

## WireShark VoIP debugging



This is a simple how-to for 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.

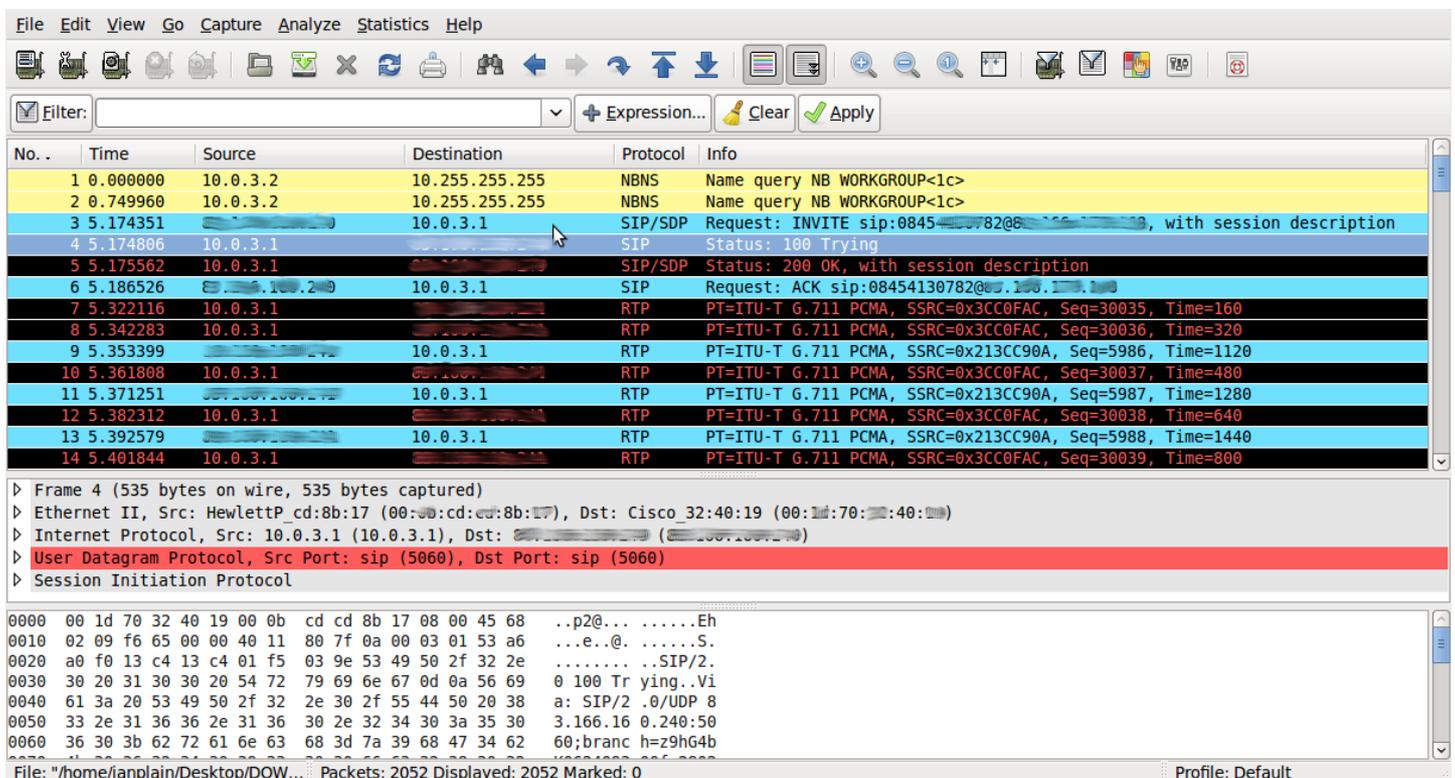
Here we have 2 commands, The first captures packets on interface eth0, -n means we wont converts addresses, -w means we just capture raw packets and udp means its only the udp packets we want and finally port 5060 means its only the sip messaging we want. In the second we dont specify port 5060 so that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



The screenshot shows the Wireshark interface with a list of captured packets. The packets are filtered to show SIP and RTP traffic. The list includes:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.3.2	10.255.255.255	NBNS	Name query NB WORKGROUP<1c>
2	0.749960	10.0.3.2	10.255.255.255	NBNS	Name query NB WORKGROUP<1c>
3	5.174351	10.0.3.1	10.0.3.1	SIP/SDP	Request: INVITE sip:0845...@... with session description
4	5.174806	10.0.3.1	10.0.3.1	SIP	Status: 100 Trying
5	5.175562	10.0.3.1	10.0.3.1	SIP/SDP	Status: 200 OK, with session description
6	5.186526	10.0.3.1	10.0.3.1	SIP	Request: ACK sip:08454130782@... with session description
7	5.322116	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3CC0FAC, Seq=30035, Time=160
8	5.342283	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3CC0FAC, Seq=30036, Time=320
9	5.353399	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x213CC90A, Seq=5986, Time=1120
10	5.361808	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3CC0FAC, Seq=30037, Time=480
11	5.371251	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x213CC90A, Seq=5987, Time=1280
12	5.382312	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3CC0FAC, Seq=30038, Time=640
13	5.392579	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x213CC90A, Seq=5988, Time=1440
14	5.401844	10.0.3.1	10.0.3.1	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3CC0FAC, Seq=30039, Time=800

The packet details pane shows the selected packet (Frame 4) with the following structure:

- Frame 4 (535 bytes on wire, 535 bytes captured)
- Ethernet II, Src: HewlettP\_cd:8b:17 (00:00:cd:08:b:17), Dst: Cisco\_32:40:19 (00:1d:70:32:40:19)
- Internet Protocol, Src: 10.0.3.1 (10.0.3.1), Dst: 10.0.3.1 (10.0.3.1)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 1d 70 32 40 19 00 0b cd cd 8b 17 08 00 45 68 ..p2@... ..Eh
0010 02 09 f6 65 00 00 40 11 80 7f 0a 00 03 01 53 a6 ...e..@. ....S.
0020 a0 f0 13 c4 13 c4 01 f5 03 9e 53 49 50 2f 32 2e ..... .SIP/2.
0030 30 20 31 30 30 20 54 72 79 69 6e 67 0d 0a 56 69 0 100 Tr ying..Vi
0040 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44 50 20 38 a: SIP/2 .0/UDP 8
0050 33 2e 31 36 3e 2e 31 36 30 2e 32 34 30 3a 35 30 3.166.16 0.240:50
0060 36 30 3b 62 72 61 6e 63 68 3d 7a 39 68 47 34 62 60;branc h=z9hG4b
```

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

To 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.

Detected 1 VoIP Call. Selected 1 Call.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
5.174	29.474	83.166.100.240	10.0.3.1 sip:0844...000@83.166.100.240	10.0.3.1 sip:0845...32@83.166.100.240	SIP	6	COMPLETED	

Total: Calls: 1 Start packets: 0 Completed calls: 1 Rejected calls: 0

Prepare Filter Graph Player Select All Close

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.

Time 10.0.3.1 83.166.100.240 Comment

Time	Message	From	To	Comment
5.174	INVITE SDP (telephone-event)	(5060)	(5060)	SIP From: sip:0844...@83.166.100.240 To:sip:0845...32@83.166.100.240
5.175	100 Trying	(5060)	(5060)	SIP Status
5.176	200 OK SDP (telephone-event)	(5060)	(5060)	SIP Status
5.187	ACK	(5060)	(5060)	SIP Request
5.322	RTP (g711A)	(13560)	(17566)	RTP Num packets:806 Duration:24.146s SSRC:0x3CC0FAC
5.353	RTP (g711A)	(13560)	(17566)	RTP Num packets:103 Duration:2.039s SSRC:0x213CC90A
7.446	RTP (telephone-event) DTMF One 1	(13560)	(17566)	RTP Num packets:8 Duration:0.239s SSRC:0x213CC90A
7.786	RTP (g711A)	(13560)	(17566)	RTP Num packets:13 Duration:0.242s SSRC:0x213CC90A
8.078	RTP (telephone-event) DTMF Two 2	(13560)	(17566)	RTP Num packets:8 Duration:0.239s SSRC:0x213CC90A
8.417	RTP (g711A)	(13560)	(17566)	RTP Num packets:12 Duration:0.221s SSRC:0x213CC90A
8.706	RTP (telephone-event) DTMF Three 3	(13560)	(17566)	RTP Num packets:8 Duration:0.239s SSRC:0x213CC90A
9.053	RTP (g711A)	(13560)	(17566)	RTP Num packets:169 Duration:3.358s SSRC:0x213CC90A
12.458	RTP (telephone-event) DTMF Pound #	(13560)	(17566)	RTP Num packets:9 Duration:0.260s SSRC:0x213CC90A
12.811	RTP (g711A)	(13560)	(17566)	RTP Num packets:698 Duration:13.942s SSRC:0x213CC90A
26.807	RTP (telephone-event) DTMF Two 2	(13560)	(17566)	RTP Num packets:8 Duration:0.238s SSRC:0x213CC90A
27.152	RTP (g711A)	(13560)	(17566)	RTP Num packets:116 Duration:2.299s SSRC:0x213CC90A
29.474	BYE	(5060)	(5060)	SIP Request
29.474	200 OK	(5060)	(5060)	SIP Status

Save As Close

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.

The screenshot shows a VoIP audio player interface with two call legs. The top leg is from 10.0.3.1:13560 to 8.100.100.241:17566, with a duration of 24.12, 0% drop by jitter buffer, and 0% out of sequence. The bottom leg is from 8.100.100.241:17566 to 10.0.3.1:13560, with a duration of 24.12, 2.7% drop by jitter buffer, and 4.4% out of sequence. The interface includes a jitter buffer control set to 50 ms, and buttons for Decode, Play, Pause, Stop, and Close.

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.

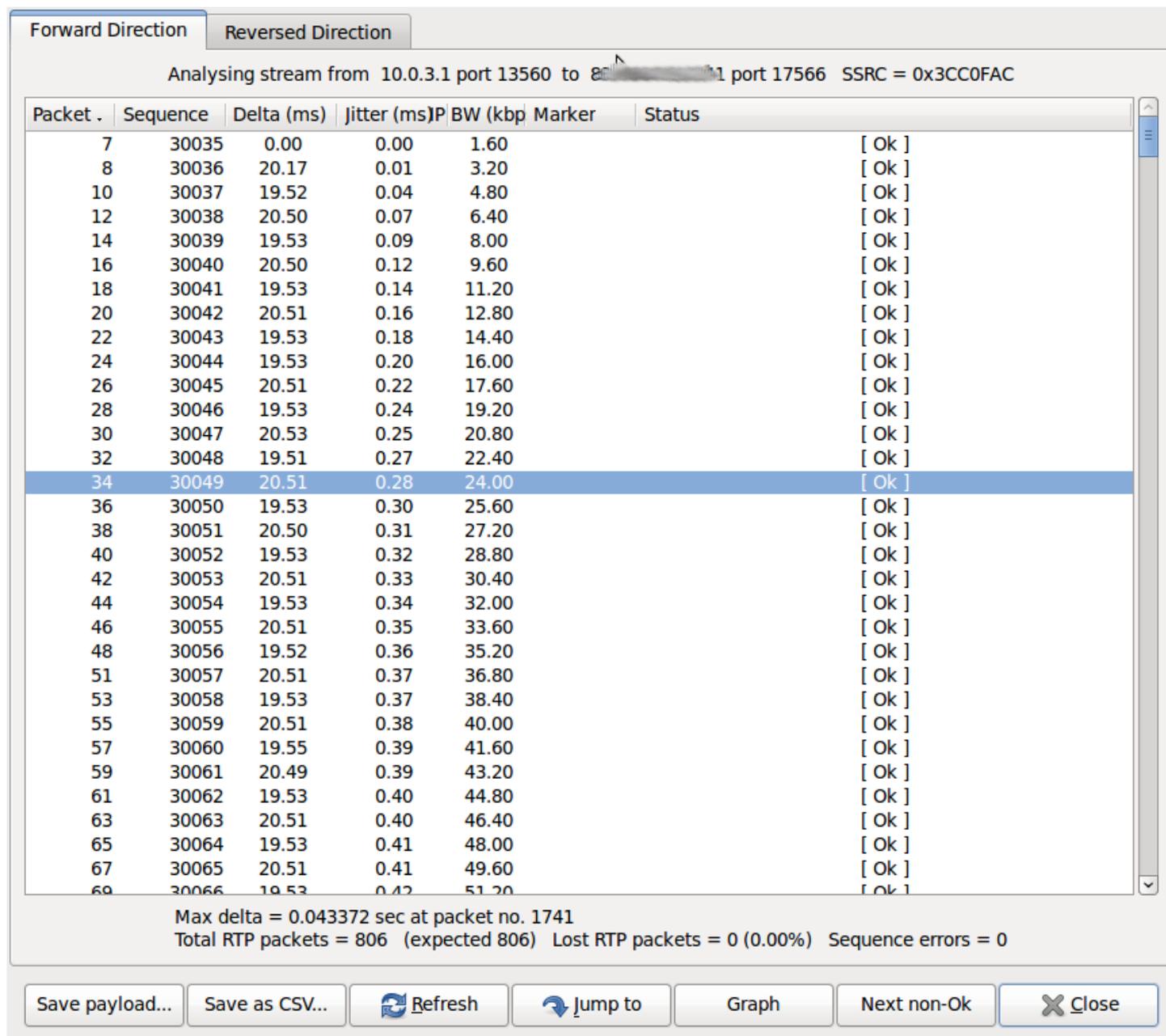
The screenshot shows a window titled "Detected 2 RTP streams. Choose one for forward and reverse direction for analysis". It contains a table with the following data:

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb
10.0.3.1	13560	8.100.100.241	17566	0x3CC0FAC	ITU-T G.711 PCMA	806	0 (0.0%)	43.37	1.95	0.54	
8.100.100.241	17566	10.0.3.1	13560	0x213CC90A	ITU-T G.711 PCMA	1162	0 (0.0%)	96.21	35.02	3.74	X

Below the table are instructions: "Select a forward stream with left mouse button" and "Select a reverse stream with SHIFT + left mouse button". At the bottom are buttons for Unselect, Find Reverse, Save As, Mark Packets, Prepare Filter, Copy, Analyze, and Close.

In this window it does show some headline statistics 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.



The screenshot shows the 'RTP Statistics' window in Wireshark, displaying a table of RTP packet statistics. The window title is 'Analysing stream from 10.0.3.1 port 13560 to 8... port 17566 SSRC = 0x3CC0FAC'. The table has columns for Packet, Sequence, Delta (ms), Jitter (ms), P/BW (kbp), Marker, and Status. Packet 34 is highlighted in blue. Below the table, summary statistics are provided: Max delta = 0.043372 sec at packet no. 1741, Total RTP packets = 806 (expected 806), Lost RTP packets = 0 (0.00%), and Sequence errors = 0. At the bottom, there are buttons for 'Save payload...', 'Save as CSV...', 'Refresh', 'Jump to', 'Graph', 'Next non-Ok', and 'Close'.

Packet	Sequence	Delta (ms)	Jitter (ms)	P/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 ]

Max delta = 0.043372 sec at packet no. 1741  
Total RTP packets = 806 (expected 806) Lost RTP packets = 0 (0.00%) Sequence errors = 0

Buttons: Save payload..., Save as CSV..., Refresh, Jump to, Graph, Next non-Ok, Close

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=\(RTP\)](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.