

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



IBM Technical Support Services



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
????????3??R??E?C~{!I"b(?wvs?$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

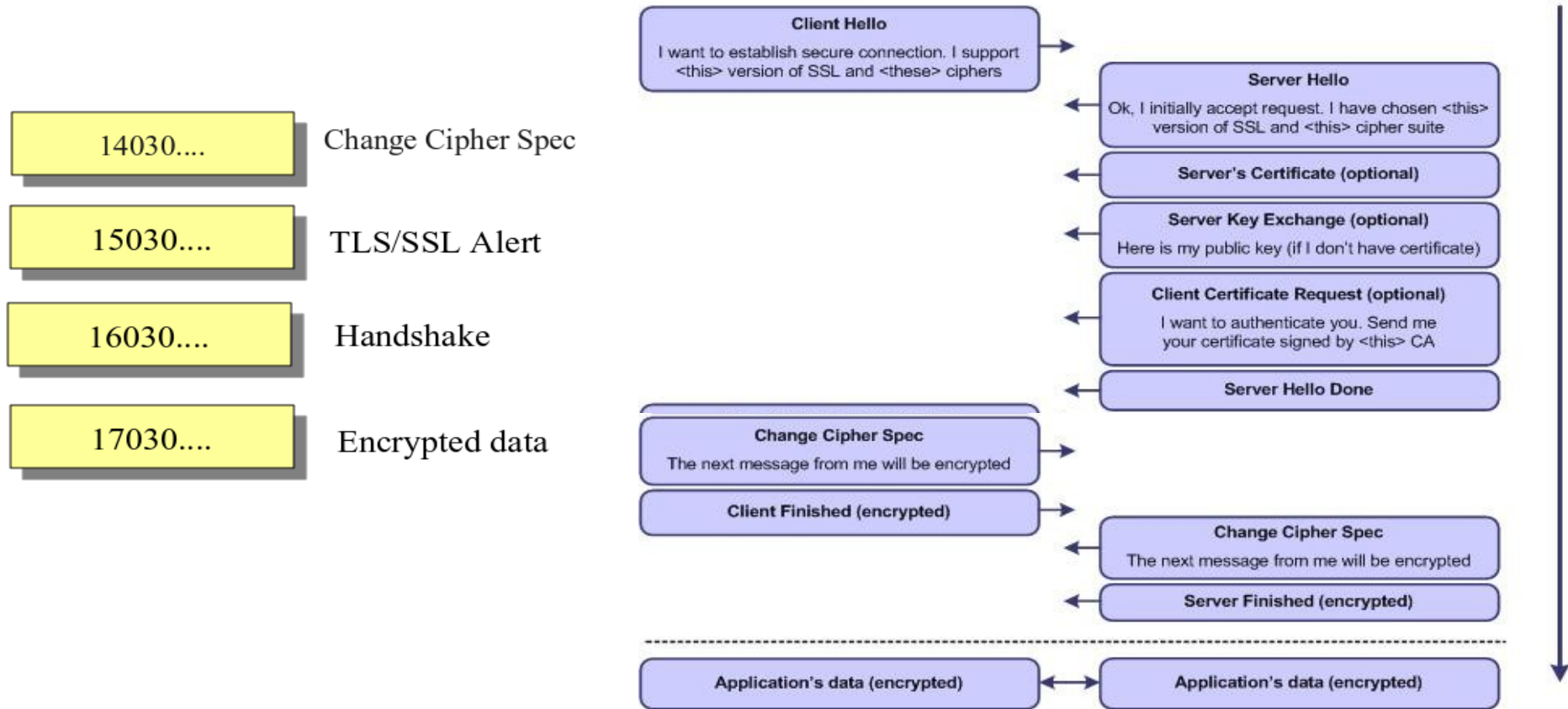
```

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



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
????????3??R??E?C~{!I"b(?wvs?$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..ç..ç..!÷.Í..!.....á...q... .đ©...i÷.Í.d...A'u...μ...í%...Đ...../.....
ê..D..Â".....!÷.Í..!.....á...£...±¿i÷.Í.....d...J..A'v-.....À
ê..D..Âđ.....!÷.Í..!.....á...~... .đx...i÷.Í.d...A'v...J.&...v..
ê..D..®Û...`...`...!÷.Í..!.....á...β... .ýDi÷.Í.....d...J..A'v&... '.....ñâ(.Ë.Ñ>ÉÁÊ>/%.Ë`
ê..D..^.....!÷.Í..!.....á...u... .đ~...i÷.Í.d...A'v...JÁ&...Â..
ê..E..[z..0..S..!÷.Í..!.....á..M..-...»²i÷.Í.....d...JÁ.A'v&...«E.....ÁÍËÑ>ÁËË.?É.Ã?Ê.ø
ê..E..[¼.....!÷.Í..!.....á...Đ... .đ©...i÷.Í.d...A'v...K.&...¶..
ê..E..D.....!÷.Í..!.....á...©... .đs...i÷.Í.d...A'v...K.&...í...ièç.è<è..
ê..E..}...ç...ç...!÷.Í..!.....á...c...hôi÷.Í.....d...K..A'®&...θ;.....ëë<Î...è<ëÎ...
ê..E..W.....!÷.Í..!.....á...§... .đ¿...i÷.Í.d...A'®...K.&...k..
ê..E..).....Ê...Ê...!÷.Í..!.....á...À.¶... .đ>...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... .đp...i÷.Í.d...A'Ô...K.&...|..
ê..E.....!÷.Í..!.....á...g)i÷.Í.....d...K..A'Ô&...î..
ê..E.....!÷.Í..!.....á...-... .đo...i÷.Í.d...A'Ô...K.&...+..
ê..E.....!÷.Í..!.....á...ô... .đn...i÷.Í.d...A'Ô...K.&...(..
ê..E..c-.....!÷.Í..!.....á...â...f.i÷.Í.....d...K..A'Ô&...í..
```

***** Bottom of Data ***



The Default Profile

Only basic information about each packet



ShopZ.SSL_RC402.SYSTCPDA.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
1	0.00000	10.9.1.17	170.225.15.117	TCP	74	13188 > ftp [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=32 TSval=371220
2	0.14685	170.225.15.117	10.9.1.17	TCP	58	ftp > 13188 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380
3	0.00001	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.14961	170.225.15.117	10.9.1.17	FTP	121	Response: 220-IBM's internal systems must only be used for conducti
5	0.00001	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [ACK] Seq=1 Ack=68 Win=65535 Len=0
6	0.14742	170.225.15.117	10.9.1.17	FTP	226	Response: 220-business or for purposes authorized by IBM management
7	0.00001	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [ACK] Seq=1 Ack=240 Win=65535 Len=0
8	0.20235	10.9.1.17	170.225.15.117	FTP	64	Request: AUTH TLS
9	0.14659	170.225.15.117	10.9.1.17	FTP	72	Response: 234 SSLv23/TLSv1
10	0.00002	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [PSH, ACK] Seq=11 Ack=258 Win=65535 Len=0
11	0.00011	10.9.1.17	170.225.15.117	FTP	114	Request: \026\003\001\0007\001\000\0003\003\001R\001\a\305\213C\376
12	0.14625	170.225.15.117	10.9.1.17	FTP	61	Response: \025\003\001\000\002\002(
13	0.00001	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [PSH, ACK] Seq=71 Ack=265 Win=65535 Len=0
14	0.00033	170.225.15.117	10.9.1.17	TCP	54	ftp > 13188 [FIN, ACK] Seq=265 Ack=71 Win=65535 Len=0
15	0.00000	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [PSH, ACK] Seq=71 Ack=266 Win=65535 Len=0
16	0.00024	10.9.1.17	170.225.15.117	TCP	54	13188 > ftp [FIN, PSH, ACK] Seq=71 Ack=266 Win=65535 Len=0
17	0.14857	170.225.15.117	10.9.1.17	TCP	54	ftp > 13188 [ACK] Seq=266 Ack=72 Win=65535 Len=0

0000 08 00 5a e1 0f 75 08 00 5a 09 01 11 08 00 45 00 ..Z..u.. Z....E.

File: "/home/mburkhar/2013/SHARE/08_BOS/ShopZ.SSL_RC402.SYSTCPDA.pcap" ... Packets: 17 Displayed: 17 Marked: 0 Load time: 0:00.060 Profile: Default



Default Profile

Adding columns to the packet list



ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save EE_Only ICMP Errors

No.	Time	ip.id	ip.len	Prot	SrcMAC	Source	TTL	Destination	src_port	dst_port	tcp_ws	Info
1	0.0000	Internet Protocol Version 4 Identification (ip.id)		TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [SYN] Seq=0 Win=65535
2	0.1414			TCP	zOS_SYSTCPDA_	shopz-FTP	64	zOS-Client	21	13188	65535	21 > 13188 [SYN, ACK] Seq=0 Ack=1
3	0.000013	0x28a1	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [ACK] Seq=1 Ack=1 Win=6
4	0.149615	0x3a59	107	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 220-IBM's internal syste
5	0.000017	0x28a4	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [ACK] Seq=1 Ack=68 Win=
6	0.147421	0x3bca	212	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 220-business or for purp
7	0.000014	0x28ac	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [ACK] Seq=1 Ack=240 Wir
8	0.202356	0x28b4	50	FTP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	Request: AUTH TLS
9	0.146597	0x3f83	58	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 234 SSLv23/TLSv1
10	0.000022	0x28b5	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [PSH, ACK] Seq=11 Ack=2
11	0.000119	0x28b6	100	FTP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	Request: \026\003\001\0007\001\000
12	0.146259	0x4102	47	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: \025\003\001\000\002\002
13	0.000010	0x28c9	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [PSH, ACK] Seq=71 Ack=2
14	0.000335	0x4103	40	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	21 > 13188 [FIN, ACK] Seq=265 Ack=
15	0.000003	0x28ca	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [PSH, ACK] Seq=71 Ack=2
16	0.000248	0x28cb	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [FIN, PSH, ACK] Seq=71
17	0.148572	0x423e	40	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	21 > 13188 [ACK] Seq=266 Ack=72 W

0000 08 00 5a e1 0f 75 08 00 5a 09 01 11 08 00 45 00 ..Z..u.. Z....E.

File: "/home/mburkhar/2013/SHARE/08_BOS/ShopZ.SSL_RC402.SYSTCPDA.pcap" ... Packets: 17 Displayed: 17 Marked: 0 Load time: 0:00.000 Profile: Default



Why use different profiles?

A trace is a trace is a trace – isn't it?



ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save EE_Only ICMP Errors

No.	Time	ip.id	ip.len	Prot	SrcMAC	Source	TTL	Destination	src_port	dst_port	tcp_ws	Info
1	0.000000	0x2898	60	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [SYN] Seq=0 Win=65535 L
2	0.146856	0x38b1	44	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	21 > 13188 [SYN, ACK] Seq=0 Ack=1
3	0.000013	0x28a1	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [ACK] Seq=1 Ack=1 Win=6
4	0.149615	0x3a59	107	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 220-IBM's internal syste
5	0.000017	0x28a4	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [ACK] Seq=1 Ack=68 Win=
6	0.147421	0x3bca	212	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 220-business or for purp
7	0.000014	0x28ac	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [ACK] Seq=1 Ack=240 Wir
8	0.202356	0x28b4	50	FTP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	Request: AUTH TLS
9	0.146597	0x3f83	58	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 234 SSLv23/TLSv1
10	0.000022	0x28b5	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [PSH, ACK] Seq=11 Ack=2
11	0.000119	0x28b6	100	FTP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	Request: \026\003\001\0007\001\000
12	0.146259	0x4102	47	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: \025\003\001\000\002\002
13	0.000010	0x28c9	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [PSH, ACK] Seq=71 Ack=2
14	0.000335	0x4103	40	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	21 > 13188 [FIN, ACK] Seq=265 Ack=
15	0.000003	0x28ca	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [PSH, ACK] Seq=71 Ack=2
16	0.000248	0x28cb	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	13188 > 21 [FIN, PSH, ACK] Seq=71
17	0.148572	0x423e	40	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	21 > 13188 [ACK] Seq=266 Ack=72 W

0000 08 00 5a e1 0f 75 08 00 5a 09 01 11 08 00 45 00 ..Z..u.. Z....E.

File: "/home/mburkhar/2013/SHARE/08_BOS/ShopZ.SSL_RC402.SYSTCPDA.pcap" ... Packets: 17 Displayed: 17 Marked: 0 Load time: 0:00.000 Profile: Default



Why use different profiles?

A trace is a trace is a trace – isn't it?

ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save 3way_HS rxmit TLS TLS_hidden

No.	Time	delta	TTL	Source	s_port	d_port	tcp.len	ACKed	RTT	whazzin	Info
1	16:27:16.600	0.000	64	zOS-Client	13188	21	0			p0f zOS Tstamp 65535:64:1:60:M*,N,W*,N,N,T	13188 > 21
2	16:27:16.747	0.146	45	shopz-FTP	2113188	21	0	1	0.146	p0f_AIX 65535:60:1:44:M*	21 > 13188
3	16:27:16.747	0.000	64	zOS-Client	13188	21	0	2	0.000	zOS ACK	13188 > 21
4	16:27:16.897	0.149	45	shopz-FTP	2113188	21	67			FTP-220 Welcome	Response: 2
5	16:27:16.897	0.000	64	zOS-Client	13188	21	0	4	0.000	zOS ACK	13188 > 21
6	16:27:17.044	0.147	45	shopz-FTP	2113188	21	172			FTP-220 Welcome	Response: 2
7	16:27:17.044	0.000	64	zOS-Client	13188	21	0	6	0.000	zOS ACK	13188 > 21
8	16:27:17.246	0.202	64	zOS-Client	13188	21	10			FTP-CMD: AUTH TLS	Request: AU
9	16:27:17.393	0.146	45	shopz-FTP	2113188	21	18	8	0.146	FTP-234 SSL OK	Response: 2
10	16:27:17.393	0.000	64	zOS-Client	13188	21	0	9	0.000	zOS ACK	13188 > 21
11	16:27:17.393	0.000	64	zOS-Client	13188	21	60			TLS Client Hello	Request: \0
12	16:27:17.539	0.146	45	shopz-FTP	2113188	21	7	11	0.146	TLS Alert	Response: \
13	16:27:17.539	0.000	64	zOS-Client	13188	21	0	12	0.000	zOS ACK	13188 > 21
14	16:27:17.540	0.000	45	shopz-FTP	2113188	21	0			tcp_down	21 > 13188
15	16:27:17.540	0.000	64	zOS-Client	13188	21	0	14	0.000	zOS ACK	13188 > 21
16	16:27:17.540	0.000	64	zOS-Client	13188	21	0			tcp_down	13188 > 21
17	16:27:17.688	0.148	45	shopz-FTP	2113188	21	0	16	0.148		21 > 13188

File: "/home/mburkhar/2013/SHARE/08_BOS/ShopZ.SSL_RC402.SYSTCPDA.pcap" ... Packets: 17 Displayed: 17 Marked: 0 Load time: 0:00.000 Profile: tcp

Why use different profiles?

Added frame.coloring_rule.name



ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save 3way_HS rxmit TLS TLS_hidden

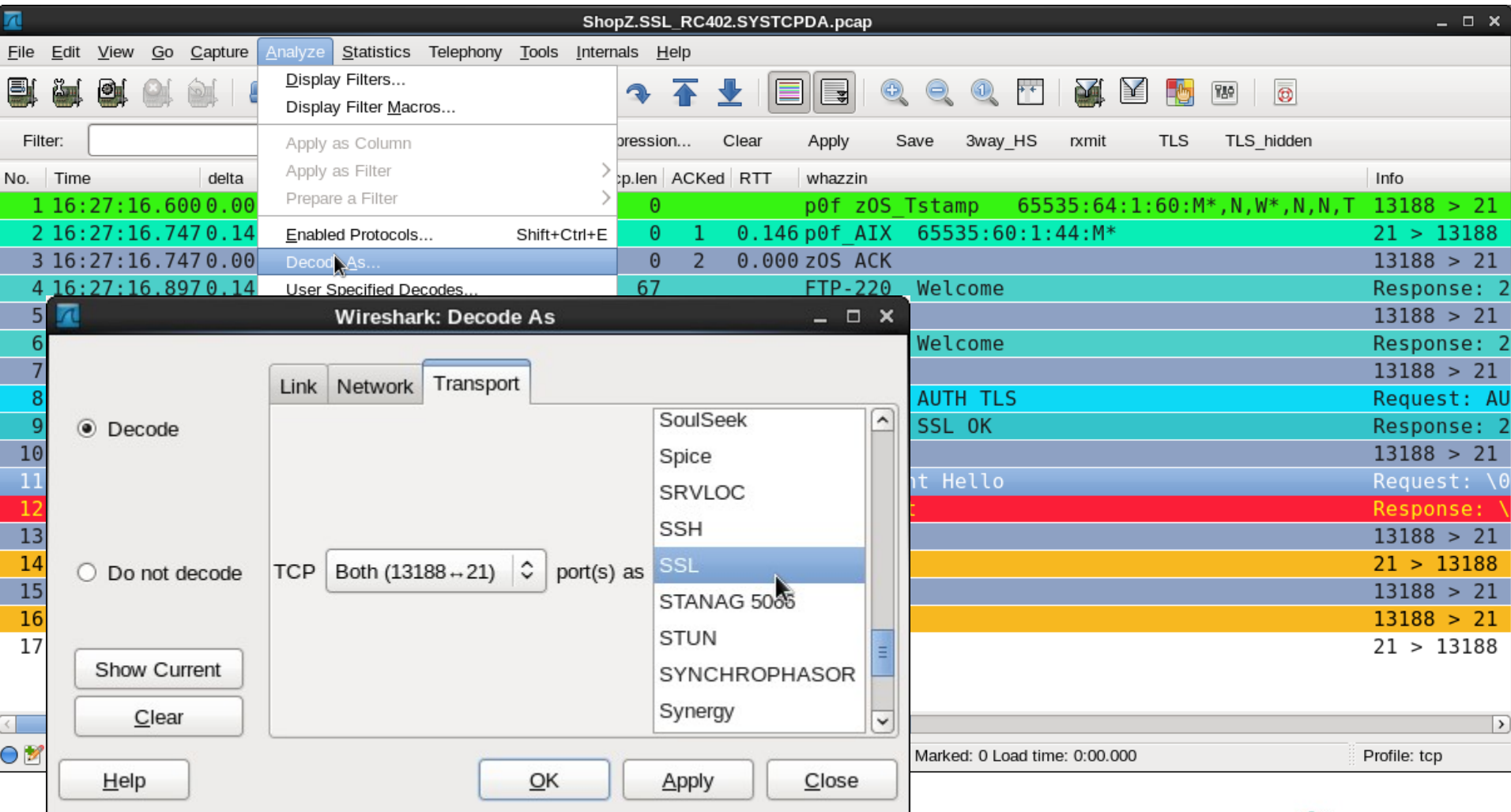
No.	Time	delta	TTL	Source	s_port	d_port	tcp.len	ACKed	RTT	whazzin	Info
1	16:27:16.600	0.000	64	zOS-Client	13188	21	0			p0f zOS	* ,N,N,T 13188 > 21
2	16:27:16.747	0.146	45	shopz-FTP	2113188		0	1	0.146	p0f_AIX	Coloring Rule Name (frame.coloring_rule.name) 21 > 13188
3	16:27:16.747	0.000	64	zOS-Client	13188	21	0	2	0.000	zOS ACK	13188 > 21
4	16:27:16.897	0.149	45	shopz-FTP	2113188		67			FTP-220 Welcome	Response: 2
5	16:27:16.897	0.000	64	zOS-Client	13188	21	0	4	0.000	zOS ACK	13188 > 21
6	16:27:17.044	0.147	45	shopz-FTP	2113188		172			FTP-220 Welcome	Response: 2
7	16:27:17.044	0.000	64	zOS-Client	13188	21	0	6	0.000	zOS ACK	13188 > 21
8	16:27:17.246	0.202	64	zOS-Client	13188	21	10			FTP-CMD: AUTH TLS	Request: AU
9	16:27:17.393	0.146	45	shopz-FTP	2113188		18	8	0.146	FTP-234 SSL OK	Response: 2
10	16:27:17.393	0.000	64	zOS-Client	13188	21	0	9	0.000	zOS ACK	13188 > 21
11	16:27:17.393	0.000	64	zOS-Client	13188	21	60			TLS Client Hello	Request: \0
12	16:27:17.539	0.146	45	shopz-FTP	2113188		7	11	0.146	TLS Alert	Response: \
13	16:27:17.539	0.000	64	zOS-Client	13188	21	0	12	0.000	zOS ACK	13188 > 21
14	16:27:17.540	0.000	45	shopz-FTP	2113188		0			tcp_down	21 > 13188
15	16:27:17.540	0.000	64	zOS-Client	13188	21	0	14	0.000	zOS ACK	13188 > 21
16	16:27:17.540	0.000	64	zOS-Client	13188	21	0			tcp_down	13188 > 21
17	16:27:17.688	0.148	45	shopz-FTP	2113188		0	16	0.148		21 > 13188

File: "/home/mburkhar/2013/SHARE/08_BOS/ShopZ.SSL_RC402.SYSTCPDA.pcap" ... Packets: 17 Displayed: 17 Marked: 0 Load time: 0:00.000 Profile: tcp



Map another protocol to well known port

Analyze → Decode As

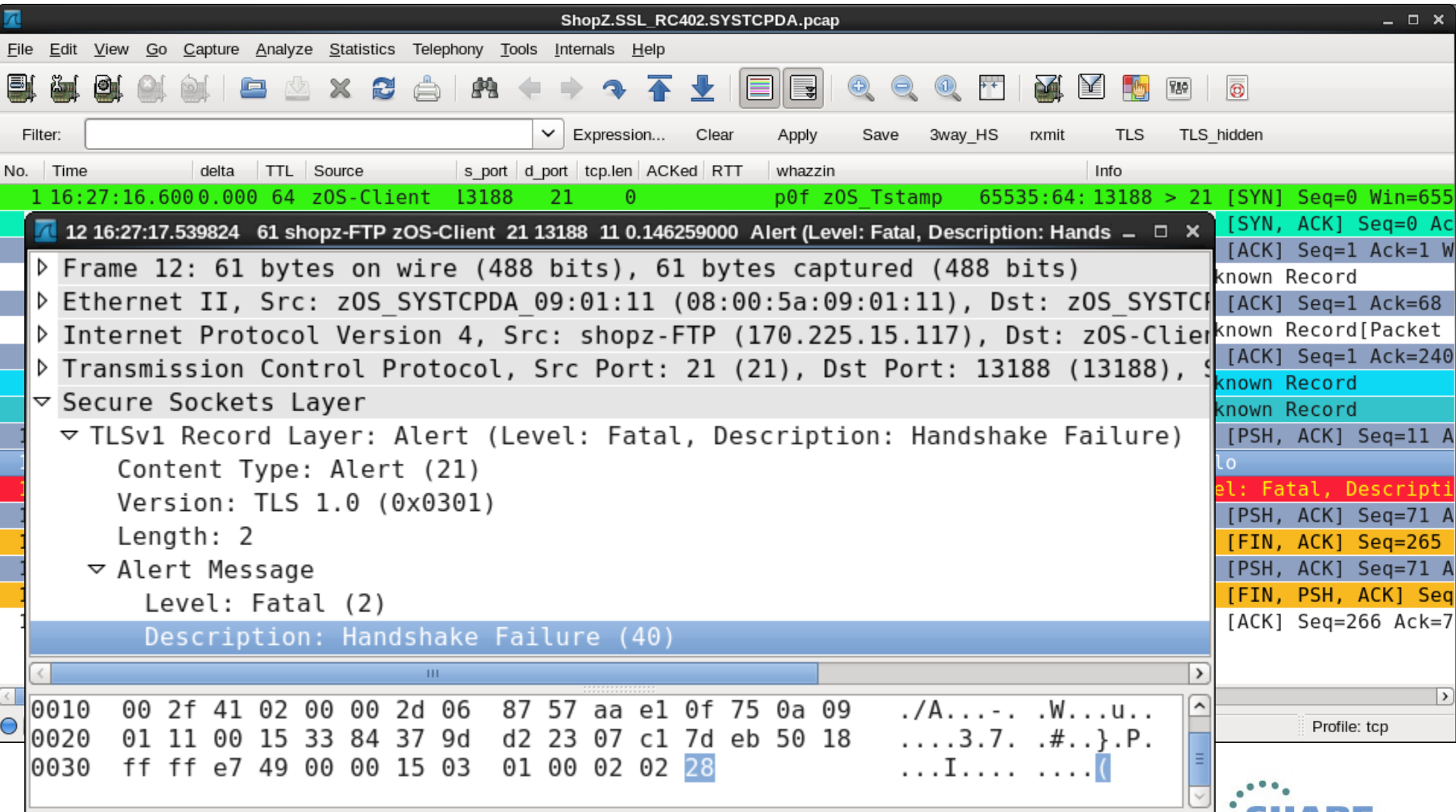


The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture for 'ShopZ.SSL_RC402.SYSTCPDA.pcap'. The packet list pane shows several packets, with packet 4 selected. The packet details pane shows the selected packet's structure, including 'zOS ACK' and 'FTP-220 Welcome'. The 'Analyze' menu is open, and the 'Decode As...' option is selected. A dialog box titled 'Wireshark: Decode As' is open, showing the 'Transport' tab. The 'Decode' radio button is selected. The 'TCP Both (13188 ↔ 21)' port pair is selected, and the 'port(s) as' dropdown menu is open, showing a list of protocols with 'SSL' selected. The 'Show Current' and 'Clear' buttons are visible, along with 'OK', 'Apply', and 'Close' buttons at the bottom of the dialog.

No.	Time	delta	Protocol	Length	ACKed	RTT	whazzin	Info
1	16:27:16.600	0.00		0			p0f zOS Tstamp 65535:64:1:60:M*,N,W*,N,N,T	13188 > 21
2	16:27:16.747	0.14		0	1	0.146	p0f_AIX 65535:60:1:44:M*	21 > 13188
3	16:27:16.747	0.00		0	2	0.000	zOS ACK	13188 > 21
4	16:27:16.897	0.14		67			FTP-220 Welcome	Response: 2

TLS Alert

Fatal Handshake Failure



The image shows a Wireshark packet capture analysis of a TLS fatal handshake failure. The main window displays the packet list, packet details, and packet bytes. The packet list shows a packet at time 12.16.27:17.539824 from shopz-FTP to zOS-Client, which is an alert. The packet details pane shows the TLSv1 Record Layer with an alert message of level Fatal (2) and description Handshake Failure (40). The packet bytes pane shows the raw data in hexadecimal and ASCII.

ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save 3way_HS rxmit TLS TLS_hidden

No.	Time	delta	TTL	Source	s_port	d_port	tcp.len	ACKed	RTT	whazzin	Info
1	16:27:16.600	0.000	64	zOS-Client	13188	21	0			p0f zOS Tstamp 65535:64:13188 > 21	[SYN] Seq=0 Win=655
12	16:27:17.539824	61	shopz-FTP	zOS-Client	21	13188	11	0.146259000		Alert (Level: Fatal, Description: Hands	[SYN, ACK] Seq=0 Ac

Frame 12: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)

Ethernet II, Src: zOS_SYSTCPDA_09:01:11 (08:00:5a:09:01:11), Dst: zOS_SYSTCPDA_09:01:11 (08:00:5a:09:01:11)

Internet Protocol Version 4, Src: shopz-FTP (170.225.15.117), Dst: zOS-Client (170.225.15.117)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 13188 (13188), Seq: 11, Len: 61

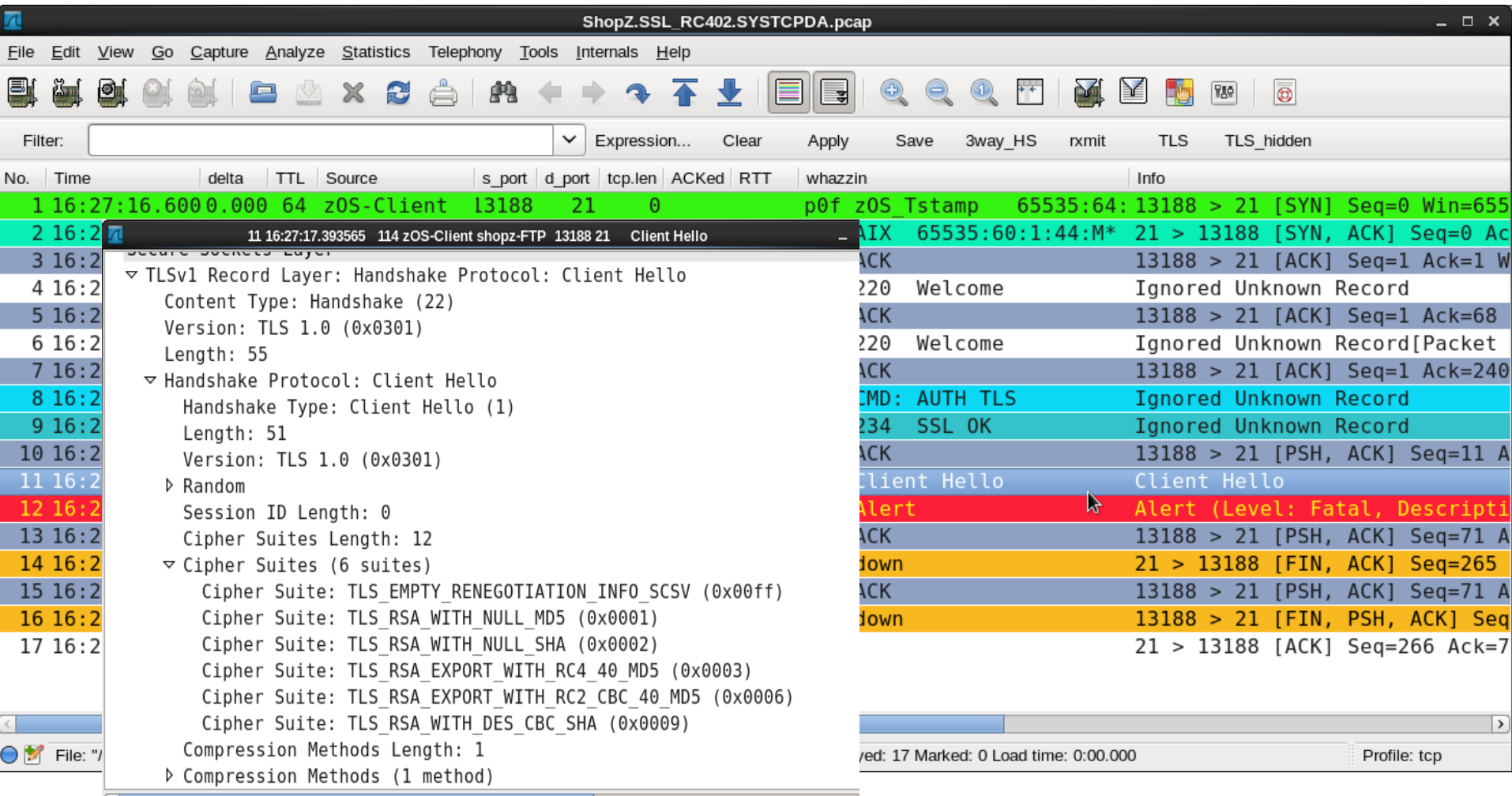
Secure Sockets Layer

- TLSv1 Record Layer: Alert (Level: Fatal, Description: Handshake Failure)
 - Content Type: Alert (21)
 - Version: TLS 1.0 (0x0301)
 - Length: 2
 - Alert Message
 - Level: Fatal (2)
 - Description: Handshake Failure (40)

```
0010  00 2f 41 02 00 00 2d 06  87 57 aa e1 0f 75 0a 09  ./A...-. .W...u..
0020  01 11 00 15 33 84 37 9d  d2 23 07 c1 7d eb 50 18  ....3.7. .#...}.P.
0030  ff ff e7 49 00 00 15 03  01 00 02 02 28          ...I.... (
```

TLS Handshake Protocol

Client Hello offering Cipher Suites



ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save 3way_HS rxmit TLS TLS_hidden

No.	Time	delta	TTL	Source	s_port	d_port	tcp.len	ACKed	RTT	whazzin	Info
1	16:27:16.600	0.000	64	zOS-Client	13188	21	0			p0f zOS Tstamp 65535:64:13188 > 21	[SYN] Seq=0 Win=655
2	16:27:16.600	0.000	64	zOS-Client	13188	21	0			p0f zOS Tstamp 65535:60:1:44:M*	21 > 13188 [SYN, ACK] Seq=0 Ac
3	16:27:16.600	0.000	64	zOS-Client	13188	21	0			ACK	13188 > 21 [ACK] Seq=1 Ack=1 W
4	16:27:16.600	0.000	64	zOS-Client	13188	21	0			220 Welcome	Ignored Unknown Record
5	16:27:16.600	0.000	64	zOS-Client	13188	21	0			ACK	13188 > 21 [ACK] Seq=1 Ack=68
6	16:27:16.600	0.000	64	zOS-Client	13188	21	0			220 Welcome	Ignored Unknown Record[Packet
7	16:27:16.600	0.000	64	zOS-Client	13188	21	0			ACK	13188 > 21 [ACK] Seq=1 Ack=240
8	16:27:16.600	0.000	64	zOS-Client	13188	21	0			COMMAND: AUTH TLS	Ignored Unknown Record
9	16:27:16.600	0.000	64	zOS-Client	13188	21	0			234 SSL OK	Ignored Unknown Record
10	16:27:16.600	0.000	64	zOS-Client	13188	21	0			ACK	13188 > 21 [PSH, ACK] Seq=11 A
11	16:27:16.600	0.000	64	zOS-Client	13188	21	0			Client Hello	Client Hello
12	16:27:16.600	0.000	64	zOS-Client	13188	21	0			Alert	Alert (Level: Fatal, Descripti
13	16:27:16.600	0.000	64	zOS-Client	13188	21	0			ACK	13188 > 21 [PSH, ACK] Seq=71 A
14	16:27:16.600	0.000	64	zOS-Client	21	13188	0			down	21 > 13188 [FIN, ACK] Seq=265
15	16:27:16.600	0.000	64	zOS-Client	13188	21	0			ACK	13188 > 21 [PSH, ACK] Seq=71 A
16	16:27:16.600	0.000	64	zOS-Client	13188	21	0			down	13188 > 21 [FIN, PSH, ACK] Seq
17	16:27:16.600	0.000	64	zOS-Client	21	13188	0			ACK	21 > 13188 [ACK] Seq=266 Ack=7

red: 17 Marked: 0 Load time: 0:00.000 Profile: tcp

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 0A40338.
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

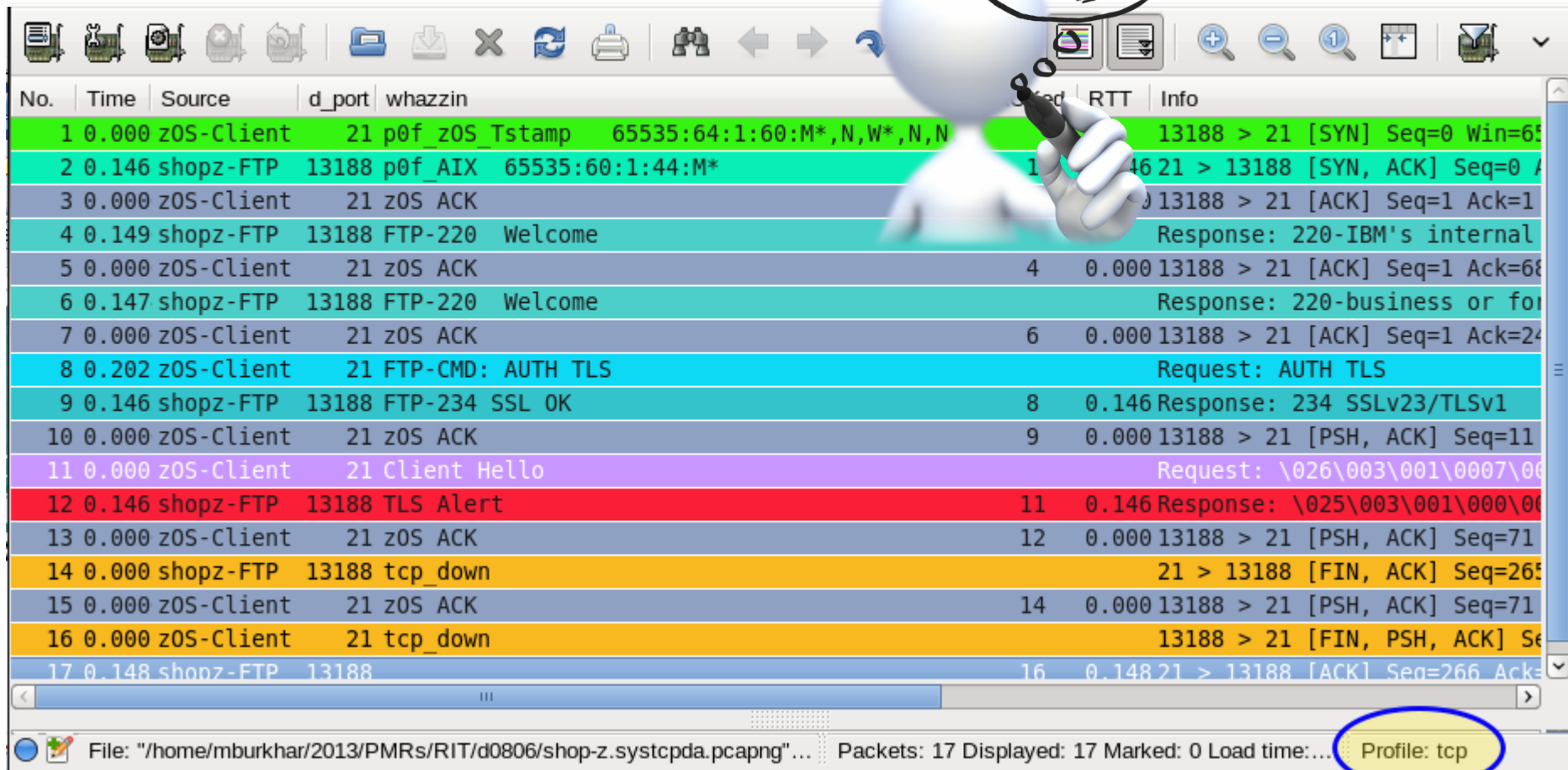
```

SRID: ATRDSB9FFJ8 Stat: OP1L1 PMR: 75741,010,010 Entitle: CCMS S* 1
Rqst: SOFTWARE SubRqst: SOFTWARE DEFECT SUPPORT *
Queu: 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,
____
.
+TIVOLI 20 -5655HAL00 -L25Z/CFEZDS-P4S4-13/08/14-10:32
+TIVOLI 20 -5655HAL00 -L25Z/CFEZDS-P4S4-13/08/14-10:32

```

Why use different profiles?

Show what's in there! Coloring Rules!

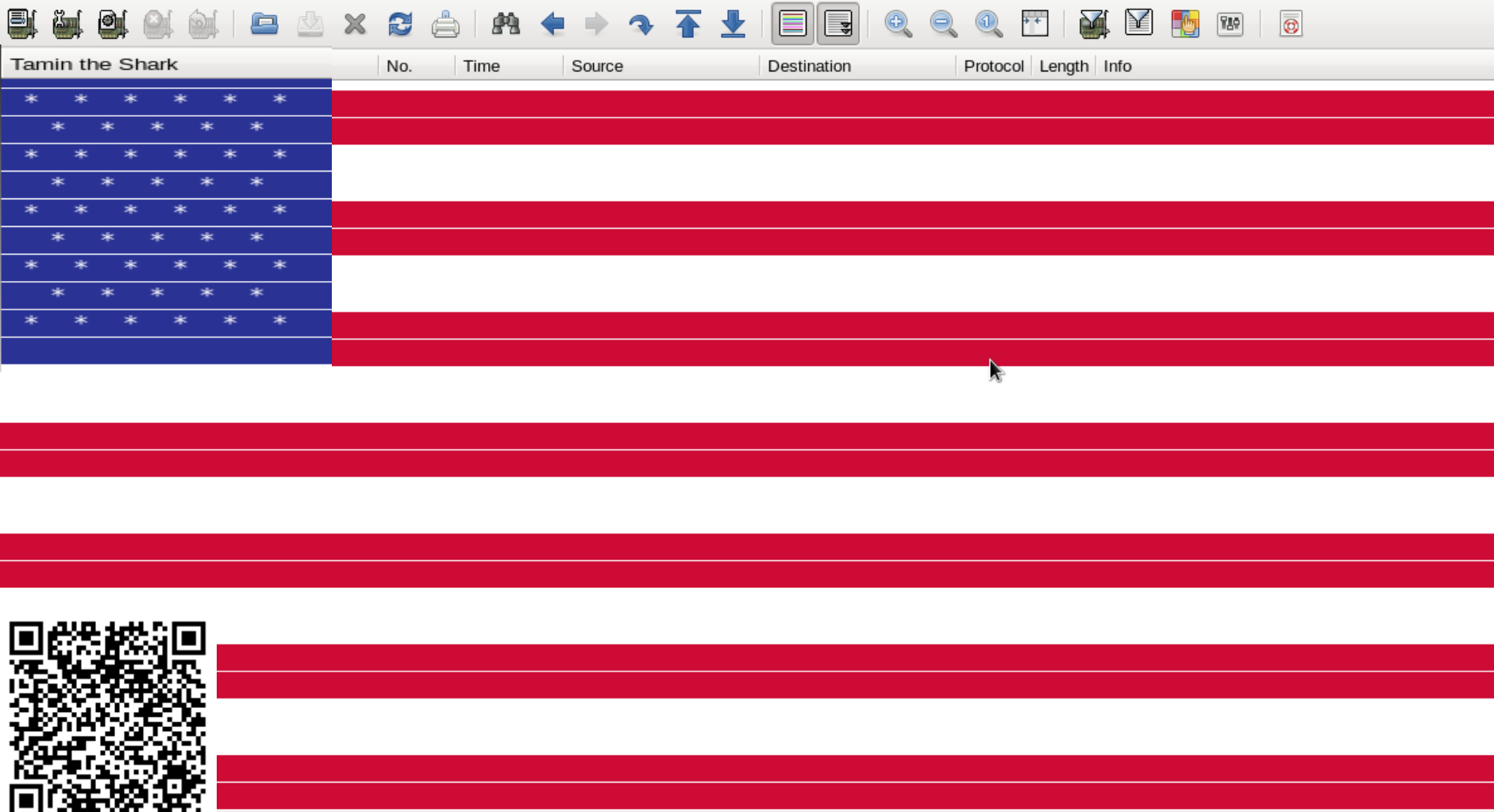


No.	Time	Source	d_port	whazzin	Seq	RTT	Info
1	0.000	zOS-Client	21	p0f_zOS_Tstamp	65535:64:1:60:M*,N,W*,N,N		13188 > 21 [SYN] Seq=0 Win=65
2	0.146	shopz-FTP	13188	p0f_AIX	65535:60:1:44:M*		13188 > 21 [SYN, ACK] Seq=0
3	0.000	zOS-Client	21	zOS ACK			13188 > 21 [ACK] Seq=1 Ack=1
4	0.149	shopz-FTP	13188	FTP-220	Welcome		Response: 220-IBM's internal
5	0.000	zOS-Client	21	zOS ACK		4	0.000 13188 > 21 [ACK] Seq=1 Ack=68
6	0.147	shopz-FTP	13188	FTP-220	Welcome		Response: 220-business or for
7	0.000	zOS-Client	21	zOS ACK		6	0.000 13188 > 21 [ACK] Seq=1 Ack=24
8	0.202	zOS-Client	21	FTP-CMD: AUTH TLS			Request: AUTH TLS
9	0.146	shopz-FTP	13188	FTP-234	SSL OK	8	0.146 Response: 234 SSLv23/TLSv1
10	0.000	zOS-Client	21	zOS ACK		9	0.000 13188 > 21 [PSH, ACK] Seq=11
11	0.000	zOS-Client	21	Client Hello			Request: \026\003\001\000\00
12	0.146	shopz-FTP	13188	TLS Alert		11	0.146 Response: \025\003\001\000\00
13	0.000	zOS-Client	21	zOS ACK		12	0.000 13188 > 21 [PSH, ACK] Seq=71
14	0.000	shopz-FTP	13188	tcp_down			21 > 13188 [FIN, ACK] Seq=265
15	0.000	zOS-Client	21	zOS ACK		14	0.000 13188 > 21 [PSH, ACK] Seq=71
16	0.000	zOS-Client	21	tcp_down			13188 > 21 [FIN, PSH, ACK] Seq=
17	0.148	shopz-FTP	13188			16	0.148 21 > 13188 [ACK] Seq=266 Ack=

File: "/home/mburkhar/2013/PMRs/RIT/d0806/shop-z.systcpda.pcapng" ... Packets: 17 Displayed: 17 Marked: 0 Load time: ... Profile: tcp

The United Colors of Wireshark

Join us at “Taming the Shark” at 4:30PM R202



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

<http://tinyurl.com/ipwizards>



Matthias Burkhard IBM Germany

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

2cIP 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



The image shows a Wireshark window titled 'shop-z.systcpda.pcapng'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help) and a toolbar with various icons. Below the toolbar is a packet list table with columns: No., Time, Source, d_port, whazzin, ACKed, RTT, and Info. The table contains 17 rows of network traffic data. At the bottom of the window, the status bar shows 'File: "/home/mburkhar/2013/PMRs/RIT/d0806/shop-z.systcpda.pcapng"... Packets: 17 Displayed: 17 Marked: 0 Load time: ... Profile: tcp'. The 'Profile: tcp' dropdown menu is circled in blue.

No.	Time	Source	d_port	whazzin	ACKed	RTT	Info
1	0.000	zOS-Client	21	p0f_zOS_Tstamp	65535:64:1:60:M*,N,W*,N,N,T		13188 > 21 [SYN] Seq=0 Win=65
2	0.146	shopz-FTP	13188	p0f_AIX	65535:60:1:44:M*	1	0.146 21 > 13188 [SYN, ACK] Seq=0 A
3	0.000	zOS-Client	21	zOS ACK		2	0.000 13188 > 21 [ACK] Seq=1 Ack=1
4	0.149	shopz-FTP	13188	FTP-220	Welcome		Response: 220-IBM's internal
5	0.000	zOS-Client	21	zOS ACK		4	0.000 13188 > 21 [ACK] Seq=1 Ack=68
6	0.147	shopz-FTP	13188	FTP-220	Welcome		Response: 220-business or fo
7	0.000	zOS-Client	21	zOS ACK		6	0.000 13188 > 21 [ACK] Seq=1 Ack=24
8	0.202	zOS-Client	21	FTP-CMD: AUTH TLS			Request: AUTH TLS
9	0.146	shopz-FTP	13188	FTP-234	SSL OK	8	0.146 Response: 234 SSLv23/TLSv1
10	0.000	zOS-Client	21	zOS ACK		9	0.000 13188 > 21 [PSH, ACK] Seq=11
11	0.000	zOS-Client	21	Client Hello			Request: \026\003\001\000\00
12	0.146	shopz-FTP	13188	TLS Alert		11	0.146 Response: \025\003\001\000\00
13	0.000	zOS-Client	21	zOS ACK		12	0.000 13188 > 21 [PSH, ACK] Seq=71
14	0.000	shopz-FTP	13188	tcp_down			21 > 13188 [FIN, ACK] Seq=265
15	0.000	zOS-Client	21	zOS ACK		14	0.000 13188 > 21 [PSH, ACK] Seq=71
16	0.000	zOS-Client	21	tcp_down			13188 > 21 [FIN, PSH, ACK] Se
17	0.148	shopz-FTP	13188			16	0.148 21 > 13188 [ACK] Seq=266 Ack



Get some hands-on experience with profiles



ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save EE_Only ICMP Errors

No.	Time	ip.id	ip.len	Prot	SrcMAC	Source	TTL	Destination	src_port	dst_port	tcp_ws	Info
1	0.000000	0x2898	60	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[SYN] Seq=0 Win=65535
2	0.146856	0x38b1	44	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535 21 > 13188	[SYN, ACK] Seq=0 Ack=1
3	0.000013	0x28a1	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[ACK] Seq=1
4	0.149615	0x3a59	107	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 220-IBM's int
5	0.000017	0x28a4	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[ACK] Seq=1
6	0.147421	0x3bca	212	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 220-business
7	0.000014	0x28ac	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[ACK] Seq=1
8	0.202356	0x28b4	50	FTP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	Request: AUTH TLS
9	0.146597	0x3f83	58	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: 234 SSLv23/TL
10	0.000022	0x28b5	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[PSH, ACK] S
11	0.000119	0x28b6	100	FTP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535	Request: \026\003\001\0
12	0.146259	0x4102	47	FTP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535	Response: \025\003\001\
13	0.000010	0x28c9	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[PSH, ACK] S
14	0.000335	0x4103	40	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535 21 > 13188	[FIN, ACK] S
15	0.000003	0x28ca	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[PSH, ACK] S
16	0.000248	0x28cb	40	TCP	zOS_SYSTCPDA_	zOS-Client	64	shopz-FTP	13188	21	65535 13188 > 21	[FIN, PSH, A
17	0.148572	0x423e	40	TCP	zOS_SYSTCPDA_	shopz-FTP	45	zOS-Client	21	13188	65535 21 > 13188	[ACK] Seq=26

0000 08 00 5a e1 0f 75 08 00 5a 09 01 11 08 00 45 00 ..Z..u.. Z....E.

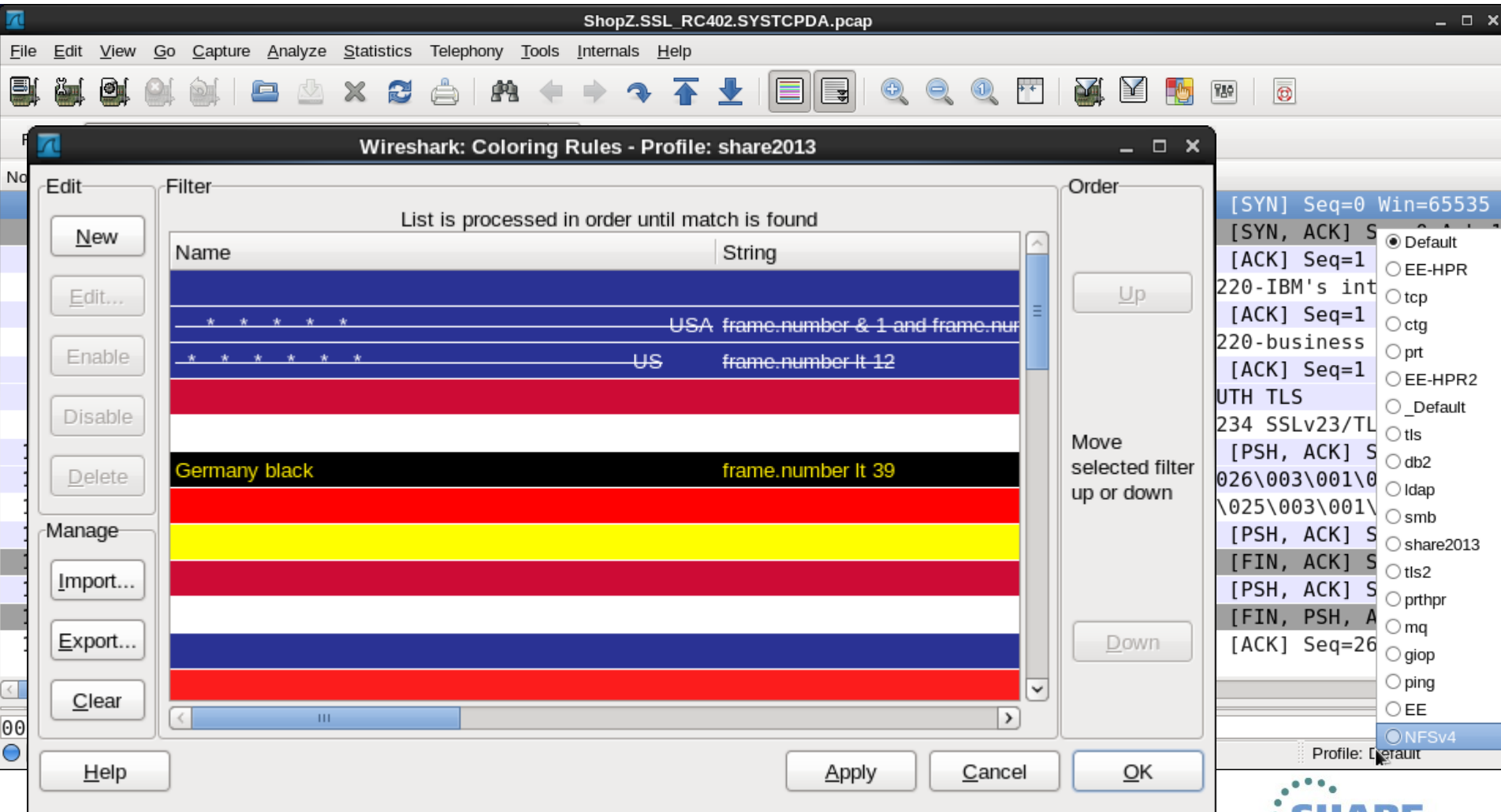
File: "/home/mburkhar/2013/SHARE/08_BOS/ShopZ.SSL_RC402.SYSTCPDA.pcap" ... Packets: 17 Displayed: 17 Marked: 0 Load time: 0:00.000 Profile: D

- Default
- EE-HPR
- tcp
- ctg
- prt
- EE-HPR2
- _Default
- tfs
- db2
- ldap
- smb
- share2013
- tfs2
- prthpr
- mq
- giop
- ping
- EE
- NFSv4



Thank You for your time!

Get some hands-on experience with profiles



ShopZ.SSL_RC402.SYSTCPDA.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Wireshark: Coloring Rules - Profile: share2013

List is processed in order until match is found

Name	String
	USA frame.number & 1 and frame.number < 12
	US frame.number lt 12
Germany black	frame.number lt 39

Order

Up

Move selected filter up or down

Down

Apply Cancel OK

[SYN] Seq=0 Win=65535
[SYN, ACK] S
[ACK] Seq=1
220-IBM's int
[ACK] Seq=1
220-business
[ACK] Seq=1
UTH TLS
234 SSLv23/TL
[PSH, ACK] S
026\003\001\0
\025\003\001\
[PSH, ACK] S
[FIN, ACK] S
[PSH, ACK] S
[FIN, PSH, A
[ACK] Seq=26

Profile: Default

- Default
- EE-HPR
- tcp
- ctg
- prt
- EE-HPR2
- _Default
- tis
- db2
- ldap
- smb
- share2013
- tis2
- prthpr
- mq
- giop
- ping
- EE
- NFSv4
- Default

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_F
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
<input checked="" type="checkbox"/>	Tamin the Shark	Custom (frame.coloring_rule.name)
<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"/>	Destination	Destination address
<input checked="" type="checkbox"/>	Protocol	Protocol
<input checked="" type="checkbox"/>	Length	Packet length (bytes)
<input checked="" type="checkbox"/>	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