WireShark VoIP debugging

This is a simple how-to fro getting packets from an Asterisk server and into wireshark and then looking at what it has to show you.

We will look at :-

1. Getting the packets out of Asterisk.
2. Opening wireshark and initial screen
3. Locating calls.
4. Graphing the Sip messages
5. Listening to the Call
6. Looking at the RTP stream

1. Getting the packets we want.

First things first we need to get the packets we want. This is far simpler than its thought. We use a simple command line tool called tcpdump, if its not installed install it now, You wont be able to live without it.

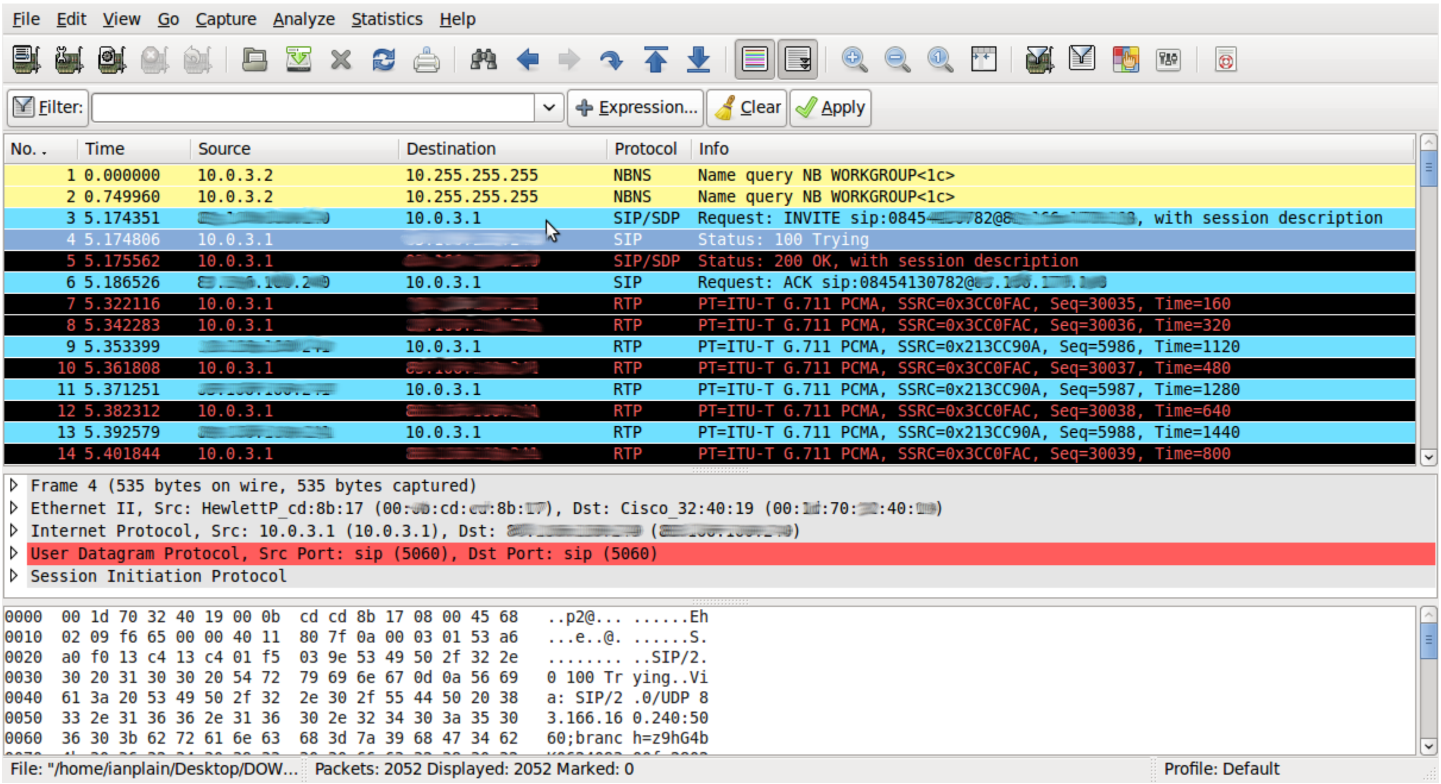
Here we have 2 commands, The first captures packets on interface eth0, -n means we wont converts addresses, -w means we just capture raw packets and udp means its only the udp packets we want and finally port 5060 means its only the sip messaging we want. In the second we dont specify port 5060 so that we get the rtp stream.

```
/usr/sbin/tcpdump -n -i eth0 -w /tmp/wireshark.pcap -s2000 udp port 5060
/usr/sbin/tcpdump -n -i eth0 -w /tmp/wireshark.pcap -s2000 udp
```

Once you have started the capture and made a call as required you will get a file called for example /tmp/wireshark.pcap copy this to your workstation via ftp or sftp as you would copy any file.

2. Wireshark

Wireshark is avalible for Linux, Windows and most other OS's. You can use it to make live captures from your workstation or as we are going to do oprn pcap files from elsewhere.

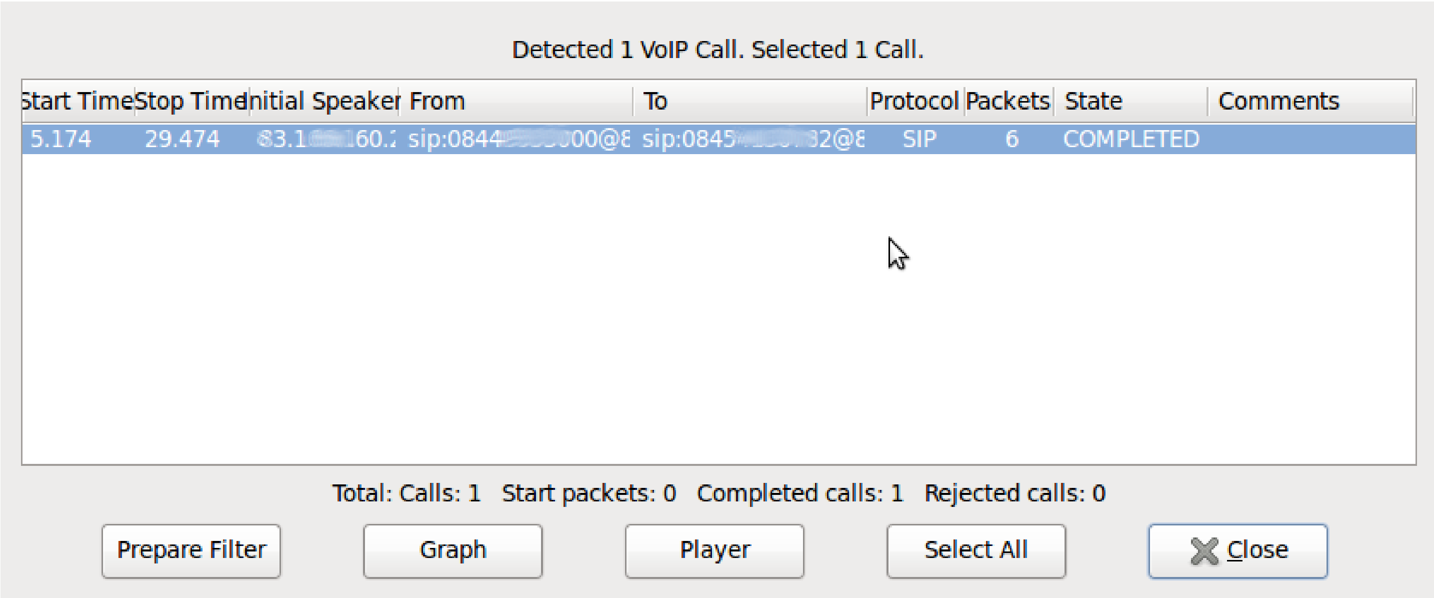


On starting Wireshark open your Pcap file and you should get a screen as above. We can see in the protocol column both SIP and RTP packets but we want to isolate our call.

3. Locating calls

Too locate our call we click on statistics then on Voip Calls and not as you might expect SIP. Sip will show you a count of each sip message in the capture.

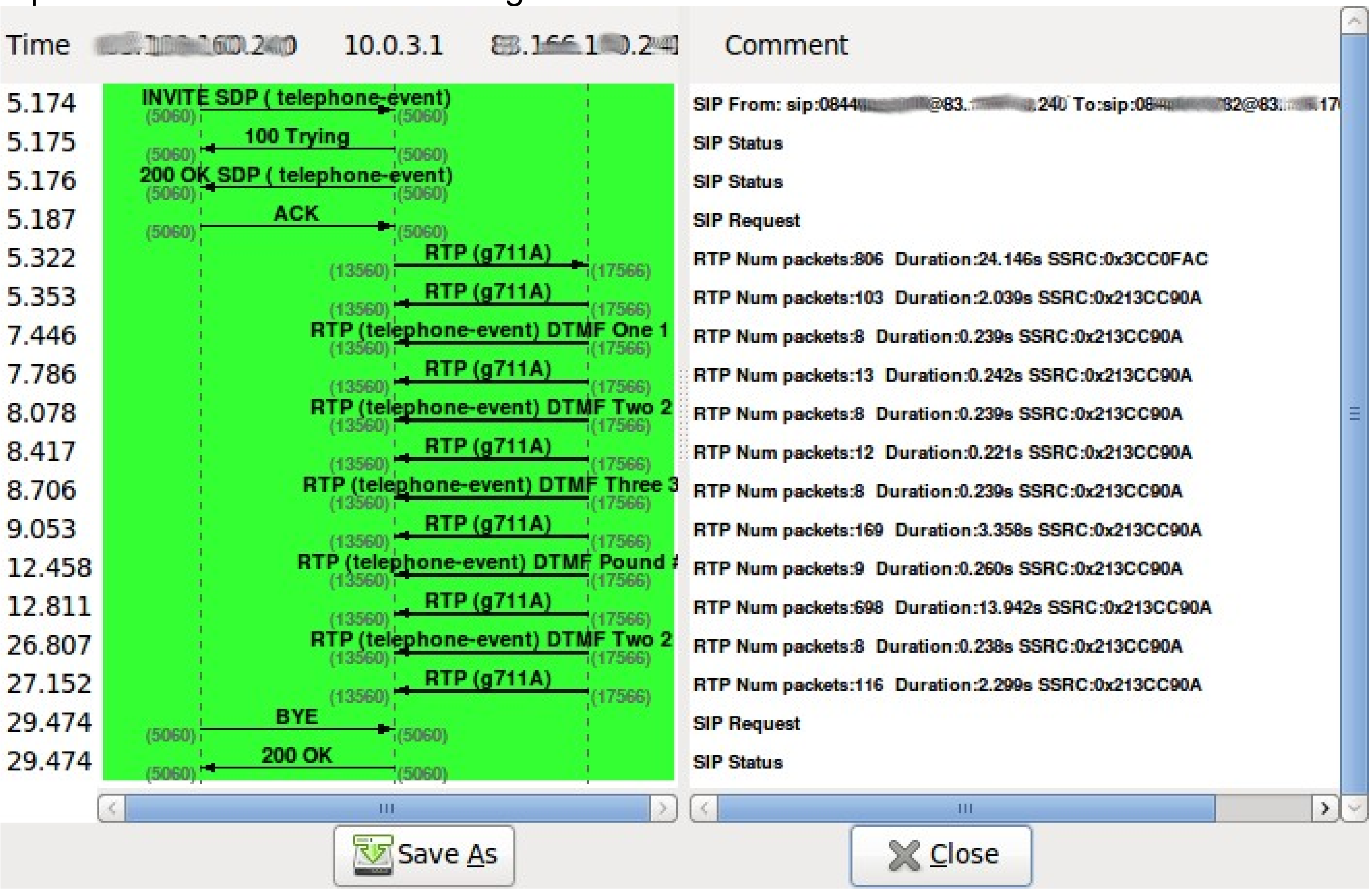
By selecting VoIP call you will get a new window as shown here.



This will show all calls in the capture and their status.

4. Graphing the calls

We can then highlight the call we want and by clicking on graph we get a visual representation of the SIP messages as below.

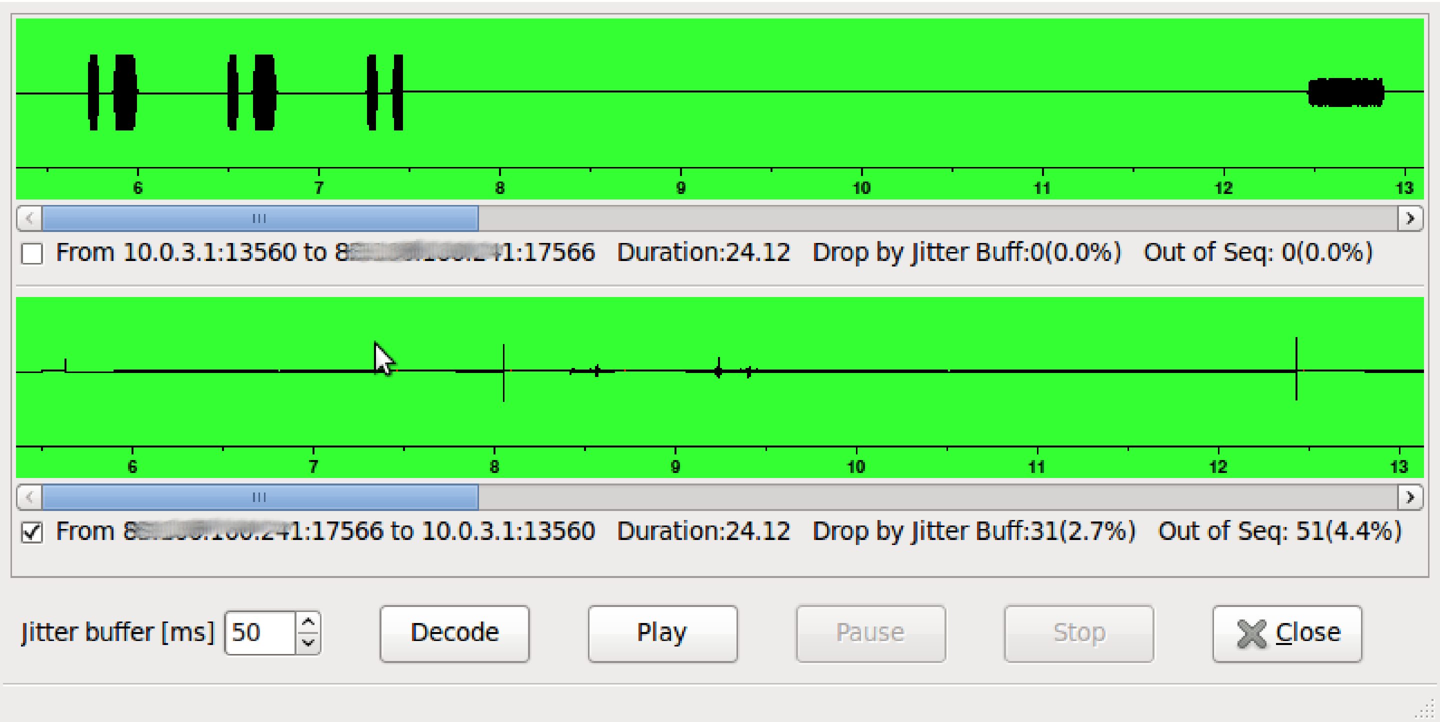


Here we can trace the messaging of the call and debug any issues we have.

This can then be saved as an ASCII version.

5. Listening to the Audio

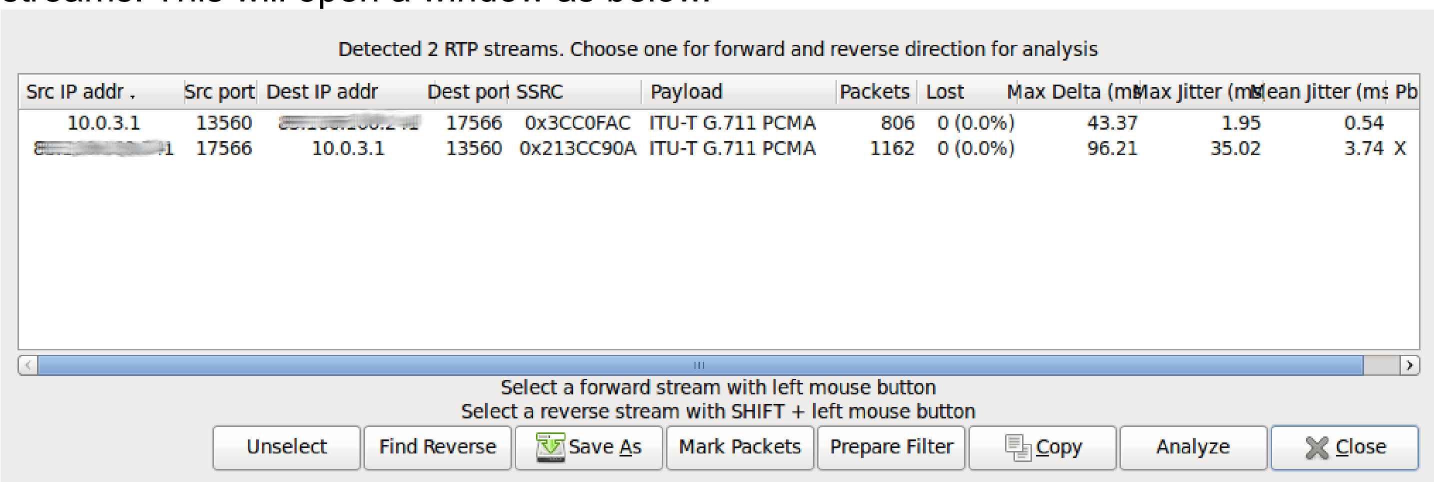
Also in the VoIP calls screen there is a player button. On clicking this you get a screen as below showing both legs of the call and its possible to play both separately or together.



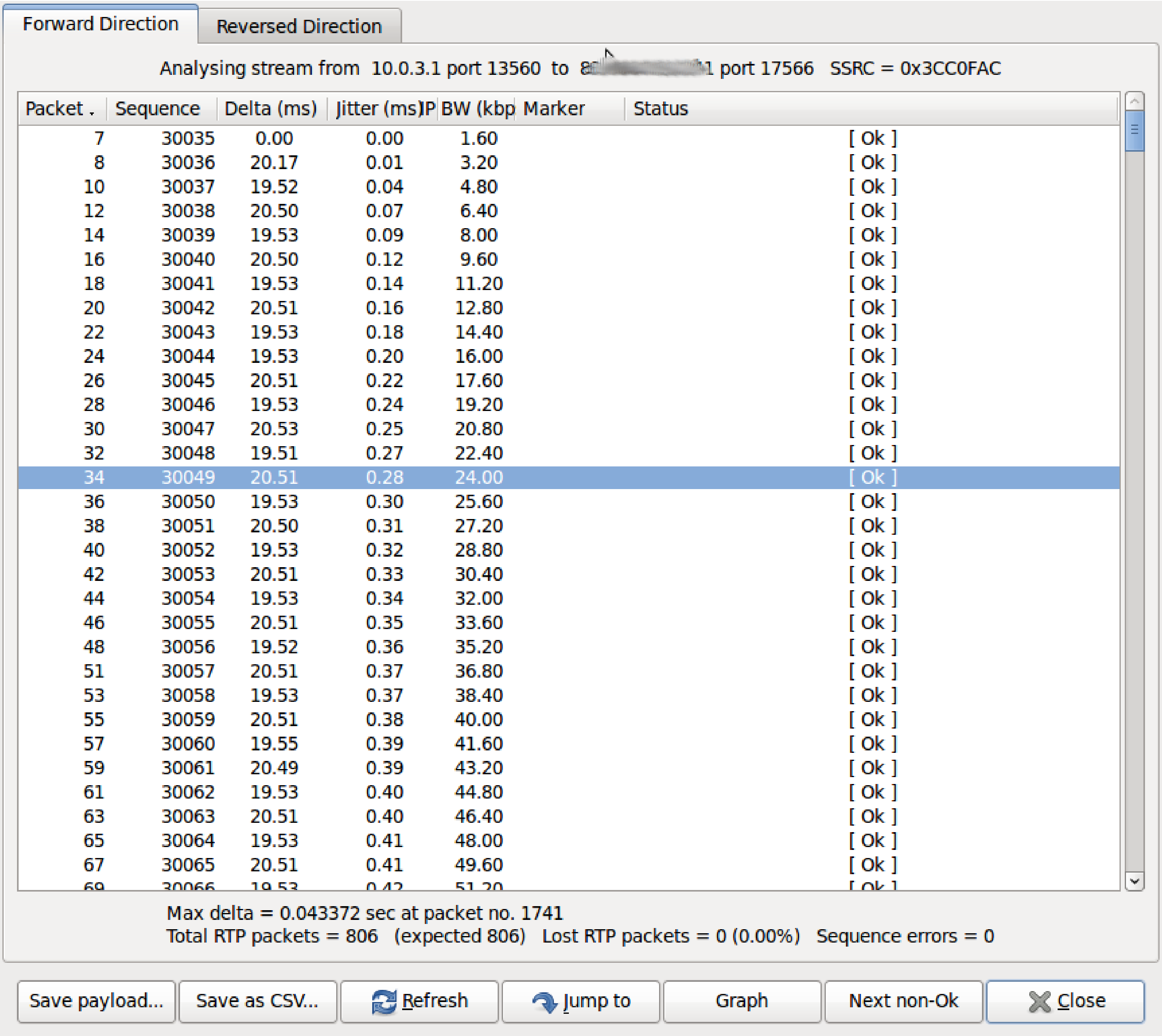
This is very useful for listening to audio from calls as well as for inband DTMF issues. Audio quality is subjective and by being able to listen to each leg of a call you can see if its poor in both directions or just one.

6. Looking at the RTP stream

Another option on the Statistics menu is RTP option. Click this and then click RTP streams. This will open a window as below.



In this window it does show some headline staistics for the call to see more detail select the stream you want to look at and click on analyze. This opens a new window that shows the data packet by packet as below.



Packet	Sequence	Delta (ms)	Jitter (ms)	IP BW (kbp	Marker	Status
7	30035	0.00	0.00	1.60		[Ok]
8	30036	20.17	0.01	3.20		[Ok]
10	30037	19.52	0.04	4.80		[Ok]
12	30038	20.50	0.07	6.40		[Ok]
14	30039	19.53	0.09	8.00		[Ok]
16	30040	20.50	0.12	9.60		[Ok]
18	30041	19.53	0.14	11.20		[Ok]
20	30042	20.51	0.16	12.80		[Ok]
22	30043	19.53	0.18	14.40		[Ok]
24	30044	19.53	0.20	16.00		[Ok]
26	30045	20.51	0.22	17.60		[Ok]
28	30046	19.53	0.24	19.20		[Ok]
30	30047	20.53	0.25	20.80		[Ok]
32	30048	19.51	0.27	22.40		[Ok]
34	30049	20.51	0.28	24.00		[Ok]
36	30050	19.53	0.30	25.60		[Ok]
38	30051	20.50	0.31	27.20		[Ok]
40	30052	19.53	0.32	28.80		[Ok]
42	30053	20.51	0.33	30.40		[Ok]
44	30054	19.53	0.34	32.00		[Ok]
46	30055	20.51	0.35	33.60		[Ok]
48	30056	19.52	0.36	35.20		[Ok]
51	30057	20.51	0.37	36.80		[Ok]
53	30058	19.53	0.37	38.40		[Ok]
55	30059	20.51	0.38	40.00		[Ok]
57	30060	19.55	0.39	41.60		[Ok]
59	30061	20.49	0.39	43.20		[Ok]
61	30062	19.53	0.40	44.80		[Ok]
63	30063	20.51	0.40	46.40		[Ok]
65	30064	19.53	0.41	48.00		[Ok]
67	30065	20.51	0.41	49.60		[Ok]
69	30066	19.53	0.42	51.20		[Ok]

As you can see its possible here to track the jitter and delta/delay full details of whats here is at http://wiki.wireshark.org/RTP_statistics?highlight=(RTP)

Conclusion

We can see that its possible to get a lot of information about calls from a simple capture, and armed with the output debugging issues will be much simpler and in the case of quality issues easier to put forward to the users.

The wireshark wiki is at http://wiki.wireshark.org/FrontPage and has all you need to know.