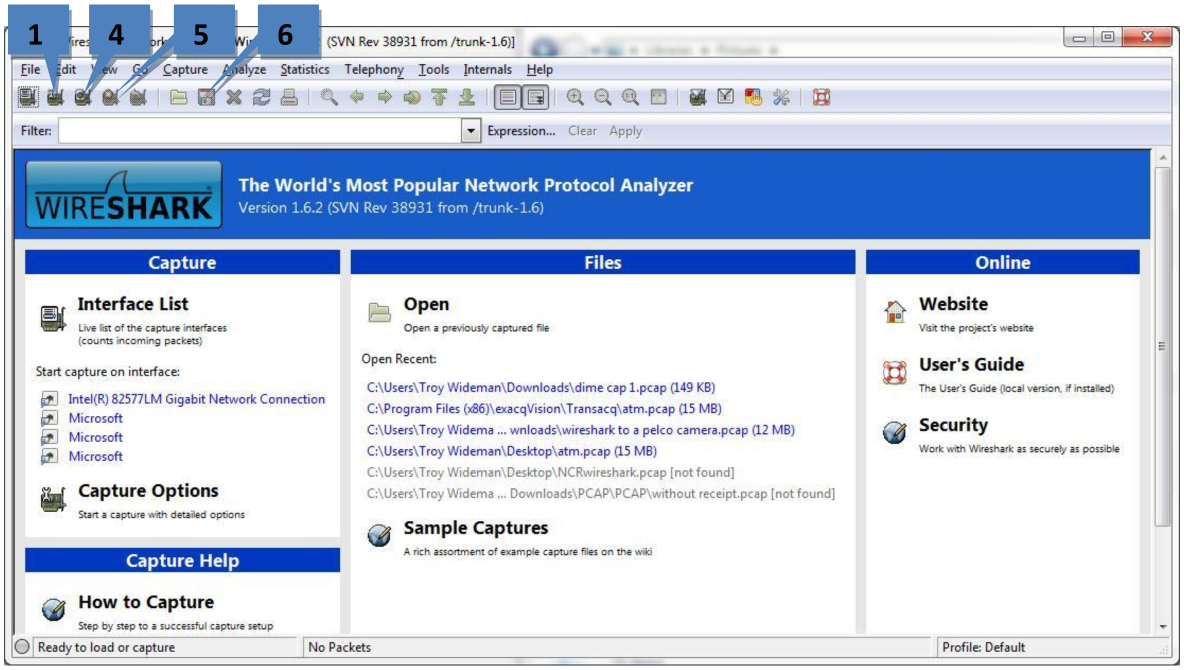
1 Introduction

This document provides information on how to effectively use Wireshark for data and packet analysis. It also provides details on setting up the interfaces and filters for effective display of packets.

- **Windows:** For the Windows OS, Wireshark can be downloaded from, http://www.wireshark.org/
- **Linux (Ubuntu):** Search for Wireshark in the Ubuntu Software Center.

2 Using Wireshark to Obtain and Save a .pcap File

To use Wireshark, complete the following steps on the main Wireshark page:



The World's Most Popular Network Protocol Analyzer
Version 1.6.2 (SVN Rev 38931 from /trunk-1.6)

Interface List — Live list of the capture interfaces (counts incoming packets)

Start capture on interface:
- Intel(R) 82577LM Gigabit Network Connection
- Microsoft
- Microsoft
- Microsoft

Capture Options — Start a capture with detailed options

Open — Open a previously captured file

Open Recent:
- C:\Users\Troy Wideman\Downloads\dime cap 1.pcap (149 KB)
- C:\Program Files (x86)\exacqVision\Transacq\atm.pcap (15 MB)
- C:\Users\Troy Widema ... wnloads\wireshark to a pelco camera.pcap (12 MB)
- C:\Users\Troy Wideman\Desktop\atm.pcap (15 MB)
- C:\Users\Troy Wideman\Desktop\NCRwireshark.pcap [not found]
- C:\Users\Troy Widema ... Downloads\PCAP\PCAP\without receipt.pcap [not found]

Sample Captures — A rich assortment of example capture files on the wiki

Website — Visit the project's website

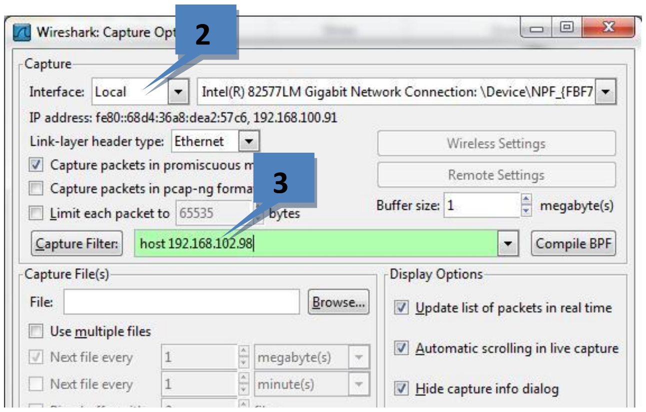
User's Guide — The User's Guide (local version, if installed)

Security — Work with Wireshark as securely as possible

How to Capture — Step by step to a successful capture setup

Ready to load or capture | No Packets | Profile: Default

1. Click the **Show the capture options…** button. This opens the following window:



Interface: Local | Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{FBF7

IP address: fe80::68d4:36a8:dea2:57c6, 192.168.100.91

Link-layer header type: Ethernet

☑ Capture packets in promiscuous m

☐ Capture packets in pcap-ng forma

☐ Limit each packet to 65535 bytes

Buffer size: 1 megabyte(s)

Capture Filter: host 192.168.102.98

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

2. Select the interface that you want to monitor from the Interface drop-down list.

3. In the field next to the **Capture Filter** button, enter the IP address of the device you want to monitor. This must always be preceded by the word **host**. For example, if you want to monitor IP address 192.168.102.98, enter **host 192.168.102.98**.

4. Back on the main page, click the **Start a new live capture** button.

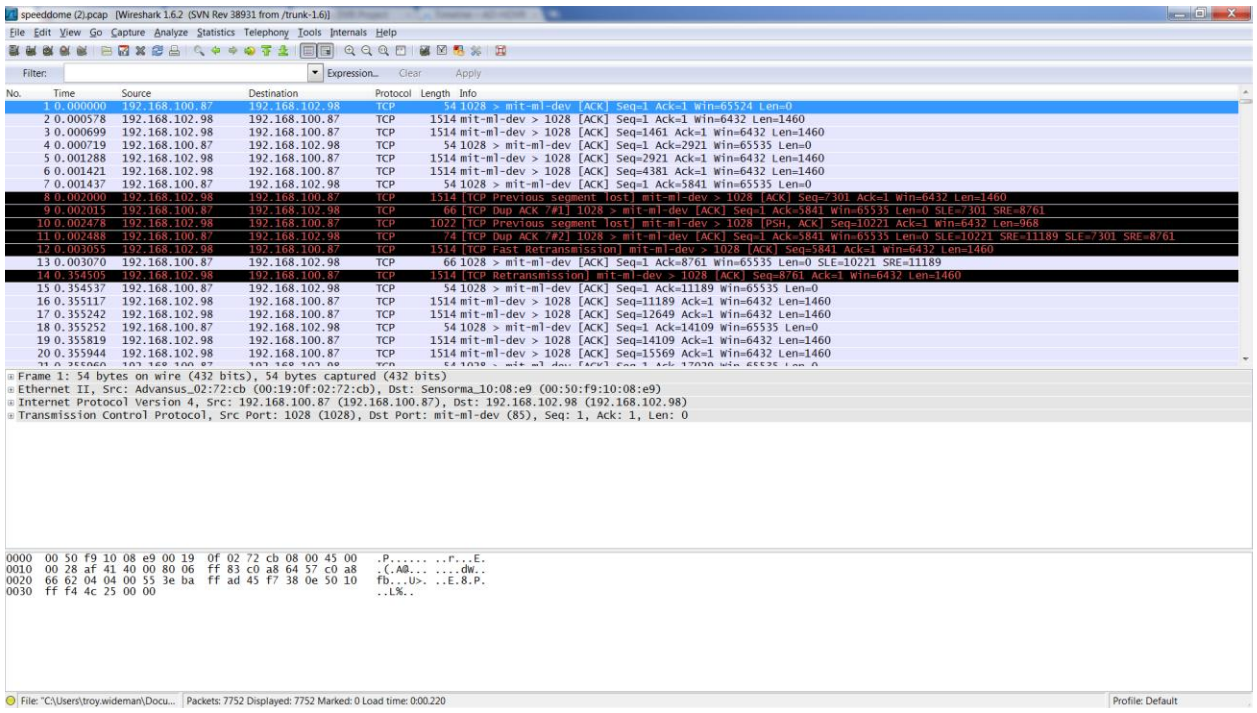
5. After the capture runs long enough to obtain the desired data, click the **Stop the running live capture** button.

   NOTE: If you do not stop the capture, it will continue to run until the hard drive is full.

6. To save the capture, click the **Save capture file as…** button. Enter a filename, select a location, and click Save.

3 Using Wireshark to Track Packets

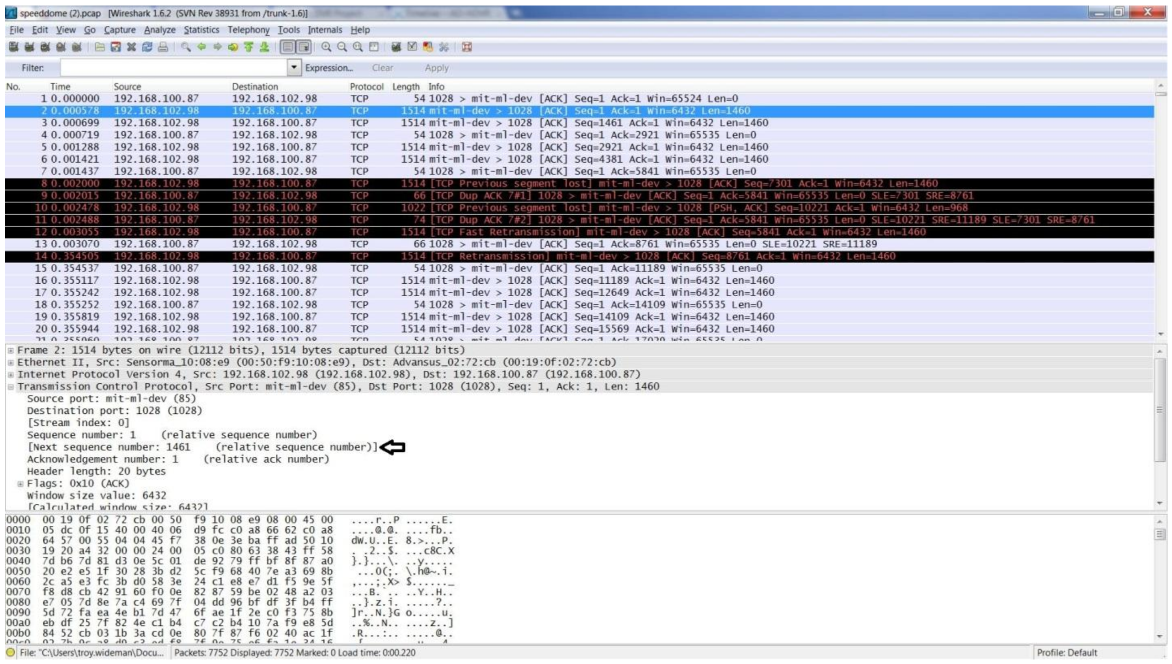
To use Wireshark to track packet losses, open a previously obtained .pcap file. It should appear similar to this:



```
speeddome (2).pcap  [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
    2 0.000578   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
    3 0.000699   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
    4 0.000719   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
    5 0.001288   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
    6 0.001421   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
    7 0.001437   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
    8 0.002000   192.168.102.98   192.168.100.87   TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
    9 0.002015   192.168.100.87   192.168.102.98   TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
   10 0.002478   192.168.102.98   192.168.100.87   TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
   11 0.002488   192.168.100.87   192.168.102.98   TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
   12 0.003055   192.168.102.98   192.168.100.87   TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
   13 0.003070   192.168.100.87   192.168.102.98   TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
   14 0.354505   192.168.102.98   192.168.100.87   TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
   15 0.354537   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
   16 0.355117   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
   17 0.355242   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
   18 0.355252   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
   19 0.355819   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
   20 0.355944   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Advansus_02:72:cb (00:19:0f:02:72:cb), Dst: Sensorma_10:08:e9 (00:50:f9:10:08:e9)
⊞ Internet Protocol Version 4, Src: 192.168.100.87 (192.168.100.87), Dst: 192.168.102.98 (192.168.102.98)
⊞ Transmission Control Protocol, Src Port: 1028 (1028), Dst Port: mit-ml-dev (85), Seq: 1, Ack: 1, Len: 0

0000  00 50 f9 10 08 e9 00 19  0f 02 72 cb 08 00 45 00   .P...... ..r...E.
0010  00 28 af 41 40 00 80 06  ff 83 c0 a8 64 57 c0 a8   .(.A@... ....dW..
0020  66 62 04 04 00 55 3e ba  ff ad 45 f7 38 0e 50 10   fb...U>. ..E.8.P.
0030  ff f4 4c 25 00 00                                  ..L%..

File: "C:\Users\troy.wideman\Docu...   Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply

Analyze the data in the window. In Frame 1, you can see the server 192.168.100.87 is requesting information from the camera 192.168.102.98.

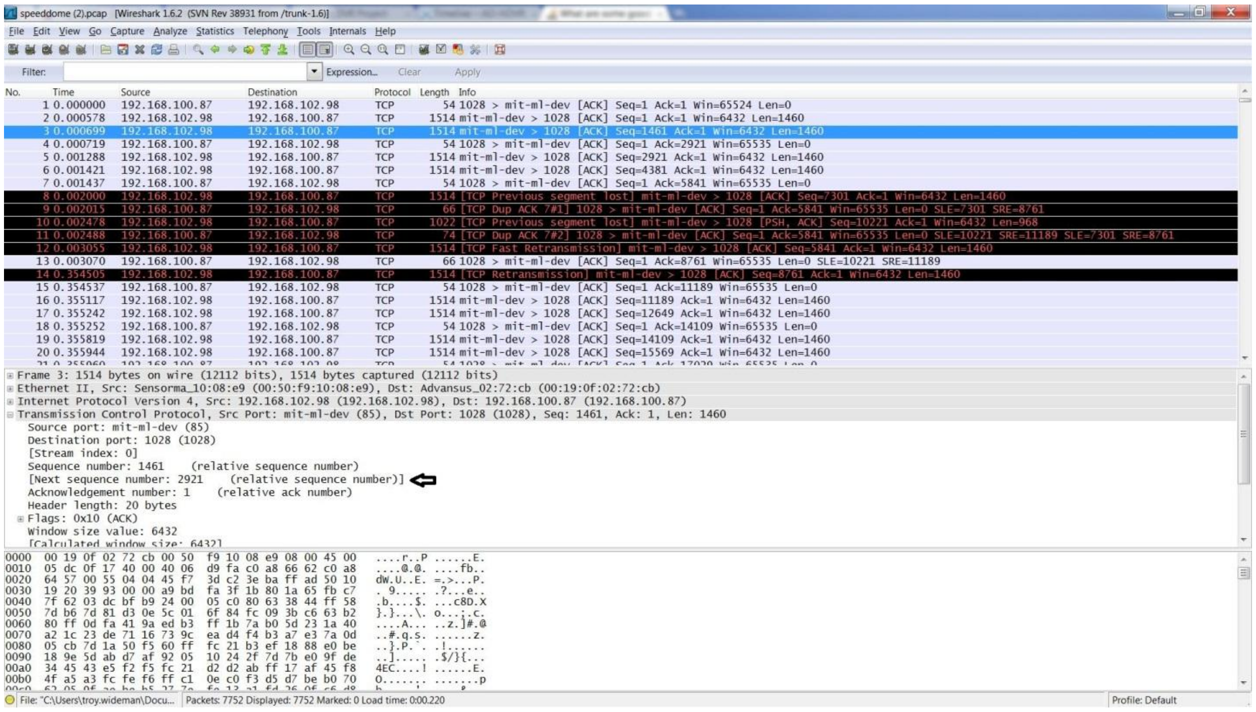


```
speeddome (2).pcap  [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
    2 0.000578   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
    3 0.000699   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
    4 0.000719   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
    5 0.001288   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
    6 0.001421   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
    7 0.001437   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
    8 0.002000   192.168.102.98   192.168.100.87   TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
    9 0.002015   192.168.100.87   192.168.102.98   TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
   10 0.002478   192.168.102.98   192.168.100.87   TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
   11 0.002488   192.168.100.87   192.168.102.98   TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
   12 0.003055   192.168.102.98   192.168.100.87   TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
   13 0.003070   192.168.100.87   192.168.102.98   TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
   14 0.354505   192.168.102.98   192.168.100.87   TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
   15 0.354537   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
   16 0.355117   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
   17 0.355242   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
   18 0.355252   192.168.100.87   192.168.102.98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
   19 0.355819   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
   20 0.355944   192.168.102.98   192.168.100.87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

⊞ Frame 2: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
⊞ Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
⊞ Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
⊟ Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 1, Ack: 1, Len: 1460
    Source port: mit-ml-dev (85)
    Destination port: 1028 (1028)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1461    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 6432
    [Calculated window size: 6432]

0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  05 dc 0f 15 40 00 40 06  d9 fc c0 a8 66 62 c0 a8   ....@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  38 0e 3e ba ff ad 50 10   dW.U..E. 8.>...P.
0030  19 20 a4 32 00 00 24 00  05 c0 80 63 38 43 ff 58   . .2..$. ...c8C.X
0040  7d b6 7d 81 d3 0e 5c 01  de 92 79 ff bf 8f 87 a0   }.}...\. ..y.....
0050  20 e2 e5 1f 30 28 3b d2  5c f9 68 40 7e a3 69 8b    ...0(;. \.h@~.i.
0060  2c a5 e3 fc 3b d0 58 3e  24 c1 e8 e7 d1 f5 9e 5f   ,...;.X> $......_
0070  f8 d8 cb 42 91 60 f0 0e  82 87 59 be 02 48 a2 03   ...B.`.. ..Y..H..
0080  e7 05 7d 8e 7a c4 69 7f  04 dd 96 bf df 3f b4 ff   ..}.z.i. .....?..
0090  5d 72 fa ea 4e b1 7d 47  6f ae 1f 2e c0 f3 75 8b   ]r..N.}G o.....u.
00a0  eb df 25 7f 82 4e c1 b4  c7 c2 b4 10 7a f9 e8 5d   ..%..N.. ....z..]
00b0  84 52 cb 03 1b 3a cd 0e  80 7f 87 f6 02 40 ac 1f   .R...:.. .....@..

File: "C:\Users\troy.wideman\Docu...   Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply

In Frame 2, you would expand the plus sign (+) next to Transmission Control Protocol. You can see the sequence number of the next packet the camera will use (1461, in this case).

Click on Frame 3 to display the following:


speeddome (2).pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
   2 0.000578  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
   3 0.000699  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
   4 0.000719  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
   5 0.001288  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
   6 0.001421  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
   7 0.001437  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
   8 0.002000  192.168.102.98  192.168.100.87  TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
   9 0.002015  192.168.100.87  192.168.102.98  TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
  10 0.002478  192.168.102.98  192.168.100.87  TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
  11 0.002488  192.168.100.87  192.168.102.98  TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
  12 0.003055  192.168.102.98  192.168.100.87  TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
  13 0.003070  192.168.100.87  192.168.102.98  TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
  14 0.354505  192.168.102.98  192.168.100.87  TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
  15 0.354537  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
  16 0.355117  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
  17 0.355242  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
  18 0.355252  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
  19 0.355819  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
  20 0.355944  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460
```

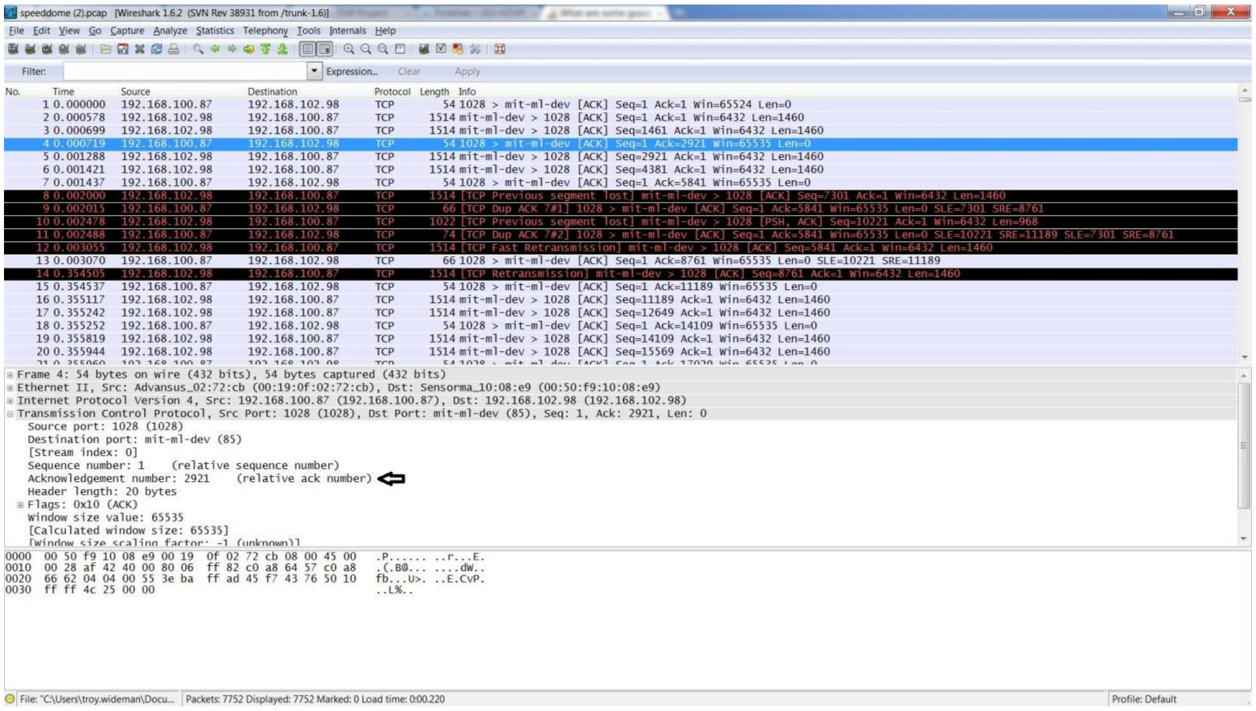
```
⊞ Frame 3: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
⊞ Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
⊞ Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
⊟ Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 1461, Ack: 1, Len: 1460
    Source port: mit-ml-dev (85)
    Destination port: 1028 (1028)
    [Stream index: 0]
    Sequence number: 1461    (relative sequence number)
    [Next sequence number: 2921    (relative sequence number)] ⇦
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 6432
    [Calculated window size: 6432]
```

```
0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  05 dc 0f 17 40 00 40 06  d9 fa c0 a8 66 62 c0 a8   ....@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  3d c2 3e ba ff ad 50 10   dW.U..E. =.>...P.
0030  19 20 39 93 00 00 a9 bd  fa 3f 1b 80 1a 65 fb c7   . 9..... .?...e..
0040  7f 62 03 dc bf b9 24 00  05 c0 80 63 38 44 ff 58   .b....$. ...c8D.X
0050  7d b6 7d 81 d3 0e 5c 01  6f 84 fc 09 3b c6 63 b2   }.}...\. o...;.c.
0060  80 ff 0d fa 41 9a ed b3  ff 1b 7a b0 5d 23 1a 40   ....A... ..z.]#.@
0070  a2 1c 23 de 71 16 73 9c  ea d4 f4 b3 a7 e3 7a 0d   ..#.q.s. ......z.
0080  05 cb 7d 1a 50 f5 60 ff  fc 21 b3 ef 18 88 e0 be   ..}.P.`. .!......
0090  18 9e 5d ab d7 af 92 05  10 24 2f 7d 7b e0 9f de   ..]..... .$/}{...
00a0  34 45 43 e5 f2 f5 fc 21  d2 d2 ab ff 17 af 45 f8   4EC....! ......E.
00b0  4f a5 a3 fc fe f6 ff c1  0e c0 f3 d5 d7 be b0 70   O....... .......p
```

```
File: "C:\Users\troy.wideman\Docu...   Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

In Frame 3, the camera finishes sending the data requested and lets the server know that the next sequence number it intends to use is 2921.

Click on Frame 4 to display the following:


speeddome (2).pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
   2 0.000578  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
   3 0.000699  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
   4 0.000719  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
   5 0.001288  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
   6 0.001421  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
   7 0.001437  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
   8 0.002000  192.168.102.98  192.168.100.87  TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
   9 0.002015  192.168.100.87  192.168.102.98  TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
  10 0.002478  192.168.102.98  192.168.100.87  TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
  11 0.002488  192.168.100.87  192.168.102.98  TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
  12 0.003055  192.168.102.98  192.168.100.87  TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
  13 0.003070  192.168.100.87  192.168.102.98  TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
  14 0.354505  192.168.102.98  192.168.100.87  TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
  15 0.354537  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
  16 0.355117  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
  17 0.355242  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
  18 0.355252  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
  19 0.355819  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
  20 0.355944  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460
```

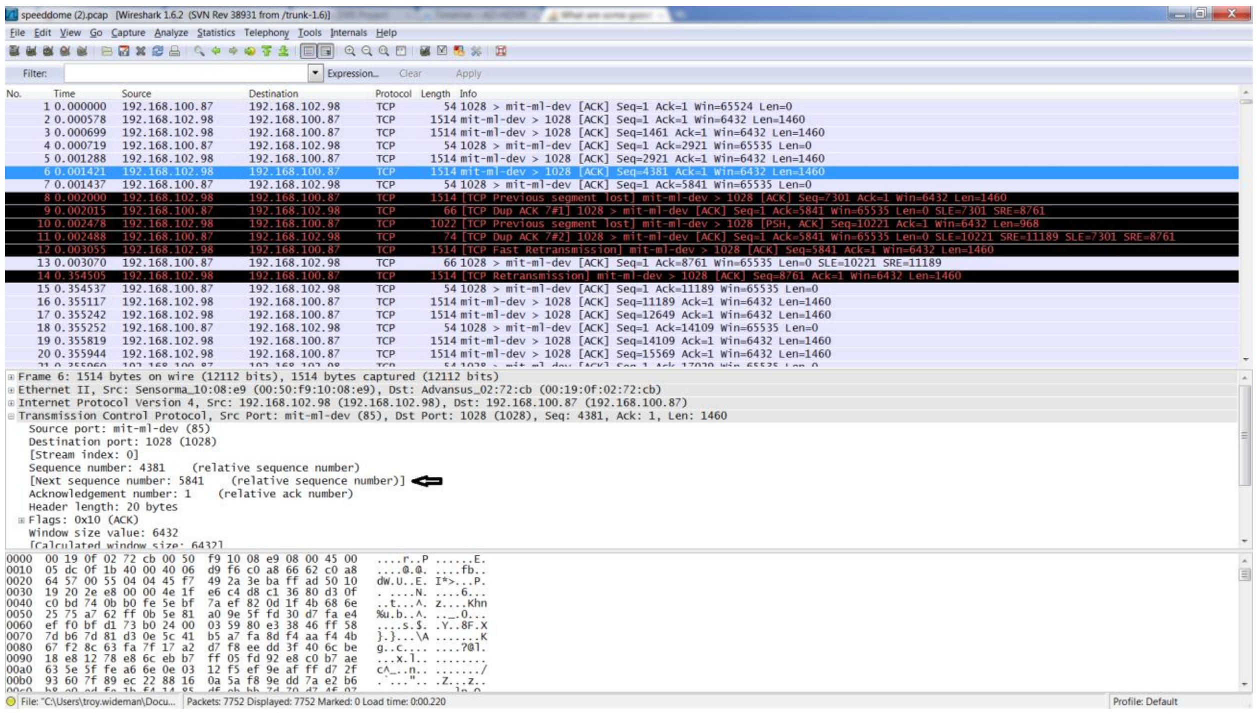
```
⊞ Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Advansus_02:72:cb (00:19:0f:02:72:cb), Dst: Sensorma_10:08:e9 (00:50:f9:10:08:e9)
⊞ Internet Protocol Version 4, Src: 192.168.100.87 (192.168.100.87), Dst: 192.168.102.98 (192.168.102.98)
⊟ Transmission Control Protocol, Src Port: 1028 (1028), Dst Port: mit-ml-dev (85), Seq: 1, Ack: 2921, Len: 0
    Source port: 1028 (1028)
    Destination port: mit-ml-dev (85)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 2921    (relative ack number) ⇦
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -1 (unknown)]
```

```
0000  00 50 f9 10 08 e9 00 19  0f 02 72 cb 08 00 45 00   .P...... ..r...E.
0010  00 28 af 42 40 00 80 06  ff 82 c0 a8 64 57 c0 a8   .(.B@... ....dW..
0020  66 62 04 04 00 55 3e ba  ff ad 45 f7 43 76 50 10   fb...U>. ..E.CvP.
0030  ff ff 4c 25 00 00                                  ..L%..
```

```
File: "C:\Users\troy.wideman\Docu...   Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

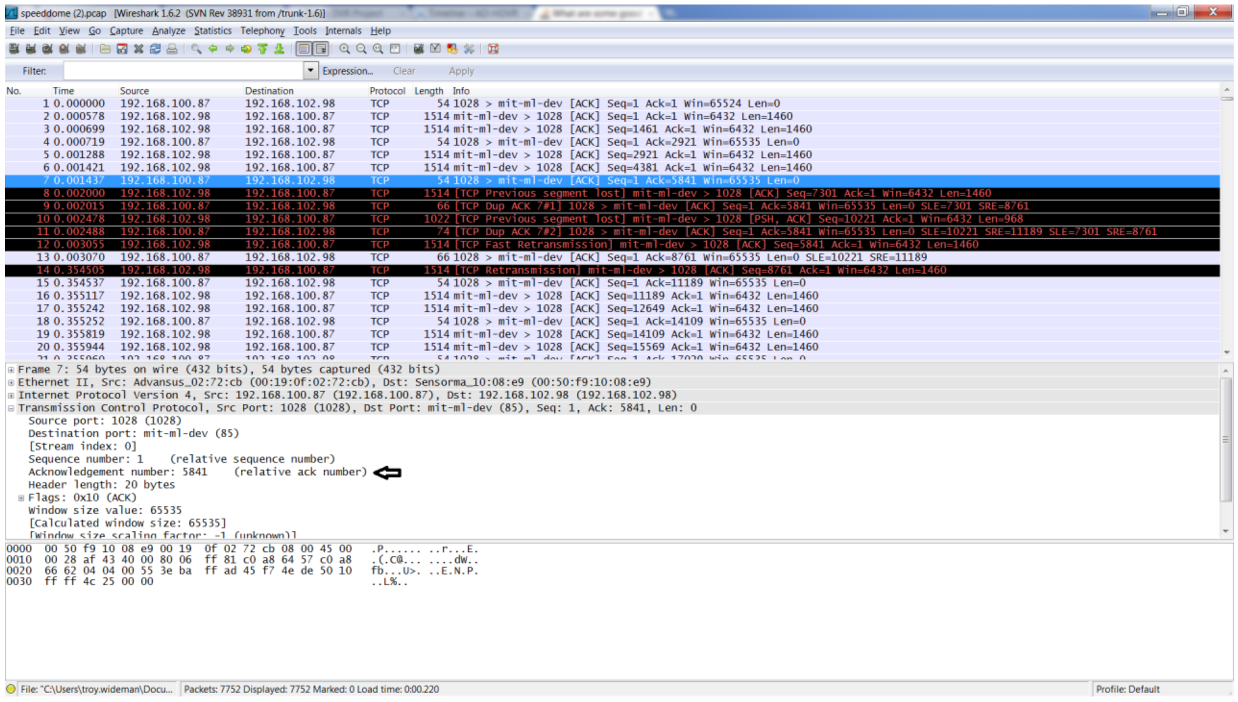
In Frame 4, the server acknowledges that the next sequence will be 2921 and requests information. This process repeats itself. This is how you can verify the information exchanged between server and camera.

In this Wireshark capture, you can see lines that are highlighted in black. This means an error has occurred.



```
speeddome (2).pcap  [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
   2 0.000578  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
   3 0.000699  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
   4 0.000719  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
   5 0.001288  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
   6 0.001421  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
   7 0.001437  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
   8 0.002000  192.168.102.98  192.168.100.87  TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
   9 0.002015  192.168.100.87  192.168.102.98  TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
  10 0.002478  192.168.102.98  192.168.100.87  TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
  11 0.002488  192.168.100.87  192.168.102.98  TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
  12 0.003055  192.168.102.98  192.168.100.87  TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
  13 0.003070  192.168.100.87  192.168.102.98  TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
  14 0.354505  192.168.102.98  192.168.100.87  TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
  15 0.354537  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
  16 0.355117  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
  17 0.355242  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
  18 0.355252  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
  19 0.355819  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
  20 0.355944  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

⊞ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
⊞ Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
⊞ Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
⊟ Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 4381, Ack: 1, Len: 1460
    Source port: mit-ml-dev (85)
    Destination port: 1028 (1028)
    [Stream index: 0]
    Sequence number: 4381    (relative sequence number)
    [Next sequence number: 5841    (relative sequence number)]  <=
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 6432
    [Calculated window size: 6432]

0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  05 dc 0f 1b 40 00 40 06  d9 f6 c0 a8 66 62 c0 a8   ....@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  49 2a 3e ba ff ad 50 10   dW.U..E. I*>...P.
0030  19 20 2e e8 00 00 4e 1f  e6 c4 d8 c1 36 80 d3 0f   . ....N. ....6...
0040  c0 bd 74 0b b0 fe 5e bf  7a ef 82 0d 1f 4b 68 6e   ..t...^. z....Khn
0050  25 75 a7 62 ff 0b 5e 81  a0 9e 5f fd 30 d7 fa e4   %u.b..^. .._.0...
0060  ef f0 bf d1 73 b0 24 00  03 59 80 e3 38 46 ff 58   ....s.$. .Y..8F.X
0070  7d b6 7d 81 d3 0e 5c 41  b5 a7 fa 8d f4 aa f4 4b   }.}...\A .......K
0080  67 f2 8c 63 fa 7f 17 a2  d7 f8 ee dd 3f 40 6c be   g..c.... ....?@l.
0090  18 e8 12 78 e8 6c eb b7  ff 05 fd 92 e8 c0 b7 ae   ...x.l.. ........
00a0  63 5e 5f fe a6 6e 0e 03  12 f5 ef 9e af ff d7 2f   c^_..n.. ......./
00b0  93 60 7f 89 ec 22 88 16  0a 5a f8 9e dd 7a e2 b6   .`..."..  .Z...z..

File: "C:\Users\troy.wideman\Docu...  Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220    Profile: Default
```

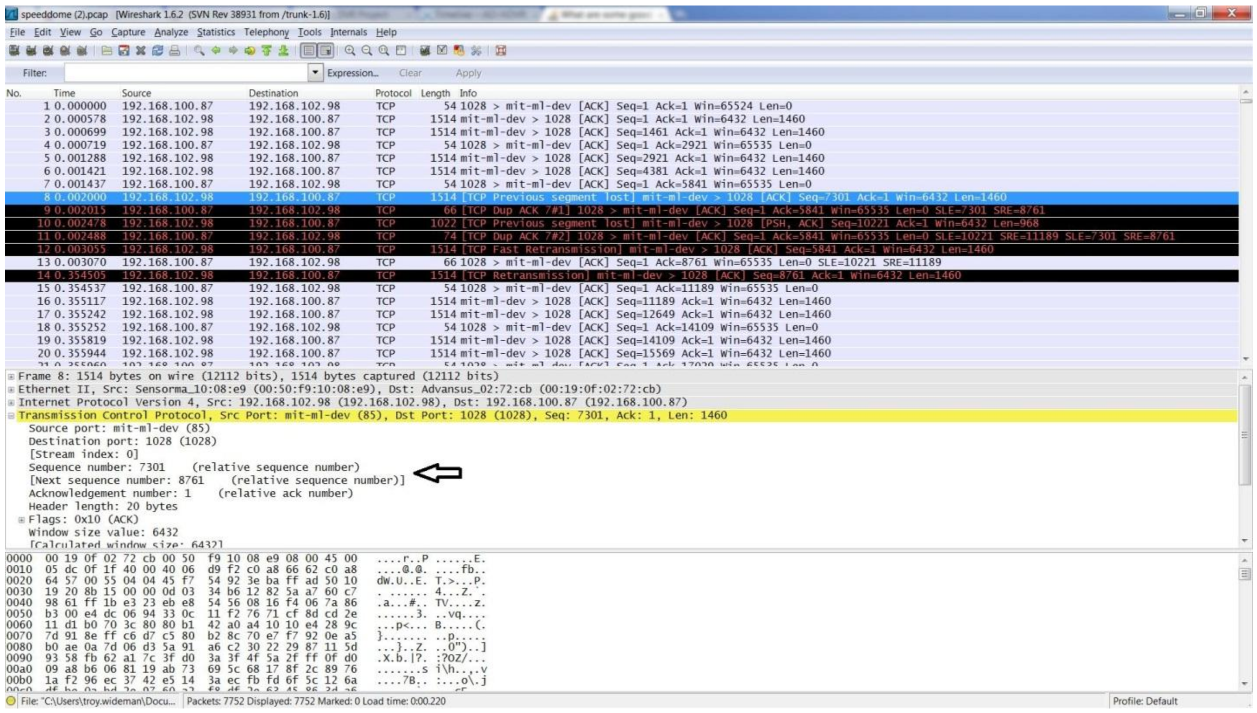
In Frame 6, the camera is finishing its previous request and telling the server that the next sequence to come will be 5841. In Frame 7, we see the following:



```
speeddome (2).pcap  [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
   2 0.000578  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
   3 0.000699  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
   4 0.000719  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
   5 0.001288  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
   6 0.001421  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
   7 0.001437  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
   8 0.002000  192.168.102.98  192.168.100.87  TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
   9 0.002015  192.168.100.87  192.168.102.98  TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
  10 0.002478  192.168.102.98  192.168.100.87  TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
  11 0.002488  192.168.100.87  192.168.102.98  TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
  12 0.003055  192.168.102.98  192.168.100.87  TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
  13 0.003070  192.168.100.87  192.168.102.98  TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
  14 0.354505  192.168.102.98  192.168.100.87  TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
  15 0.354537  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
  16 0.355117  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
  17 0.355242  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
  18 0.355252  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
  19 0.355819  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
  20 0.355944  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

⊞ Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Advansus_02:72:cb (00:19:0f:02:72:cb), Dst: Sensorma_10:08:e9 (00:50:f9:10:08:e9)
⊞ Internet Protocol Version 4, Src: 192.168.100.87 (192.168.100.87), Dst: 192.168.102.98 (192.168.102.98)
⊟ Transmission Control Protocol, Src Port: 1028 (1028), Dst Port: mit-ml-dev (85), Seq: 1, Ack: 5841, Len: 0
    Source port: 1028 (1028)
    Destination port: mit-ml-dev (85)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 5841    (relative ack number)  <=
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -1 (unknown)]

0000  00 50 f9 10 08 e9 00 19  0f 02 72 cb 08 00 45 00   .P...... ..r...E.
0010  00 28 af 43 40 00 80 06  ff 81 c0 a8 64 57 c0 a8   .(.C@... ....dW..
0020  66 62 04 04 00 55 3e ba  ff ad 45 f7 4e de 50 10   fb...U>. ..E.N.P.
0030  ff ff 4c 25 00 00                                  ..L%..

File: "C:\Users\troy.wideman\Docu...  Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220    Profile: Default
```

In Frame 7, the server acknowledges that the next sequence will be 5841 and requests information.

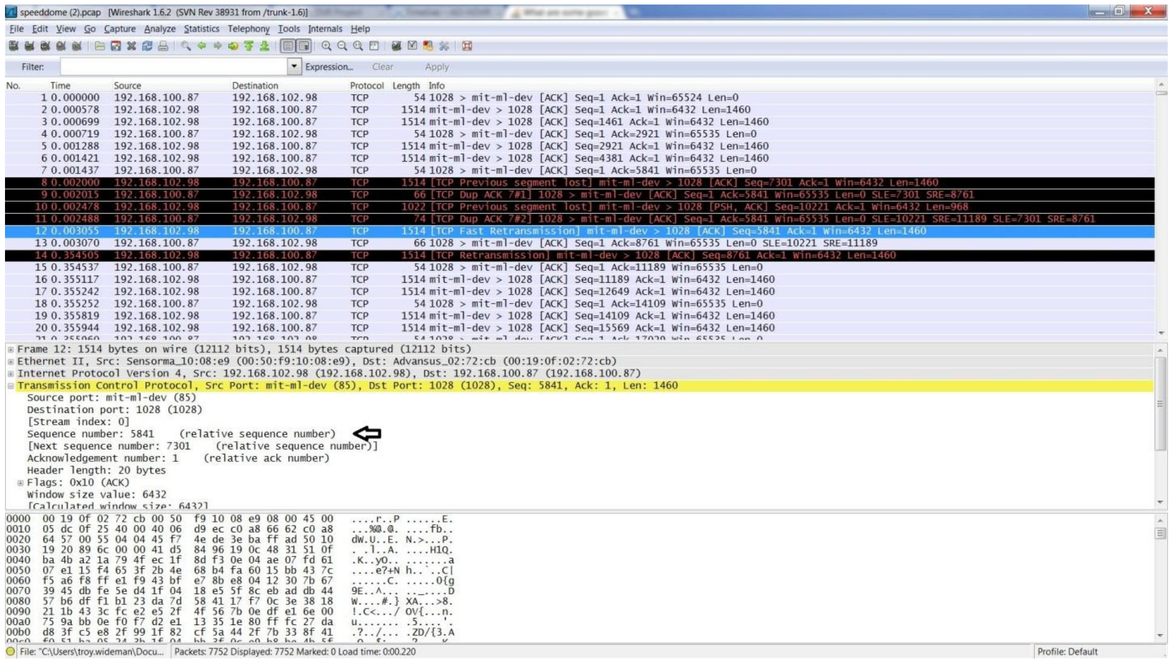
Frame 8 displays the following information:



```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
    2 0.000578  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
    3 0.000699  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
    4 0.000719  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
    5 0.001288  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
    6 0.001421  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
    7 0.001437  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
    8 0.002000  192.168.102.98  192.168.100.87  TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
    9 0.002015  192.168.100.87  192.168.102.98  TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
   10 0.002478  192.168.102.98  192.168.100.87  TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
   11 0.002488  192.168.100.87  192.168.102.98  TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
   12 0.003055  192.168.102.98  192.168.100.87  TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
   13 0.003070  192.168.100.87  192.168.102.98  TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
   14 0.354505  192.168.102.98  192.168.100.87  TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
   15 0.354537  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
   16 0.355117  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
   17 0.355242  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
   18 0.355252  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
   19 0.355819  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
   20 0.355944  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 7301, Ack: 1, Len: 1460
  Source port: mit-ml-dev (85)
  Destination port: 1028 (1028)
  [Stream index: 0]
  Sequence number: 7301    (relative sequence number)
  [Next sequence number: 8761    (relative sequence number)]
  Acknowledgement number: 1    (relative ack number)
  Header length: 20 bytes
 Flags: 0x10 (ACK)
  Window size value: 6432

0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  05 dc 0f 1f 40 00 40 06  d9 f2 c0 a8 66 62 c0 a8   ....@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  54 92 3e ba ff ad 50 10   dW.U..E. T.>...P.
0030  19 20 8b 15 00 00 0d 03  34 b6 12 82 5a a7 60 c7   . ...... 4...Z.`.
0040  98 61 ff 1b e3 23 eb e8  54 56 08 16 f4 06 7a 86   .a...#.. TV....z.
0050  b3 00 e4 dc 06 94 33 0c  11 f2 76 71 cf 8d cd 2e   ......3. ..vq....
0060  11 d1 b0 70 3c 80 80 b1  42 a0 a4 10 10 e4 28 9c   ...p<... B.....(.
0070  7d 91 8e ff c6 d7 c5 80  b2 8c 70 e7 f7 92 0e a5   }....... ..p.....
0080  b0 ae 0a 7d 06 d3 5a 91  a6 c2 30 22 29 87 11 5d   ...}..Z. ..0")..]
0090  93 58 fb 62 a1 7c 3f d0  3a 3f 4f 5a 2f ff 0f d0   .X.b.|?. :?OZ/...
00a0  09 a8 b6 06 81 19 ab 73  69 5c 68 17 8f 2c 89 76   .......s i\h..,.v
00b0  1a f2 96 ec 37 42 e5 14  3a ec fb fd 6f 5c 12 6a   ....7B.. :...o\.j

File: "C:\Users\troy.wideman\Docu...  Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

Frame 8 displays an error. The sequence number should have been 5841 but arrived as 7301. Thus, it is listed as TCP Previous Segment Lost.

Several duplicate acknowledgements from the server appear in Frames 9 and 11, and another lost segment from the camera in Frame 10, before Frame 12 is displayed:

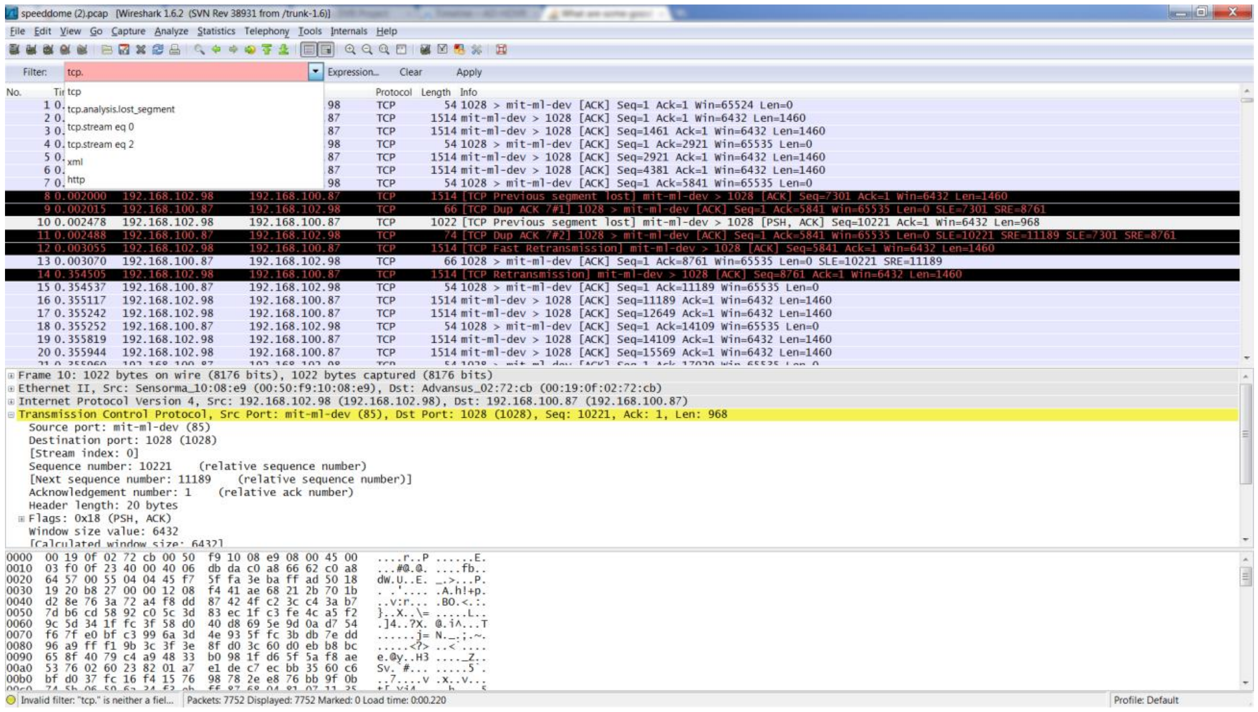


```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
    2 0.000578  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
    3 0.000699  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
    4 0.000719  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
    5 0.001288  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
    6 0.001421  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
    7 0.001437  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
    8 0.002000  192.168.102.98  192.168.100.87  TCP      1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
    9 0.002015  192.168.100.87  192.168.102.98  TCP        66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
   10 0.002478  192.168.102.98  192.168.100.87  TCP      1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
   11 0.002488  192.168.100.87  192.168.102.98  TCP        74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
   12 0.003055  192.168.102.98  192.168.100.87  TCP      1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
   13 0.003070  192.168.100.87  192.168.102.98  TCP        66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
   14 0.354505  192.168.102.98  192.168.100.87  TCP      1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
   15 0.354537  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
   16 0.355117  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
   17 0.355242  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
   18 0.355252  192.168.100.87  192.168.102.98  TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
   19 0.355819  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
   20 0.355944  192.168.102.98  192.168.100.87  TCP      1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 5841, Ack: 1, Len: 1460
  Source port: mit-ml-dev (85)
  Destination port: 1028 (1028)
  [Stream index: 0]
  Sequence number: 5841    (relative sequence number)
  [Next sequence number: 7301    (relative sequence number)]
  Acknowledgement number: 1    (relative ack number)
  Header length: 20 bytes
 Flags: 0x10 (ACK)
  Window size value: 6432

0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  05 dc 0f 25 40 00 40 06  d9 ec c0 a8 66 62 c0 a8   ...%@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  4e de 3e ba ff ad 50 10   dW.U..E. N.>...P.
0030  19 20 89 6c 00 00 41 d5  84 96 19 0c 48 31 51 0f   . .l..A. ....H1Q.
0040  ba 4b a2 1a 79 4f ec 1f  8d f3 0e 04 ae 07 fd 61   .K..yO.. .......a
0050  07 e1 15 f4 65 3f 2b 4e  68 b4 fa 60 15 bb 43 7c   ....e?+N h..`..C|
0060  f5 a6 f8 ff e1 f9 43 bf  e7 8b e8 04 12 30 7b 67   ......C. .....0{g
0070  39 45 db fe 5e d4 1f 04  18 e5 5f 8c eb ad db 44   9E..^... .._....D
0080  57 b6 df f1 b1 23 da 7d  58 41 17 f7 0c 3e 38 18   W....#.} XA...>8.
0090  21 1b 43 3c fc e2 e5 2f  4f 56 7b 0e df e1 6e 00   !.C<.../ OV{...n.
00a0  75 9a bb 0e f0 f7 d2 e1  13 35 1e 80 ff fc 27 da   u....... .5....'.
00b0  d8 3f c5 e8 2f 99 1f 82  cf 5a 44 2f 7b 33 8f 41   .?../... .ZD/{3.A

File: "C:\Users\troy.wideman\Docu...  Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

In Frame 12, the camera has tried to retransmit the lost segment that was reported previously (5841). This continues with the other lost segment in Frame 10 until the server and the camera get synced back up. This is how you can identify if the server and camera are losing packets in the exchange of information.

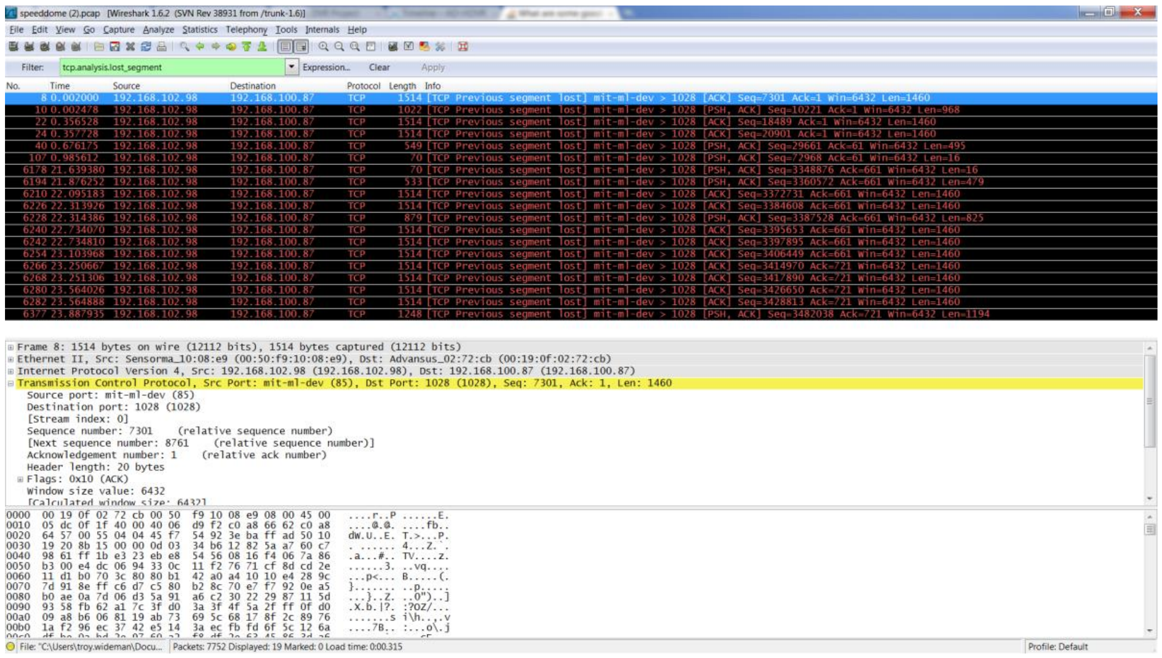
4 Using Wireshark Filters

There are additional ways to easily identify problems within the capture:



```
speeddome (2).pcap  [Wireshark 1.6.2  (SVN Rev 38931 from /trunk-1.6)]
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Internals  Help
Filter: tcp.                                              Expression...   Clear   Apply
No.   Ti tcp                                              Protocol Length Info
  1 0.   tcp.analysis.lost_segment                   98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0
  2 0.   tcp.stream eq 0                             87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1 Ack=1 Win=6432 Len=1460
  3 0.   tcp.stream eq 2                             87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=1461 Ack=1 Win=6432 Len=1460
  4 0.   xml                                         98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len=0
  5 0.   http                                        87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=2921 Ack=1 Win=6432 Len=1460
  6 0.                                               87   TCP      1514 mit-ml-dev > 1028 [ACK] Seq=4381 Ack=1 Win=6432 Len=1460
  7 0.                                               98   TCP        54 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0
  8 0.002000  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
  9 0.002015  192.168.100.87   192.168.102.98   TCP    66 [TCP Dup ACK 7#1] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=7301 SRE=8761
 10 0.002478  192.168.102.98   192.168.100.87   TCP  1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
 11 0.002488  192.168.100.87   192.168.102.98   TCP    74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seq=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7301 SRE=8761
 12 0.003055  192.168.102.98   192.168.100.87   TCP  1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460
 13 0.003070  192.168.100.87   192.168.102.98   TCP    66 1028 > mit-ml-dev [ACK] Seq=1 Ack=8761 Win=65535 Len=0 SLE=10221 SRE=11189
 14 0.354505  192.168.102.98   192.168.100.87   TCP  1514 [TCP Retransmission] mit-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460
 15 0.354537  192.168.100.87   192.168.102.98   TCP    54 1028 > mit-ml-dev [ACK] Seq=1 Ack=11189 Win=65535 Len=0
 16 0.355117  192.168.102.98   192.168.100.87   TCP  1514 mit-ml-dev > 1028 [ACK] Seq=11189 Ack=1 Win=6432 Len=1460
 17 0.355242  192.168.102.98   192.168.100.87   TCP  1514 mit-ml-dev > 1028 [ACK] Seq=12649 Ack=1 Win=6432 Len=1460
 18 0.355252  192.168.100.87   192.168.102.98   TCP    54 1028 > mit-ml-dev [ACK] Seq=1 Ack=14109 Win=65535 Len=0
 19 0.355819  192.168.102.98   192.168.100.87   TCP  1514 mit-ml-dev > 1028 [ACK] Seq=14109 Ack=1 Win=6432 Len=1460
 20 0.355944  192.168.102.98   192.168.100.87   TCP  1514 mit-ml-dev > 1028 [ACK] Seq=15569 Ack=1 Win=6432 Len=1460

⊞ Frame 10: 1022 bytes on wire (8176 bits), 1022 bytes captured (8176 bits)
⊞ Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
⊞ Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
⊟ Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 10221, Ack: 1, Len: 968
    Source port: mit-ml-dev (85)
    Destination port: 1028 (1028)
    [Stream index: 0]
    Sequence number: 10221    (relative sequence number)
    [Next sequence number: 11189    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size value: 6432
    [Calculated window size: 6432]

0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  03 f0 0f 23 40 00 40 06  db da c0 a8 66 62 c0 a8   ...#@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  5f fa 3e ba ff ad 50 18   dW.U..E. _.>...P.
0030  19 20 b8 27 00 00 12 08  f4 41 ae 68 21 2b 70 1b   . .'.... .A.h!+p.
0040  d2 8e 76 3a 72 a4 f8 dd  87 42 4f c2 3c c4 3a b7   ..v:r... .BO.<.:.
0050  7d b6 cd 58 92 c0 5c 3d  83 ec 1f c3 fe 4c a5 f2   }..X..\= .....L..
0060  9c 5d 34 1f fc 3f 58 d0  40 d8 69 5e 9d 0a d7 54   .]4..?X. @.i^...T
0070  f6 7f e0 bf c3 99 6a 3d  4e 93 5f fc 3b db 7e dd   ......j= N._.;.~.
0080  96 a9 ff f1 9b 3c 3f 3e  8f d0 3c 60 d0 eb b8 bc   .....<?> ..<`....
0090  65 8f 40 79 c4 a9 48 33  b0 98 1f d6 5f 5a f8 ae   e.@y..H3 ...._Z..
00a0  53 76 02 60 23 82 01 a7  e1 de c7 ec bb 35 60 c6   Sv.`#... .....5`.
00b0  bf d0 37 fc 16 f4 15 76  98 78 2e e8 76 bb 9f 0b   ..7....v .x..v...

Invalid filter: "tcp." is neither a fiel...   Packets: 7752 Displayed: 7752 Marked: 0 Load time: 0:00.220   Profile: Default
```

Type **tcp.** in the **Filter** box to see options that you can select to filter the capture. For example, you can select **tcp.analysis.lost_segment** to see the following:



```
speeddome (2).pcap  [Wireshark 1.6.2  (SVN Rev 38931 from /trunk-1.6)]
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Internals  Help
Filter: tcp.analysis.lost_segment                       Expression...   Clear   Apply
No.  Time       Source           Destination      Protocol Length Info
   8 0.002000   192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460
  10 0.002478   192.168.102.98   192.168.100.87   TCP  1022 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=6432 Len=968
  22 0.356528   192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=18489 Ack=1 Win=6432 Len=1460
  24 0.357728   192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=20901 Ack=1 Win=6432 Len=1460
  40 0.676175   192.168.102.98   192.168.100.87   TCP   549 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=29661 Ack=61 Win=6432 Len=495
 107 0.985612   192.168.102.98   192.168.100.87   TCP    70 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=72968 Ack=61 Win=6432 Len=16
6178 21.639380  192.168.102.98   192.168.100.87   TCP    70 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=3348876 Ack=661 Win=6432 Len=16
6194 21.876252  192.168.102.98   192.168.100.87   TCP   533 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=3360572 Ack=661 Win=6432 Len=479
6210 22.095183  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3372731 Ack=661 Win=6432 Len=1460
6226 22.313926  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3384608 Ack=661 Win=6432 Len=1460
6228 22.314386  192.168.102.98   192.168.100.87   TCP   879 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=3387528 Ack=661 Win=6432 Len=825
6240 22.734070  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3395653 Ack=661 Win=6432 Len=1460
6242 22.734810  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3397895 Ack=661 Win=6432 Len=1460
6254 23.103968  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3406449 Ack=661 Win=6432 Len=1460
6266 23.250667  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3414970 Ack=721 Win=6432 Len=1460
6268 23.251306  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3417890 Ack=721 Win=6432 Len=1460
6280 23.564026  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3426650 Ack=721 Win=6432 Len=1460
6282 23.564888  192.168.102.98   192.168.100.87   TCP  1514 [TCP Previous segment lost] mit-ml-dev > 1028 [ACK] Seq=3428813 Ack=721 Win=6432 Len=1460
6377 23.887935  192.168.102.98   192.168.100.87   TCP  1248 [TCP Previous segment lost] mit-ml-dev > 1028 [PSH, ACK] Seq=3482038 Ack=721 Win=6432 Len=1194

⊞ Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
⊞ Ethernet II, Src: Sensorma_10:08:e9 (00:50:f9:10:08:e9), Dst: Advansus_02:72:cb (00:19:0f:02:72:cb)
⊞ Internet Protocol Version 4, Src: 192.168.102.98 (192.168.102.98), Dst: 192.168.100.87 (192.168.100.87)
⊟ Transmission Control Protocol, Src Port: mit-ml-dev (85), Dst Port: 1028 (1028), Seq: 7301, Ack: 1, Len: 1460
    Source port: mit-ml-dev (85)
    Destination port: 1028 (1028)
    [Stream index: 0]
    Sequence number: 7301    (relative sequence number)
    [Next sequence number: 8761    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 6432
    [Calculated window size: 6432]

0000  00 19 0f 02 72 cb 00 50  f9 10 08 e9 08 00 45 00   ....r..P ......E.
0010  05 dc 0f 1f 40 00 40 06  d9 f2 c0 a8 66 62 c0 a8   ....@.@. ....fb..
0020  64 57 00 55 04 04 45 f7  54 92 3e ba ff ad 50 10   dW.U..E. T.>...P.
0030  19 20 8b 15 00 00 0d 03  34 b6 12 82 5a a7 60 c7   . ...... 4...Z.`.
0040  98 61 ff 1b e3 23 eb e8  54 56 08 16 f4 06 7a 86   .a...#.. TV....z.
0050  b3 00 e4 dc 06 94 33 0c  11 f2 76 71 cf 8d cd 2e   ......3. ..vq....
0060  11 d1 b0 70 3c 80 80 b1  42 a0 a4 10 10 e4 28 9c   ...p<... B.....(.
0070  7d 91 8e ff c6 d7 c5 80  b2 8c 70 e7 f7 92 0e a5   }....... ..p.....
0080  b0 ae 0a 7d 06 d3 5a 91  a6 c2 30 22 29 87 11 5d   ...}..Z. ..0")..]
0090  93 58 fb 62 a1 7c 3f d0  3a 3f 4f 5a 2f ff 0f d0   .X.b.|?. :?OZ/...
00a0  09 a8 b6 06 81 19 ab 73  69 5c 68 17 8f 2c 89 76   .......s i\h..,.v
00b0  1a f2 96 ec 37 42 e5 14  3a ec fb fd 6f 5c 12 6a   ....7B.. :...o\.j

File: "C:\Users\troy.wideman\Docu...   Packets: 7752 Displayed: 19 Marked: 0 Load time: 0:00.315   Profile: Default
```

This example shows all the lost segments within the capture so that you can identify the frame number to focus on. There are other helpful filters you can experiment with.

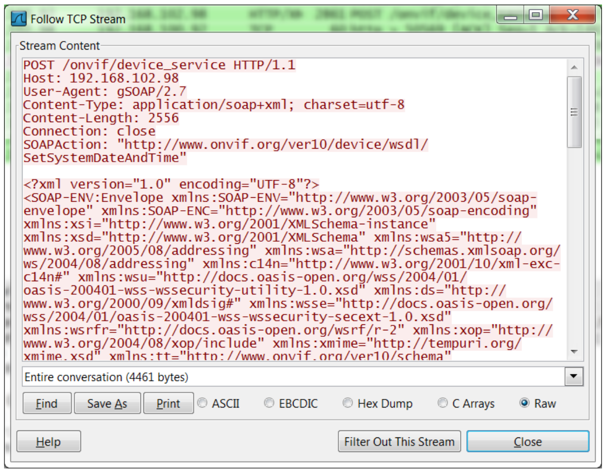
Additional helpful filters:

- **xml**: allows you see each SOAP call in a Wireshark trace.
- **eth.addr == ff:ff:ff:ff:ff:ff**: looks for broadcast messages.
- **udp:** on ONVIF cameras, finds the **ws-discovery** response from the camera during a network scan.
- **ip.src_host == XXX.XXX.XXX.XXX:** filters on a specific IP address.

Information about more filters is available at: http://wiki.wireshark.org/CaptureFilters

5 Using Wireshark to Obtain ONVIF RTSP Stream Information

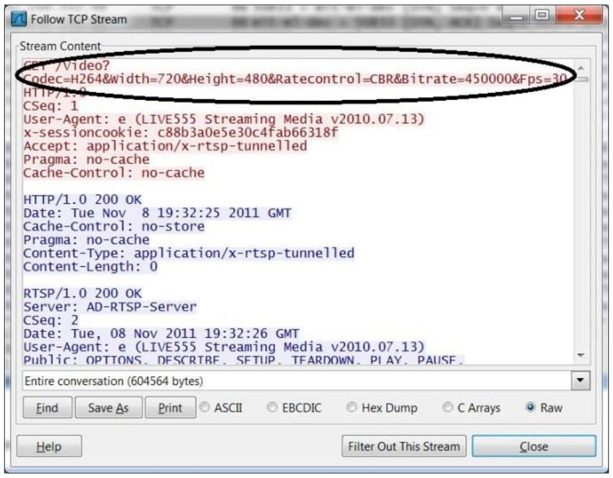
If you need to know information about how the camera is connecting to the server, start the capture on the desired camera and connect to the camera in exacqVision Client. After the connection is successful in the client, stop the capture. Then type in **tcp.stream eq XX** (where XX equals the TCP stream of interest). A window similar to this should be displayed:



```
POST /onvif/device_service HTTP/1.1
Host: 192.168.102.98
User-Agent: gSOAP/2.7
Content-Type: application/soap+xml; charset=utf-8
Content-Length: 2556
Connection: close
SOAPAction: "http://www.onvif.org/ver10/device/wsdl/
SetSystemDateAndTime"

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-
envelope" xmlns:SOAP-ENC="http://www.w3.org/2003/05/soap-encoding"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsa5="http://
www.w3.org/2005/08/addressing" xmlns:wsa="http://schemas.xmlsoap.org/
ws/2004/08/addressing" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-
c14n#" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/
oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://
www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/
wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsrfr="http://docs.oasis-open.org/wsrf/r-2" xmlns:xop="http://
www.w3.org/2004/08/xop/include" xmlns:xmime="http://tempuri.org/
xmime.xsd" xmlns:tt="http://www.onvif.org/ver10/schema"
```

Entire conversation (4461 bytes)

This will allow you to find out about the ONVIF stream with the camera. You can also find the address of the RTSP stream if the camera supports RTSP:

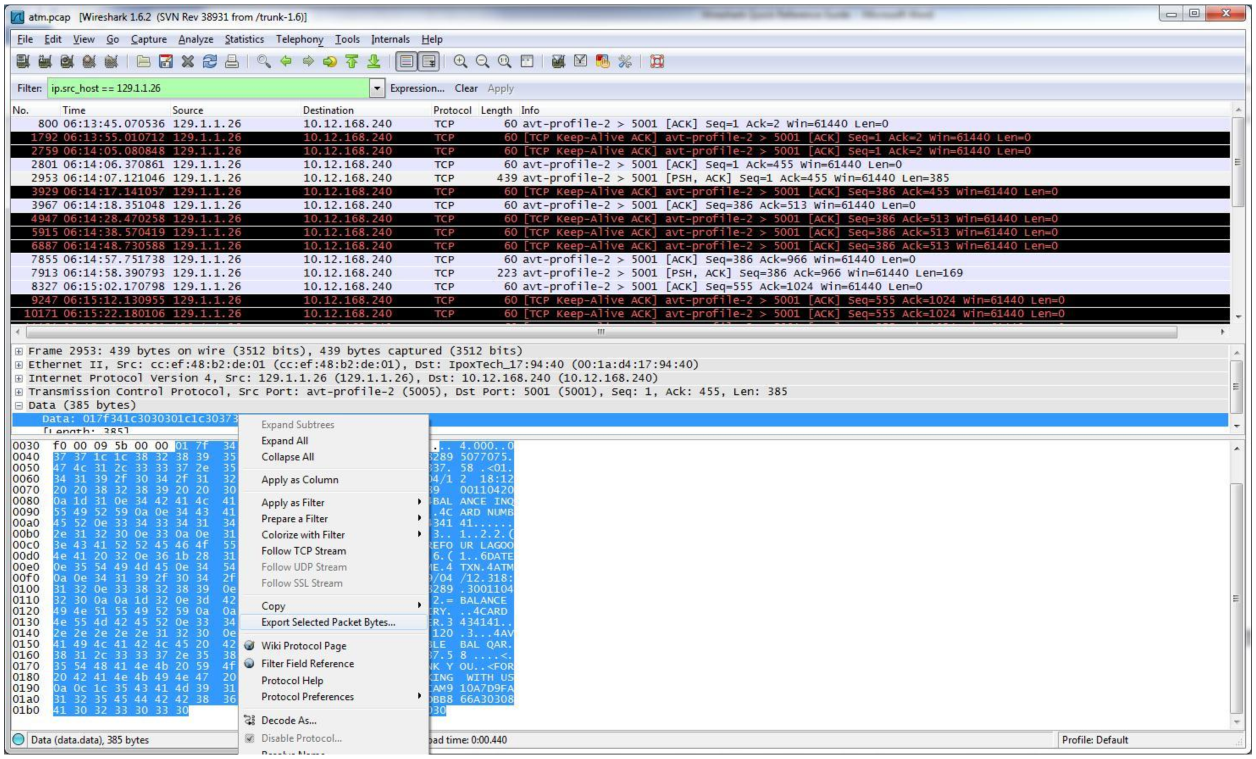


```
GET /video?
Codec=H264&Width=720&Height=480&Ratecontrol=CBR&Bitrate=450000&Fps=30
HTTP/1.0
CSeq: 1
User-Agent: e (LIVE555 Streaming Media v2010.07.13)
x-sessioncookie: c88b3a0e5e30c4fab66318f
Accept: application/x-rtsp-tunnelled
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.0 200 OK
Date: Tue Nov  8 19:32:25 2011 GMT
Cache-Control: no-store
Pragma: no-cache
Content-Type: application/x-rtsp-tunnelled
Content-Length: 0

RTSP/1.0 200 OK
Server: AD-RTSP-Server
CSeq: 2
Date: Tue, 08 Nov 2011 19:32:26 GMT
User-Agent: e (LIVE555 Streaming Media v2010.07.13)
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE,
```

Entire conversation (604564 bytes)

6 Using Wireshark to Export ATM/POS Data

When you are looking at a .pcap file from an ATM or POS transaction, the data can be extracted for use with a program called netcat to play back the information and find appropriate SOT and EOT and filters.



```
No.   Time            Source       Destination    Protocol Length Info
  800 06:13:45.070536 129.1.1.26   10.12.168.240  TCP       60 avt-profile-2 > 5001 [ACK] Seq=1 Ack=2 Win=61440 Len=0
 1792 06:13:55.010712 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=1 Ack=2 Win=61440 Len=0
 2759 06:14:05.080848 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=1 Ack=2 Win=61440 Len=0
 2801 06:14:06.370861 129.1.1.26   10.12.168.240  TCP       60 avt-profile-2 > 5001 [ACK] Seq=1 Ack=455 Win=61440 Len=0
 2953 06:14:07.121046 129.1.1.26   10.12.168.240  TCP      439 avt-profile-2 > 5001 [PSH, ACK] Seq=1 Ack=455 Win=61440 Len=385
 3929 06:14:17.141057 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=386 Ack=455 Win=61440 Len=0
 3967 06:14:18.351048 129.1.1.26   10.12.168.240  TCP       60 avt-profile-2 > 5001 [ACK] Seq=386 Ack=513 Win=61440 Len=0
 4947 06:14:28.470258 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=386 Ack=513 Win=61440 Len=0
 5915 06:14:38.570419 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=386 Ack=513 Win=61440 Len=0
 6887 06:14:48.730588 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=386 Ack=513 Win=61440 Len=0
 7855 06:14:57.751738 129.1.1.26   10.12.168.240  TCP       60 avt-profile-2 > 5001 [ACK] Seq=386 Ack=966 Win=61440 Len=0
 7913 06:14:58.390793 129.1.1.26   10.12.168.240  TCP      223 avt-profile-2 > 5001 [PSH, ACK] Seq=386 Ack=966 Win=61440 Len=169
 8327 06:15:02.170798 129.1.1.26   10.12.168.240  TCP       60 avt-profile-2 > 5001 [ACK] Seq=555 Ack=1024 Win=61440 Len=0
 9247 06:15:12.130955 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=555 Ack=1024 Win=61440 Len=0
10171 06:15:22.180106 129.1.1.26   10.12.168.240  TCP       60 [TCP Keep-Alive ACK] avt-profile-2 > 5001 [ACK] Seq=555 Ack=1024 Win=61440 Len=0
```

```
⊞ Frame 2953: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
⊞ Ethernet II, Src: cc:ef:48:b2:de:01 (cc:ef:48:b2:de:01), Dst: IpoxTech_17:94:40 (00:1a:d4:17:94:40)
⊞ Internet Protocol Version 4, Src: 129.1.1.26 (129.1.1.26), Dst: 10.12.168.240 (10.12.168.240)
⊞ Transmission Control Protocol, Src Port: avt-profile-2 (5005), Dst Port: 5001 (5001), Seq: 1, Ack: 455, Len: 385
⊟ Data (385 bytes)
    Data: 017f341c3030301c1c30373
    [Length: 385]
```

```
0030  f0 00 09 5b 00 00 01 7f  34     ... 4.000..0
0040  37 37 1c 1c 38 32 38 39  35     289 5077075.
0050  47 4c 31 2c 33 33 37 2e  35     37. 58 .<01.
0060  34 31 39 2f 30 34 2f 31  32     4/1 2  18:12
0070  20 20 38 32 38 39 20 20  30     9   00110420
0080  0a 1d 31 0e 34 42 41 4c  41     BAL ANCE INQ
0090  55 49 52 59 0a 0e 34 43  41     .4C ARD NUMB
00a0  45 52 0e 33 34 33 34 31  34     341 41......
00b0  2e 31 32 30 0e 33 0a 0e  31     3.. 1..2.2.(
00c0  3e 43 41 52 52 45 46 4f  55     EFO UR LAGOO
00d0  4e 41 20 32 0e 36 1b 28  31     6.( 1..6DATE
00e0  0e 35 54 49 4d 45 0e 34  54     E.4 TXN.4ATM
00f0  0a 0e 34 31 39 2f 30 34  2f     /04 /12.318:
0100  31 32 0e 33 38 32 38 39  0e     289 .3001104
0110  32 30 0a 0a 1d 32 0e 3d  42     2.= BALANCE
0120  49 4e 51 55 49 52 59 0a  0a     RY. ..4CARD
0130  4e 55 4d 42 45 52 0e 33  34     R.3 434141..
0140  2e 2e 2e 2e 2e 31 32 30  0e     120 .3...4AV
0150  41 49 4c 41 42 4c 45 20  42     LE  BAL QAR.
0160  38 31 2c 33 33 37 2e 35  38     7.5 8 ....<.
0170  35 54 48 41 4e 4b 20 59  4f     K Y OU..<FOR
0180  20 42 41 4e 4b 49 4e 47  20     ING  WITH US
0190  0a 0c 1c 35 43 41 4d 39  31     AM9 10A7D9FA
01a0  31 32 35 45 44 42 42 38  36     BB8 66A30308
01b0  41 30 32 33 30 33 30            30
```

Data (data.data), 385 bytes   ad time: 0:00.440

In this example, you could right-click on the data and choose **Export Selected Packet Bytes.** In the save dialog box, enter the filename **name.bin**. This file can then be used in netcat to play back the transaction.

7 Additional Information

- Using Wireshark, look at the length of each message. If the length exceeds the MTU of the system plus 24 bytes of header information, fragmention is highly likely.
- Select View, Time Display Format, and Time of Day to see the time when the cap file was taken determine when things in the .pcap file occurred.
- To avoid installing Wireshark on the local computer, you can run it from a flash drive or other storage media.
- Wireshark is capable of extensive troubleshooting of networking problems. For more information, visit http://www.wireshark.org/.