#SHAREorg

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

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com
de.linkedin.com/in/mreede/

http://tinyurl.com/*wire*SHARE

Session 15189 SHARE in Anaheim

Wireshark Name Resolution
MAC addresses, IP addresses

Help → About wireshark → Folders: Global Configuration

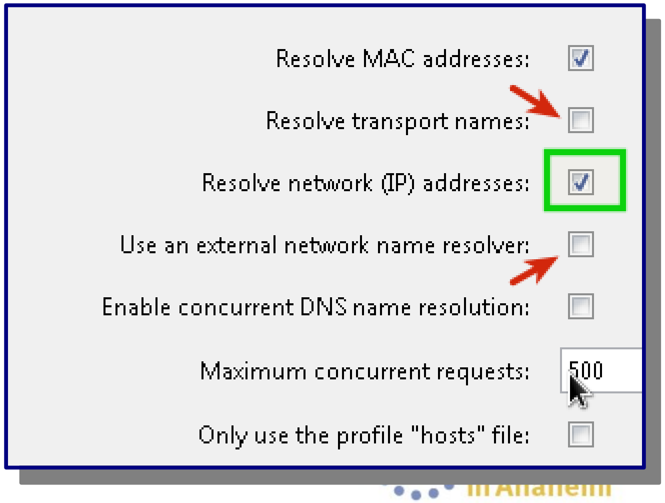
- **`manuf`** resolves MAC prefixes to vendors
- Requires Administrator privileges to change

Help → About wireshark → Folders: Personal Configuration

- **`ethers`** resolves full MAC addresses to a name
- **`hosts`** resolves ip addresses to names (without DNS!)

Edit → Preferences → Name Resolution

- Disable Transport resolution
- Do not use external DNS!



Resolve MAC addresses: ☑

Resolve transport names: ☐

Resolve network (IP) addresses: ☑

Use an external network name resolver: ☐

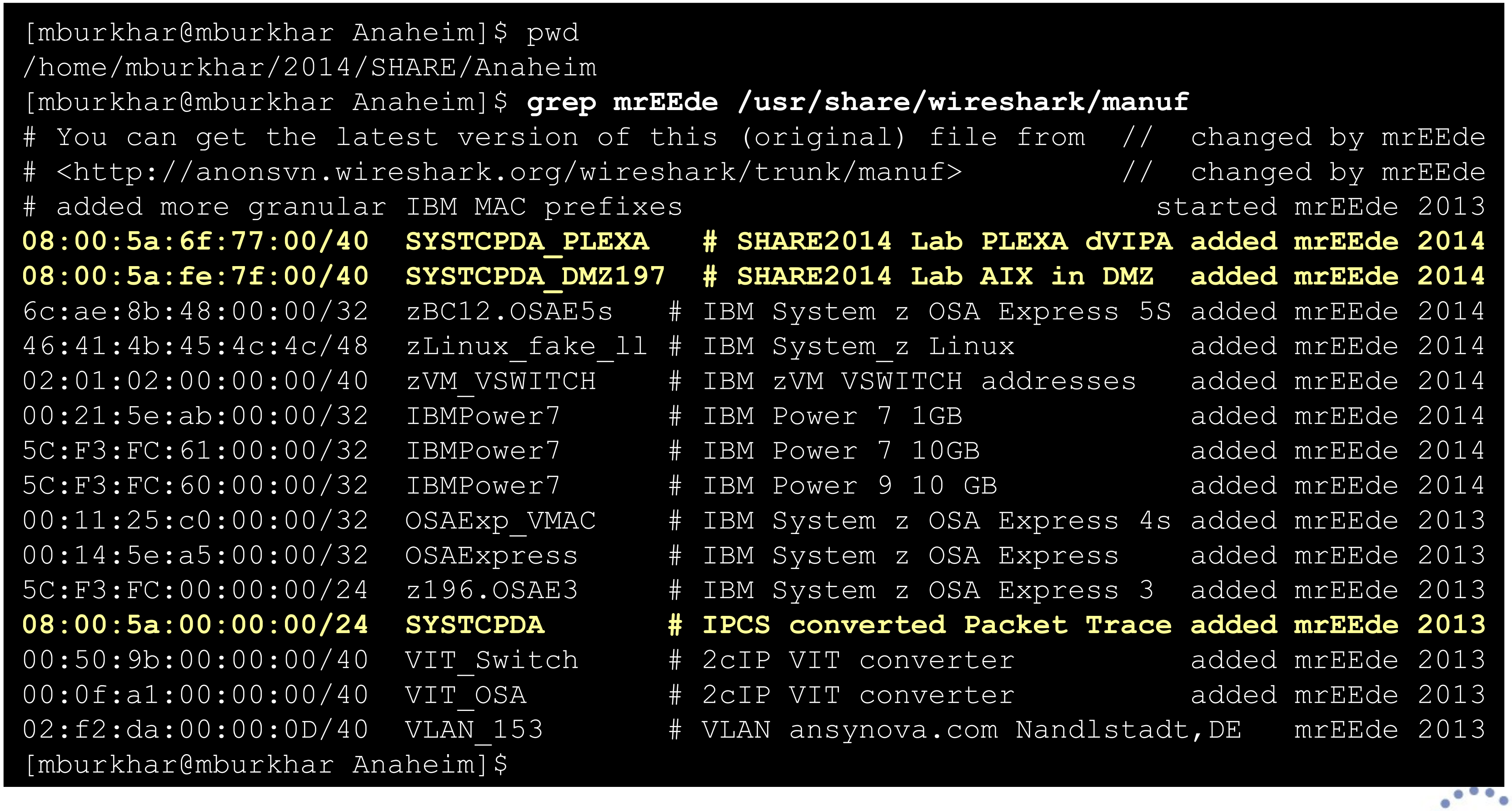
Enable concurrent DNS name resolution: ☐

Maximum concurrent requests: 500

Only use the profile "hosts" file: ☐

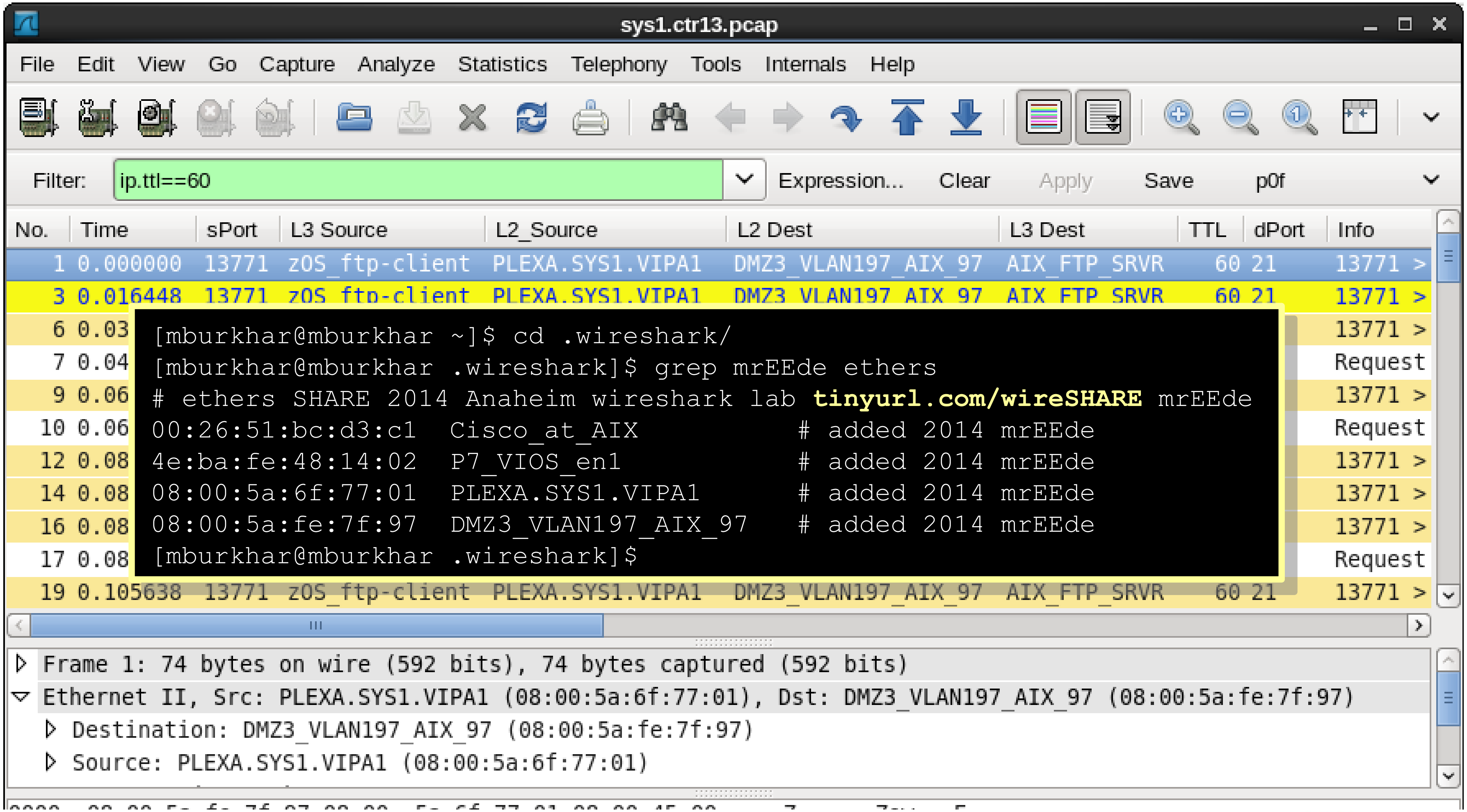
Resolving Ethernet MAC Prefixes
Global Config: `manuf`

Admin rights are required to change this file!



```
[mburkhar@mburkhar Anaheim]$ pwd
/home/mburkhar/2014/SHARE/Anaheim
[mburkhar@mburkhar Anaheim]$ grep mrEEde /usr/share/wireshark/manuf
# You can get the latest version of this (original) file from  //  changed by mrEEde
# <http://anonsvn.wireshark.org/wireshark/trunk/manuf>         //  changed by mrEEde
# added more granular IBM MAC prefixes                           started mrEEde 2013
08:00:5a:6f:77:00/40  SYSTCPDA_PLEXA   # SHARE2014 Lab PLEXA dVIPA added mrEEde 2014
08:00:5a:fe:7f:00/40  SYSTCPDA_DMZ197  # SHARE2014 Lab AIX in DMZ  added mrEEde 2014
6c:ae:8b:48:00:00/32  zBC12.OSAE5s   # IBM System z OSA Express 5S added mrEEde 2014
46:41:4b:45:4c:4c/48  zLinux_fake_ll # IBM System_z Linux          added mrEEde 2014
02:01:02:00:00:00/40  zVM_VSWITCH    # IBM zVM VSWITCH addresses   added mrEEde 2014
00:21:5e:ab:00:00/32  IBMPower7      # IBM Power 7 1GB             added mrEEde 2014
5C:F3:FC:61:00:00/32  IBMPower7      # IBM Power 7 10GB            added mrEEde 2014
5C:F3:FC:60:00:00/32  IBMPower7      # IBM Power 9 10 GB           added mrEEde 2014
00:11:25:c0:00:00/32  OSAExp_VMAC    # IBM System z OSA Express 4s added mrEEde 2013
00:14:5e:a5:00:00/32  OSAExpress     # IBM System z OSA Express    added mrEEde 2013
5C:F3:FC:00:00:00/24  z196.OSAE3     # IBM System z OSA Express 3  added mrEEde 2013
08:00:5a:00:00:00/24  SYSTCPDA       # IPCS converted Packet Trace added mrEEde 2013
00:50:9b:00:00:00/40  VIT_Switch     # 2cIP VIT converter          added mrEEde 2013
00:0f:a1:00:00:00/40  VIT_OSA        # 2cIP VIT converter          added mrEEde 2013
02:f2:da:00:00:0D/40  VLAN_153       # VLAN ansynova.com Nandlstadt,DE   mrEEde 2013
[mburkhar@mburkhar Anaheim]$
```

Resolving Full Ethernet MAC Addresses
Personal Config: ethers


sys1.ctr13.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save p0f

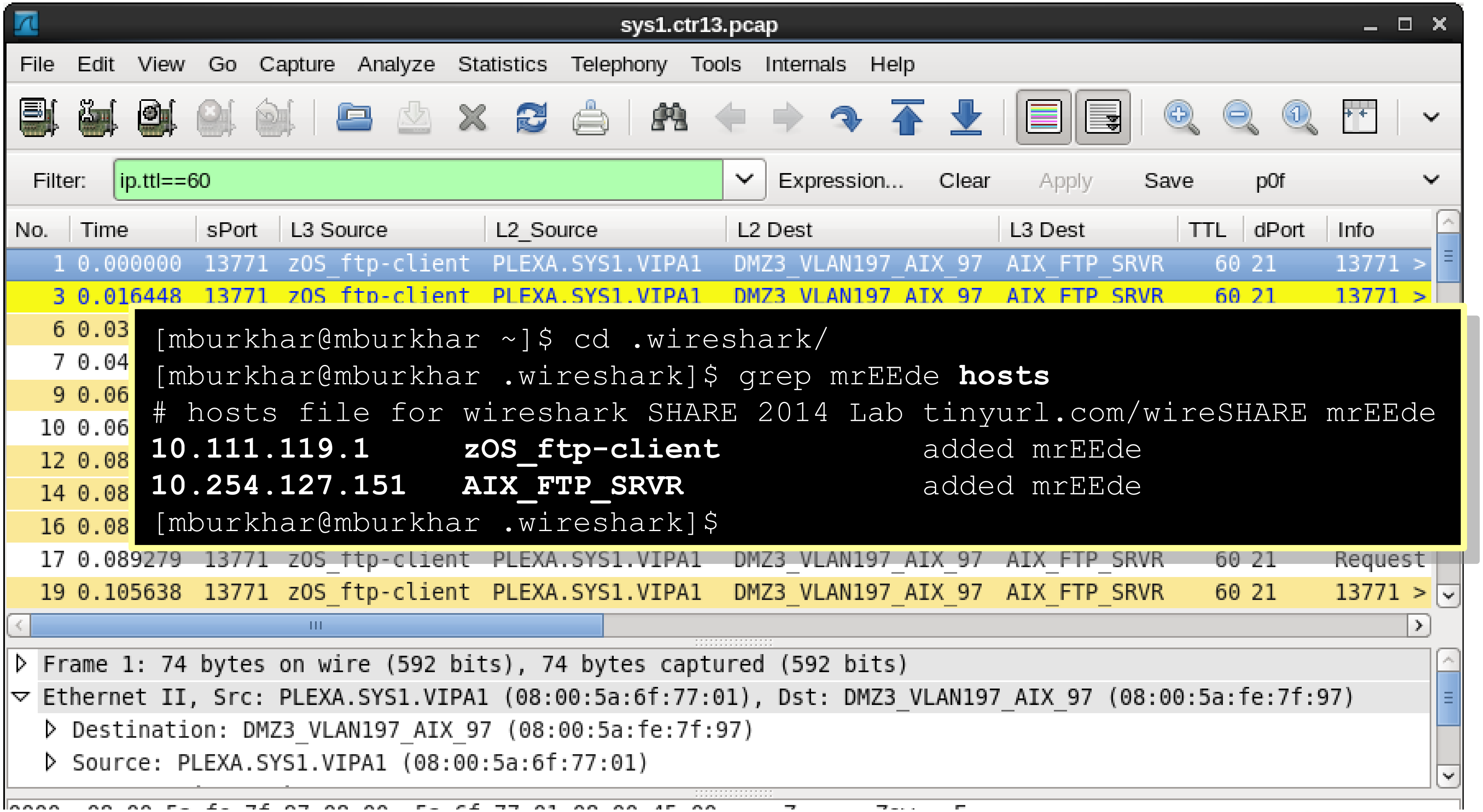
Filter: ip.ttl==60

```
No. Time      sPort L3 Source      L2_Source         L2 Dest              L3 Dest      TTL dPort Info
  1 0.000000  13771 zOS_ftp-client PLEXA.SYS1.VIPA1  DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR  60 21   13771 >
  3 0.016448  13771 zOS_ftp-client PLEXA.SYS1.VIPA1  DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR  60 21   13771 >
  6 0.03                                                                                       13771 >
  7 0.04                                                                                       Request
  9 0.06                                                                                       13771 >
 10 0.06                                                                                       Request
 12 0.08                                                                                       13771 >
 14 0.08                                                                                       13771 >
 16 0.08                                                                                       13771 >
 17 0.08                                                                                       Request
 19 0.105638  13771 zOS_ftp-client PLEXA.SYS1.VIPA1  DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR  60 21   13771 >
```

```
[mburkhar@mburkhar ~]$ cd .wireshark/
[mburkhar@mburkhar .wireshark]$ grep mrEEde ethers
# ethers SHARE 2014 Anaheim wireshark lab tinyurl.com/wireSHARE mrEEde
00:26:51:bc:d3:c1  Cisco_at_AIX           # added 2014 mrEEde
4e:ba:fe:48:14:02  P7_VIOS_en1            # added 2014 mrEEde
08:00:5a:6f:77:01  PLEXA.SYS1.VIPA1       # added 2014 mrEEde
08:00:5a:fe:7f:97  DMZ3_VLAN197_AIX_97    # added 2014 mrEEde
[mburkhar@mburkhar .wireshark]$
```

```
▷ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▽ Ethernet II, Src: PLEXA.SYS1.VIPA1 (08:00:5a:6f:77:01), Dst: DMZ3_VLAN197_AIX_97 (08:00:5a:fe:7f:97)
  ▷ Destination: DMZ3_VLAN197_AIX_97 (08:00:5a:fe:7f:97)
  ▷ Source: PLEXA.SYS1.VIPA1 (08:00:5a:6f:77:01)
```

Resolving IP addresses
Personal Config: hosts


sys1.ctr13.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save p0f

Filter: ip.ttl==60

```
No.  Time      sPort  L3 Source       L2_Source          L2 Dest              L3 Dest        TTL dPort Info
  1 0.000000  13771  zOS_ftp-client  PLEXA.SYS1.VIPA1   DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR   60 21     13771 >
  3 0.016448  13771  zOS_ftp-client  PLEXA.SYS1.VIPA1   DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR   60 21     13771 >
  6 0.03
  7 0.04
  9 0.06
 10 0.06
 12 0.08
 14 0.08
 16 0.08
 17 0.089279  13771  zOS_ftp-client  PLEXA.SYS1.VIPA1   DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR   60 21     Request
 19 0.105638  13771  zOS_ftp-client  PLEXA.SYS1.VIPA1   DMZ3_VLAN197_AIX_97  AIX_FTP_SRVR   60 21     13771 >
```

```
[mburkhar@mburkhar ~]$ cd .wireshark/
[mburkhar@mburkhar .wireshark]$ grep mrEEde hosts
# hosts file for wireshark SHARE 2014 Lab tinyurl.com/wireSHARE mrEEde
10.111.119.1      zOS_ftp-client                    added mrEEde
10.254.127.151    AIX_FTP_SRVR                      added mrEEde
[mburkhar@mburkhar .wireshark]$
```

```
▷ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▽ Ethernet II, Src: PLEXA.SYS1.VIPA1 (08:00:5a:6f:77:01), Dst: DMZ3_VLAN197_AIX_97 (08:00:5a:fe:7f:97)
  ▷ Destination: DMZ3_VLAN197_AIX_97 (08:00:5a:fe:7f:97)
  ▷ Source: PLEXA.SYS1.VIPA1 (08:00:5a:6f:77:01)
```

Wireshark Filters
TCP Session Setup and Termination

TCP sessions are started with the 3-way-Handshake

- Client sends SYN packet
- Server sends SYN_ACK packet
- Client sends ACK to acknowledge the SYN_ACK

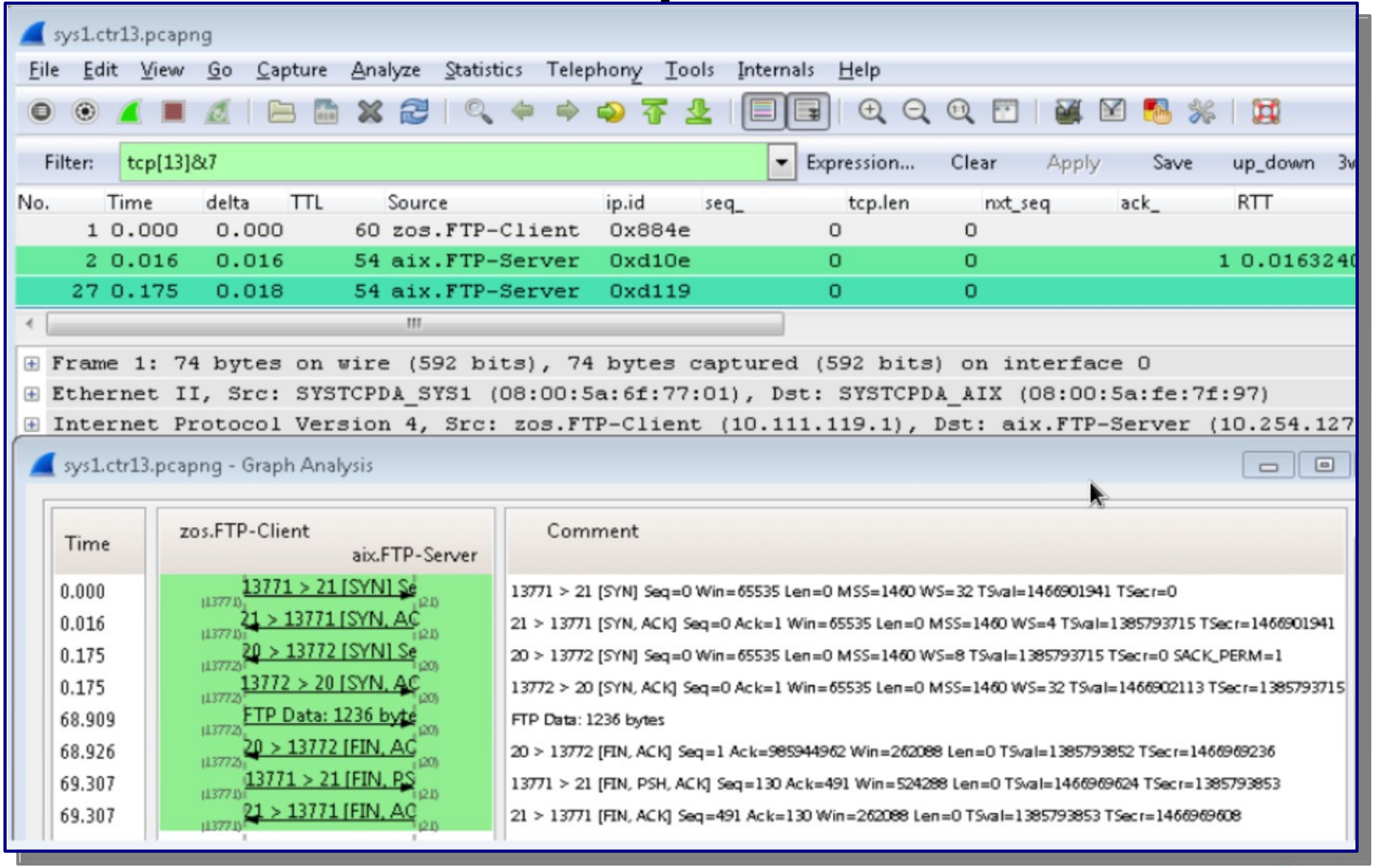
TCP sessions are ended normally with either side sending a FIN and ACKing the partner's FIN

TCP sessions can also be ended by RESET packet. This immediatel breaks the session and the applications will see nasty errno returncodes like ECONNRESET

The SYN,FIN,RST flags are at offset13 into the TCP header

The filter `tcp[13]&7` matches when any of those are set.

up_down Filter tcp[13]&7
Statistics → Flow Graph



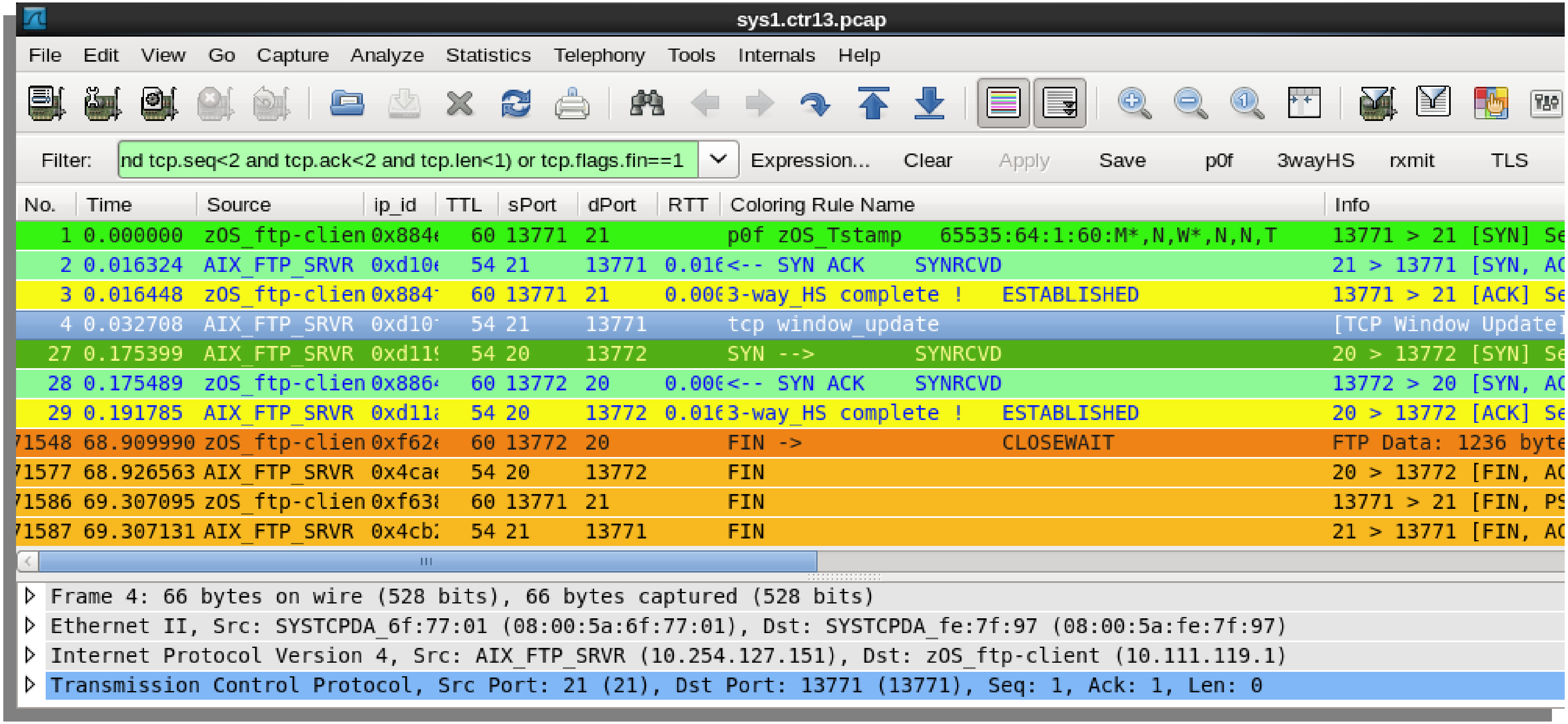
Filter: tcp[13]&7

```
No.      Time    delta     TTL   Source            ip.id     seq_       tcp.len     nxt_seq     ack_     RTT
      1 0.000     0.000     60 zos.FTP-Client    0x884e            0          0
      2 0.016     0.016     54 aix.FTP-Server    0xd10e            0          0                         1 0.016324
     27 0.175     0.018     54 aix.FTP-Server    0xd119            0          0
```

```
⊞ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: SYSTCPDA_SYS1 (08:00:5a:6f:77:01), Dst: SYSTCPDA_AIX (08:00:5a:fe:7f:97)
⊞ Internet Protocol Version 4, Src: zos.FTP-Client (10.111.119.1), Dst: aix.FTP-Server (10.254.127
```

Time	zos.FTP-Client aix.FTP-Server	Comment
0.000	(13771) 13771 > 21 [SYN] Se (21)	13771 > 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1466901941 TSecr=0
0.016	(13771) 21 > 13771 [SYN, AC (21)	21 > 13771 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=4 TSval=1385793715 TSecr=1466901941
0.175	(13772) 20 > 13772 [SYN] Se (20)	20 > 13772 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=1385793715 TSecr=0 SACK_PERM=1
0.175	(13772) 13772 > 20 [SYN, AC (20)	13772 > 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 TSval=1466902113 TSecr=1385793715
68.909	(13772) FTP Data: 1236 byte (20)	FTP Data: 1236 bytes
68.926	(13772) 20 > 13772 [FIN, AC (20)	20 > 13772 [FIN, ACK] Seq=1 Ack=985944962 Win=262088 Len=0 TSval=1385793852 TSecr=1466969236
69.307	(13771) 13771 > 21 [FIN, PS (21)	13771 > 21 [FIN, PSH, ACK] Seq=130 Ack=491 Win=524288 Len=0 TSval=1466969624 TSecr=1385793853
69.307	(13771) 21 > 13771 [FIN, AC (21)	21 > 13771 [FIN, ACK] Seq=491 Ack=130 Win=262088 Len=0 TSval=1385793853 TSecr=1466969608

Colors Columns and Filters
Wireshark Profiles



Filter: nd tcp.seq<2 and tcp.ack<2 and tcp.len<1) or tcp.flags.fin==1

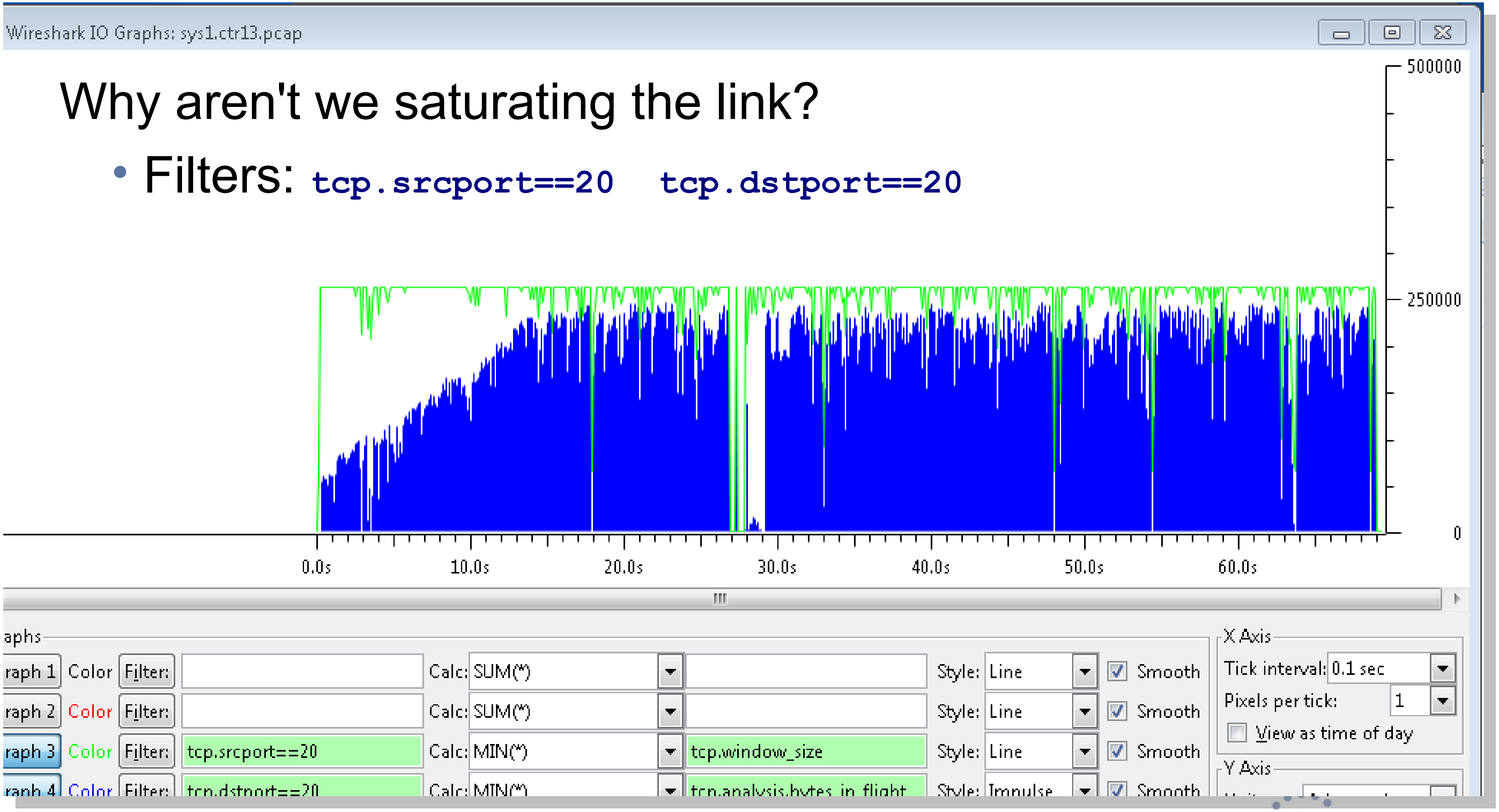
```
No.   Time      Source        ip_id   TTL sPort dPort RTT   Coloring Rule Name                                   Info
    1 0.000000  zOS_ftp-clien 0x884    60 13771 21          p0f zOS_Tstamp    65535:64:1:60:M*,N,W*,N,N,T        13771 > 21 [SYN] Se
    2 0.016324  AIX_FTP_SRVR  0xd10    54 21    13771 0.01  <-- SYN ACK      SYNRCVD                             21 > 13771 [SYN, AC
    3 0.016448  zOS_ftp-clien 0x884    60 13771 21    0.00  3-way_HS complete !     ESTABLISHED                  13771 > 21 [ACK] Se
    4 0.032708  AIX_FTP_SRVR  0xd10    54 21    13771       tcp window_update                                    [TCP Window Update]
   27 0.175399  AIX_FTP_SRVR  0xd11    54 20    13772       SYN -->          SYNRCVD                             20 > 13772 [SYN] Se
   28 0.175489  zOS_ftp-clien 0x886    60 13772 20    0.00  <-- SYN ACK      SYNRCVD                             13772 > 20 [SYN, AC
   29 0.191785  AIX_FTP_SRVR  0xd11    54 20    13772 0.01  3-way_HS complete !     ESTABLISHED                  20 > 13772 [ACK] Se
71548 68.909990 zOS_ftp-clien 0xf62    60 13772 20          FIN ->                  CLOSEWAIT                    FTP Data: 1236 byte
71577 68.926563 AIX_FTP_SRVR  0x4ca    54 20    13772       FIN                                                  20 > 13772 [FIN, AC
71586 69.307095 zOS_ftp-clien 0xf63    60 13771 21          FIN                                                  13771 > 21 [FIN, PS
71587 69.307131 AIX_FTP_SRVR  0x4cb    54 21    13771       FIN                                                  21 > 13771 [FIN, AC
```

```
▷ Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▷ Ethernet II, Src: SYSTCPDA_6f:77:01 (08:00:5a:6f:77:01), Dst: SYSTCPDA_fe:7f:97 (08:00:5a:fe:7f:97)
▷ Internet Protocol Version 4, Src: AIX_FTP_SRVR (10.254.127.151), Dst: zOS_ftp-client (10.111.119.1)
▷ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 13771 (13771), Seq: 1, Ack: 1, Len: 0
```

Bring your Sunglasses!

Profile SHARE2014: `colorfilters preferences dfilters`

sys1.ctr13.pcap
Statistics → IO Graph – rwin vs. inflight data



Why aren't we saturating the link?

- Filters: `tcp.srcport==20` `tcp.dstport==20`

aphs

raph 1	Color	Filter:		Calc: SUM(*)		Style: Line	☑	Smooth
raph 2	Color	Filter:		Calc: SUM(*)		Style: Line	☑	Smooth
raph 3	Color	Filter:	tcp.srcport==20	Calc: MIN(*)	tcp.window_size	Style: Line	☑	Smooth
raph 4	Color	Filter:	tcp.dstport==20	Calc: MIN(*)	tcp.analysis.bytes_in_flight	Style: Impulse	☑	Smooth

X Axis

Tick interval: 0.1 sec

Pixels per tick: 1

☐ View as time of day

Y Axis

sys1.ctr13.pcap
BDP Bandwidth-Delay-Product

The Throughput of streaming workload requires sufficient Receive Buffer sizes to maintain a constant flow of data

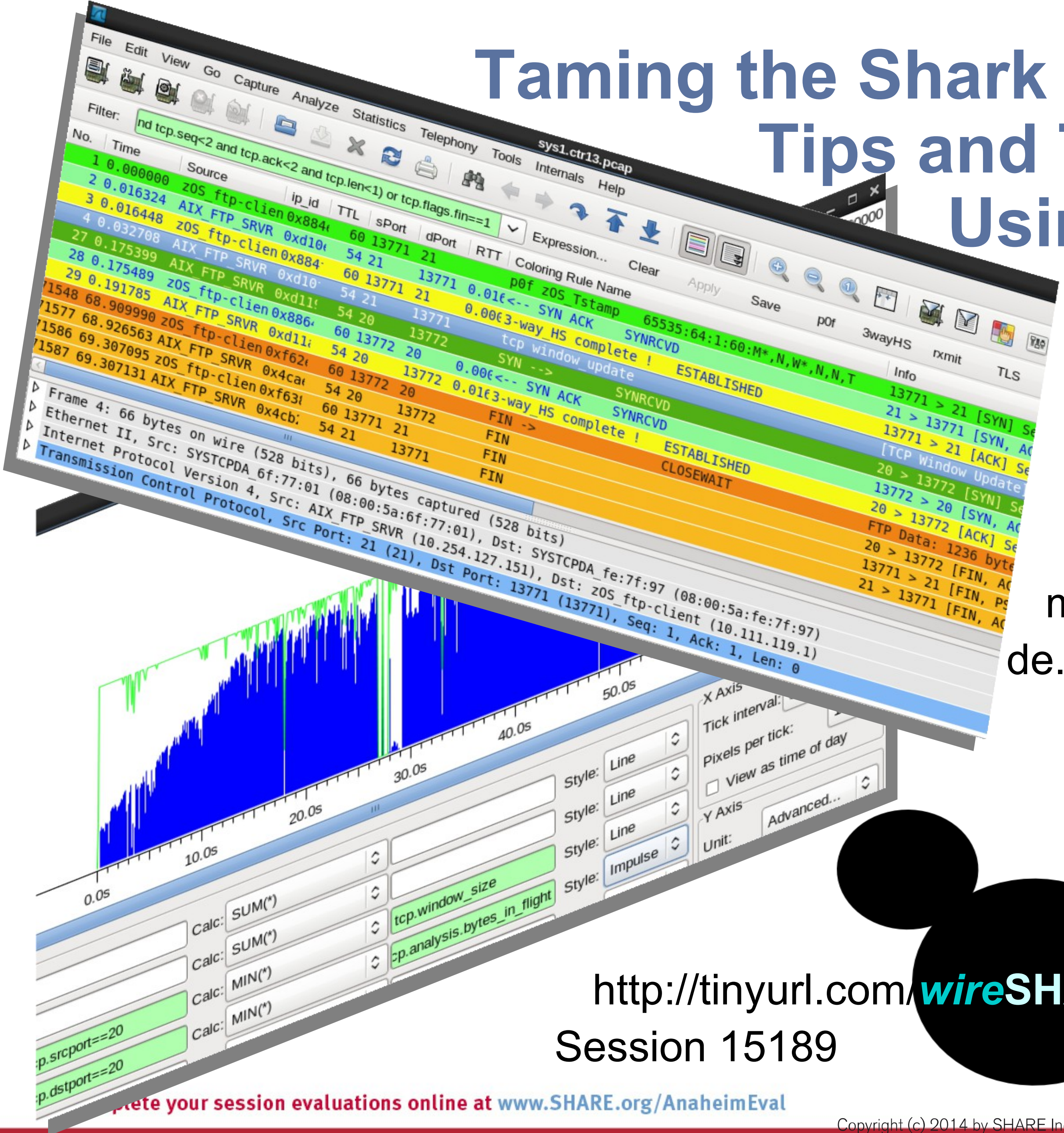
The BDP helps to calculate the required windowsizes.

- http://en.wikipedia.org/wiki/Bandwidth-delay_product

Given the RTT and Windowsize offerings, is the customer's expectation of 50MB/s FTP throughput realistic?

- What bandwidth is required to send at 50 MegaByte/s?
  - 1 MegaByte is 1024*1204 bytes
  - 1 Bytes is 8 bits
  - 1 Mbit is 1000*1000 bits
- How large would the window sizes have to be?
  - http://www.speedguide.net/bdp.php

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



```
nd tcp.seq<2 and tcp.ack<2 and tcp.len<1) or tcp.flags.fin==1

No. Time     Source        ip_id TTL sPort dPort RTT   Coloring Rule Name                      Info
 1 0.000000  zOS_ftp-clien 0x884  60 13771 21          p0f zOS_Tstamp 65535:64:1:60:M*,N,W*,N,N,T  13771 > 21 [SYN] Se
 2 0.016324  AIX_FTP_SRVR  0xd10  54 21    13771 0.016 <-- SYN ACK      SYNRCVD               21 > 13771 [SYN, AC
 3 0.016448  zOS_ftp-clien 0x884  60 13771 21    0.000 3-way_HS complete !  ESTABLISHED       13771 > 21 [ACK] Se
 4 0.032708  AIX_FTP_SRVR  0xd10  54 21    13771       tcp window_update                      [TCP Window Update]
27 0.175399  AIX_FTP_SRVR  0xd11  54 20    13772       SYN -->          SYNRCVD               20 > 13772 [SYN] Se
28 0.175489  zOS_ftp-clien 0x886  60 13772 20    0.006 <-- SYN ACK      SYNRCVD               13772 > 20 [SYN, AC
29 0.191785  AIX_FTP_SRVR  0xd11  54 20    13772 0.016 3-way_HS complete !  ESTABLISHED       20 > 13772 [ACK] Se
1548 68.909990 zOS_ftp-clien 0xf62 60 13772 20         FIN ->           CLOSEWAIT             FTP Data: 1236 byte
1577 68.926563 AIX_FTP_SRVR 0x4ca  54 20    13772       FIN                                    20 > 13772 [FIN, AC
1586 69.307095 zOS_ftp-clien 0xf63 60 13771 21          FIN                                    13771 > 21 [FIN, PS
1587 69.307131 AIX_FTP_SRVR 0x4cb  54 21    13771       FIN                                    21 > 13771 [FIN, AC

▷ Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▷ Ethernet II, Src: SYSTCPDA_6f:77:01 (08:00:5a:6f:77:01), Dst: SYSTCPDA_fe:7f:97 (08:00:5a:fe:7f:97)
▷ Internet Protocol Version 4, Src: AIX_FTP_SRVR (10.254.127.151), Dst: zOS_ftp-client (10.111.119.1)
▷ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 13771 (13771), Seq: 1, Ack: 1, Len: 0
```

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com
de.linkedin.com/in/mreede/

http://tinyurl.com/*wire*SHARE

Session 15189

SHARE in Anaheim