

Traffic Flow Wireshark Capture

capture.cap [Wireshark 1.6.3 (SVN Rev 39702 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
2197	26.986992	10.0.8.73	10.0.8.42	TCP	68	36795 > mysql [ACK] Seq=1453 Ack=969 Win=501 Len=0 TSval=2960212595 TSecr=1286760830
2198	26.993368	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=419, Time=67040
2199	27.005360	127.0.0.1	127.0.0.1	TCP	74	bandwiz-system > 56486 [PSH, ACK] Seq=37 Ack=25 Win=256 Len=6 TSval=2960212600 TSecr=2960211582
2200	27.005702	127.0.0.1	127.0.0.1	TCP	72	56486 > bandwiz-system [PSH, ACK] Seq=25 Ack=43 Win=257 Len=4 TSval=2960212600 TSecr=2960212600
2201	27.005742	127.0.0.1	127.0.0.1	TCP	68	bandwiz-system > 56486 [ACK] Seq=43 Ack=29 Win=256 Len=0 TSval=2960212600 TSecr=2960212600
2202	27.013267	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=420, Time=67200
2203	27.025219	10.0.8.73	10.0.8.42	TCP	68	52261 > mysql [ACK] Seq=1387 Ack=925 Win=394 Len=0 TSval=2960212605 TSecr=1286760829
2204	27.033225	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=421, Time=67360
2205	27.053313	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=422, Time=67520
2206	27.073270	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=423, Time=67680
2207	27.093263	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=424, Time=67840
2208	27.105353	10.0.8.73	10.0.8.42	MySQL	79	Request Query
2209	27.105739	10.0.8.42	10.0.8.73	MySQL	79	Response OK
2210	27.105807	10.0.8.73	10.0.8.42	TCP	68	52260 > mysql [ACK] Seq=1398 Ack=936 Win=484 Len=0 TSval=2960212625 TSecr=1286760949
2211	27.105858	10.0.8.73	10.0.8.42	MySQL	81	Request Query
2212	27.106051	10.0.8.42	10.0.8.73	MySQL	79	Response OK
2213	27.106118	10.0.8.73	10.0.8.42	MySQL	89	Request Query
2214	27.106417	10.0.8.42	10.0.8.73	MySQL	79	Response OK
2215	27.106556	10.0.8.73	10.0.8.42	MySQL	89	Request Query
2216	27.106838	10.0.8.42	10.0.8.73	MySQL	79	Response OK
2217	27.106882	10.0.8.73	10.0.8.42	TCP	68	52261 > mysql [ACK] Seq=1408 Ack=936 Win=394 Len=0 TSval=2960212625 TSecr=1286760950
2218	27.113445	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=425, Time=68000
2219	27.117434	10.0.6.73	10.1.0.248	SSH	116	Encrypted response packet len=48
2220	27.133313	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=426, Time=68160
2221	27.145236	10.0.8.73	10.0.8.42	TCP	68	52260 > mysql [ACK] Seq=1432 Ack=958 Win=484 Len=0 TSval=2960212635 TSecr=1286760949
2222	27.153562	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=427, Time=68320
2223	27.173377	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=428, Time=68480
2224	27.193559	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=429, Time=68640
2225	27.209181	10.1.0.248	10.0.6.73	TCP	68	60311 > ssh [ACK] Seq=1 Ack=1473 Win=160 Len=0 TSval=113538825 TSecr=2960212628
2226	27.213231	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=430, Time=68800
2227	27.233708	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=431, Time=68960
2228	27.253258	67.16.104.172	10.0.6.73	RTP	216	PT=ITU-T G.711 PCMU, SSRC=0x3E6E7CB5, Seq=432, Time=69120

Frame 2283: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 67.16.104.172 (67.16.104.172), Dst: 10.0.6.73 (10.0.6.73)

User Datagram Protocol, Src Port: 52220 (52220), Dst Port: 65534 (65534)

Real-Time Transport Protocol

```

0000  00 00 00 01 00 06 00 1f 9e 8b de f7 00 00 08 00  ....@. 6...c.h.
0010  45 20 00 c8 00 00 40 00 36 11 88 00 43 10 68 ac  E....@. 6...c.h.
0020  0a 00 06 49 cb fc ff fe 00 b4 00 00 80 00 01 d0  ...I.....
0030  00 01 22 00 3e 6e 7c b5 ff ff ff ff ff ff ff ff  ..'.>n].....
0040  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
0050  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
0060  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
0070  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
0080  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
0090  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
00a0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....

```