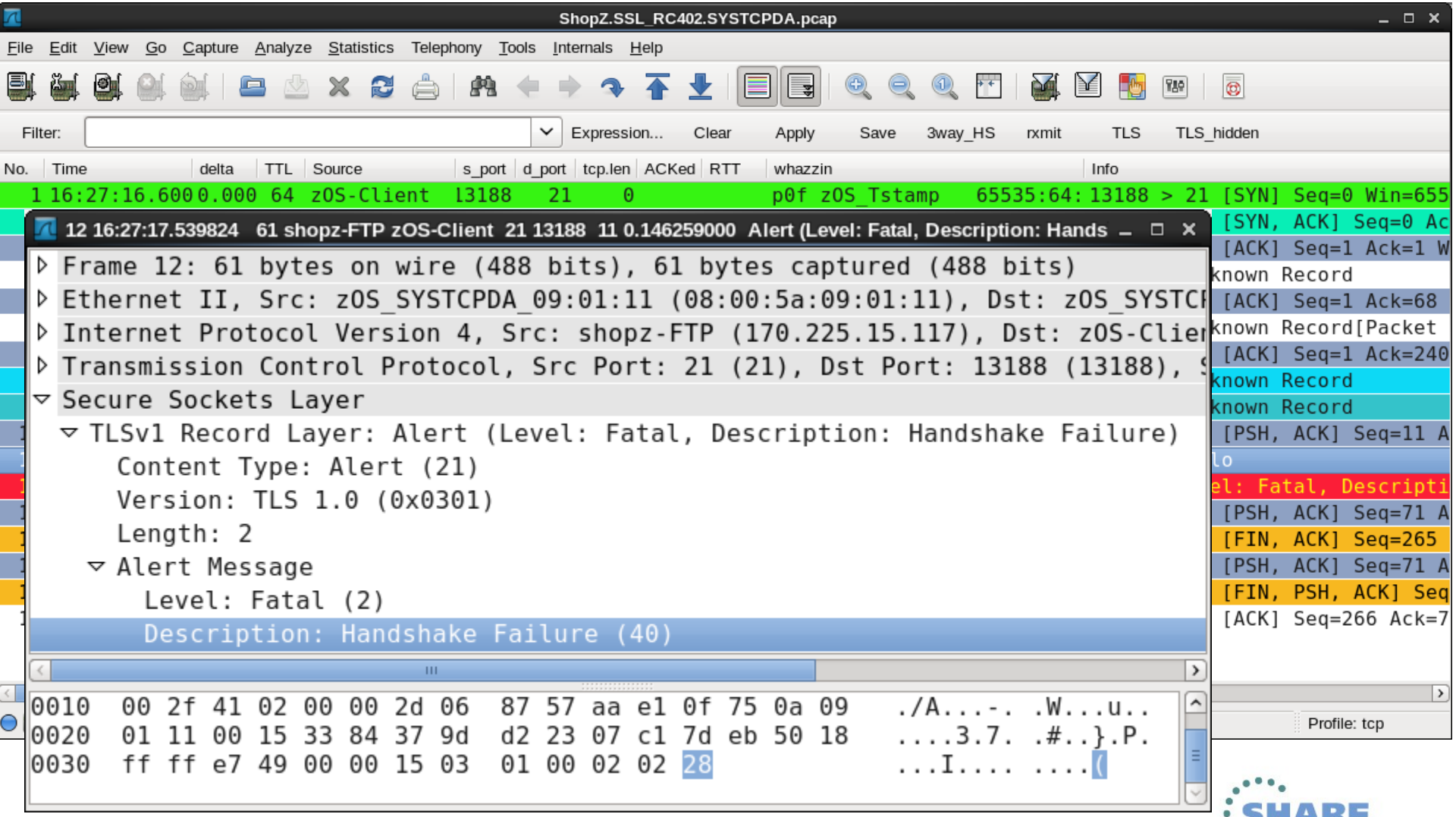
Why use different profiles?
Added frame.coloring_rule.name



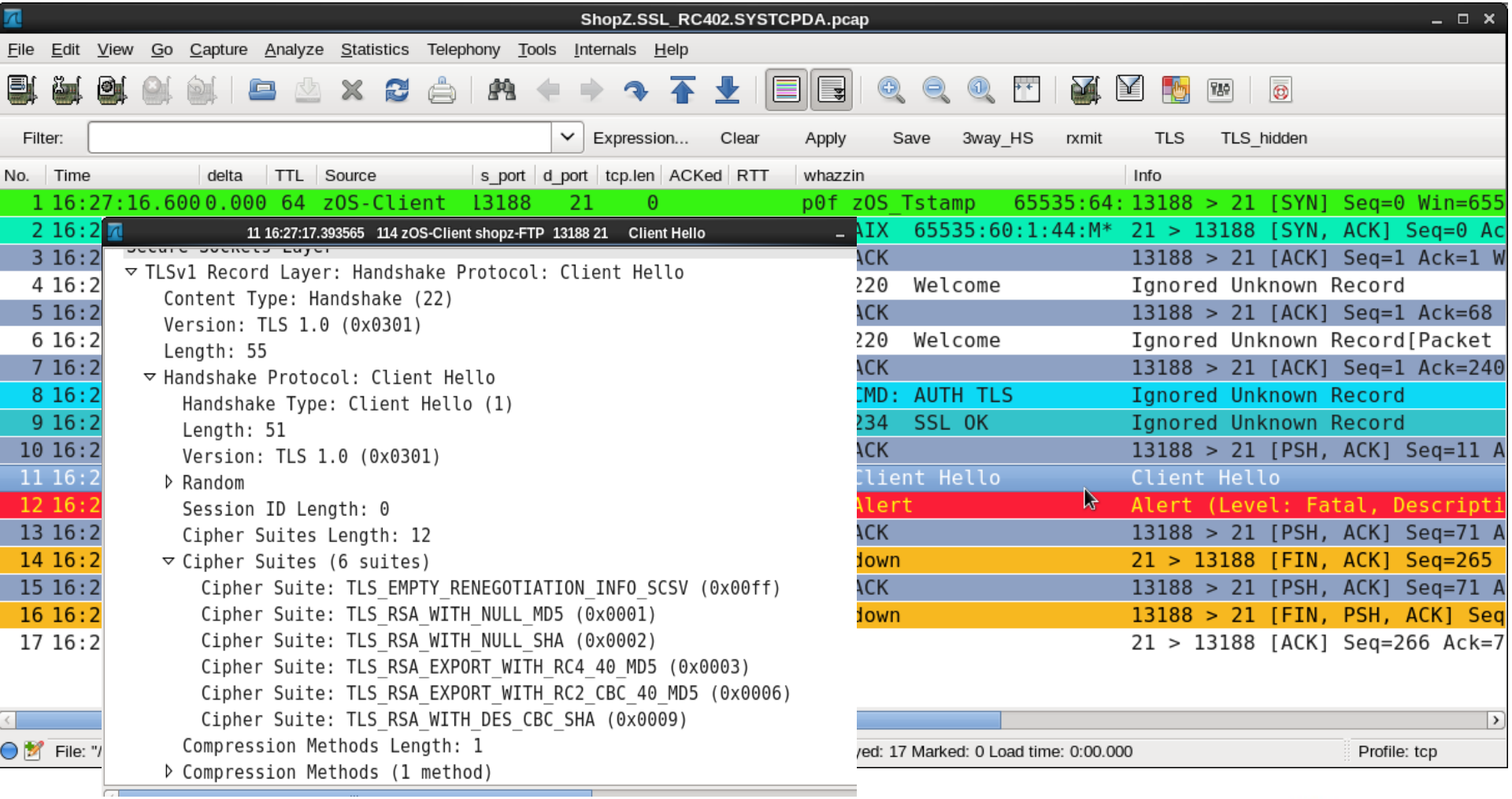
Map another protocol to well known port
Analyze → Decode As



TLS Alert
Fatal Handshake Failure



TLS Handshake Protocol
Client Hello offering Cipher Suites



FTPDATA CIPHERSUITE definitions

```
; Name of a ciphersuite that can be passed to the partner during
; the TLS handshake. None, some, or all of the following may be
; specified. The number to the far right is the cipherspec id
; that corresponds to the ciphersuite's name.
 CIPHERSUITE       SSL_NULL_MD5      ; 01
 CIPHERSUITE       SSL_NULL_SHA      ; 02
 CIPHERSUITE       SSL_RC4_MD5_EX    ; 03
 CIPHERSUITE       SSL_RC4_MD5       ; 04
 CIPHERSUITE       SSL_RC4_SHA       ; 05
 CIPHERSUITE       SSL_RC2_MD5_EX    ; 06
 CIPHERSUITE       SSL_DES_SHA       ; 09
 CIPHERSUITE       SSL_3DES_SHA      ; 0A
```

Starting GSKSRVR
F GSKSRVR,D CRYPTO

```
-S GSKSRVR
 SYS1 R= GSKSRVR  IEF695I START GSKSRVR  WITH JOBNAME GSKSRVR  IS ASSIGNED TO
USER
 SYS1 R= GSKSRVR  GSKSRVR , GROUP GRPSYSTC
&SYS1 R= GSKSRVR  IEF403I GSKSRVR - STARTED - TIME=13.14.23
 SYS1 R= GSKSRVR  GSK01001I System SSL version 3.23, Service level OA40338.
 SYS1 R= GSKSRVR  GSK01003I SSL server initialization complete.
-F GSKSRVR,D CRYPTO
 SYS1 R= GSKSRVR  GSK01009I Cryptographic status
 SYS1 R= GSKSRVR  Algorithm       Hardware    Software
 SYS1 R= GSKSRVR  DES                 56          56
 SYS1 R= GSKSRVR  3DES                --          --
 SYS1 R= GSKSRVR  AES                 --          --
 SYS1 R= GSKSRVR  RC2                 --          40
 SYS1 R= GSKSRVR  RC4                 --          40
 SYS1 R= GSKSRVR  RSA Encrypt         --        4096
 SYS1 R= GSKSRVR  RSA Sign            --        4096
 SYS1 R= GSKSRVR  DSS                 --        1024
 SYS1 R= GSKSRVR  SHA-1              160         160
 SYS1 R= GSKSRVR  SHA-2              512         512
 SYS1 R= GSKSRVR  ECC                 --          --
```

FTP from z/OS to ShopZ failed
TLS Security issue during SMP/E download

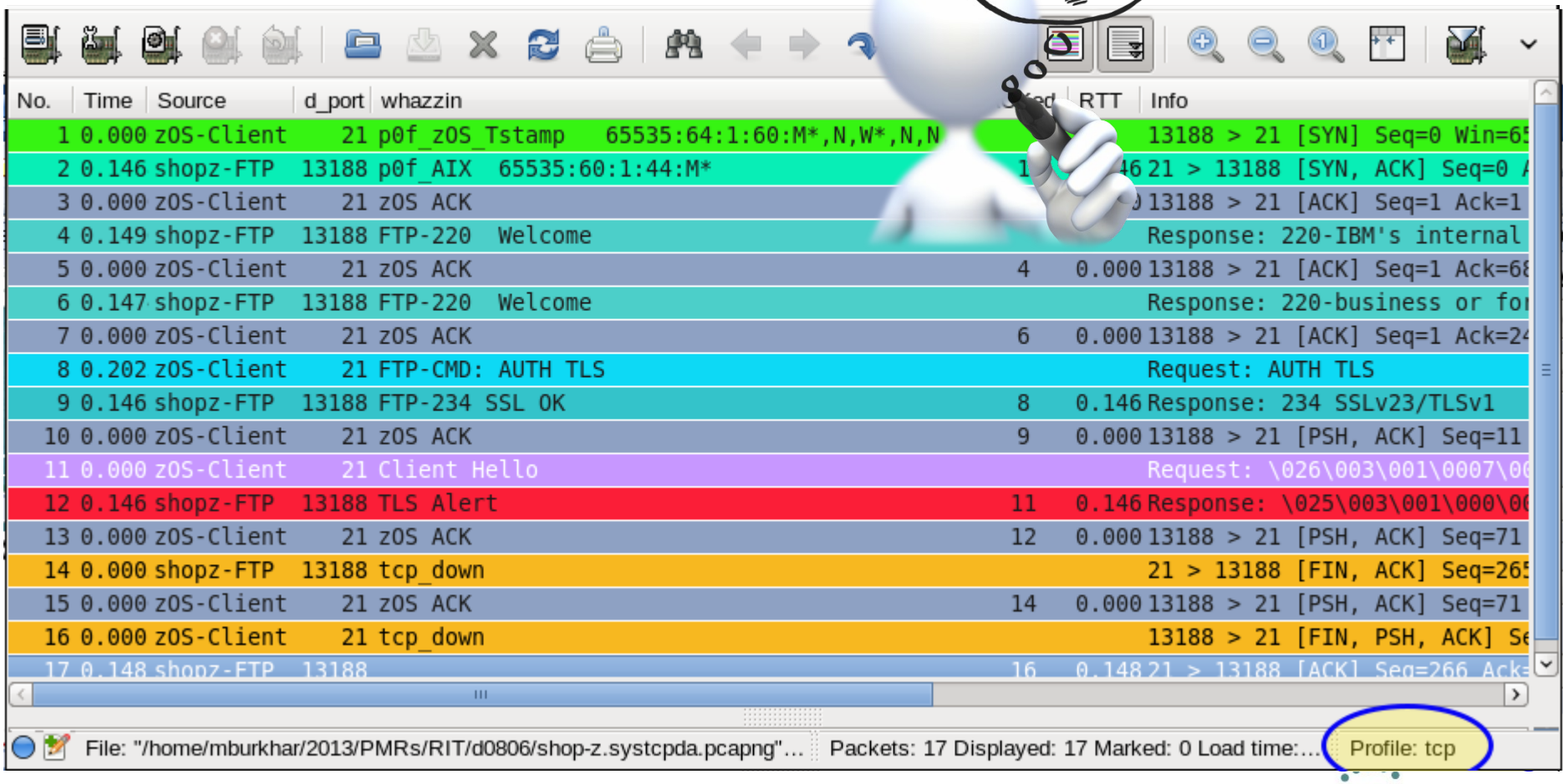
- The Problem
  - FTP to ShopZ failed with `secure_socket_init RC = 402`
    - It worked before (last successful download in January 2013)
    - Nothing changed at the z/OS V1R13 FTP client side
- The Evidence
  - Standard SYSTCPDA packet trace to external CTRACE writer
    - IPCS Trace Formatter shows server is closing the connection
    - AUTH TLS command got FTP-234 SSL OK message
- The Tool: wireshark with customized Profiles
  - Default Profile
    - More Custom Fileds “Added as Column”
  - TCP Profile
    - New coloring rules assigned to highlight events

Problem Summary and Solution Sometimes you better look twice...

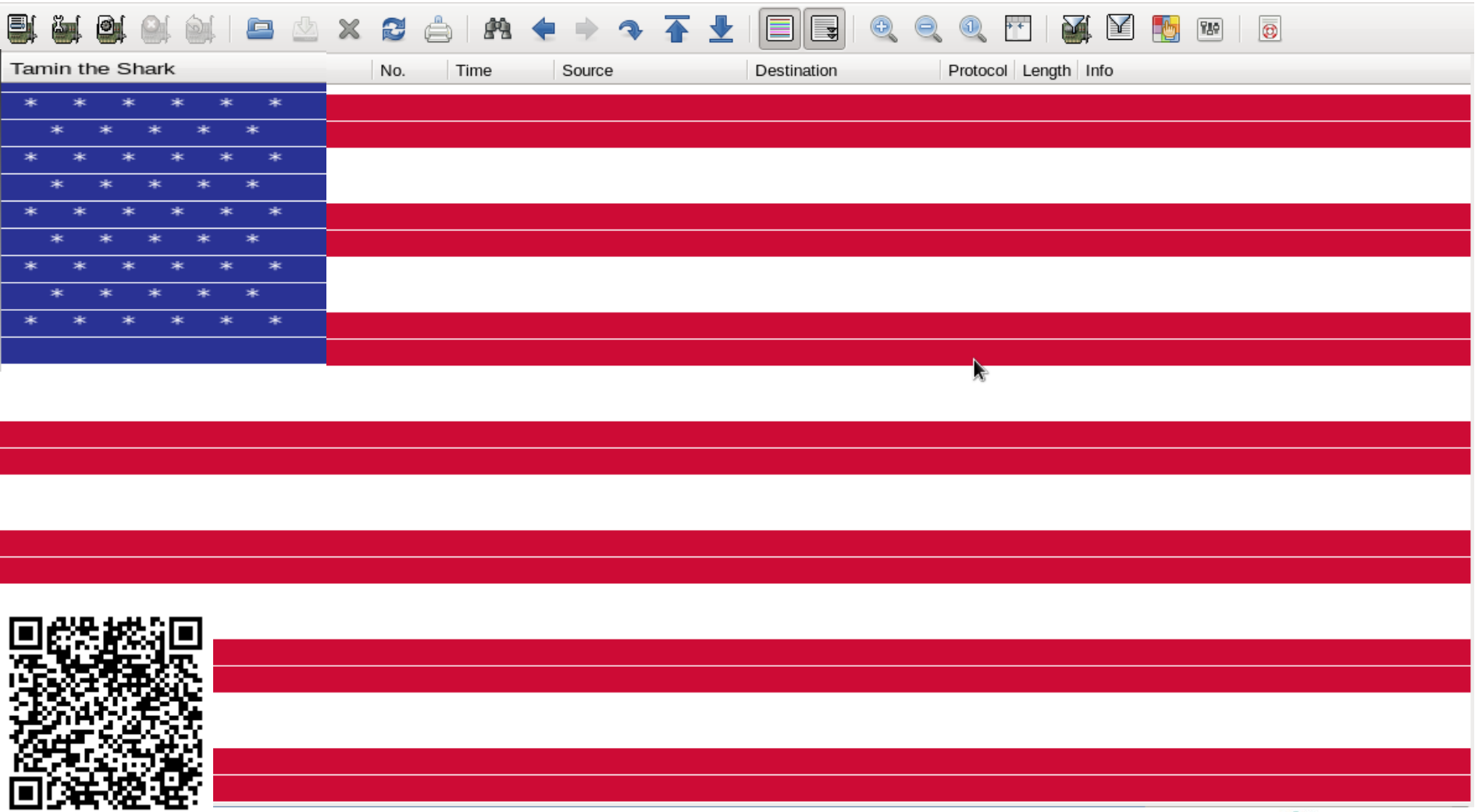
- The Problem
  - FTP to ShopZ failed with **`secure_socket_init RC = 402`**
    - The ShopZ no longer accepts old ciphers
- The Evidence
  - Packet Trace shows AES and 3DES were not offered
    - Requires CPACF feature enabled
    - Requires SSL V3 FMID to be applied
- The Solution

```
SRID: ATRDSB9FFJ8 Stat: OP1L1   PMR: 75741,010,610  Entitle: CCMS S* 1
Rqst: SOFTWARE SubRqst: SOFTWARE DEFECT SUPPORT                    *
Queue: EBBNET Ctr: 25A S4 P4 01 Con:                               *
Comp: 5655HAL00___ Rel: 1D0    ConPh.                  SC: 72 * IE
.
Weitere Kommentare
After installing SSL V3 extension Fmid JCPT3D1 (Security Level 3) the
"F GSKSRVR,D CRYPTO" shows now the enablement for 3DES and AES. The
testjob is working well and successful.
Problem is solved, thanks for all your help, PMR can be closed.
Regards,
[redacted]
.
 +TIVOLI 20              -5655HAL00   -L25Z/CFEZOS-P4S4-13/08/14-10:32
 +TIVOLI 20              -5655HAL00   -L25Z/CFEZOS-P4S4-13/08/14-10:32
```

Why use different profiles?
Show what's in there! Coloring Rules!



The United Colors of Wireshark
Join us at “Taming the Shark” at 4:30PM R202



13282: Taming the Shark - Tips and Tricks on Using Wireshark Hands-on Lab

Thursday, August 15, 2013: 4:30 PM-5:30 PM
oom 202 (Hynes Convention Center)
peaker: Matthias Burkhard(IBM Corporation)

SHARE in Boston

Thank You for attending this session!

Come to "Taming the Shark" - A wireshark Hands On Lab Session at 4:30PM R202

Thank You for your Time at SHARE

Matthias Burkhard IBM Germany

http://tinyurl.com/ipwizards

ip.wizards@groups.facebook.com

Your feedback is important:

This was session 13631 at SHARE in Boston 2013

Towards the OSA and beyond

FTP ShopZ TLS Problem Analysis

2clP Output
FTP-CTRL session

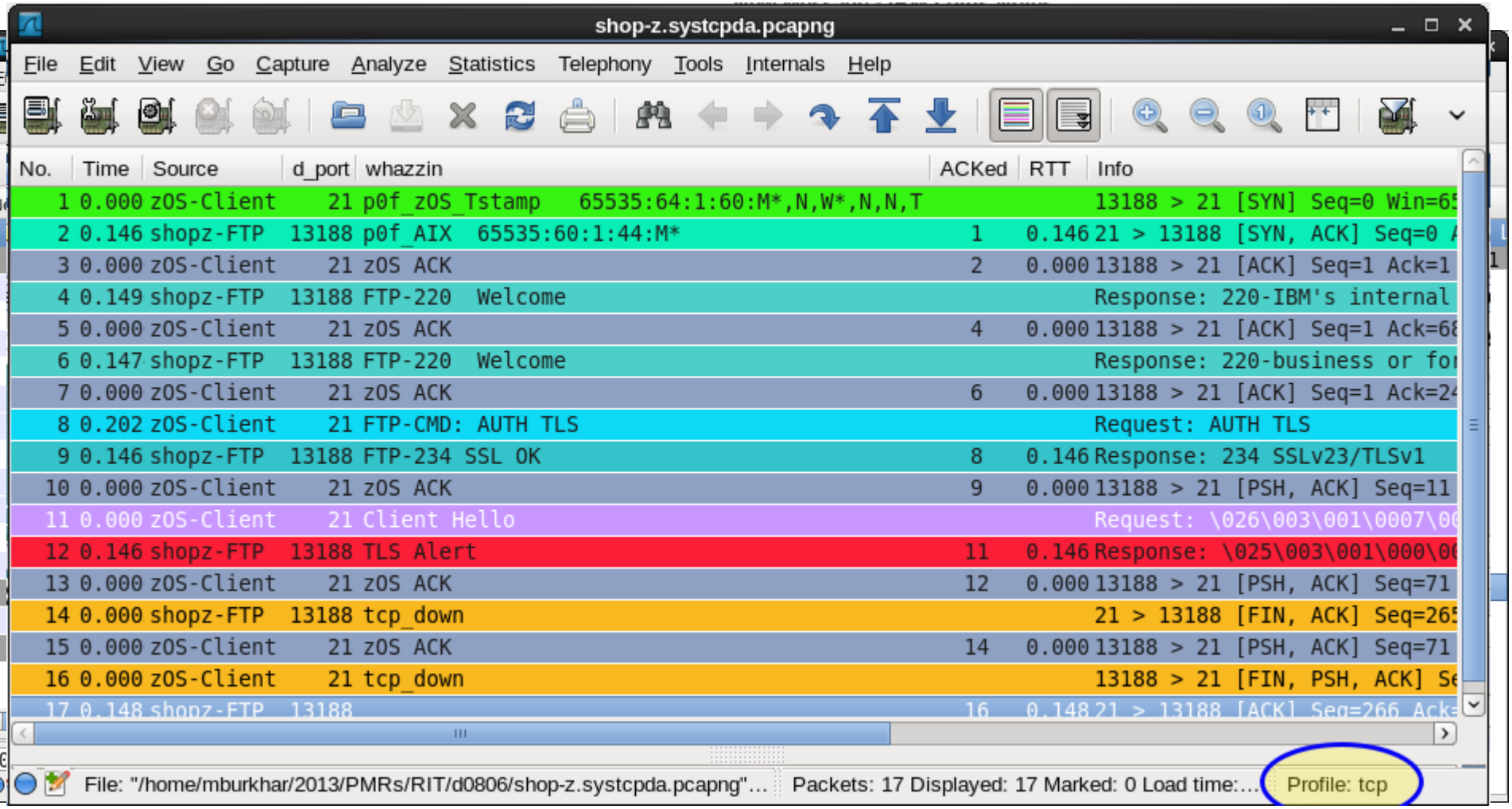
File Options Macros

2cIP - TRACE ANALYSIS PANEL

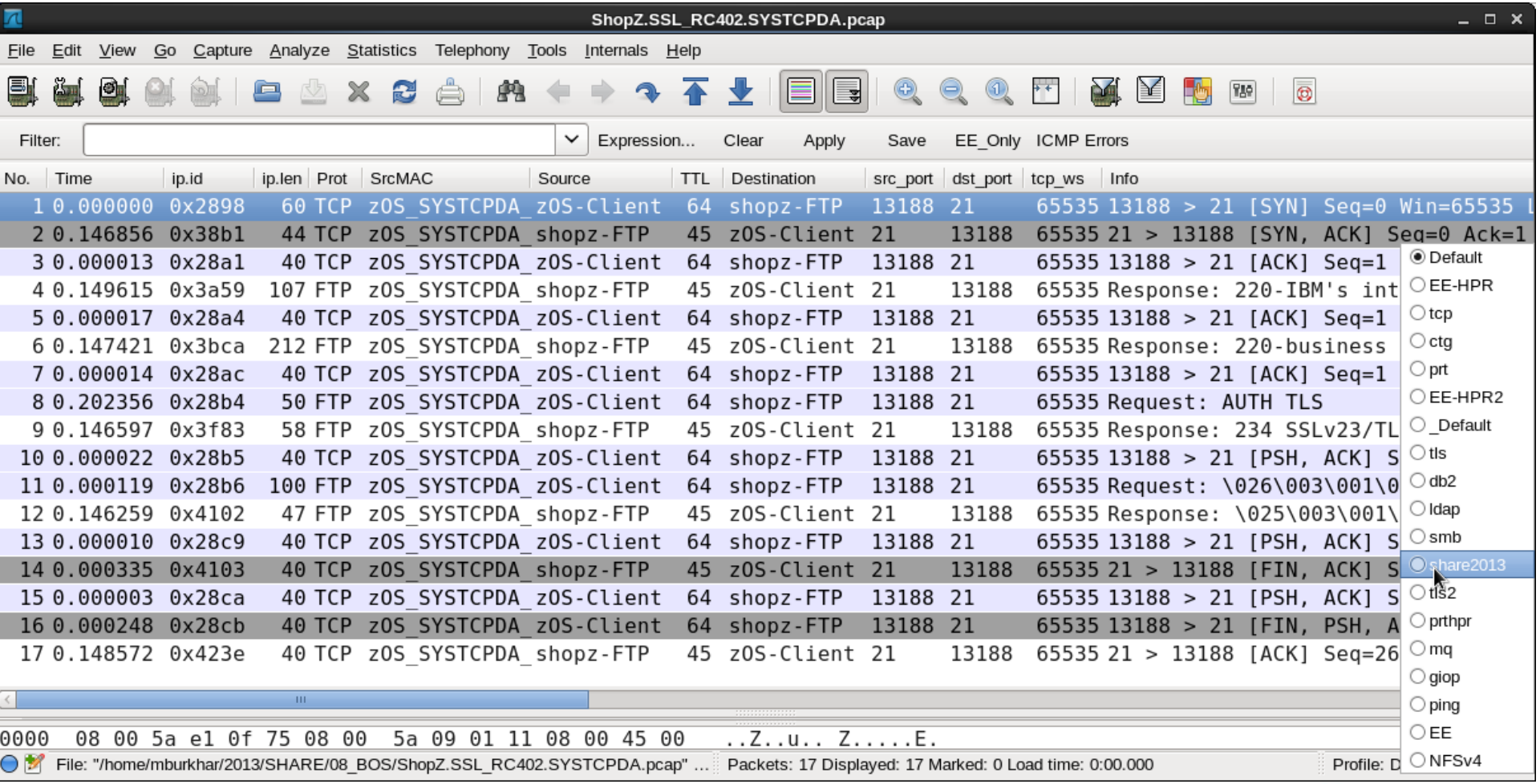
Command ===>

No	RecNo	Time(Delta)	SIGCHECK	IP Address (+ Port	TTL	Iden		IP Address (+ Port	Iden	Description (short)
--Trace	SYSTCPDA									
1	1	0.000.000	zos:OSA1492 _02M_Tstamp	10.9.1.17(13188)	64	2898	->	170.225.15.117(21)		TCP/FTP S MSS=1452 WS=5
2	2	0.146.856	AIX:VPN1420 64k	10.9.1.17(13188)	45		<-	170.225.15.117(21)	38B1	TCP/FTP SA MSS=1380
3	3	0.000.013		10.9.1.17(13188)	64	28A1	->	170.225.15.117(21)		TCP/FTP A
4	4	0.149.615		10.9.1.17(13188)	45		<-	170.225.15.117(21)	3A59	TCP/FTP/220-IBM's AP
5	5	0.000.017		10.9.1.17(13188)	64	28A4	->	170.225.15.117(21)		TCP/FTP A
6	6	0.147.421		10.9.1.17(13188)	45		<-	170.225.15.117(21)	3BCA	TCP/FTP/220-business AP
7	7	0.000.014		10.9.1.17(13188)	64	28AC	->	170.225.15.117(21)		TCP/FTP A
8	8	0.202.356		10.9.1.17(13188)	64	28B4	->	170.225.15.117(21)		TCP/FTP/AUTH AP
9	9	0.146.597		10.9.1.17(13188)	45		<-	170.225.15.117(21)	3F83	TCP/FTP/234 AP
10	10	0.000.022		10.9.1.17(13188)	64	28B5	->	170.225.15.117(21)		TCP/FTP AP
11	11	0.000.119		10.9.1.17(13188)	64	28B6	->	170.225.15.117(21)		TCP/FTP AP Client_Hello
12	12	0.146.259		10.9.1.17(13188)	45		<-	170.225.15.117(21)	4102	TCP/FTP AP Alert:handshake_
13	13	0.000.010		10.9.1.17(13188)	64	28C9	->	170.225.15.117(21)		TCP/FTP AP
14	14	0.000.335		10.9.1.17(13188)	45		<-	170.225.15.117(21)	4103	TCP/FTP AF
15	15	0.000.003		10.9.1.17(13188)	64	28CA	->	170.225.15.117(21)		TCP/FTP AP
16	16	0.000.248		10.9.1.17(13188)	64	28CB	->	170.225.15.117(21)		TCP/FTP AFP
17	17	0.148.572		10.9.1.17(13188)	45		<-	170.225.15.117(21)	423E	TCP/FTP A

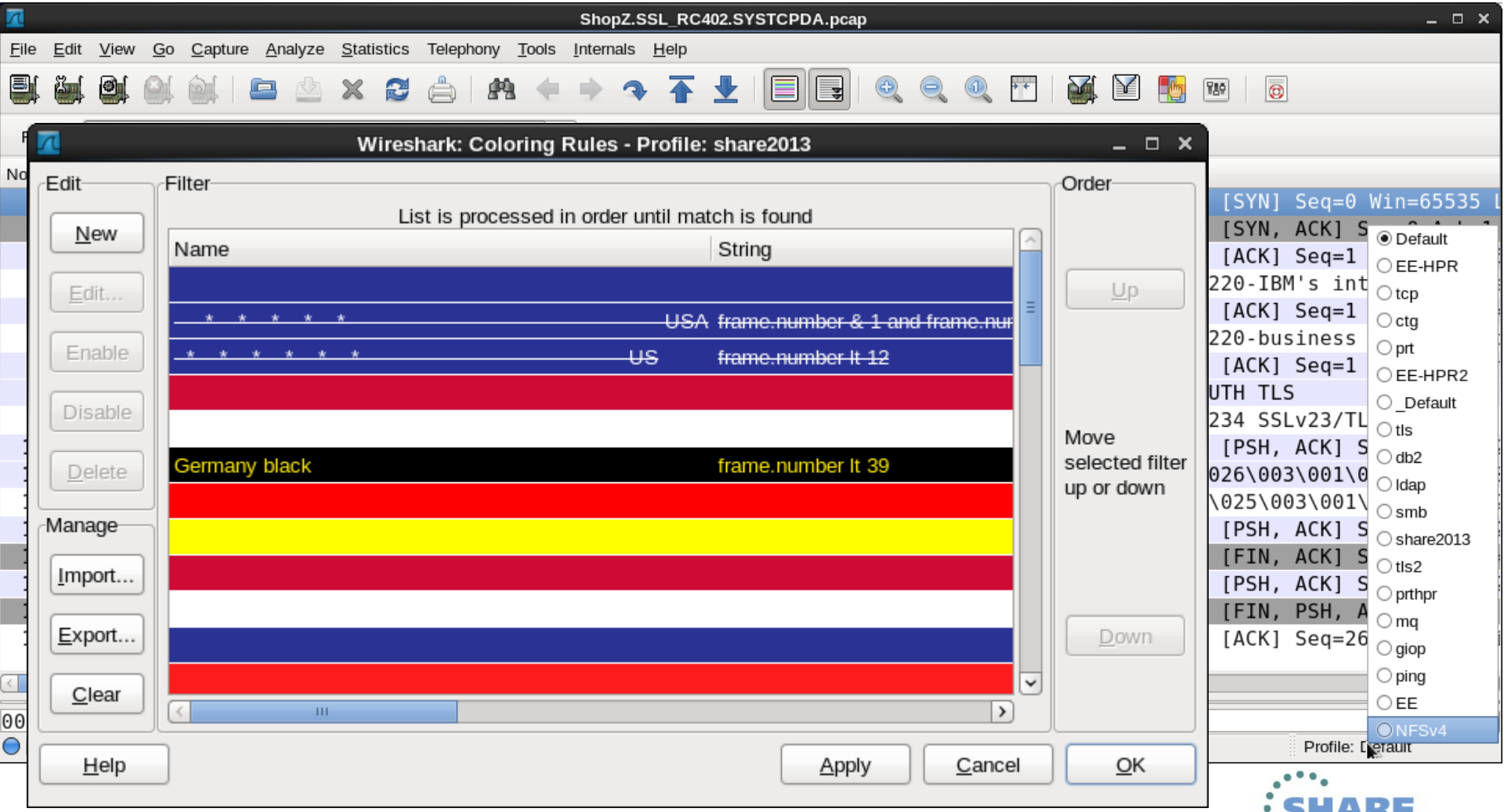
Taming the Shark – Lab Session at 4:30PM
Get some hands-on experience with profiles

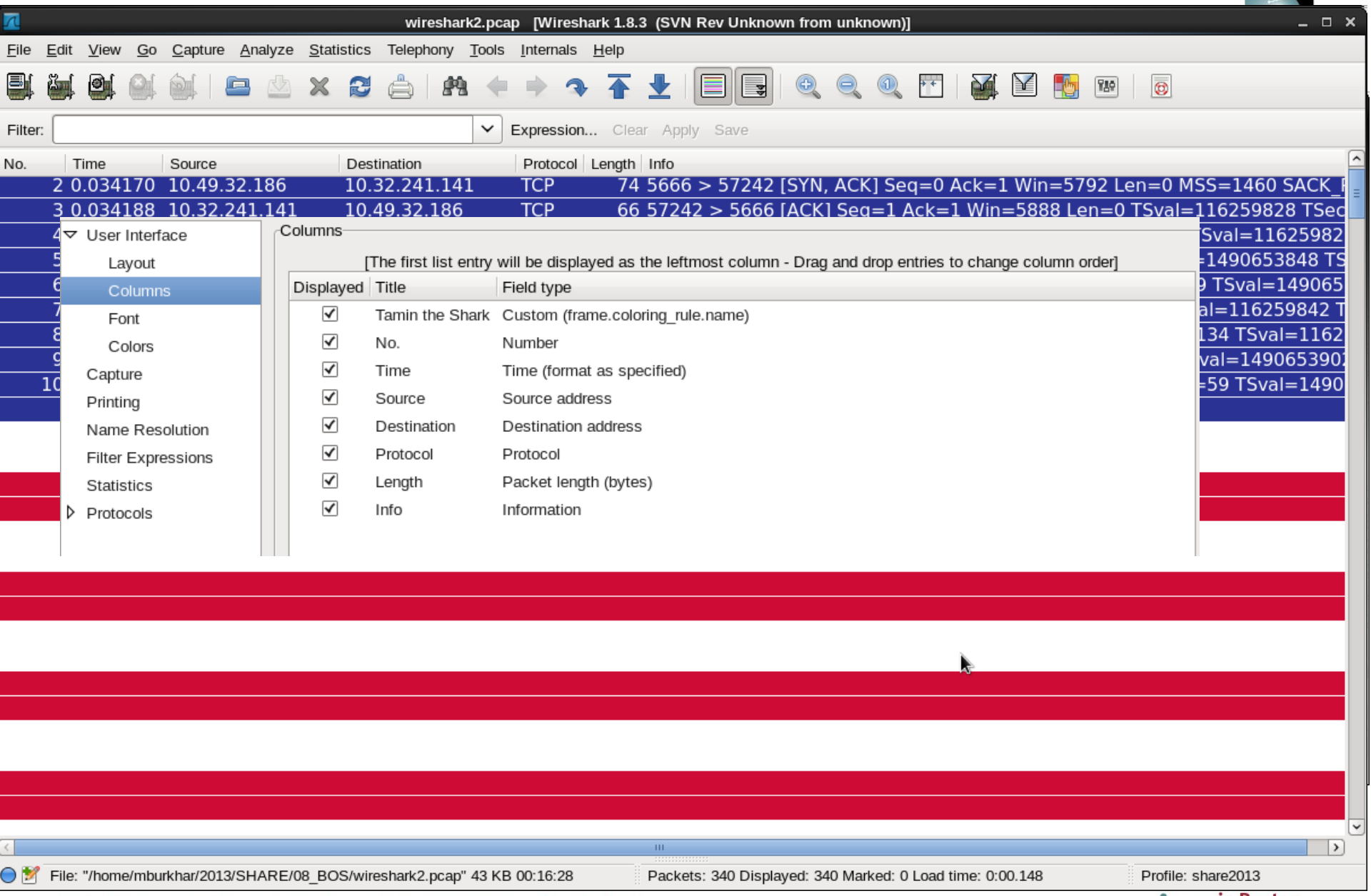


Get some hands-on experience with profiles



Thank You for your time!
Get some hands-on experience with profiles




wireshark2.pcap [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
2 0.034170 10.49.32.186 10.32.241.141 TCP 74 5666 > 57242 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_
3 0.034188 10.32.241.141 10.49.32.186 TCP 66 57242 > 5666 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=116259828 TSec
User Interface
Layout
Columns
Font
Colors
Capture
Printing
Name Resolution
Filter Expressions
Statistics
Protocols
Columns
[The first list entry will be displayed as the leftmost column - Drag and drop entries to change column order]
Displayed Title Field type
Tamin the Shark Custom (frame.coloring_rule.name)
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
File: "/home/mburkhar/2013/SHARE/08_BOS/wireshark2.pcap" 43 KB 00:16:28
Packets: 340 Displayed: 340 Marked: 0 Load time: 0:00.148
Profile: share2013