

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, <u>http://www.wireshark.org/</u>
- Linux (Ubuntu): Search for Wireshark in the Ubuntu Software Center.





+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

USA (Corporate Headquarters) Mexico Europe/Middle East/Asia Central Europe

Page 1 of 9 9/6/2012

Using Wireshark to Obtain and Save a .pcap File

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



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



- 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.



www.exacq.com



+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

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 3	8931 from /trunk-1.6)]	ant - Insta-40-004 - A	- 0 - X-
Eile Edit View Go	Capture Analyze Statistics	Telephony Iools Internal	Help	
	8 🖬 🗶 😂 🖴 🔍 🍬 🤞	💊 ኛ 🛓 🔲 🖬 🔍 (2, Q. 🗹 📓 🗹 🥵 🗧	
Filter:		Expression	n_ Clear Apply	
No. Time	Source	Destination	Protocol Length Info	
1 0.000000	192.168.100.87	192.168.102.98	TCP 54 1028 > mit-m1-dev [ACK] Seg=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 m1t-m1-dev > 1028 [ACK] Seq=4381 Ack=1 W1n=6432 Len=1460	
7 0.001437	192.168.100.87	192.168.102.98	1CP 54 1028 > mit-mi-dev [A(K] Sed=1 A(K=3841 Win=0535 Left=0 1544 [Crop Derived Proceeding of the minimum derive 1028 [Crop 2201 Add 1 min 6423 Left 1460	
9.0.002000	192.168.102.98	102 168 102 08	1. If $(1CP)$ Previous segment rost intentineve > 1028 [Ack] seq=: 301 Ack=1 with=0422 Lett=1400 66 [TCP Dup Ack 741 1028 with=0404 [Ack] Son=1 Ack_S841 win=6525 [an=0515=7201 Spc=9761	
10.0.002015	192.168.102.98	192.168.100.87	TCP 1022 [CF Dup Ack r_{11}] 1000 / min dev [Ack] Seq=1 Ack-3041 min-60333 [CF r_{12}] Seq=1 (012) [CF Dup Ack] Seq=1023 [CF Dup Ack] Seq=1003 [CF Dup Ack] Seq=1003 [CF Du	
11 0.002488	192,168,100,87	192,168,102,98	TCP 74 [TCP Dup ACK 7#2] 1028 > mit-ml-dev [ACK] Seg=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=73	01 SRE=8761
12 0.003055	192.168.102.98	192.168.100.87	TCP 1514 [TCP Fast Retransmission] mit-ml-dev > 1028 [ACK] Seg=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-m]-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	192.168.100.8/	192.168.102.98	TCP 54 1028 > mTT-mT-dev [ACK] Sed=1 ACK=14109 Win=5555 Len=0	
20.0.255044	102 168 102 08	192.108.100.87	10^{12} 1514 m11-m1-00V > 1020 [ACK] Set[=14109 ACK=1 w11=0452 Lett=1400 TCD 1514 m11-m1-00V > 1020 [ACK] Set[=14109 ACK=1 w11=0452 Lett=1400	
20 0. 333944	107 160 100 07	107 160 107 00	TCP 1314 mil (mil 'dev / 1020 [ACK] 364=1305 ACK=1 mil-6432 [cel=1400	
E Frame 1: 54 by	tes on wire (432 bit	ts), 54 bytes captur	d (432 bits)	
Ethernet II, S	rc: Advansus_02:72:0	cb (00:19:0f:02:72:c), Dst: Sensorma_10:08:e9 (00:50:f9:10:08:e9)	
Internet Proto	col Version 4, Src:	192.168.100.87 (192	168.100.87), Dst: 192.168.102.98 (192.168.102.98)	
Transmission C	control Protocol, Sro	c Port: 1028 (1028),	Dst Port: mit-ml-dev (85), Seq: 1, Ack: 1, Len: 0	
0000 00 50 f9 1	0 08 e9 00 19 Of 0	2 72 cb 08 00 45 00	.PE.	
0010 00 28 af 4	1 40 00 80 06 ff 8	3 c0 a8 64 57 c0 a8	. (, A@ dW	
0020 66 62 04 0 0030 ff f4 4c 7	14 00 33 Se Da TT at	u 43 17 38 08 30 10	100>E.O.P.	
0050 11 11 10 1				
File: "C:\Users\troy.w	ideman\Docu Packets: 775	52 Displayed: 7752 Marked: 0	oad time: 0:00.220	Profile: Default

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 38	8931 from /trunk-1.6)]	Sugar	· Instant Advector -		_ 0	x
Eile Edit View	Go Capture Analyze Statistics	Telephony Iools Interna	ils <u>H</u> elp				
	() 🖻 🖬 🗶 🖓 🖨 🍳 🍝 🔶	💊 ኛ 🛓 🔲 🖬 🍳	Q Q 🖻 🗆	😹 🗵 🧐 🎉 🖼			
Filter:		 Express 	ion Clear	r Apply			
No. Time	Source	Destination	Protocol	Length Info			-
1 0.000	0000 192.168.100.87	192.168.102.98	тср	54 1028 > mit-ml-	dev [ACK]	Seq=1 Ack=1 Win=65524 Len=0	
3 0.000	699 192.168.102.98	192.168.100.87	TCP	1514 mit-ml-dev > 1	028 [ACK]	Seq=1461 Ack=1 Win=6432 Len=1460	-
4 0.000	719 192.168.100.87	192.168.102.98	TCP	54 1028 > mit-m]-	dev [ACK	Seq=1 Ack=2921 Win=65535 Len=0	
5 0.001	421 192.168.102.98	192.168.100.8/	TCP	1514 mit-ml-dev > 1 1514 mit-ml-dev > 1	028 [ACK	Seq=2921 ACK=1 W1N=6432 Len=1460	
7 0.001	437 192.168.100.87	192.168.102.98	TCP	54 1028 > mit-ml-	dev [ACK]	Seq=1 Ack=5841 Win=65535 Len=0	
8 0.002	102.168.102.98	192.168.100.87	TCP	1514 [TCP Previous	segment	lost] mit-m]-dev > 1028 [ACK] Seq=7301 Ack=1 Win=6432 Len=1460	
10 0.002	478 192.168.102.98	192.168.102.98	TCP	1022 TCP Previous	segment	> mic-mi-dev [Ack] Sed=1 Ack=3041 Win=03535 Len=0 SLC=7301 SkC=8701	
11 0.002	488 192.168.100.87	192.168.102.98	тср	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 0.003	102.168.102.98	192.168.100.87	TCP	1514 [TCP Fast Retr	ansmissio	on] mit-ml-dev > 1028 [ACK] Seg=5841 Ack=1 Win=6432 Len=1460	
14 0. 354	505 192.168.102.98	192.168.100.87	TCP	1514 TCP Retransmi	ssion m	it-m]-dev > 1028 [ACK] Seg=8761 ACk=1 Win=6432 Len=1460	
15 0.354	537 192.168.100.87	192.168.102.98	ТСР	54 1028 > mit-ml-	dev [ACK]	Seq=1 Ack=11189 Win=65535 Len=0	
16 0.355	11/ 192.168.102.98	192.168.100.8/	TCP	1514 mit-ml-dev > 1 1514 mit-ml-dev > 1	028 [ACK	Seq=11189 ACK=1 Win=6432 Len=1460	
18 0.355	252 192.168.100.87	192.168.102.98	TCP	54 1028 > mit-ml-	dev [ACK]	Seq=1 Ack=14109 Win=65535 Len=0	
19 0.355	819 192.168.102.98	192.168.100.87	TCP	1514 mit-ml-dev > 1	028 [ACK]	Seq=14109 Ack=1 Win=6432 Len=1460	
20 0. 355	1944 192.168.102.98	192.108.100.8/	TCP	1514 mit-mi-dev > 1	day FACK	Seq=15509 ACK=1 W1n=0432 Len=1400	*
■ Frame 2: 1	514 bytes on wire (12112	2 bits), 1514 bytes	captured	(12112 bits)	0.10.05.	N3 - 73 LA	
Internet P	rotocol Version 4. Src:	192.168.102.98 (19	29), UST: 2.168.102.	98). Dst: 192.168.10	0.87 (19)	2 168 100 87)	
■ Transmissi	on Control Protocol, Src	Port: mit-ml-dev	(85), Dst	Port: 1028 (1028), S	eq: 1, A	ck: 1, Len: 1460	
Source po	ort: mit-ml-dev (85)						
[Stream i	index: 0]						
Sequence	number: 1 (relative	sequence number)		_			
[Next sec	quence number: 1461 (relative sequence r	umber)]	2			
Header 16	ength: 20 bytes	Tacive ack number)					
■ Flags: 0	(10 (ACK)						
Window si	ize value: 6432						-
0000 00 19	Of 02 72 cb 00 50 f9 10	0 08 e9 08 00 45 00	r	PE.			
0010 05 dc 0020 64 57	0f 15 40 00 40 06 d9 fc 00 55 04 04 45 f7 38 0e	c c0 a8 66 62 c0 a8 B 3e ba ff ad 50 10	dw. U., E	1fb 8 > P			
0030 19 20	a4 32 00 00 24 00 05 c0	0 80 63 38 43 ff 58	25	c8C.X			
0040 /d bb 0050 20 e2	e5 1f 30 28 3b d2 5c f9	9 68 40 7e a3 69 8b	}0(;	. \.h@~.i.			
0060 2c a5	e3 fc 3b d0 58 3e 24 c1	1 e8 e7 d1 f5 9e 5f	,; ; X	S			
0080 e7 05	7d 8e 7a c4 69 7f 04 dc	d 96 bf df 3f b4 ff	}.z.1	?			
0090 5d 72 00a0 eb df	ra ea 4e b1 7d 47 6f ae 25 7f 82 4e c1 b4 c7 c2	e 1† 2e c0 f3 75 8b 2 b4 10 7a f9 e8 5d]rN.]	G 0u.			
00b0 84 52	cb 03 1b 3a cd 0e 80 7f	f 87 f6 02 40 ac 1f	.R	@			-
File: "C:\Users\!	troy.wideman\Docu Packets: 775	52 Displayed: 7752 Marked: 0	Load time: 0:0	00.220		Profile: Default	

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).







+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

Click on Frame 3 to display the following:

speeddome (2).pcap	[Wireshark 1.6.2 (SVN Rev	38931 from /trunk-1.6)]	Property of the Toronton	AD ADM . A WHAT AN	unte por - 1		_ 0 <mark>_ x</mark>
Eile Edit View Go	Capture Analyze Statistic	cs Telephony Iools Intern	als Help				
.	B 🖬 🗙 🖉 🔒 I 🔍 🌳 I	🕈 🧔 🎖 🗶 🔲 🗐 🔍	Q Q 🗹 📓 🖉 🔧	1 g			
Filter:		 Expres 	sion. Clear Apply				
No. Time	Source	Destination	Protocol Length Info				
1 0.000000	192.168.100.87	192.168.102.98	TCP 54 102	8 > mit-ml-dev [AC	K] Seq=1 Ack=1 Win=65524 Len=0	0	
2 0.000578	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [AC	<pre>K] Seq=1 Ack=1 Win=6432 Len=14</pre>	460	
3 0.000699	192.168.102.98	192.168.100.8/	TCP 1514 mit	-ml-dev > 1028 [AC	K] Seq=1461 Ack=1 Win=6432 Ler	n=1460	
4 0.000/19	102.108.100.8/	192.108.102.98	TCD 1514 mit	a > mit-mi-dev [AC	() Seq=1 ACK=2921 WIN=00000 Le	en=0 a 1460	
6.0.001288	192.108.102.98	192.108.100.87	TCP 1514 mit	-m1-dev > 1028 [AC	K] Seq=2921 ACK=1 Win=6432 Ler	n=1460	
7 0.001437	192,168,100,87	192 168 102 98	TCP 54 102	8 > mit-ml-dev [AC	C] Seg=1 Ack=5841 Win=65535 Le	en=0	
8 0.002000	192,168,102,98	192,168,100,87	TCP 1514 [TC	P Previous segment	lost] mit-ml-dev > 1028 [ACK]	1 Seg=7301 Ack=1 Win=6432 Len=1460	
9 0.002015	192.168.100.87	192.168.102.98	TCP 66 [TC	P Dup ACK 7#1] 102	8 > mit-ml-dev [ACK] Seg=1 Ack	k=5841 Win=65535 Len=0 SLE=7301 SRE=8761	
10 0.002478	192.168.102.98	192.168.100.87	TCP 1022 [TC	P 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	тер 74 [те	P Dup ACK 7#2] 102	8 > mit-ml-dev [ACK] Seq=1 Ack	k=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 [TC	P Fast Retransmiss	ion] mit-ml-dev > 1028 [ACK] S	5eq=5841 Ack=1 Win=6432 Len=1460	
13 0.003070	192.168.100.87	192.168.102.98	TCP 66 102	8 > mit-ml-dev [AC	<] Seq=1 Ack=8761 Win=65535 Le	en=0 SLE=10221 SRE=11189	
14 0. 354505	192.168.102.98	192.168.100.87	TCP 1514 [TC	P Retransmission]	<pre>nit-ml-dev > 1028 [ACK] Seq=87</pre>	761 Ack=1 Win=6432 Len=1460	
15 0. 35453/	192.168.100.8/	192.168.102.98	TCP 54 102	8 > mit-mi-dev [AC	K] Seq=1 ACK=11189 Win=65535 L	Len=0	
10 0. 35511/	192.108.102.98	192.108.100.87	TCP 1514 mit	-m1-dev > 1028 [AC	() Seq=11189 ACK=1 Win=0432 Le	en=1460	
1/ 0. 333242	192.100.102.90	102 168 102 08	TCP 54 107	<pre>-mi-uev > 1020 [AC 8 > mit-ml-dov [AC</pre>	() Seq=12049 ACK=1 WIN=0452 Le	en=1400	
10 0.355810	192.108.100.8/	192.108.102.98	TCP 1514 mit	-m]-day > 1028 [AC	() Seq=14109 Ack=1 Win=6432 Le	en=1460	
20.0.355944	192 168 102 98	192 168 100 87	TCP 1514 mit	-m]-dev > 1028 [AC	C] Seq=15569 Ack=1 Win=6432 Let	en=1460	
21 0 255060	103 160 100 07	103 160 103 00	TCD 54103	0 . mit ml day [AC	1 500 1 Act 17030 Win 65525 1		
■ Frame 3: 1514	bytes on wire (121)	12 bits), 1514 bytes	captured (12112 bi	ts)			
Ethernet II, S	Src: Sensorma_10:08:	:e9 (00:50:f9:10:08:	e9), Dst: Advansus_	02:72:cb (00:19:0f	:02:72:cb)		
Internet Proto	ocol Version 4, Src:	: 192.168.102.98 (19	2.168.102.98), Dst:	192.168.100.87 (1	92.168.100.87)		
Transmission C	Control Protocol, Sr	rc Port: mit-ml-dev	(85), Dst Port: 102	8 (1028), Seq: 146	l, Ack: 1, Len: 1460		
Source port:	mit-ml-dev (85)						
Destination	port: 1028 (1028)						
Estream mue	x. 0] hon: 1461 (rolat	ivo soquenco numbor)				
ENext seguen	ce number: 2021	(relative sequence)	number)] 🦛				
Acknowledgem	ent number: 1 (r	elative ack number)					
Header lengt	h: 20 bytes						
■ Flags: 0x10	(ACK)						
Window size	value: 6432						
[Calculated	window size: 64321						*
0000 00 19 Of 0	02 72 cb 00 50 f9 1	10 08 e9 08 00 45 00)PE				
0010 05 dc 0f 1	L/ 40 00 40 06 d9 1	ra c0 a8 66 62 c0 a8	dw u E - > f				8
0030 19 20 39 9	93 00 00 a9 bd fa	3f 1b 80 1a 65 fb c7	9				
0040 7f 62 03 0	dc bf b9 24 00 05 d	c0 80 63 38 44 ff 58	.b\$c8D.	x			
0050 7d b6 7d 8	31 d3 Oe 5c 01 6f 8	84 fc 09 3b c6 63 b2	}.}\. 0;.0				
0050 80 11 00 1	Ta 41 9a ed b3 TT J	1D /a DU 50 23 1a 40	# a.sZ. J#.	Q.			
0080 05 cb 7d 1	La 50 f5 60 ff fc	21 b3 ef 18 88 e0 be	3.P. 1.				
0090 18 9e 5d a	ab d7 af 92 05 10	24 2f 7d 7b e0 9f de]\$/}{				
00a0 34 45 43 6	es t2 f5 fc 21 d2 d	d2 ab ff 17 af 45 f8	4EC1E				
0000 41 63 63 1	ha ha hs 37 7a fa	to is us u/ De DU /(h 1 0	þ			
File: "C:\Users\troy.w	videman\Docu Packets: 7	752 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)]	Property	Colonia abability dama	per serve poor - C		
Eile Edit View Go	apture Analyze Statistic	s Telephony Tools Intern	als Help				
	🖬 🗶 😅 📇 I 🔍 🌩 I	+ - 7 🗶 🔲 🔍 Q	Q Q 🗹	🖉 🗹 🥵 🎉			
Filter:		 Expres 	sion Cle	ar 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=146	0	
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	541028 > mit-ml-dev [ACK] Seq=1 Ack=2921 Win=65535 Len		
5 0.001288	192.168.102.98	192.168.100.87	TCP	1514 mit-ml-dev > 1028 [ACK] Seq=2921 ACK=1 W1n=6432 Len=	1460	
7 0 001421	192.108.102.98	192.168.100.8/	TCP	1014 mit-mi-dev > 1028 [ACK] Seq=4381 ACK=1 Win=0432 Len=	1460	
7 0.001437	192.108.100.87	192.108.102.98	TCP	1514 [TCR Provious soom	ACK] SEGET ACK=3841 WHI=03333 LEN	See-7301 Ack-1 Win-6432 Lan-1460	
9.0.002015	192.168.100.87	192.168.102.98	TCP	66 TCP Dup ACK 7#11 1	028 > mit-ml-dev [ACK] Seg=1 Ack=	5841 Win=65535 Len=0 SI F=7301 SRF=8761	
10 0, 002478	192.168.102.98	192.168.100.87	TCP	1022 [TCP Previous segme	nt lost] mit-ml-dev > 1028 [PSH.	ACK] Seg=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] 1	028 > mit-ml-dev [ACK] Seg=1 Ack=	5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=7	301 SRE=8761
12 0.003055	192.168.102.98	192.168.100.87	TCP	1514 [TCP Fast Retransmi	ssion] mit-ml-dev > 1028 [ACK] Se	q=5841 Ack=1 Win=6432 Len=1460	
13 0.003070	192.168.100.87	192.168.102.98	TCP	661028 > 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=876	1 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 Le	n=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 Le	n=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	192.108.102.98	192.168.100.8/	TCP	1514 mit-mi-dev > 1028 [ACK] Seq=13509 ACK=1 W1n=0432 Len	=1400	-
■ Frame 4: 54 byt	es on wire (432 bi	its), 54 bytes captu	red (432	bits)			
BEthernet II. Sr	c: Advansus_02:72:	cb (00:19:0f:02:72:	cb), Dst:	Sensorma_10:08:e9 (00:50:	f9:10:08:e9)		
Internet Protoc	ol Version 4, Src:	: 192.168.100.87 (19	2.168.100	0.87), Dst: 192.168.102.98	(192.168.102.98)		
Transmission Co	ntrol Protocol, Sr	rc Port: 1028 (1028)	, Dst Por	t: mit-ml-dev (85), Seq: 1	, Ack: 2921, Len: 0		
Source port:	1028 (1028)						
Destination p	ort: mit-ml-dev (8	5)					-
[Stream index	: 0]						
Sequence numb	er: 1 (relative	sequence number)	· •				
Acknowledgeme	nt number: 2921	(relative ack numbe	er) 🤤				
Header Tength	: 20 bytes						
Bridgs: 0x10 (ALL CEEDE						
Calculated w	indow cizo: 655251						
[Window size	scaling factor: =1	(unknown)]					-
0000 00 50 f9 10	08 e9 00 19 Of (02 72 cb 08 00 45 00	P	r F			
0010 00 28 af 42	40 00 80 06 ff 8	82 c0 a8 64 57 c0 a8	. (.B@.	dw			
0020 66 62 04 04	00 55 3e ba ff a	ad 45 f7 43 76 50 10	fbl	J>E.CvP.			
0030 TT TT 4C 25	00 00		L%				
Eile: "C\Users\troy.wic	ieman\Docu. Packets 7	752 Displayed: 7752 Marked: I	Load time:	3:00.220			Profile: Default
- Inter anyoders (no). Inte	Tuckets /	on any offer 1102 marked.	cost units	A REAL PROPERTY OF THE PROPERTY OF			



www.exacq.com



+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

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 /runk-1.6)]	_ 0 <mark>_ × .</mark>
Elle Edit View Go Capture Analyze Statistics Telephony Iools Internals Help	
● ● ● ● ■ ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
Filter: Expression_ Clear Apply	
No. Time Source Destination Protocol Length Info	*
10.000000 192.168.100.87 192.168.102.98 TCP 541028 > mit-ml-dev [ACK] Seq=1 Ack=1 Win=65524 Len=0	
20.000578 192.168.102.98 192.168.100.87 TCP 1514 m1t-m1-dev > 1028 [ACK] Seq=1 ACK=1 win=6432 Len=1460 [ACK] Seq=1 ACK=1 win=6432 [ACK] Seq=1 ACK=1	
3.0.000099 192.106.102.98 192.106.100.67 1CP 1314 mil-mi-deV > 1026 [Ack] 5ed=1401 Ack=1 Win=0432 Left=1400	
50.00128 192.168.102.98 192.168.100.87 TCP 1514 192.9 102.8 Sec. 2011 Ackel Se	
6 0.001421 192.168.102.98 192.168.100.87 TCP 1514 mit-mi-dev > 1028 fACK1 Sec=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] Seg=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-mi-dev > 1028 [PSH, Ack] Seq=10221 Ack=1 With=6432 Len=968	201 CDF 0261
110.00/2486 192.106.100.87 192.106.102.98 1CP /4 [1CP Dup ACK 7#2] 1028 > mit=mi=0eV [ACK] Seq=1 ACK=3841 Win=05535 Left=0221 SRE=11289 SLE=7 150.002055 102.168 102.08 103 168 100 87 TCP 1514 [TCP Dark Paterson Field and Board States] 1028 [ACK] SRE=740	301 SRE=8/01
13 0 003070 132 100 100 87 132 100 100 98 TCP 66 1028 > mit mil-mil-mil-mil-mil-mil-mil-mil-mil-mil-	
14 0.354505 192.168.102.98 192.168.100.87 TCP 1514 [TCP Retransmission] mit-m-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-m]-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 0.35522 192.168.100.87 192.168.102.98 TCP 54 1028 > mt = m1 - dev [Ack] Seq=1 Ack=14109 win=5555 Len=0	
19/0.555619/19/2.106.102.98/19/2.106.100.87/1CP/1514/mit=mid=002>10/28/EACK/Seq=14109/ACK=1/mit=0432/Len=1460/ 20/0.255044/10/162/162/102/162/102/162/102/162/102/162/162/162/162/162/162/162/162/162/16	
200,33394 152,100,102,50 152,100,100,07 (CF 1)4 mit mit dev 2,1020 [RAN] 364-1305 RANAT MIN-0922 Len-1400 11 0 355060 101 160 101 00 7 101 160 101 00 770 541030 wit $= 1$ dati 5470 Towa 1 Atol 17300 with 65555 (san 0	*
🖩 Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)	*
BEthernet 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)	
B Fransmission Control Protocol, Src Port: mit-mi-dev (85), USt Port: 1028 (1028), Seq: 4381, ACK: 1, Len: 1400	
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 Tength: 20 bytes	
■ Flags: 0x10 (Ack) Wilder size ville: 6422	
(Calculated window size 6432)	-
0000 00 19 0F 02 72 cb 00 50 F9 10 08 e9 08 00 45 00	
0010 05 dc 0f 1b 40 00 40 06 d9 f6 c0 a8 66 62 c0 a8	(=)
0020 64 57 00 55 04 04 45 17 49 28 36 08 1T 80 50 10 0 Mk/U.E. I*>P.	
0040 c0 bd 74 0b cf 52 bf 7a cf 82 cd 1f 46 68 ce	
0050 25 75 a7 62 ff 0b 5e 81 a0 9e 5f fd 30 d7 fa e4 %u.b^0	
0000 er tu br dl /3 00 24 00 03 29 80 e3 38 46 11 58	
0080 67 f2 8c 63 fa 7f 17 a2 d7 f8 ee dd 3f 40 6c be g	
0090 18 e8 12 78 e8 6c eb b7 ff 05 fd 92 e8 c0 b7 aex.l.	
UUau b3 be 5T TE ab be Ue U3 12 T5 ET 9E at TT 07 2T CA_{-1} , n	
NOT NO 20 14 25 TH	(*)

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:

📶 speed	dome (2).pcap	[Wireshark 1.6.2 (SVN Rev	38931 from /trunk-1.6)]	Report + Treating	ACTION A MARTIN	e some poor - Th				_ 0 <mark>_ x</mark>
<u>File</u>	t <u>V</u> iew <u>G</u> o g	<u>C</u> apture <u>A</u> nalyze <u>S</u> tatisti	cs Telephony <u>I</u> ools Interna	als <u>H</u> elp						
	8 94 94 12	🔀 🗶 😂 🖂 🔍 🍝	🏟 🥥 🏅 👱 🔲 🗐 🍳	् ् 🔍 🖄 📓 🖉 🥵						
Filter			 Express 	ion Clear Appl						
No.	Time	Source	Destination	Protocol Length Info						A
1	0.000000	192.168.100.87	192.168.102.98	TCP 54 102	8 > mit-ml-dev [Ad	[K] Seq=1 Ack=1 Win=6	65524 Len=0			
2	0.000578	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [AG	CK] Seq=1 Ack=1 Win=0	5432 Len=1460			
	0.000699	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [AG	[K] Seq=1461 Ack=1 W	in=6432 Len=1460)		
4	0.000719	192.168.100.87	192.168.102.98	TCP 54 102	8 > mit-ml-dev [AG	CKJ Seq=1 Ack=2921 W	in=65535 Len=0			
	0.001288	102.108.102.98	102 168 100 87	TCD 1514 mit	-ml-dev > 1028 [Ad	_K] Seq=2921 ACK=1 W	in=0432 Len=1460			
	0.001421	192.168.102.98	192.108.100.87	TCP 1014 mill	$\frac{1028}{8}$ mit-ml-dev [A	[K] Seq=1 Ack=5841 W	in=65535 Len=0	,		
	0.002000	192.168.102.98	192,168,100,87	тср 1514 [то	P Previous segment	t lost] mit-ml-dev >	1028 [ACK] Seg=	7301 Ack=1 Win=6432 L	en=1460	
9	0.002015	192.168.100.87	192.168.102.98	тср 66 [тс	P Dup ACK 7#1] 10	28 > 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	тср 1022 [тс	Previous segment	t 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	тср 74 [тс	Dup ACK 7#2] 10.	28 > mit-ml-dev [ACK]] Seq=1 Ack=5841	. Win=65535 Len=0 SLE=	10221 SRE=11189 SLE=73	01 SRE=8761
1	0.003055	192.168.102.98	192.168.100.8/	TCP 1514 [TC	P Fast Retransmis	5100] m1t-m1-dev > 10	J28 [ACK] Seq=58	41 Ack=1 Win=6432 Len	=1460	
1	0.354505	192.108.100.87	192.108.102.98	TCP 00 102	S > mit-mi-dev [Ad P Potransmission]	mit=ml=dov > 1028	CK1 Sog=8761 Ac	k=1_Win=6432_Len=1460		
19	0.354537	192,168,100,87	192.168.102.98	TCP 54 102	8 > mit-ml-dev [Ad	[K] Seg=1 Ack=11189)	vin=65535 Len=0	K=1 WHI=0452 Cell=1400		
10	0.355117	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [A([K] Seg=11189 Ack=1 N	vin=6432 Len=146	i0		
17	0.355242	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [A([K] Seq=12649 Ack=1 N	vin=6432 Len=146	0		
18	0.355252	192.168.100.87	192.168.102.98	TCP 54 102	8 > mit-ml-dev [AG	[K] Seq=1 Ack=14109 N	vin=65535 Len=0			
19	0.355819	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [AG	CK] Seq=14109 Ack=1 N	vin=6432 Len=146	i0		
20	0.355944	192.168.102.98	192.168.100.87	TCP 1514 mit	-ml-dev > 1028 [AG	CK] Seq=15569 Ack=1 N	Vin=6432 Len=146	i0		
Eram	7: 54 byt	tes on wire (432 b	its), 54 bytes captu	red (432 bits)						<u>^</u>
Ether	net II, Sr	c: Advansus_02:72	:cb (00:19:0f:02:72:	cb), Dst: Sensorma_	10:08:e9 (00:50:f9	9:10:08:e9)				
🗉 Inter	net Protoc	col Version 4, Src	: 192.168.100.87 (19	2.168.100.87), Dst:	192.168.102.98 (192.168.102.98)				
Trans	mission Co	ontrol Protocol, S	rc Port: 1028 (1028)	, Dst Port: mit-ml-	dev (85), Seq: 1,	Ack: 5841, Len: 0				
Sou	rce port:	1028 (1028)	1 (1)							
Des	tination p	ort: mit-mi-dev (85)							=
Lot Sec	uence numb	er:1 (relativ	sequence number)							
Ack	nowledgeme	nt number: 5841	(relative ack number	er) 🗲						
Неа	der length	: 20 bytes								
∋ Fla	gs: 0x10 (ACK)								
Win	dow size v	alue: 65535								
[Ca	lculated w	indow size: 65535	Contractor (NT							
0000	nnow 5170 00 50 £0 10	Scaling factor' -	02 72 cb 08 00 45 00	0						
0010	0 28 af 43	3 40 00 80 06 ff	81 c0 a8 64 57 c0 a8	. (.c@dw.						
0020	6 62 04 04	4 00 55 3e ba ff	ad 45 f7 4e de 50 10	fbU>E.N.F						
0030	T TT 4C 25	5 00 00		L%						
File: "(:\Users\troy.wid	deman\Docu Packets:	752 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.



www.exacq.com



+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

Frame 8 displays the following information:

speeddome (2).pcap	[Wireshark 1.6.2 (SVN Rev	38931 from /trunk-1.6)]	Paget 1 A	nation of the local division of the second	he en er	a per - R	
Eile Edit View Go	Capture Analyze Statistic	s Telephony <u>T</u> ools Intern	als <u>H</u> elp				
<u><u></u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u>	B 🖬 🗶 😂 🖴 I 🔍 🌳 🛛) 🞝 ኛ 🗶 🔲 🗐 Q	Q Q 🗹 🖉 🖉) 🕵 🖗 🖼			
Filter:		 Expres 	sion Clear	Apply			
No. Time	Source	Destination	Protocol Lengt	h Info			
1 0.000000	192.168.100.87	192.168.102.98	TCP .	541028 > mit-ml-dev	[ACK]	Seq=1 Ack=1 Win=65524 Len=0	
2 0.000578	192.168.102.98	192.168.100.87	TCP 15:	14 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 15:	14 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	541028 > mit-ml-dev	[ACK]	Seq=1 Ack=2921 Win=65535 Len=0	
5 0.001288	192.168.102.98	192.168.100.87	TCP 15	14 mit-ml-dev > 1028	[ACK]	Seq=2921 Ack=1 Win=6432 Len=1460	
6 0.001421	192.168.102.98	192.168.100.8/	TCP 15.	14 mit-mi-dev > 1028	[ACK]	Seq=4381 ACK=1 W1n=6432 Len=1460	
/ 0.00143/	192.108.100.8/	192.108.102.98	TCP 15	54 1028 > mit-mi-dev	LACK	Seq=1 ACK=3641 W1N=03333 Len=U	
9.0.002000	192.106.102.96	192.100.100.07	TCP 15.	56 TCP DUD ACK 7#11	1028	stj mit-mi-dev > 1026 [ACK] Sed=7301 ACK=1 Win=0432 Len=1400	
10.0.002478	192 168 102 98	192.168.100.87	TCP 10	22 ITCP Previous seg	ment lo	st] mit-m]-dev [Ack] Seq=1 Ack-3641 win-03333 Len=0 SEE=7301 SRE=0.01	
11 0.002488	192.168.100.87	192,168,102,98	TCP	74 TCP Dup ACK 7#21	1028 >	mit-m]-dev [ACK] Seg=1 Ack=5841 Win=65535 Len=0 SLE=10221 SRE=11189 SLE=730	1 SRE=8761
12 0.003055	192.168.102.98	192.168.100.87	TCP 15	14 [TCP Fast Retransm	mission] mit-m]-dev > 1028 [ACK] Seq=5841 Ack=1 Win=6432 Len=1460	
13 0.003070	192.168.100.87	192.168.102.98	тср (661028 > 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 15:	14 TCP Retransmissio	on] mit	-ml-dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460	
15 0. 35453/	192.108.100.8/	192.108.102.98	TCD 15	54 1028 > m1t-m1-dev	[ACK]	Seq=1 ACK=11189 W1N=05535 Len=U	
17 0 255242	192.100.102.90	192.108.100.87	TCD 15	14 mit-mi-dev > 1028	[ACK]	Seg=1169 Ack=1 Win=6432 Len=1460	
18 0 355252	192.108.102.90	192.168 102 98	TCP 13.	54 1028 > mit-ml-dev	[ACK]	Seg-1 Ack-14100 Win-65535 Len-0	
19.0.355819	192 168 102 98	192 168 100 87	TCP 15	14 mit-ml-dev > 1028	[ACK]	Seg=14109 Ack=1 Win=6432 Len=1460	
20 0. 355944	192.168.102.98	192.168.100.87	TCP 15	14 mit-ml-dev > 1028	[ACK]	Seg=15569 Ack=1 Win=6432 Len=1460	
21 0 255060	107 160 100 07	107 160 107 00	TCD	unh [m +im , 000113	FACU1	Can 1 Ack 17070 Win 65525 Lan 0	
⊮ Frame 8: 1514	bytes on wire (1211	2 bits), 1514 bytes	captured (121	12 bits)			
Ethernet II, S	<pre>Sensorma_10:08:</pre>	e9 (00:50:f9:10:08:	e9), Dst: Adva	unsus_02:72:cb (00:19	9:01:02	:72:cb)	
Internet Proto	col Version 4, Src:	192.168.102.98 (19	2.168.102.98),	Dst: 192.168.100.8/	7 (192.	168.100.8/)	
Source port:	mit-ml-day (85)	c Port: mit-mi-dev	(85), DST Port	: 1028 (1028), Seq:	7301,	ACK: 1, Len: 1400	
Destination	nort: 1028 (1028)						1
[Stream inde	x: 0]						
Sequence num	ber: 7301 (relat	ive sequence number		-			
[Next sequen	ce number: 8761	(relative sequence	number)]				
Acknowledgem	ent number: 1 (re	elative ack number)					
Header lengt	h: 20 bytes						
■ Flags: 0x10	(ACK)						
Window size	value: 6432						
ICalculated	window size: 64321						
0000 00 19 0F 0	02 72 CD 00 50 T9 1	0 08 e9 08 00 45 00)P	E.			1
0020 64 57 00 5	55 04 04 45 f7 54 9	2 3e ba ff ad 50 10	dw.UE. T.	>P.			
0030 19 20 8b 1	L5 00 00 0d 03 34 b	6 12 82 5a a7 60 c7	4.	Z.`.			
0040 98 61 ff 1	Lb e3 23 eb e8 54 5	6 08 16 f4 06 7a 86	5 .a# T∖	/z.			
0050 D3 00 e4 0 0060 11 d1 b0 7	1C 06 94 33 0C 11 T	2 /6 /1 CT 80 C0 20	P	vq			
0070 7d 91 8e f	f c6 d7 c5 80 b2 8	ac 70 e7 f7 92 0e as	}	p			
0080 b0 ae 0a 7	'd 06 d3 5a 91 a6 c	2 30 22 29 87 11 50	i}z	0")]			
0090 93 58 fb 6	52 a1 7c 3f d0 3a 3	of 4f 5a 2f ff 0f d0) .X.b. ?. ;?	POZ/			
00b0 1a f2 96 4	o 81 19 40 /3 69 5	c fb fd 6f 5c 12 6a	78	0\.i			
norn df ha na h	1 20 07 60 22 F0	IF 7. 62 AS 06 24 76					
Eile: "C\[kers\trow w	ideman\Docu Packets 77	52 Dicolayed: 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:

speeddome (2).pcap	[Wireshark 1.6.2 (SVN Rev	38931 from /trunk-1.6)]	August - La D	matrix . 40 million . 7 . 4 mil	het are n	rin par - D	_ 0 <u>_ X</u>
Eile Edit View Go	Capture Analyze Statistic	s Telephony Iools Interna	als Help				
	3×2819 +	+ 🛛 7 1 🗐 Q	0,0,0	0 🥦 🖗 🙀			
Filter:		Express	ion Clear	Apply			
No. Time	Source	Destination	Protocol Leng	th 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 15	14 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 15	14 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 15	14 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 15	14 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 > m1t-ml-dev	[ACK]	Seq=1 Ack=5841 W1n=65535 Len=0	
8 0.002000	192.168.102.98	192.168.100.87	TCP 15	14 LTCP Previous seg	ment I	ost] m1t-m1-dev > 1028 [ACK] Seq=/301 ACk=1 W1=6432 Len=1460	
9 0.002015	192.108.100.8/	192.168.102.98	TCP 10	66 [ICP DUD ACK /#1]	1028	> mit-mi-dev [ACK] Seq=1 ACK=3641 Win=05351 Len=0 SLE=/301 SKE=8/01	
11 0 002478	192.100.102.90	192.108.100.87	TCP 10	74 TTCP Previous seg	1079	USLJ MICHNI-00V > 1020 [PSH, ALK] S0[=10221 ACK=1 WIN=0452 L01=900 mit-mi-day [ArV] Con-1 Ack_S041 Win 6525 Lon-0 CIE_1021 CDE_11190 CIE_7201 CDE_9761	
12.0.002468	192.168.102.98	192.168.100.87	TCP 15	14 [TCP East Potrans]	niccio	> mitchindev (Ack) Selet Ack Soft Mitchild (Cener Steel 1022) She 1109 Steel JOI She 5/01	
13.0.003070	192 168 100 87	192 168 102 98	TCP	66 1028 > mit-ml-dev	[ACK]	Seg-1 Ack=8761 Win=65535 Len=0 SLE=10221 SEE=11189	
14.0.354505	192.168.102.98	192,168,100,87	TCP 15	14 ITCP Retransmissi	onl mi	t = m - dev > 1028 [ACK] Seq=8/61 ACK=1 Win=6432 Len=1460	
15 0, 354537	192,168,100,87	192,168,102,98	TCP	54 1028 > mit-ml-dev	[ACK]	Seg=1 Ack=11189 Win=65535 Len=0	
16 0.355117	192.168.102.98	192.168.100.87	TCP 15	14 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 15	14 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 15	14 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 15	14 mit-ml-dev > 1028	[ACK]	Seq=15569 Ack=1 Win=6432 Len=1460	-
030325 0 FC	103 160 100 07	103 160 103 00	TCD	54 1070 - mit ml dou	[ACV]	500 1 Act 17070 Win 65525 I on 0	
Ethomot II St	bytes on wire (12)	(00.50.60.10.08)	s Captured (1.	2112 DILSJ	0.05.0	2 - 72 - 64 2	<u>^</u>
a Ethernet 11, 51	c. Sensorma_10.00.	102 168 102 08 (10	2 168 102 08)	Det: 102 168 100 8	7 (102	162 100 87)	
Transmission Co	ntrol Protocol St	C Port: mit-ml-dev	(85) Det Por	t: 1028 (1028) Seg:	5841	Ack-1 Len- 1460	
Source port:	mit-ml-dev (85)	crore. mrc mr dev	(05), 050 101	c. 1020 (1020), 5cq.	5041,	Act, 1, Lui, 1999	
Destination p	ort: 1028 (1028)						=
[Stream index	: 0]						
Sequence numb	er: 5841 (relat	ive sequence number)					
[Next sequenc	e number: 7301	(relative sequence r	umber)]				
Acknowledgeme	nt number: 1 (r	elative ack number)					
Header length	: 20 bytes						
	ACK)						
Window size v	alue: 6432						-
ICalculated w	100w \$17e 64321			1			
0000 00 19 0f 02	2 72 cb 00 50 f9 1	10 08 e9 08 00 45 00	P .	E.			-
0020 64 57 00 55	04 04 45 f7 4e 0	de 3e ba ff ad 50 10	dw. U. F. N	> P.			(=)
0030 19 20 89 60	00 00 41 d5 84 9	96 19 Oc 48 31 51 Of	1A	H1Q.			
0040 ba 4b a2 1a	a 79 4f ec 1f 8d f	F3 Oe O4 ae O7 fd 61	.Ky0	a			
0050 0/ e1 15 f4	65 31 20 4e 68 t	04 fa 60 15 bb 43 /c	e7+N h				
0070 39 45 db fe	5e d4 1f 04 18 e	es 5f 8c eb ad db 44	QF A	D			
0080 57 b6 df f1	b1 23 da 7d 58 4	41 17 f7 Oc 3e 38 18	W#.} X	A>8.			
0090 21 1b 43 30	fc e2 e5 2f 4f	56 7b 0e df e1 6e 00	1.C 0</td <td>V{n.</td> <td></td> <td></td> <td></td>	V{n.			
00b0 d8 36 c5 of	TU T/ d2 e1 13	35 1e 80 ff fc 27 da	u	70/12 4			
00-0 fo 51 ba 00	34 36 1F 04 66	of 0c of be bo th sf	· · · · · ·	20/15.A			*
File: "C:\Users\troy.wid	teman\Docu Packets 7	752 Displayed: 7752 Marked: 0	Load time: 0:00 220	0		Profile: Default	t

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.



www.exacq.com



+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

Using Wireshark Filters

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

speeddome (2).pcap [Wireshark 1.6.2 (SVN Rev 38931 fr	rom /trunk-1.6)]	Instant all still of a West on our	apper a la	
File Edit View Go Capture Analyze Statistics Telep	phony Iools Internals Help			
		M 12 🥦 😹 110		
Filter: tcp.	Expression Clea	Apply		
No. Tir tcp	Protocol	Length Info	and and error a	*
1 0. tcp.analysis.lost_segment	98 TCP 87 TCP	54 1028 > mit-ml-dev [ACK] 5 1514 mit-ml-dev > 1028 [ACK] 5	eq=1 Ack=1 Win=65524 Len=0	
3 0 tcp.stream eq 0	87 TCP	1514 mit-ml-dev > 1028 [ACK] 5	eg=1461 Ack=1 Win=6432 Len=1460	
4 0, tcp.stream eq 2	98 TCP	54 1028 > mit-ml-dev [ACK] S	eq=1 Ack=2921 Win=65535 Len=0	
5 0. xml	87 TCP	1514 mit-m]-dev > 1028 [ACK] 5	eq=2921 Ack=1 Win=6432 Len=1460	
6 0.	87 TCP	1514 mit-ml-dev > 1028 [ACK] S	eq=4381 Ack=1 Win=6432 Len=1460	
8.0.002000 192 168 102 98 192	98 TCP	54 1028 > Mit-Mit-dev [ACK] S	eq=1 ACK=5841 WIN=05555 Len=0 t] mit=ml=dev > 1028 [ACK] Sec=7301 Ack=1 Win=6432 L	an-1460
9 0.002015 192 168 100.87 192	2.168.102.98 TCP	66 [TCP Dup ACK 7#1] 1028 >	mit-ml-dev [ACK] Seg=1 Ack=5841 Win=65535 Len=0 SLE=	7301 SRE=8761
10 0.002478 192.168.102.98 192	2.168.100.87 TCP	1022 [TCP Previous segment los	t] mit-m]-dev > 1028 [PSH, ACK] Seq=10221 Ack=1 Win=	5432 Len=968
11 0.002488 192.168.100.87 192	2.168.102.98 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	2.168.100.87 TCP 2.168.102.98 TCP	66 1028 > mit-ml-dov [ACK] S	mit-mi-dev > 1028 [ACK] Seq=3841 ACK=1 Win=0432 Len: on=1 Ack=8761 Win=65525 Lon=0 SLE=10221 SPE=11180	=1460
14 0 354505 192 168 102 98 192	2.168.102.98 TCP	1514 TCP Retransmission _ mit	m_1 -dev > 1028 [ACK] Seq=8761 Ack=1 Win=6432 Len=1460	
15 0.354537 192.168.100.87 192	2.168.102.98 TCP	54 1028 > mit-ml-dev [ACK] S	eg=1 Ack=11189 Win=65535 Len=0	
16 0.355117 192.168.102.98 192	2.168.100.87 TCP	1514 mit-m]-dev > 1028 [ACK] 5	eq=11189 Ack=1 Win=6432 Len=1460	
17 0.355242 192.168.102.98 192	2.168.100.87 TCP	1514 mit-ml-dev > 1028 [ACK] S	eq=12649 Ack=1 Win=6432 Len=1460	
18 0.355252 192.168.100.87 192	2.168.102.98 TCP	54 1028 > mit-ml-dev [ACK] 5	eq=1 Ack=14109 Win=65535 Len=0	
20.0 355044 102 168 102 08 102	2 168 100 87 TCP	1514 mit-ml-dev > 1028 [ACK] 5	eq=14109 ACK=1 Win=6432 Len=1460	
20 0.333344 192.100.102.30 132 31 0 355060 103 160 100 07 10	3 160 103 00 TCD	total and the state of the stat	an 1 Ack 17030 Win 65525 Jan 0	
Frame 10: 1022 bytes on wire (8176 bit	ts), 1022 bytes captured	(8176 bits)	NN 1.5	A
Ethernet II, Src: Sensorma_10:08:e9 (0 Internet Protocol Version 4 Src: 102	168 103 08 (103 168 103	Advansus_02:/2:cb (00:19:0F:02: 08) pct: 102 168 100 87 (102 1	/2:CD) 68 100 87)	
Transmission Control Protocol, Src Por	t: mit-ml-dev (85), Dst	Port: 1028 (1028), Seg: 10221.	Ack: 1. Len: 968	
Source port: mit-ml-dev (85)				
Destination port: 1028 (1028)				=
[Stream index: 0]				
Sequence number: 10221 (relative s	sequence number)			
Acknowledgement number: 1 (relativ	ve ack number)			
Header length: 20 bytes				
■ Flags: 0x18 (PSH, ACK)				
Window size value: 6432				
ICalculated window size: 64321	a0 08 00 45 00 m	D E		
0010 03 f0 0f 23 40 00 40 06 db da c0	a8 66 62 c0 a8	fb		â
0020 64 57 00 55 04 04 45 f7 5f fa 3e	ba ff ad 50 18 dw.U	>,P.		
0030 19 20 b8 2/ 00 00 12 08 t4 41 ae 0040 d2 8e 76 3a 72 a4 f8 dd 87 42 4f	68 21 2b /0 1b	A.h!+p.		
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?	. @.i^T		
0080 96 a9 ff f1 9b 3c 3f 3e 8f d0 3c	60 d0 eb b8 bc	= m,.~. ><		
0090 65 8f 40 79 c4 a9 48 33 b0 98 1f	d6 5f 5a f8 ae e.@y	3Z		
00a0 53 76 02 60 23 82 01 a7 e1 de c7 00b0 bf d0 37 fc 16 f4 15 76 08 78 20	ec bb 35 60 c6 Sv. #.			
0000 74 56 06 50 65 24 F2 ab FF 97 69	04 01 07 11 25 +F V44	ч		
Doublid filter "ten" is neither a fiel Dacketer 7752 Dien	nlaved: 7757 Marked: 0 Load time: 0	0.220		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)]	Name of	A Treatment of the	1000.0 4 *	hat are some p								_ 0 _ x
Eile Edit View Go	apture Analyze Statistic	s Telephony Iools Internal	ils <u>H</u> elp											
	2×28	0 7 1 EE Q	9.9.2	a 🗹 🥵 % i 🕯	H									
Filter: tcp.analysis	.lost_segment	Expressi	ion Clear	Apply										
No. Time	Source	Destination	Protocol L	ength Info										
8 0.002000	192.168.102.98	192,168,100,87	TCP	1514 [TCP P	previous seg	ment lost]	mit-ml-dev	> 1028	[ACK] Se	q=7301 Ack=1	Win=6432 L	en=1460		
10 0.002478	192.168.102.98	192.168.100.87	TCP	1022 [TCP P	previous seg	ment lost]	mit-ml-dev	> 1028	[PSH, AC	K] Seq=10221	Ack=1 Win=	5432 Len=968		
22 0.356528	192.168.102.98	192.168,100.87	TCP	1514 [TCP P	revious seg	ment lost]	mit-ml-dev	> 1028	[ACK] Sei	q=18489 Ack=	1 Win=6432	_en=1460		
24 0.357728	192.168.102.98	192.168.100.87	TCP	1514 [TCP P	revious seg	ment lost]	mit-ml-dev	> 1028	[ACK] Se	q=20901 Ack=	1 Win=6432	.en=1460		
40 0.676175	192.168.102.98	192.168.100.87	TCP	549 [TCP P	revious seg	ment lost]	mit-ml-dev	> 1028	[PSH, ACI	K] Seq=29661	Ack=61 Win	=6432 Len=49	5	
107 0.985612	192.168.102.98	192.168.100.87	TCP	70 [TCP P	revious seg	ment [ost]	mit-ml-dev	> 1028	LPSH, AC	K] Seq=/2968	Ack=b1 Win	=6432 Len=16		
61/8 21.639380	192.168.102.98	192.168.100.87	ICP	70 LICP P	revious seg	ment lost]	mit-mi-dev	> 1028	LPSH, ACI	K] Seq=33488	76 ACK=001	111=6432 Len	=10	
6210 22 005192	192.108.102.98	192,168,100,87	TCP	533 [ICP P	revious seg	ment lost]	mit-mi-dev	> 1028	LPSH, ACI	K] Seq=33005	72 ACK=001	V1n=0432 Len	=479	
0210 22.090180	192.100.102.90	192.108.100.87	TCP	1514 LICP P	revious sec	ment losti	mit-mi-dev	> 1020	TACKI SE	= 3384608 Ac	K=001 WIN=0	+32 Len=1460		
6228 22 31 3920	192 168 102 98	192 168 100 87	TCP	879 TCP P	revious seg	ment lost	mit ml dev	> 1028	TDCU AC	K1 Seg-33975	28 Ack-661	in-6432 Lon	-875	
6240 22 734020	192 168 102 98	192 168 100 87	TCP	1514 TCP P	revious seg	ment lost	mit-ml-dev	> 1028	TACK Se	n=3395653 Ac	k=661 Win=6	132 Len=1460		
6242 22 734810	192 168 102 98	192 168 100 87	TCP	1514 TCP P	revious seg	ment lost	mit-ml-dev	> 1028	[ACK] Se	-3397895 AC	x-661 Win-6	132 Len-1460		
6254 23, 103968	192 168 102 98	192 168 100 87	TCP	1514 TCP P	revious sec	ment lost	mit-ml-dev	> 1028	TACK1 Se	n=3406449 Ac	k=661 Win=6	132 Len=1460		
6266 23, 250667	192, 168, 102, 98	192, 168, 100, 87	TCP	1514 TCP P	revious sec	ment lost]	mit-ml-dev	> 1028	ACK Se	n=3414970 Ac	k=721 Win=6	132 Len=1460		
6268 23.251306	192.168.102.98	192,168,100,87	TCP	1514 TCP P	revious sec	ment lost1	mit-ml-dev	> 1028	TACKT Se	g=3417890 Ac	k=721 Win=6	132 Len=1460		
6280 23.564026	192.168.102.98	192.168.100.87	TCP	1514 TCP P	revious sec	ment lost1	mit-ml-dev	> 1028	ACK Se	g=3426650 Ac	k=721 Win=6	432 Len=1460		
6282 23.564888	192.168.102.98	192,168,100,87	TCP	1514 TCP P	revious sec	ment lost]	mit-ml-dev	> 1028	[ACK] Se	g=3428813 Ac	k=721 Win=6	132 Len=1460		
 Ethernet II, Sr Internet Protoc Transmission Co Source port: 1 Destination po 	c: Sensorma_10:08: col Version 4, Src: introl Protocol, Sr mit-ml-dev (85) ort: 1028 (1028)	e9 (00:50:f9:10:08:e 192.168.102.98 (192 c Port: mit-ml-dev ((85), Dst F	Advansus_02: 98), Dst: 19 Port: 1028 (72:cb (00:1 2.168.100.8 1028), Seq:	9:0f:02:72 7 (192.168 7301, Ack	:cb) .100.87) : 1, Len: 1	460						
[Stream index Sequence number [Next sequence Acknowledgement Header length = Flags: 0x10 (A	: 0] er: 7301 (relat e number: 8761 nt number: 1 (re : 20 bytes ACK)	ive sequence number) (relative sequence n elative ack number)	umber)]											
Window size v	alue: 6432													
[Calculated w	indow size: 64321													
0000 00 19 0f 02 0010 05 dc 0f 1f 0020 64 57 00 55 0030 19 20 8b 15 0040 98 61 ff 1b 0050 b3 00 e4 dc 0060 11 d1 b0 70	72 cb 00 50 f9 1 40 00 40 06 d9 f 04 04 45 f7 54 9 00 00 0d 03 34 b 0 e3 23 eb e8 54 5 06 94 33 0c 11 f 3c 80 80 b1 42 a	0 08 e9 08 00 45 00 2 c0 a8 66 62 c0 a8 2 3e ba ff ad 50 10 6 12 82 5a a7 60 c7 6 08 16 f4 06 7a 86 2 76 71 cf 8d cd 2e 0 a4 10 10 e4 28 9c		PE. fb . T.>P. . 4Z. . TVZ. Vq . B(.										Ē
0070 7d 91 8e ff 0080 b0 ae 0a 7d 0090 93 58 fb 62 00a0 09 a8 b6 06 00b0 1a f2 96 ec 0 file "C\Users\troy.wid	c6 d7 c5 80 b2 8 l l6 d3 5a 91 a6 c a1 7c 3f d0 3a 3 s1 19 ab 73 69 5 37 42 e5 14 3a 4 ab ac ac ac ac ac ac ac ac ac ab ac ac	cc 70 e7 f7 92 0e a5 2 30 22 29 87 11 5d f 4f 5a 2f ff 0f d0 c 68 17 8f 2c 89 76 c fb fd 6f 5c 12 6a f2 0 63 45 86 2d 2c 52 Displayed: 19 Marked: 0 L0	}	0")] .:?oz/ s i\hv .:o\.j										- 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.







+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

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

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:



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:









+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347

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.



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.

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/.



www.exacq.com



+1.317.845.5710 +5255.56080817 +44.1438.310163 +31.485.324.347