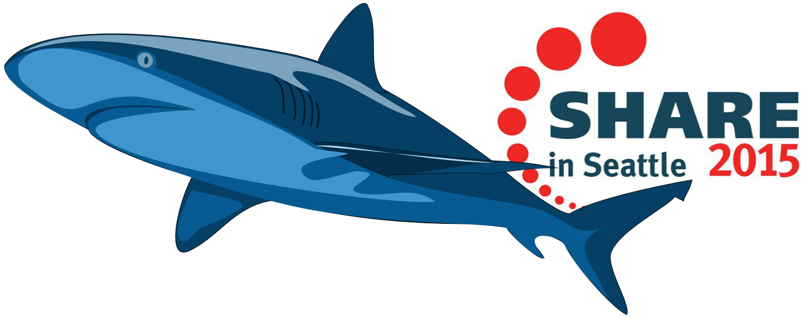
SHARK@SHARE https://ibm.biz/SHARKatSHARE



wireshark Hands-On Lab

Thursday, March 5, 2015

01:45 PM – 02:45 PM

Sheraton Seattle, Redwood

Session 16752

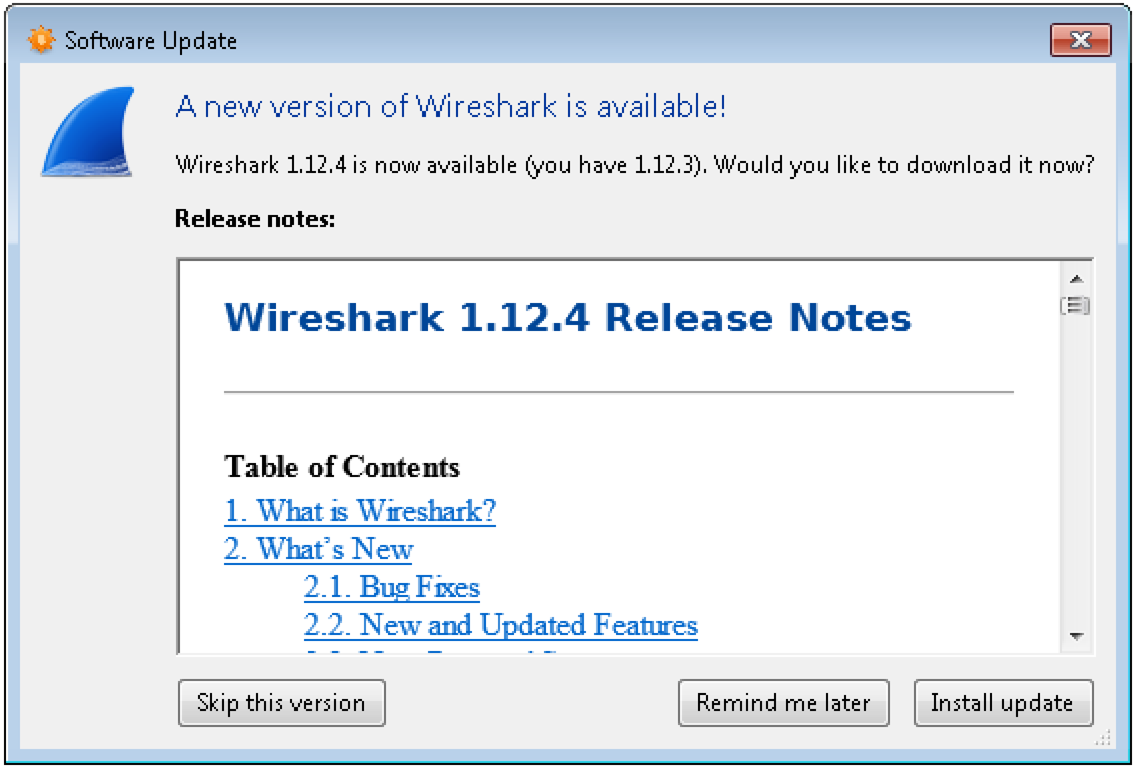
Matthias Burkhard IBM Germany

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence.**

Wireshark Lab Demo

- Starting wireshark: Start → Programs → wireshark
  - Updating wireshark ? No thanks, not now!



A new version of Wireshark is available!

Wireshark 1.12.4 is now available (you have 1.12.3). Would you like to download it now?

Release notes:

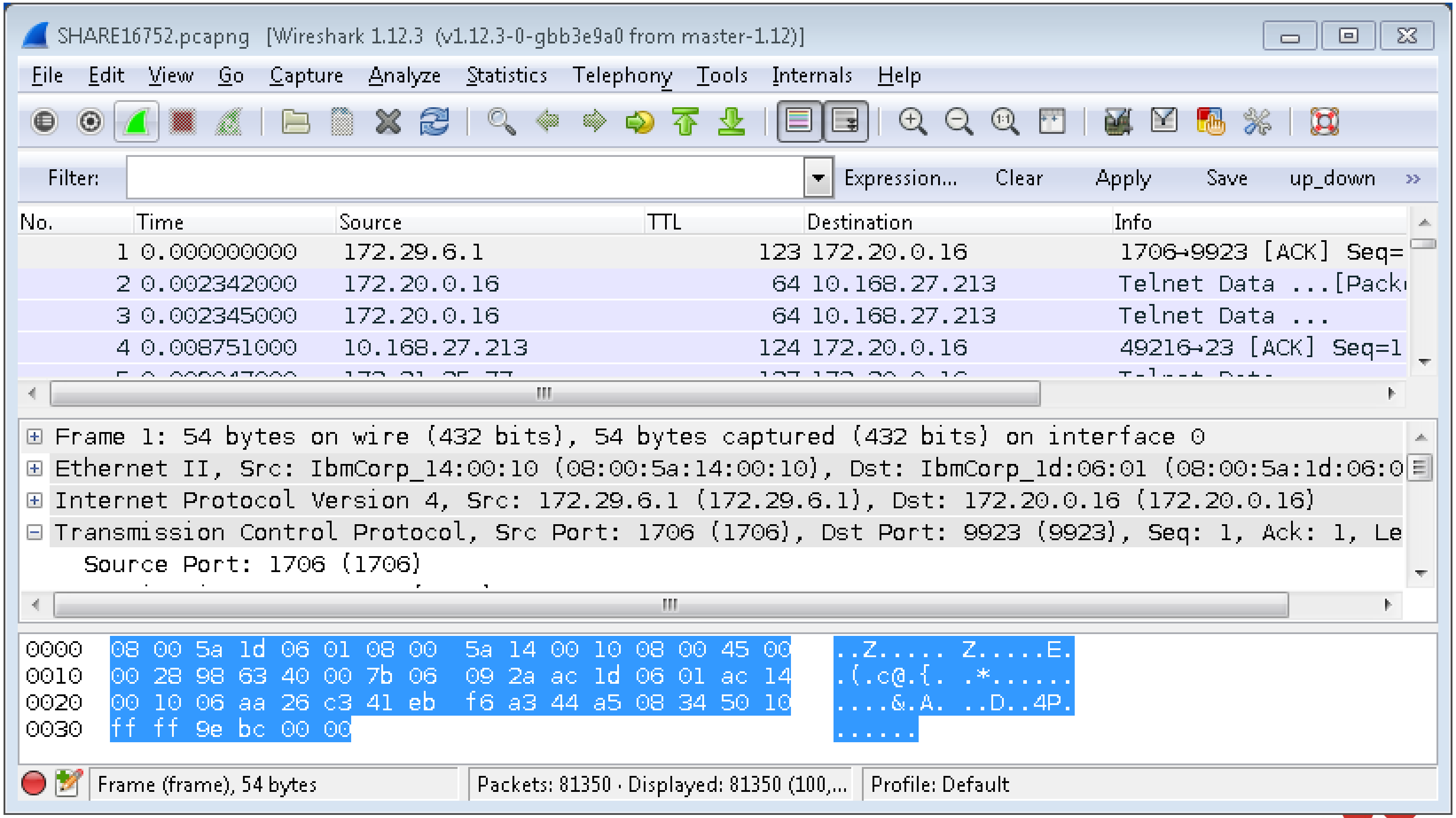
Wireshark 1.12.4 Release Notes

Table of Contents

1. What is Wireshark?
2. What's New
   - 2.1. Bug Fixes
   - 2.2. New and Updated Features

Wireshark Lab - Layout

- 3 areas in wireshark: Packet List, Packet Details, Hexview



SHARE16752.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save up_down

```
No.    Time          Source           TTL  Destination     Info
     1 0.000000000   172.29.6.1        123 172.20.0.16      1706→9923 [ACK] Seq=
     2 0.002342000   172.20.0.16        64 10.168.27.213    Telnet Data ...[Pack
     3 0.002345000   172.20.0.16        64 10.168.27.213    Telnet Data ...
     4 0.008751000   10.168.27.213     124 172.20.0.16      49216→23 [ACK] Seq=1
```

```
⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: IbmCorp_14:00:10 (08:00:5a:14:00:10), Dst: IbmCorp_1d:06:01 (08:00:5a:1d:06:0
⊞ Internet Protocol Version 4, Src: 172.29.6.1 (172.29.6.1), Dst: 172.20.0.16 (172.20.0.16)
⊟ Transmission Control Protocol, Src Port: 1706 (1706), Dst Port: 9923 (9923), Seq: 1, Ack: 1, Le
    Source Port: 1706 (1706)
```

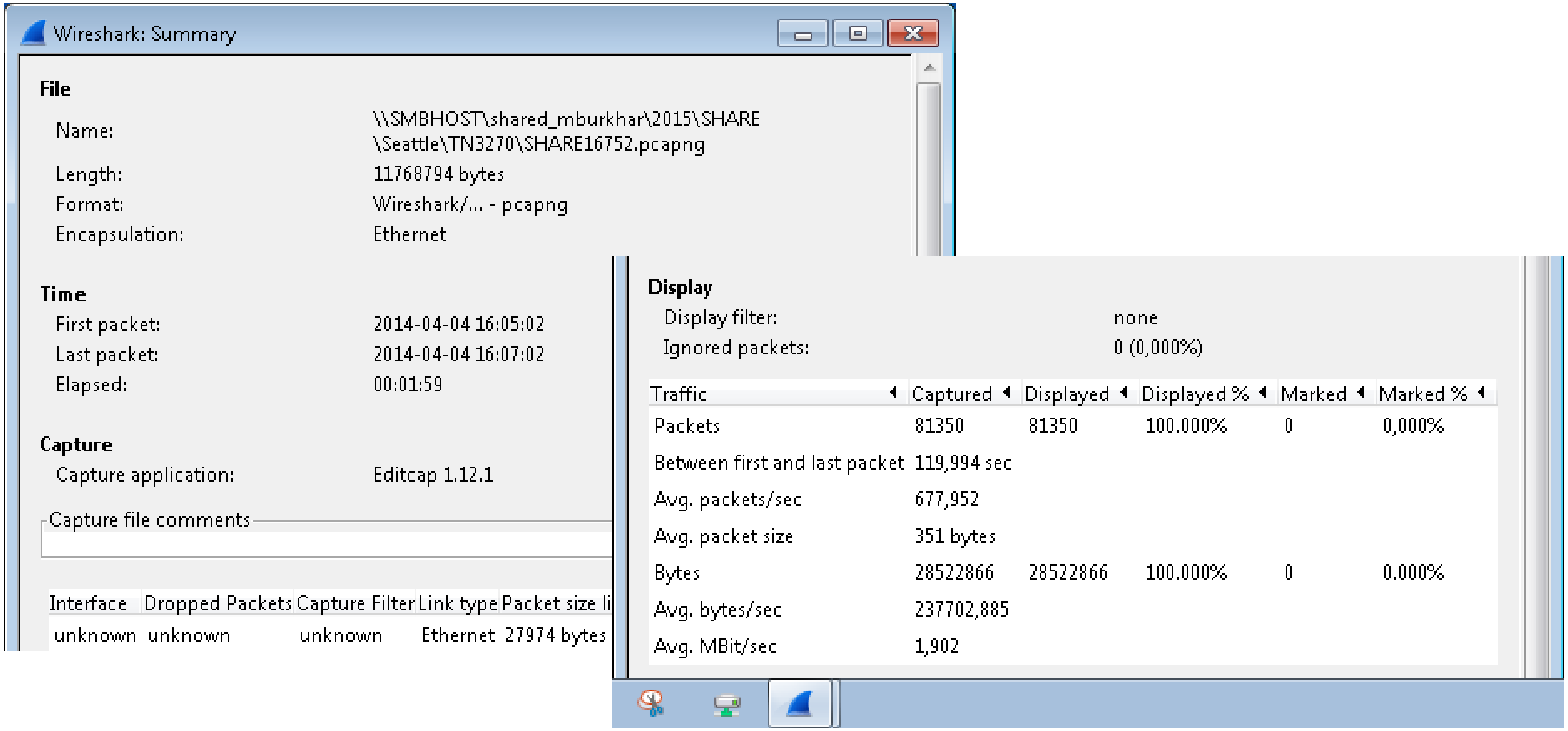
```
0000  08 00 5a 1d 06 01 08 00  5a 14 00 10 08 00 45 00   ..Z..... Z.....E.
0010  00 28 98 63 40 00 7b 06  09 2a ac 1d 06 01 ac 14   .(.c@.{. .*......
0020  00 10 06 aa 26 c3 41 eb  f6 a3 44 a5 08 34 50 10   ....&.A. ..D..4P.
0030  ff ff 9e bc 00 00                                  ......
```

Frame (frame), 54 bytes | Packets: 81350 · Displayed: 81350 (100,... | Profile: Default

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Wireshark Lab - Statistics → Summary

- Overall Information about the trace file



Wireshark: Summary

File

Name: \\SMBHOST\shared_mburkhar\2015\SHARE \Seattle\TN3270\SHARE16752.pcapng

Length: 11768794 bytes

Format: Wireshark/... - pcapng

Encapsulation: Ethernet

Time

First packet: 2014-04-04 16:05:02

Last packet: 2014-04-04 16:07:02

Elapsed: 00:01:59

Capture

Capture application: Editcap 1.12.1

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size li
unknown	unknown	unknown	Ethernet	27974 bytes

Display

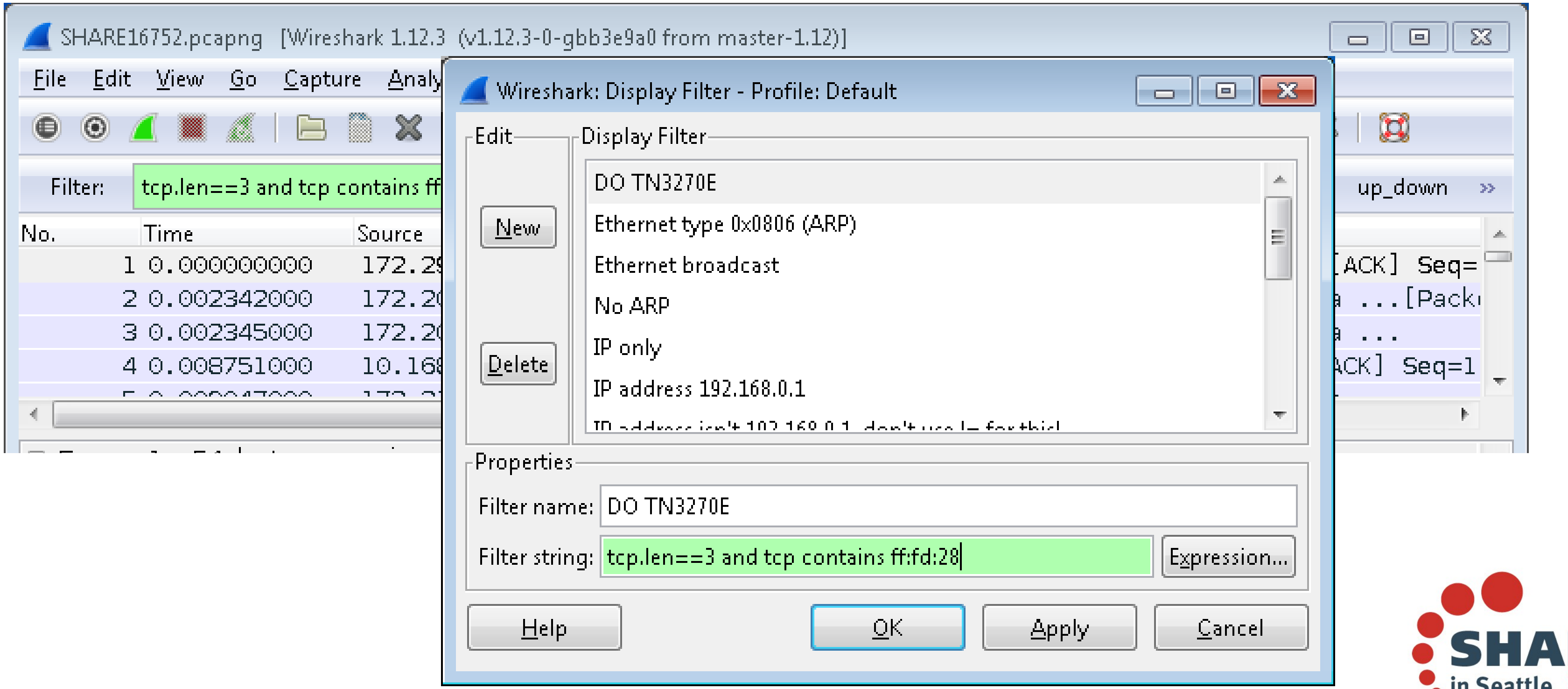
Display filter: none

Ignored packets: 0 (0,000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	81350	81350	100.000%	0	0,000%
Between first and last packet	119,994 sec				
Avg. packets/sec	677,952				
Avg. packet size	351 bytes				
Bytes	28522866	28522866	100.000%	0	0.000%
Avg. bytes/sec	237702,885				
Avg. MBit/sec	1,902				

Wireshark Lab - Display Filter

- Syntax check in filter: green, yellow, red
  - Looking for unencrypted TN3270 traffic?
  - Filtering on DO TN3270E command sent by server
  - Always 3 bytes only: FFFD28


SHARE16752.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: tcp.len==3 and tcp contains ff

Wireshark: Display Filter - Profile: Default

Display Filter:
- DO TN3270E
- Ethernet type 0x0806 (ARP)
- Ethernet broadcast
- No ARP
- IP only
- IP address 192.168.0.1
- IP address isn't 192.168.0.1, don't use != for this!

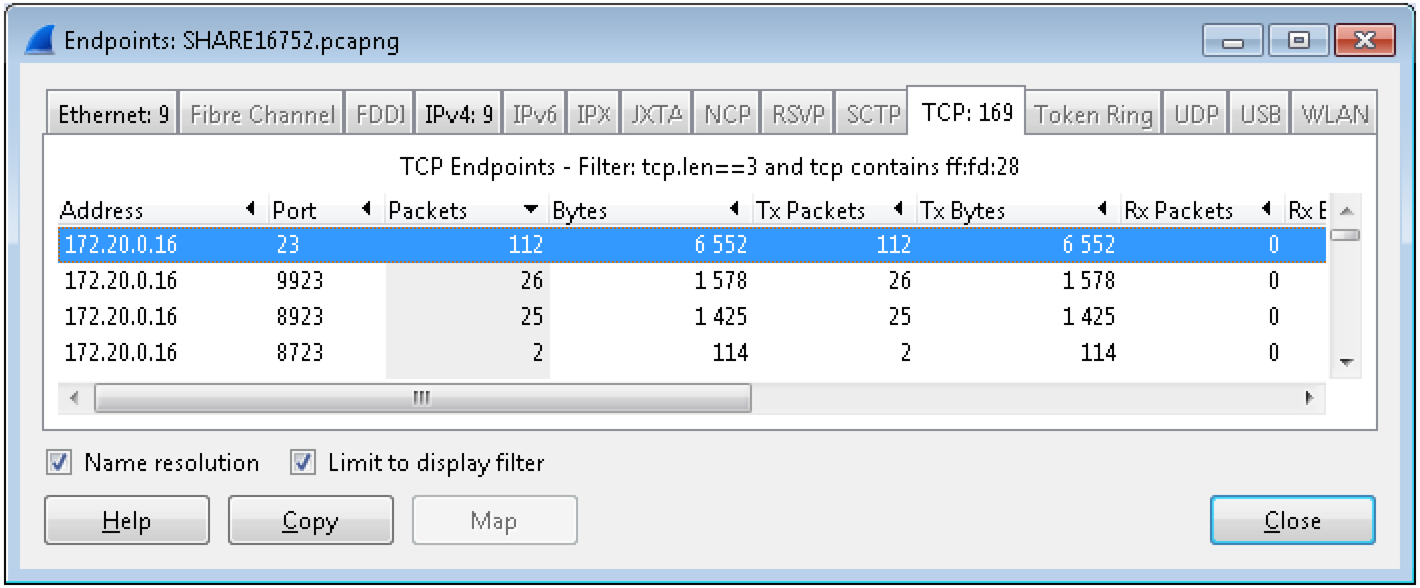
Properties

Filter name: DO TN3270E

Filter string: tcp.len==3 and tcp contains ff:fd:28

Wireshark Lab - Statistics → Endpoints

- Find out how many TCP ports the TN3270 Server is using
  - Check the Limit to display filter
  - 4 TCP ports are found sending DO TN3270E commands
  - 23, 9923, 8923, 8723



Endpoints: SHARE16752.pcapng

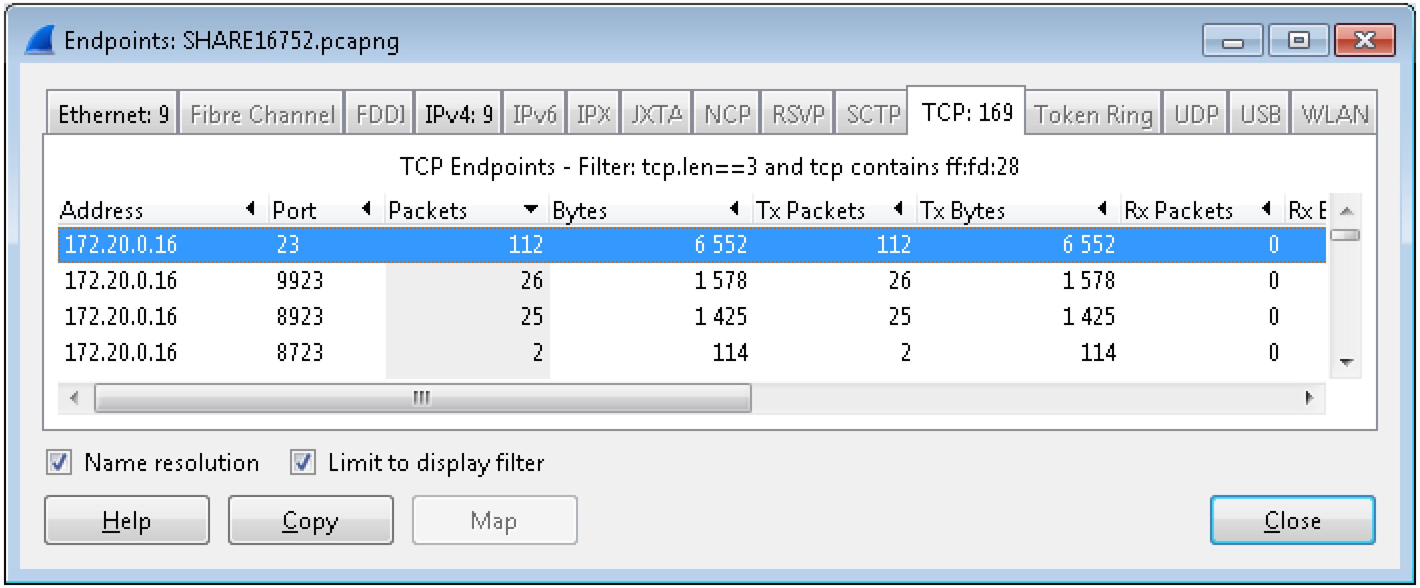
TCP Endpoints - Filter: tcp.len==3 and tcp contains ff:fd:28

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx E
172.20.0.16	23	112	6 552	112	6 552	0	
172.20.0.16	9923	26	1 578	26	1 578	0	
172.20.0.16	8923	25	1 425	25	1 425	0	
172.20.0.16	8723	2	114	2	114	0	

☑ Name resolution ☑ Limit to display filter

Wireshark Lab - Statistics → Endpoints

- Find out how many TCP ports the TN3270 Server is using
  - Check the Limit to display filter
  - 4 TCP ports are found sending DO TN3270E commands
  - 23, 9923, 8923, 8723



Endpoints: SHARE16752.pcapng

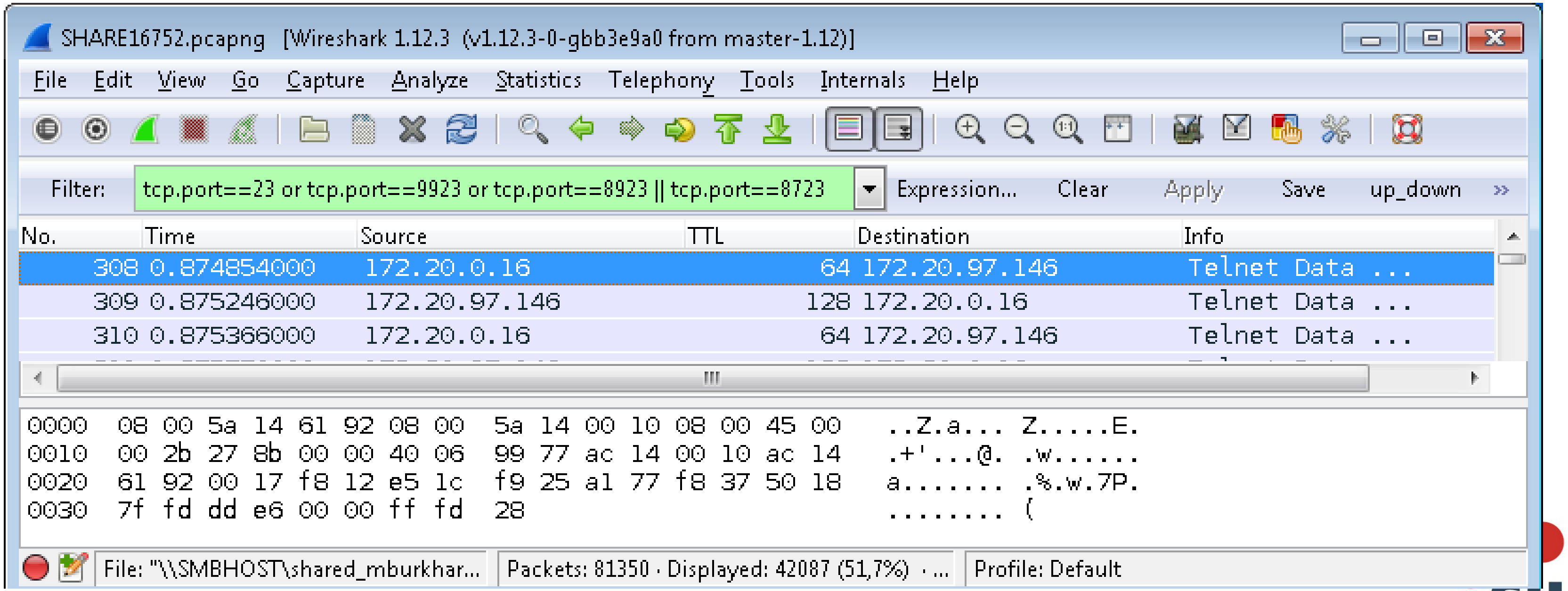
TCP Endpoints - Filter: tcp.len==3 and tcp contains ff:fd:28

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx E
172.20.0.16	23	112	6 552	112	6 552	0	
172.20.0.16	9923	26	1 578	26	1 578	0	
172.20.0.16	8923	25	1 425	25	1 425	0	
172.20.0.16	8723	2	114	2	114	0	

☑ Name resolution ☑ Limit to display filter

Wireshark Lab - Filter multiple ports

- Filters can combine multiple checks
  - Use the 'or' operator to filter on all telnet ports
  - 4 TCP ports are found sending DO TN3270E commands
  - Notice the number of packets that passed the filter at the bottom of the screen



SHARE16752.pcapng   [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: tcp.port==23 or tcp.port==9923 or tcp.port==8923 || tcp.port==8723

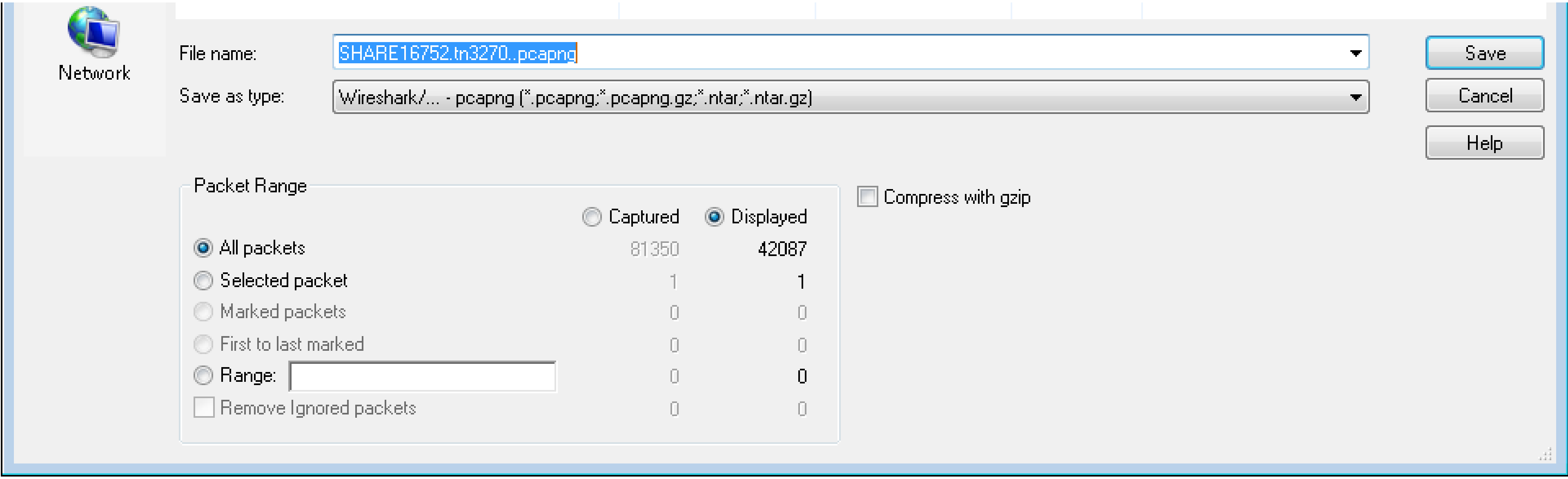
```
No.      Time              Source                     TTL  Destination             Info
     308 0.874854000       172.20.0.16                  64 172.20.97.146           Telnet Data ...
     309 0.875246000       172.20.97.146               128 172.20.0.16             Telnet Data ...
     310 0.875366000       172.20.0.16                  64 172.20.97.146           Telnet Data ...
```

```
0000  08 00 5a 14 61 92 08 00  5a 14 00 10 08 00 45 00   ..Z.a... Z.....E.
0010  00 2b 27 8b 00 00 40 06  99 77 ac 14 00 10 ac 14   .+'...@. .w......
0020  61 92 00 17 f8 12 e5 1c  f9 25 a1 77 f8 37 50 18   a....... .%.w.7P.
0030  7f fd dd e6 00 00 ff fd  28                        ........ (
```

File: "\\SMBHOST\shared_mburkhar...   Packets: 81350 · Displayed: 42087 (51,7%) · ...   Profile: Default

Wireshark Lab - Save filtered packets

- File → Export specified packets
  - Creates a new trace file with a subset of packets
  - Use a name that you recognize what the contents is



File name: SHARE16752.tn3270..pcapng

Save as type: Wireshark/... - pcapng (*.pcapng;*.pcapng.gz;*.ntar;*.ntar.gz)

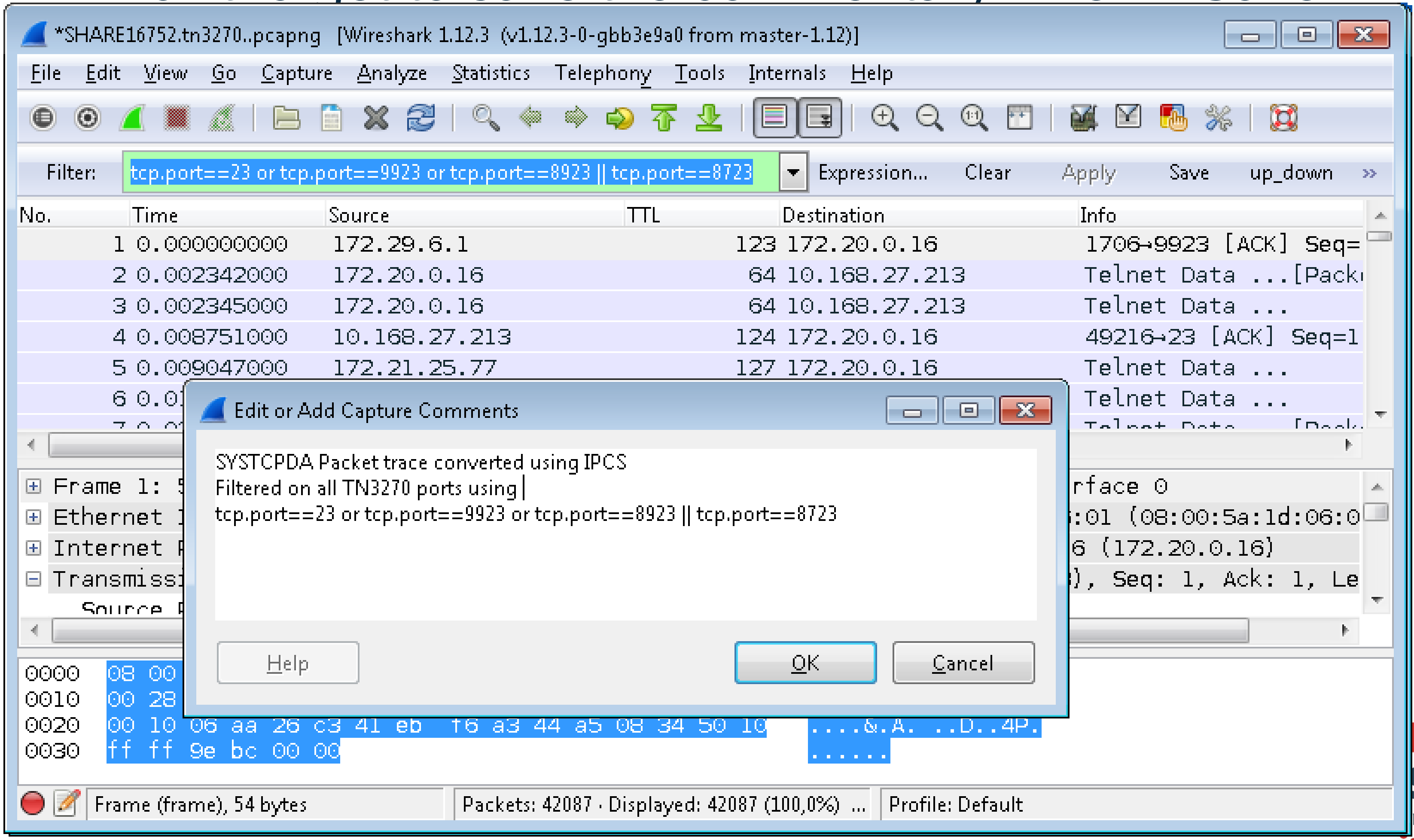
Packet Range

	○ Captured	● Displayed
● All packets	81350	42087
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

□ Compress with gzip

Wireshark Lab - Comment the trace file

- Allows to pass 'Meta Information' in the tracefile
- Don't forget to save the commentary: File → Save


*SHARE16752.tn3270..pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save up_down
Edit or Add Capture Comments
Help OK Cancel

Filter: tcp.port==23 or tcp.port==9923 or tcp.port==8923 || tcp.port==8723

```
No.   Time          Source          TTL  Destination     Info
    1 0.000000000   172.29.6.1      123  172.20.0.16     1706→9923 [ACK] Seq=
    2 0.002342000   172.20.0.16      64  10.168.27.213   Telnet Data ...[Pack
    3 0.002345000   172.20.0.16      64  10.168.27.213   Telnet Data ...
    4 0.008751000   10.168.27.213   124  172.20.0.16     49216→23 [ACK] Seq=1
    5 0.009047000   172.21.25.77    127  172.20.0.16     Telnet Data ...
    6 0.01                                               Telnet Data ...
```

SYSTCPDA Packet trace converted using IPCS
Filtered on all TN3270 ports using
tcp.port==23 or tcp.port==9923 or tcp.port==8923 || tcp.port==8723

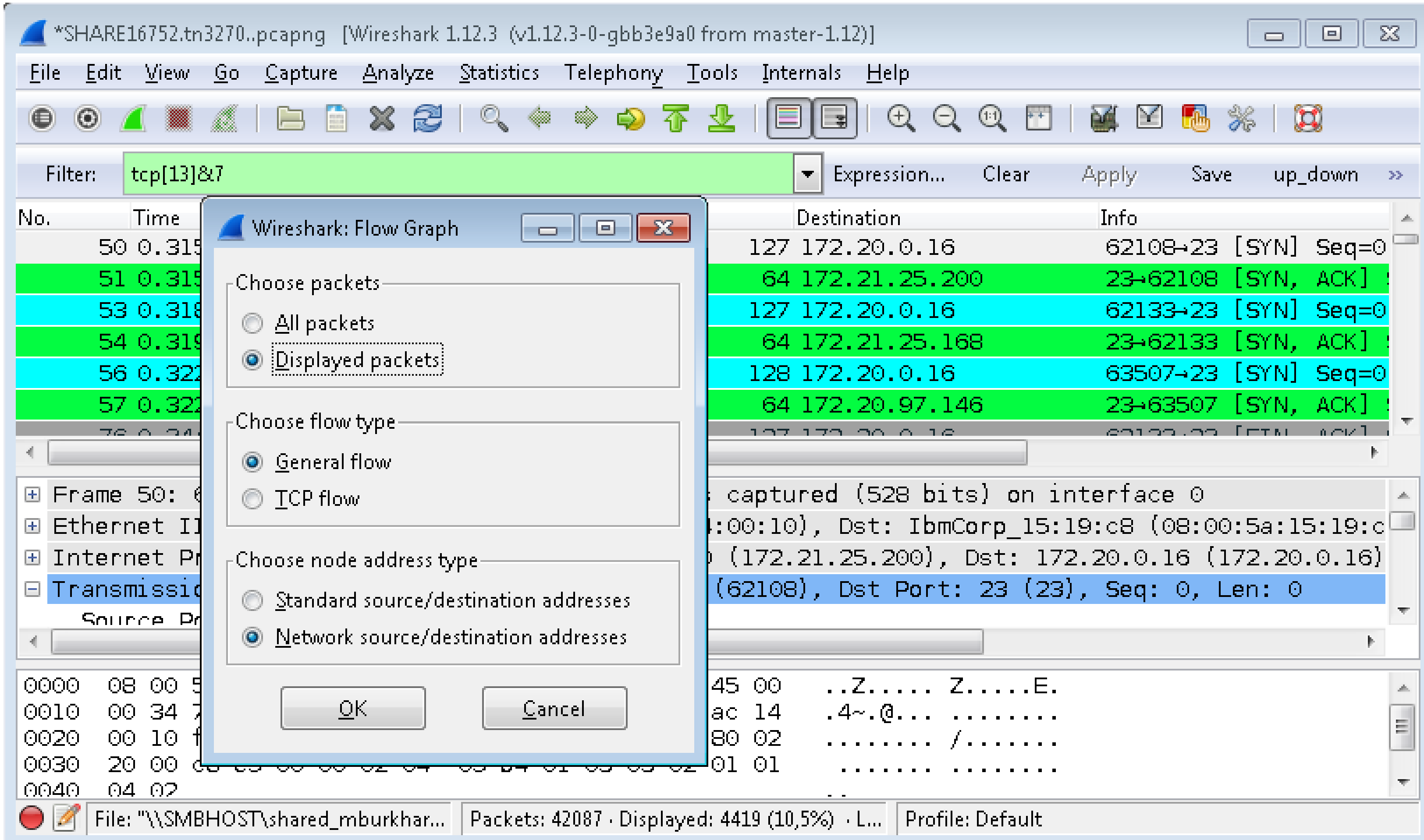
```
⊞ Frame 1: 5                 rface 0
⊞ Ethernet I                 :01 (08:00:5a:1d:06:0
⊞ Internet P                 6 (172.20.0.16)
⊟ Transmissi                 ), Seq: 1, Ack: 1, Le
    Source P
```

```
0000  08 00
0010  00 28
0020  00 10 06 aa 26 c3 41 eb  f6 a3 44 a5 08 34 50 10   ....&.A. ..D..4P.
0030  ff ff 9e bc 00 00                                  ......
```

Frame (frame), 54 bytes | Packets: 42087 · Displayed: 42087 (100,0%) ... | Profile: Default

Wireshark Lab - Statistics – Flow Graph

- Show all Packets over a vertical time line
- Can use filters to draw different colored graphs



*SHARE16752.tn3270..pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save up_down

Filter: tcp[13]&7

```
No.     Time                      Destination      Info
   50 0.315            127 172.20.0.16         62108→23 [SYN] Seq=0
   51 0.315             64 172.21.25.200       23→62108 [SYN, ACK]
   53 0.318            127 172.20.0.16         62133→23 [SYN] Seq=0
   54 0.319             64 172.21.25.168       23→62133 [SYN, ACK]
   56 0.322            128 172.20.0.16         63507→23 [SYN] Seq=0
   57 0.322             64 172.20.97.146       23→63507 [SYN, ACK]
```

```
⊞ Frame 50: (                                 captured (528 bits) on interface 0
⊞ Ethernet II                                 :00:10), Dst: IbmCorp_15:19:c8 (08:00:5a:15:19:c
⊞ Internet Pr                                 (172.21.25.200), Dst: 172.20.0.16 (172.20.0.16)
⊟ Transmissio                                 (62108), Dst Port: 23 (23), Seq: 0, Len: 0
    Source Po
```

```
0000  08 00 5                 45 00    ..Z.....  Z.....E.
0010  00 34 7                 ac 14    .4~.@...  ........
0020  00 10 f                 80 02    ........  /.......
0030  20 00                   01 01     .......  ........
0040  04 02
```

Wireshark: Flow Graph

Choose packets
- ○ All packets
- ● Displayed packets

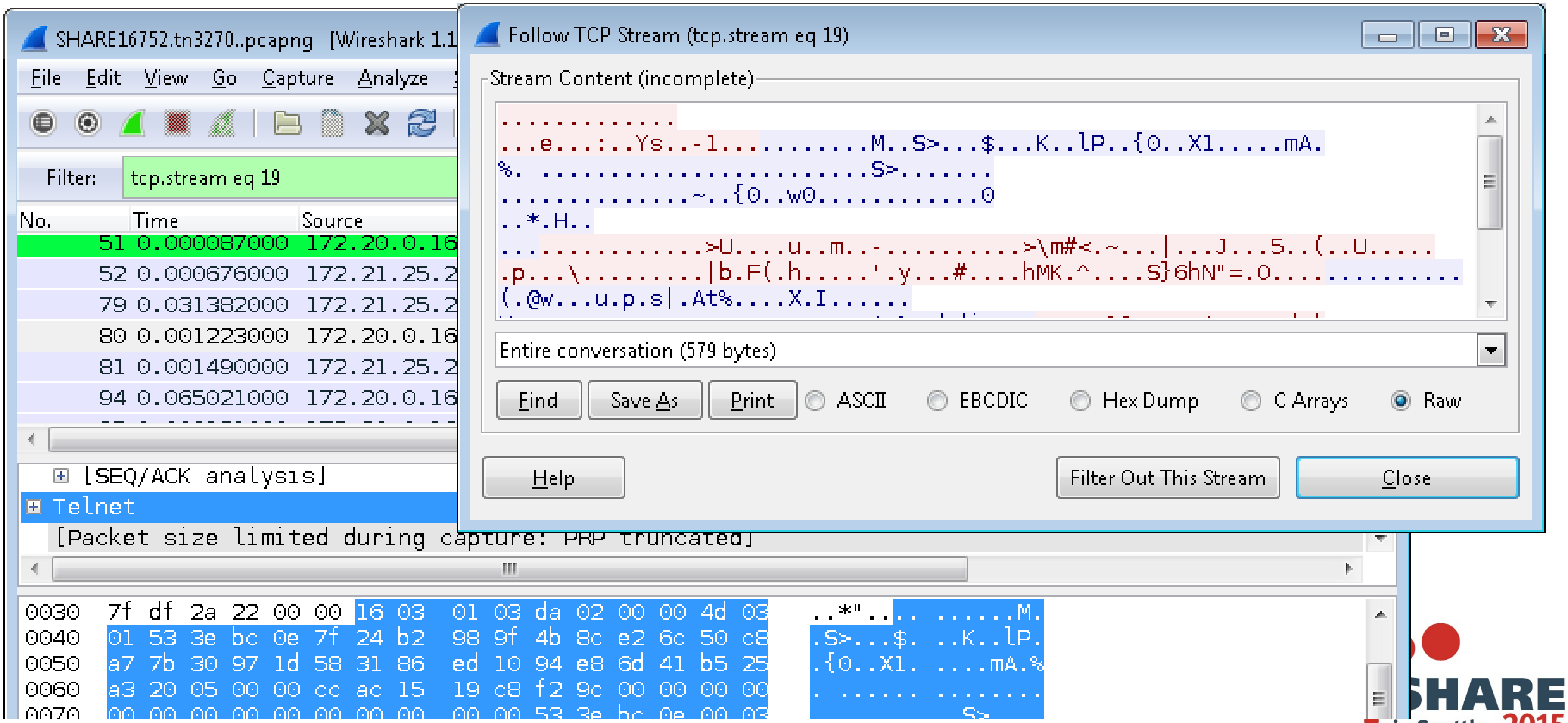
Choose flow type
- ● General flow
- ○ TCP flow

Choose node address type
- ○ Standard source/destination addresses
- ● Network source/destination addresses

File: "\\SMBHOST\shared_mburkhar... | Packets: 42087 · Displayed: 4419 (10,5%) · L... | Profile: Default

Wireshark Lab - Follow TCP Stream

- Rightclick on any packet of the TCP session
- Follow TCP stream opens a view of all data
- Creates a filter on tcp.stream



SHARE16752.tn3270..pcapng [Wireshark 1.1
File Edit View Go Capture Analyze

Filter: tcp.stream eq 19

```
No.         Time          Source
        51 0.000087000 172.20.0.16
        52 0.000676000 172.21.25.2
        79 0.031382000 172.21.25.2
        80 0.001223000 172.20.0.16
        81 0.001490000 172.21.25.2
        94 0.065021000 172.20.0.16
```

```
⊞ [SEQ/ACK analysis]
⊞ Telnet
  [Packet size limited during capture: PRP truncated]
```

```
0030  7f df 2a 22 00 00 16 03  01 03 da 02 00 00 4d 03   ..*"... ......M.
0040  01 53 3e bc 0e 7f 24 b2  98 9f 4b 8c e2 6c 50 c8   .S>...$. ..K..lP.
0050  a7 7b 30 97 1d 58 31 86  ed 10 94 e8 6d 41 b5 25   .{0..X1. ....mA.%
0060  a3 20 05 00 00 cc ac 15  19 c8 f2 9c 00 00 00 00   . ...... ........
0070  00 00 00 00 00 00 00 00  00 00 53 3e bc 0e 00 03   ........ ..S>....
```

Stream Content (incomplete)

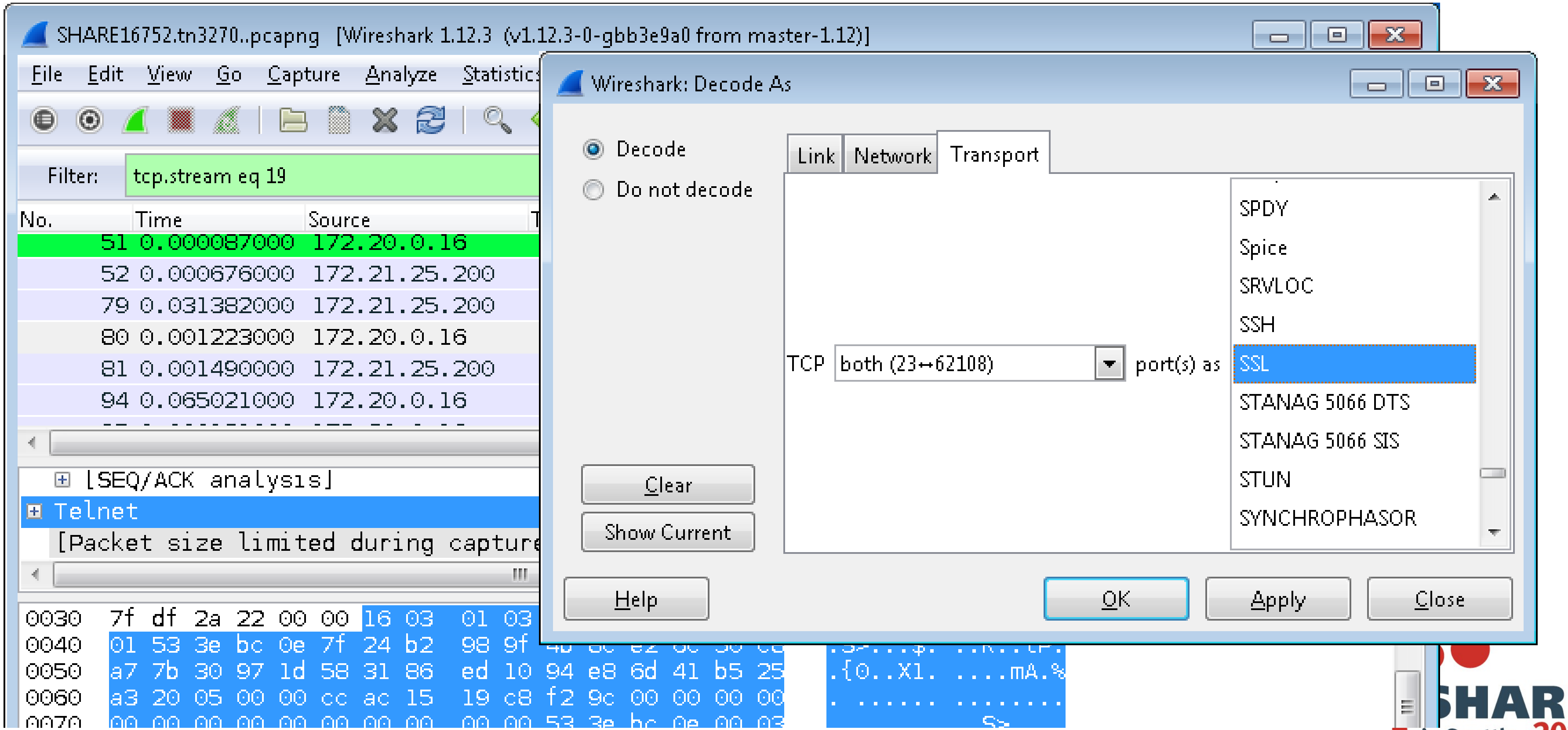
```
..............
...e...:..Ys..-1...........M..S>...$...K..lP..{0..X1.....mA.
%. .........................S>.......
..............~..{0..w0............0
..*.H..
..............>U....u..m..-...........>\m#<.~...|...J...5..(..U.....
.p...\..........|b.F(.h.....'.y...#....hMK.^....S}6hN"=.0..............
(.@w...u.p.s|.At%....X.I......
```

Entire conversation (579 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Wireshark Lab - Decode AS

- If the protocol is not what wireshark thinks it is
- 160301 looks like a TLS Negotiation packet
  - Rightclick on any packet → Decode as “SSL”



Filter: tcp.stream eq 19

```
No.        Time          Source
     51 0.000087000 172.20.0.16
     52 0.000676000 172.21.25.200
     79 0.031382000 172.21.25.200
     80 0.001223000 172.20.0.16
     81 0.001490000 172.21.25.200
     94 0.065021000 172.20.0.16
```

```
⊞ [SEQ/ACK analysis]
⊞ Telnet
  [Packet size limited during capture
```

```
0030  7f df 2a 22 00 00 16 03  01 03
0040  01 53 3e bc 0e 7f 24 b2  98 9f
0050  a7 7b 30 97 1d 58 31 86  ed 10 94 e8 6d 41 b5 25   .{0..X1. ....mA.%
0060  a3 20 05 00 00 cc ac 15  19 c8 f2 9c 00 00 00 00   . ...... ........
```

● Decode

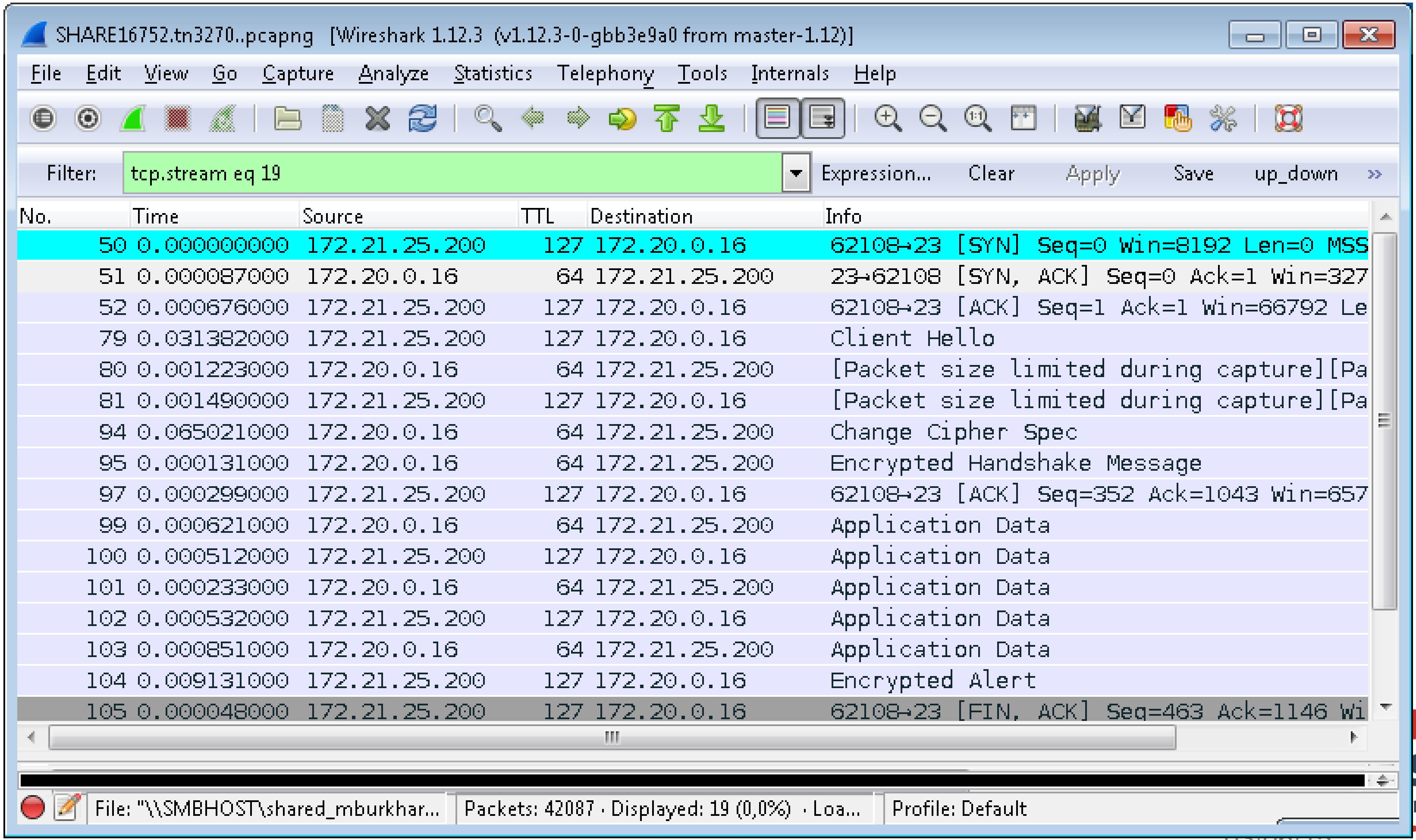
○ Do not decode

TCP both (23↔62108) port(s) as SSL

SPDY
Spice
SRVLOC
SSH
SSL
STANAG 5066 DTS
STANAG 5066 SIS
STUN
SYNCHROPHASOR

Wireshark Lab - Decode AS

- Now all port 23 traffic is mapped to SSL Protocol
- Sessions terminate after an Encrypted Alert



SHARE16752.tn3270..pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save up_down

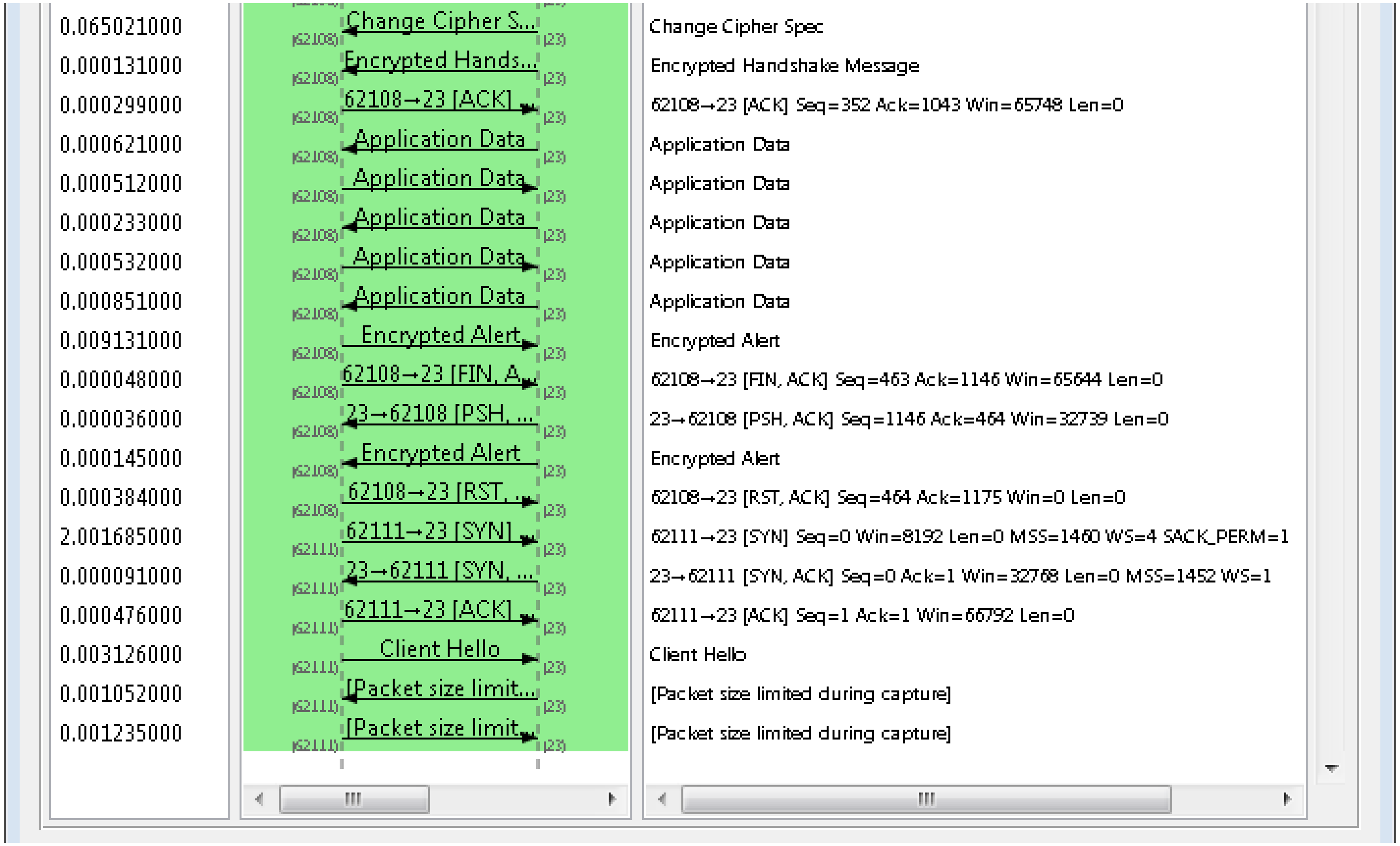
Filter: tcp.stream eq 19

No.	Time	Source	TTL	Destination	Info
50	0.000000000	172.21.25.200	127	172.20.0.16	62108→23 [SYN] Seq=0 Win=8192 Len=0 MSS
51	0.000087000	172.20.0.16	64	172.21.25.200	23→62108 [SYN, ACK] Seq=0 Ack=1 Win=327
52	0.000676000	172.21.25.200	127	172.20.0.16	62108→23 [ACK] Seq=1 Ack=1 Win=66792 Le
79	0.031382000	172.21.25.200	127	172.20.0.16	Client Hello
80	0.001223000	172.20.0.16	64	172.21.25.200	[Packet size limited during capture][Pa
81	0.001490000	172.21.25.200	127	172.20.0.16	[Packet size limited during capture][Pa
94	0.065021000	172.20.0.16	64	172.21.25.200	Change Cipher Spec
95	0.000131000	172.20.0.16	64	172.21.25.200	Encrypted Handshake Message
97	0.000299000	172.21.25.200	127	172.20.0.16	62108→23 [ACK] Seq=352 Ack=1043 Win=657
99	0.000621000	172.20.0.16	64	172.21.25.200	Application Data
100	0.000512000	172.21.25.200	127	172.20.0.16	Application Data
101	0.000233000	172.20.0.16	64	172.21.25.200	Application Data
102	0.000532000	172.21.25.200	127	172.20.0.16	Application Data
103	0.000851000	172.20.0.16	64	172.21.25.200	Application Data
104	0.009131000	172.21.25.200	127	172.20.0.16	Encrypted Alert
105	0.000048000	172.21.25.200	127	172.20.0.16	62108→23 [FIN, ACK] Seq=463 Ack=1146 Wi

File: "\\SMBHOST\shared_mburkhar... Packets: 42087 · Displayed: 19 (0,0%) · Loa... Profile: Default

Wireshark Lab - Conversation Filter – IP

- Following a single client's traffic
- Sessions terminate after an Encrypted Alert
- And restart after 2 seconds

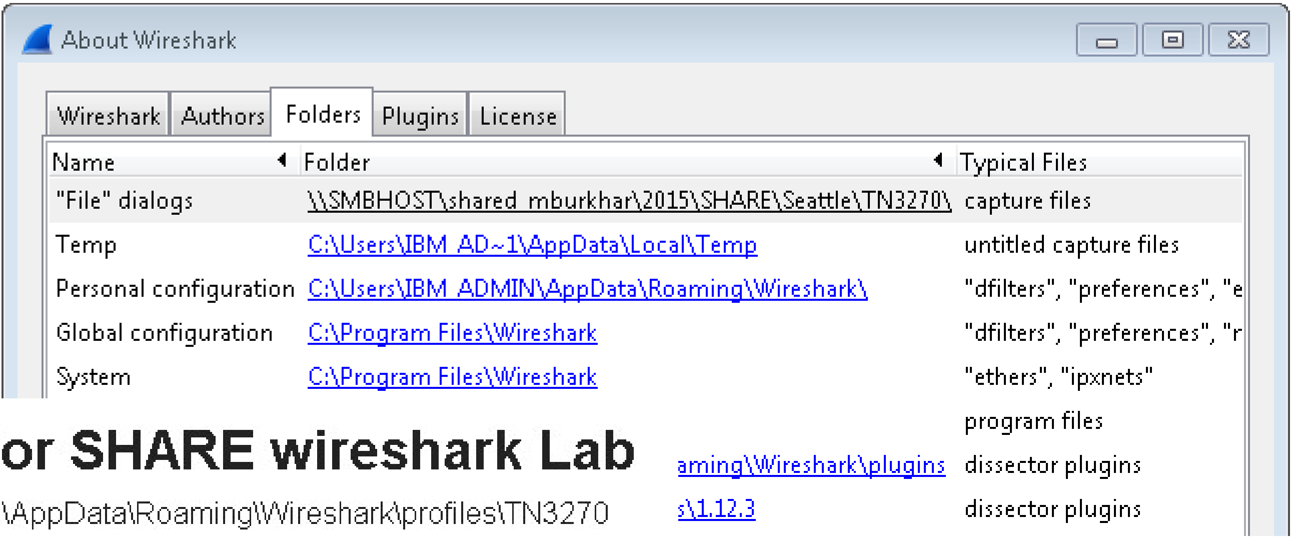


```
0.065021000  |62108| ← Change Cipher S...    |23|  Change Cipher Spec
0.000131000  |62108| ← Encrypted Hands...    |23|  Encrypted Handshake Message
0.000299000  |62108| → 62108→23 [ACK]       |23|  62108→23 [ACK] Seq=352 Ack=1043 Win=65748 Len=0
0.000621000  |62108| ← Application Data      |23|  Application Data
0.000512000  |62108| → Application Data      |23|  Application Data
0.000233000  |62108| ← Application Data      |23|  Application Data
0.000532000  |62108| → Application Data      |23|  Application Data
0.000851000  |62108| ← Application Data      |23|  Application Data
0.009131000  |62108| → Encrypted Alert       |23|  Encrypted Alert
0.000048000  |62108| → 62108→23 [FIN, A...   |23|  62108→23 [FIN, ACK] Seq=463 Ack=1146 Win=65644 Len=0
0.000036000  |62108| ← 23→62108 [PSH, ...    |23|  23→62108 [PSH, ACK] Seq=1146 Ack=464 Win=32739 Len=0
0.000145000  |62108| ← Encrypted Alert       |23|  Encrypted Alert
0.000384000  |62108| → 62108→23 [RST, ...    |23|  62108→23 [RST, ACK] Seq=464 Ack=1175 Win=0 Len=0
2.001685000  |62111| → 62111→23 [SYN]       |23|  62111→23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
0.000091000  |62111| ← 23→62111 [SYN, ...    |23|  23→62111 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1452 WS=1
0.000476000  |62111| → 62111→23 [ACK]       |23|  62111→23 [ACK] Seq=1 Ack=1 Win=66792 Len=0
0.003126000  |62111| → Client Hello          |23|  Client Hello
0.001052000  |62111| ← [Packet size limit... |23|  [Packet size limited during capture]
0.001235000  |62111| → [Packet size limit    |23|  [Packet size limited during capture]
```

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Wireshark Lab - Profile TN3270

- Download the files to your Personal Configuration Folder
- Help → About wireshark → Folders



Name	Folder	Typical Files
"File" dialogs	\\SMBHOST\shared_mburkhar\2015\SHARE\Seattle\TN3270\	capture files
Temp	C:\Users\IBM_AD~1\AppData\Local\Temp	untitled capture files
Personal configuration	C:\Users\IBM_ADMIN\AppData\Roaming\Wireshark\	"dfilters", "preferences", "e
Global configuration	C:\Program Files\Wireshark	"dfilters", "preferences", "r
System	C:\Program Files\Wireshark	"ethers", "ipxnets"
		program files
	aming\Wireshark\plugins	dissector plugins
	s\1.12.3	dissector plugins

Wireshark Profile for SHARE wireshark Lab

Download to : C:\Users\SmartSource\AppData\Roaming\Wireshark\profiles\TN3270

Display Filters: dfilters

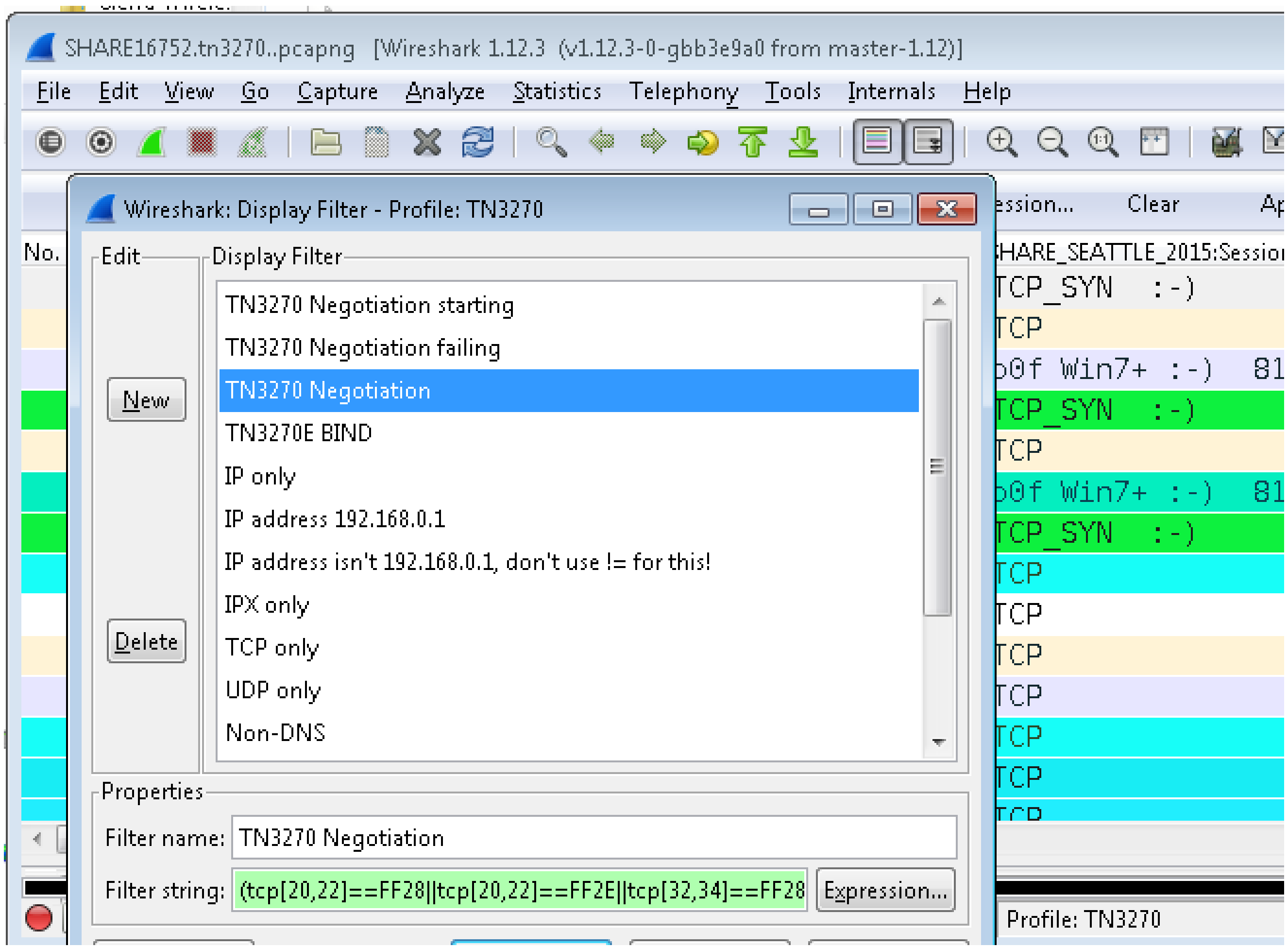
Coloring Rules: colorfilters

Preferences: preferences

Disabled Protos: disabled_protos

Wireshark Lab - TN3270 Negotiation fails

- Filter on TN3270 Negotiation

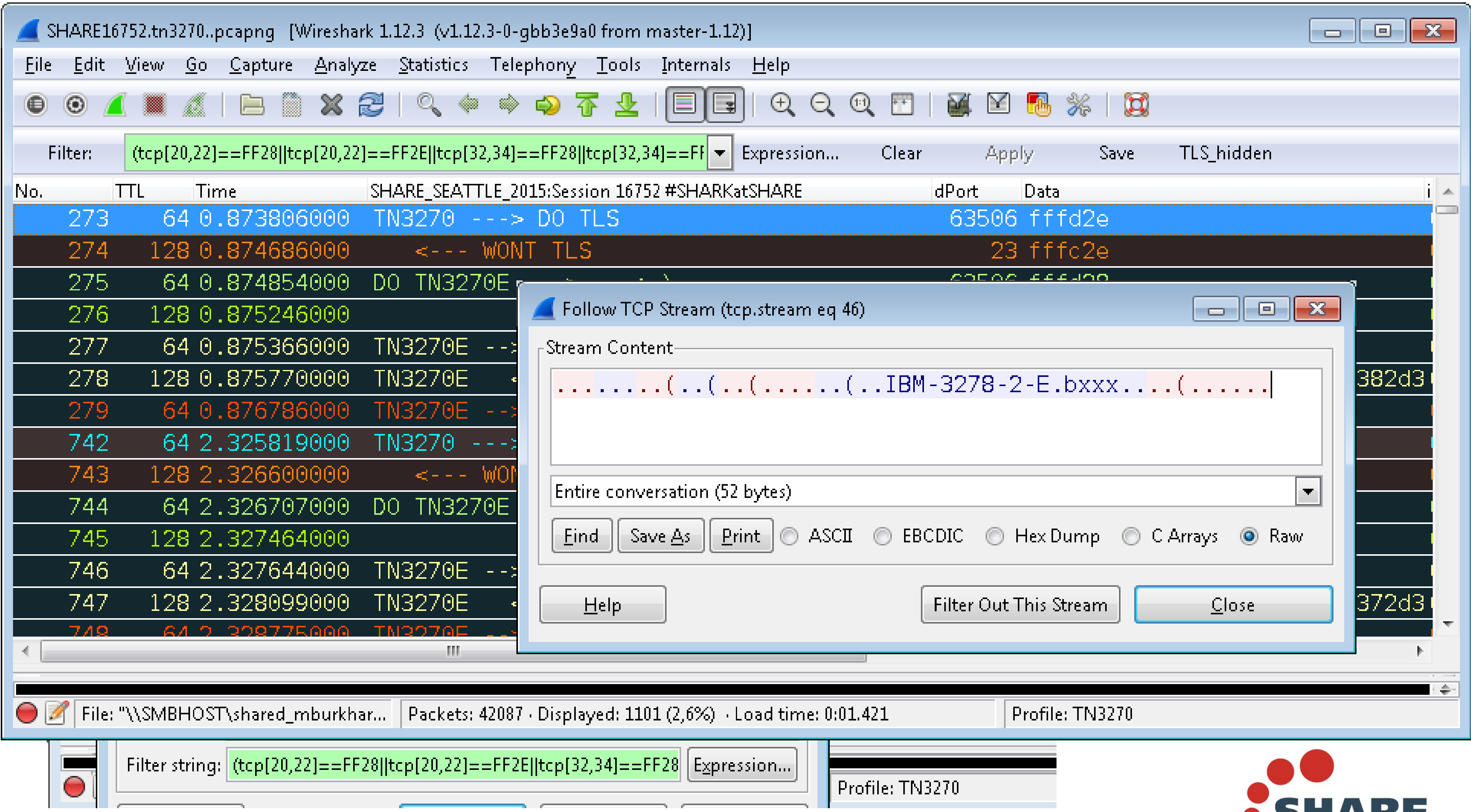


TN3270 Negotiation starting
TN3270 Negotiation failing
TN3270 Negotiation
TN3270E BIND
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
Non-DNS

Filter name: TN3270 Negotiation

Filter string: (tcp[20,22]==FF28||tcp[20,22]==FF2E||tcp[32,34]==FF28

Wireshark Lab - TN3270 Negotiation fails



SHARE16752.tn3270..pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (tcp[20,22]==FF28||tcp[20,22]==FF2E||tcp[32,34]==FF28||tcp[32,34]==FF

Expression... Clear Apply Save TLS_hidden

```
No.       TTL  Time         SHARE_SEATTLE_2015:Session 16752 #SHARKatSHARE   dPort  Data
   273     64  0.873806000  TN3270  ---> DO TLS                              63506  fffd2e
   274    128  0.874686000     <--- WONT TLS                                    23  fffc2e
   275     64  0.874854000  DO TN3270E                                       63506  fffd28
   276    128  0.875246000
   277     64  0.875366000  TN3270E --
   278    128  0.875770000  TN3270E   <                                              382d3
   279     64  0.876786000  TN3270E --
   742     64  2.325819000  TN3270  ---
   743    128  2.326600000     <--- WON
   744     64  2.326707000  DO TN3270E
   745    128  2.327464000
   746     64  2.327644000  TN3270E --
   747    128  2.328099000  TN3270E   <                                              372d3
   748     64  2.328775000  TN3270E --
```

Follow TCP Stream (tcp.stream eq 46)

Stream Content

```
........(..(..(......(..IBM-3278-2-E.bxxx....(......
```

Entire conversation (52 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

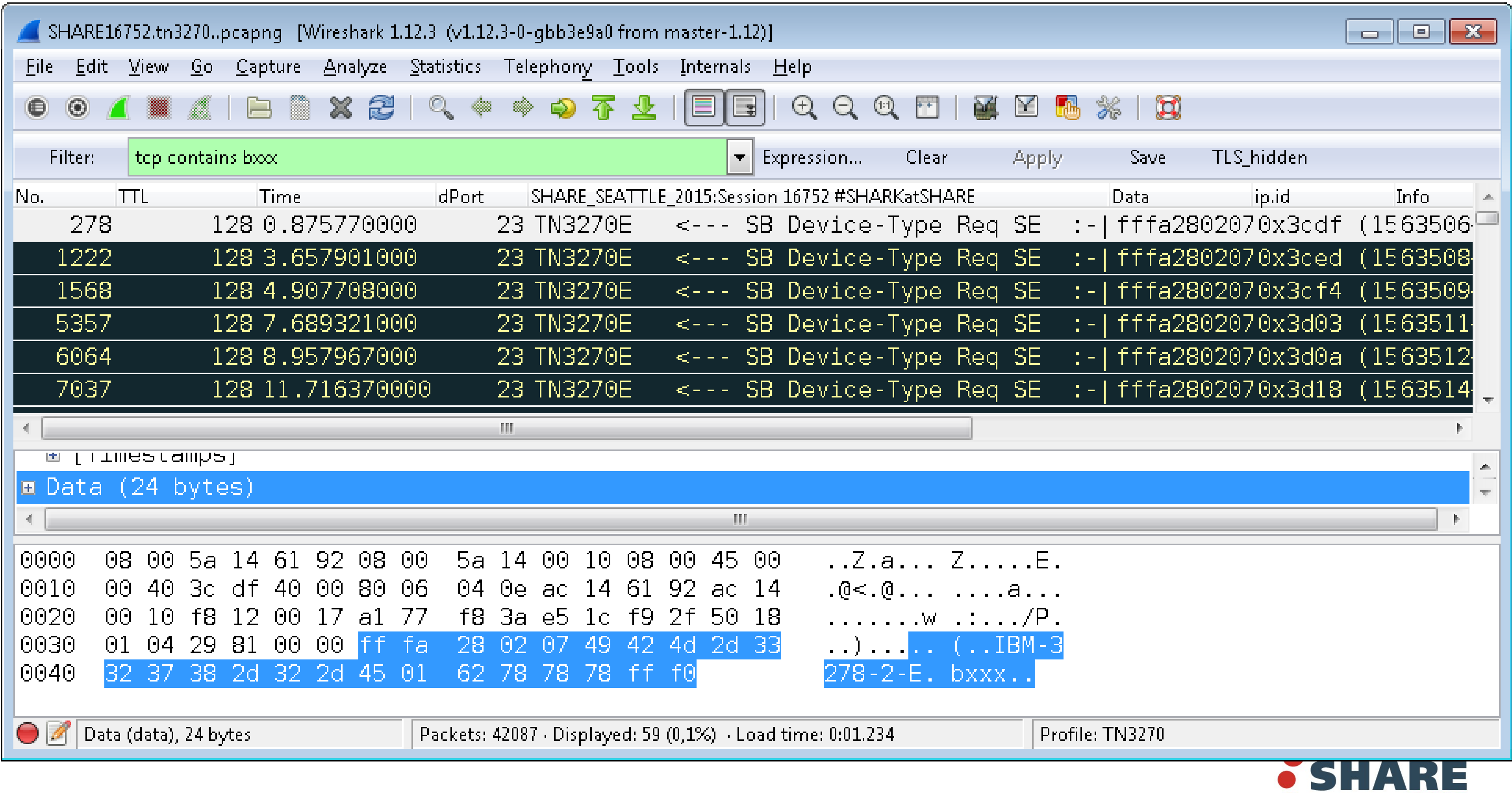
File: "\\SMBHOST\shared_mburkhar... Packets: 42087 · Displayed: 1101 (2,6%) · Load time: 0:01.421 Profile: TN3270

Filter string: (tcp[20,22]==FF28||tcp[20,22]==FF2E||tcp[32,34]==FF28

Profile: TN3270

Wireshark Lab - Filter on LUName

- Filter on any ASCII string using the contains operator



SHARE16752.tn3270..pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save TLS_hidden

Filter: tcp contains bxxx

```
No.     TTL   Time          dPort  SHARE_SEATTLE_2015:Session 16752 #SHARKatSHARE   Data        ip.id    Info
   278  128 0.875770000     23 TN3270E    <--- SB Device-Type Req SE    :-| fffa280207 0x3cdf (1563506
  1222  128 3.657901000     23 TN3270E    <--- SB Device-Type Req SE    :-| fffa280207 0x3ced (1563508
  1568  128 4.907708000     23 TN3270E    <--- SB Device-Type Req SE    :-| fffa280207 0x3cf4 (1563509
  5357  128 7.689321000     23 TN3270E    <--- SB Device-Type Req SE    :-| fffa280207 0x3d03 (1563511
  6064  128 8.957967000     23 TN3270E    <--- SB Device-Type Req SE    :-| fffa280207 0x3d0a (1563512
  7037  128 11.716370000    23 TN3270E    <--- SB Device-Type Req SE    :-| fffa280207 0x3d18 (1563514
```

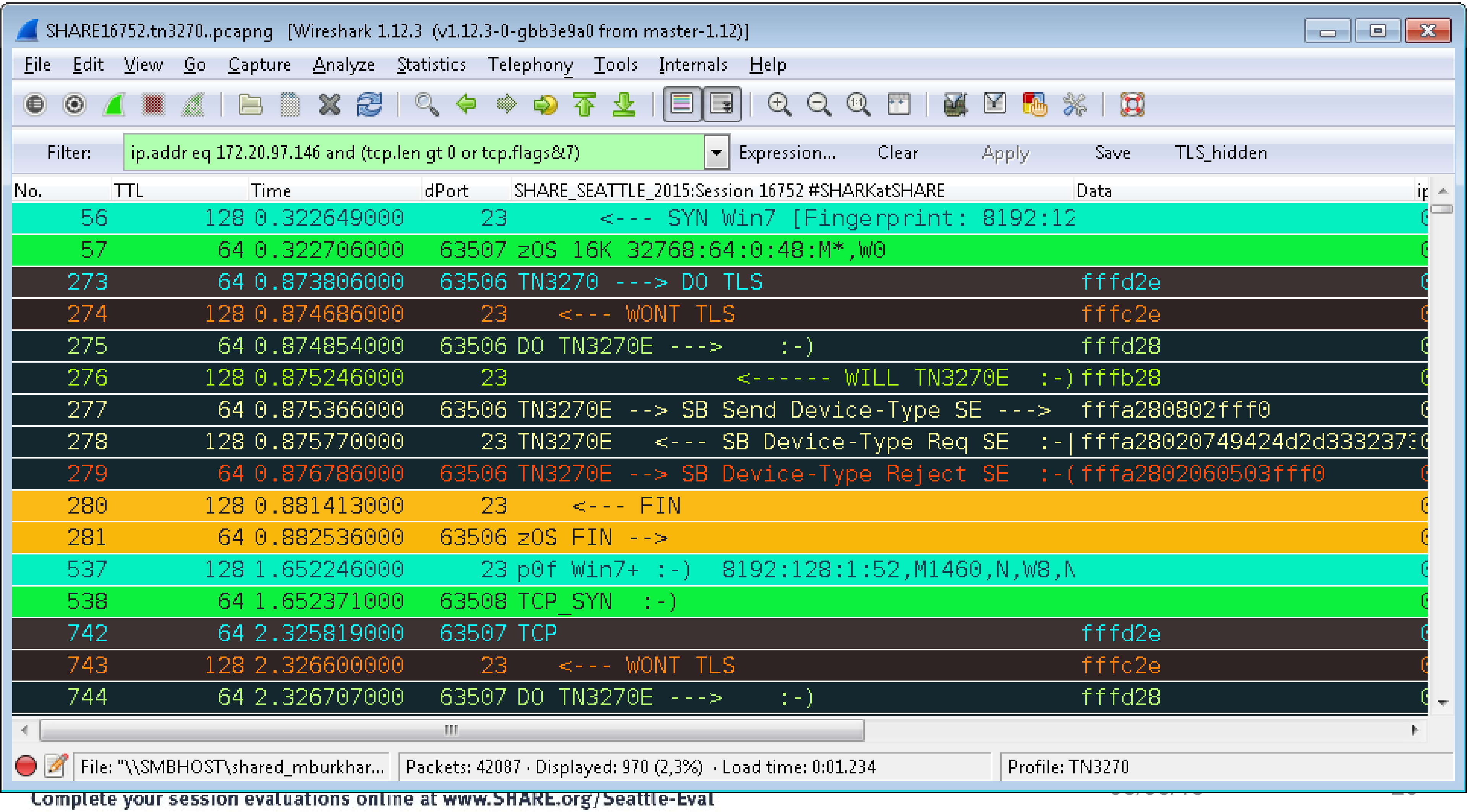
```
⊞ [Timestamps]
⊞ Data (24 bytes)
```

```
0000  08 00 5a 14 61 92 08 00  5a 14 00 10 08 00 45 00   ..Z.a... Z.....E.
0010  00 40 3c df 40 00 80 06  04 0e ac 14 61 92 ac 14   .@<.@... ....a...
0020  00 10 f8 12 00 17 a1 77  f8 3a e5 1c f9 2f 50 18   .......w .:.../P.
0030  01 04 29 81 00 00 ff fa  28 02 07 49 42 4d 2d 33   ..)..... (..IBM-3
0040  32 37 38 2d 32 2d 45 01  62 78 78 78 ff f0         278-2-E. bxxx..
```

Data (data), 24 bytes | Packets: 42087 · Displayed: 59 (0,1%) · Load time: 0:01.234 | Profile: TN3270

Wireshark Lab - Filter on single Client

- Very short lived TCP connections
- Closing after TN3270E negotiation fails



SHARE16752.tn3270..pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: ip.addr eq 172.20.97.146 and (tcp.len gt 0 or tcp.flags&7)

```
No.   TTL  Time         dPort  SHARE_SEATTLE_2015:Session 16752 #SHARKatSHARE  Data
 56   128 0.322649000     23      <--- SYN Win7 [Fingerprint: 8192:12
 57    64 0.322706000  63507 zOS 16K 32768:64:0:48:M*,W0
273    64 0.873806000  63506 TN3270 ---> DO TLS                            fffd2e
274   128 0.874686000     23    <--- WONT TLS                              fffc2e
275    64 0.874854000  63506 DO TN3270E --->     :-)                       fffd28
276   128 0.875246000     23                  <------- WILL TN3270E   :-)  fffb28
277    64 0.875366000  63506 TN3270E --> SB Send Device-Type SE --->       fffa280802fff0
278   128 0.875770000     23 TN3270E    <--- SB Device-Type Req SE    :-|  fffa28020749424d2d333237
279    64 0.876786000  63506 TN3270E --> SB Device-Type Reject SE    :-(  fffa2802060503fff0
280   128 0.881413000     23     <--- FIN
281    64 0.882536000  63506 zOS FIN -->
537   128 1.652246000     23 p0f Win7+ :-)  8192:128:1:52,M1460,N,W8,N
538    64 1.652371000  63508 TCP_SYN  :-)
742    64 2.325819000  63507 TCP                                           fffd2e
743   128 2.326600000     23    <--- WONT TLS                              fffc2e
744    64 2.326707000  63507 DO TN3270E --->     :-)                       fffd28
```

File: "\\SMBHOST\shared_mburkhar...   Packets: 42087 · Displayed: 970 (2,3%) · Load time: 0:01.234   Profile: TN3270

Wireshark Lab Reference

- What the TCP payload looks like

Telnet Negotiation

```
FFFD2E DO   TLS
FFFC2E WONT TLS
FFFD28 DO   TN3270E
FFFB28 WILL TN3270E
FFFA28 SB TN3270E
          00 Associate
          01 Connect
          02 Dev-Type
          03 Functions
          04 Is
          05 Reason
          06 Reject
          07 Request
          08 Send
```

Keepalive Probes

```
FFFB06 WILL TIMEMARK
FFFC06 WONT TIMEMARK
FFFD06 DO TIMEMARK
```

```
8055010301 SSLV2 ClientHello V31
14 --- Change Cipher Spec ---
1403vv 0001 01 ChangeCipherSpec
15 --- Alert ----------------
1603vv xxxx yy
    00  SSL3.0
16 --- Handshake Protocol ---
1603vv xxxx yy
    00  SSL3.0
    01  TLS1.0
    02  TLS1.1
    03  TLS1.2
            01 ClientHello
            02 ServerHello
            0B Certificate
            0E ServerHelloDone
            10 ClientKeyExchange
17 --- Application Data ---
1703vv xxxx yy Encrypted ApplData
```