

# WebRTC

- The technology
  - Possible problems
  - Troubleshooting
- ICE and STUN traffic
- DTLS traffic
- SRTP traffic
  - Recognizing SRTP packets
  - Decoding SRTP packets
  - Decoded SRTP traffic
  - SRTP packet header
  - The list of SRTP and RTP streams taking part in a WebRTC session
  - SRTP stream analysis

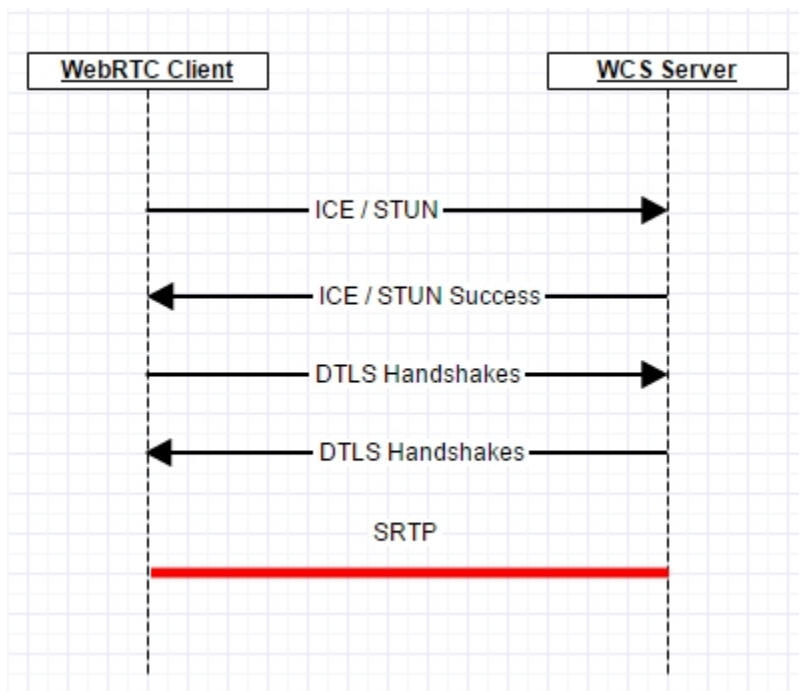
## The technology

The WebRTC technology uses three main specifications in networking:

ICE and STUN  
DTLS  
SRTP

To establish a WebRTC connection, [ICE](#) is used. The web client sends [STUN](#)-requests to the WCS server, the WCS server responds to these requests and hence confirms it is ready to establish connection.

On the next stage, parties exchange SSL certificates via [DTLS](#) and establish an encrypted channel between the web client and the WCS server. When the connection is established, [SRTP](#) traffic is transmitted.



## Possible problems

In most cases problems are related to UDP traffic of ICE, STUN, DTLS, SRTP not flowing between parts of the system.

## Troubleshooting

Make sure all the traffic that takes part in establishing a WebRTC sessions and sending media data is unhindered and passes freely between call participants. Media ports of the WCS server in the range of [31000-32000] by default must be open to receive the incoming UDP traffic. If the WCS server is behind NAT and has an external IP address, make sure UDP packets sent to this external address are correctly routed to the corresponding ports of the WCS server behind NAT.

## ICE and STUN traffic

The image displays the Wireshark network traffic analysis interface. At the top, the title bar reads "log.pcap [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]". The main menu includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, packet selection, and analysis.

The packet list pane shows a table of captured packets. The first column is "No.", the second is "Time", the third is "Source", the fourth is "Destination", the fifth is "Protocol", and the sixth is "Length". The "Info" column provides details about each packet. The filter bar at the top of the packet list is set to "stun".

The packet details pane shows the selected packet (Frame 16) with the following structure:

- Ethernet II, Src: Intel (08:00:00:00:00:00), Dst: Intel (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1
- Transmission Control Protocol, Src Port: 80, Dst Port: 80
- Session Traversal Utilities Protocol (STUN), Src: 192.168.1.1, Dst: 192.168.1.1

The packet bytes pane shows the raw data of the selected packet, displayed in hexadecimal and ASCII. The data is a STUN packet, and the ASCII view shows the text "STUN" repeated multiple times.

The status bar at the bottom indicates the current file is "C:\tmp\3\log.pcap", the packet count is 1057, and the display filter is "2 (2.4%)". The load time is 0:00:023. The profile is set to "Default".

DTLS starts working directly after ICE has established connection. Exchange of SSL certificates is several Handshake messages resulting in an established secure connection to transfer media data.

The image displays the Wireshark network protocol analyzer interface. The title bar indicates the capture file is 'log.pcap' and the version is 'Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains icons for various functions like opening files, saving, and filtering. The 'Filter' field is set to 'dtls'. The packet list pane shows 107 packets, with the first 103 packets being DTLSv1 messages. The packet details pane shows the selected packet (103) as an 'Encrypted Alert'. The packet bytes pane shows the raw data of the selected packet. The status bar at the bottom indicates the file path 'C:\tmp\3\log.pcap', the size '143 kB', the time '00:00:33', the number of packets '1057', the display filter 'Displayed: 8 (0,8%)', the load time '0:00:020', and the profile 'Default'.

| No.  | Time      | Source         | Destination    | Protocol | Length | Info  |
|------|-----------|----------------|----------------|----------|--------|---|
| 23   | 28.093212 | 188.40.69.75   | 92.127.221.146 | DTLSv1.  | 180    | Client Hello  |
| 26   | 28.137884 | 188.40.69.75   | 92.127.221.146 | DTLSv1.  | 180    | Client Hello  |
| 27   | 28.196537 | 92.127.221.146 | 188.40.69.75   | DTLSv1.  | 883    | Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done                |
| 28   | 28.216232 | 188.40.69.75   | 92.127.221.146 | DTLSv1.  | 825    | Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message |
| 30   | 28.224506 | 188.40.69.75   | 92.127.221.146 | DTLSv1.  | 825    | Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message |
| 31   | 28.322495 | 92.127.221.146 | 188.40.69.75   | DTLSv1.  | 133    | Change Cipher Spec, Encrypted Handshake Message   |
| 32   | 28.324976 | 92.127.221.146 | 188.40.69.75   | DTLSv1.  | 133    | Change Cipher Spec, Encrypted Handshake Message   |
| 1057 | 33.428850 | 92.127.221.146 | 188.40.69.75   | DTLSv1.  | 103    | Encrypted Alert   |

## Recognizing SRTP packets

log.pcap [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

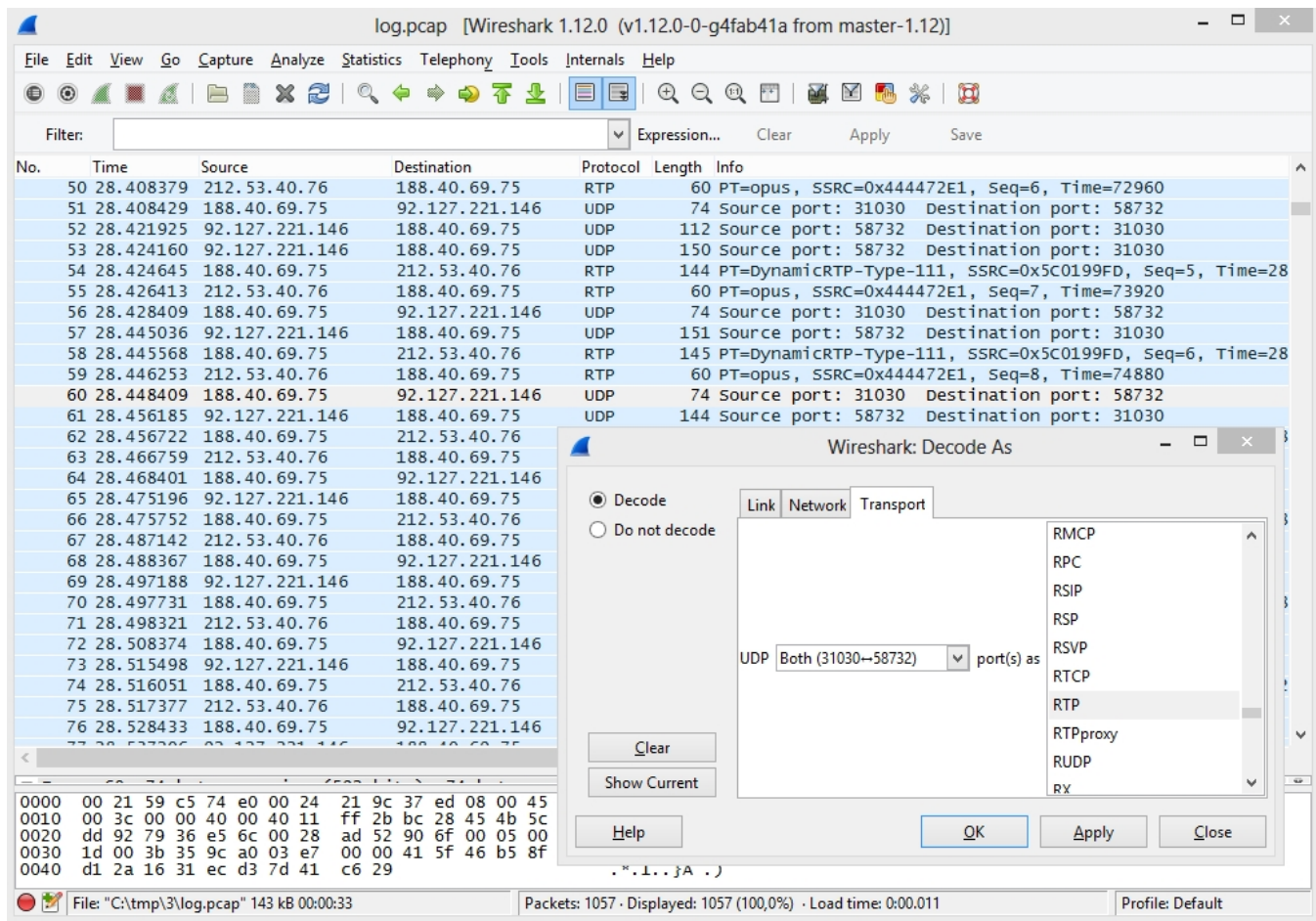
Filter: Expression... Clear Apply Save

| No. | Time      | Source         | Destination    | Protocol | Length | Info  |
|-----|-----------|----------------|----------------|----------|--------|---|
| 50  | 28.408379 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=6, Time=72960                 |
| 51  | 28.408429 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |
| 52  | 28.421925 | 92.127.221.146 | 188.40.69.75   | UDP      | 112    | Source port: 58732 Destination port: 31030                  |
| 53  | 28.424160 | 92.127.221.146 | 188.40.69.75   | UDP      | 150    | Source port: 58732 Destination port: 31030                  |
| 54  | 28.424645 | 188.40.69.75   | 212.53.40.76   | RTP      | 144    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=5, Time=73000  |
| 55  | 28.426413 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=7, Time=73920                 |
| 56  | 28.428409 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |
| 57  | 28.445036 | 92.127.221.146 | 188.40.69.75   | UDP      | 151    | Source port: 58732 Destination port: 31030                  |
| 58  | 28.445568 | 188.40.69.75   | 212.53.40.76   | RTP      | 145    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=6, Time=74000  |
| 59  | 28.446253 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=8, Time=74880                 |
| 60  | 28.448409 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |
| 61  | 28.456185 | 92.127.221.146 | 188.40.69.75   | UDP      | 144    | Source port: 58732 Destination port: 31030                  |
| 62  | 28.456722 | 188.40.69.75   | 212.53.40.76   | RTP      | 138    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=7, Time=75000  |
| 63  | 28.466759 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=9, Time=75840                 |
| 64  | 28.468401 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |
| 65  | 28.475196 | 92.127.221.146 | 188.40.69.75   | UDP      | 150    | Source port: 58732 Destination port: 31030                  |
| 66  | 28.475752 | 188.40.69.75   | 212.53.40.76   | RTP      | 144    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=8, Time=76000  |
| 67  | 28.487142 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=10, Time=76800                |
| 68  | 28.488367 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |
| 69  | 28.497188 | 92.127.221.146 | 188.40.69.75   | UDP      | 144    | Source port: 58732 Destination port: 31030                  |
| 70  | 28.497731 | 188.40.69.75   | 212.53.40.76   | RTP      | 138    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=9, Time=77000  |
| 71  | 28.498321 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=11, Time=77760                |
| 72  | 28.508374 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |
| 73  | 28.515498 | 92.127.221.146 | 188.40.69.75   | UDP      | 141    | Source port: 58732 Destination port: 31030                  |
| 74  | 28.516051 | 188.40.69.75   | 212.53.40.76   | RTP      | 135    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=10, Time=78000 |
| 75  | 28.517377 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=12, Time=78720                |
| 76  | 28.528433 | 188.40.69.75   | 92.127.221.146 | UDP      | 74     | Source port: 31030 Destination port: 58732                  |

File: "C:\tmp\3\log.pcap" 143 kB 00:00:33 Packets: 1057 · Displayed: 1057 (100,0%) · Load time: 0:00.011 Profile: Default

## Decoding SRTP packets

Wireshark can decode the UDP packets it found if we explicitly specify the protocol. In the packet properties select 'Decode As..', then select the RTP protocol for all packets that run between the browser (port 31030) and the WCS server (port 58732). These ports are reserved dynamically, so in your case the values might be different.



## Decoded SRTP traffic

As a result of decoding the protocol, Wireshark will display the decoded SRTP traffic:



log.pcap [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

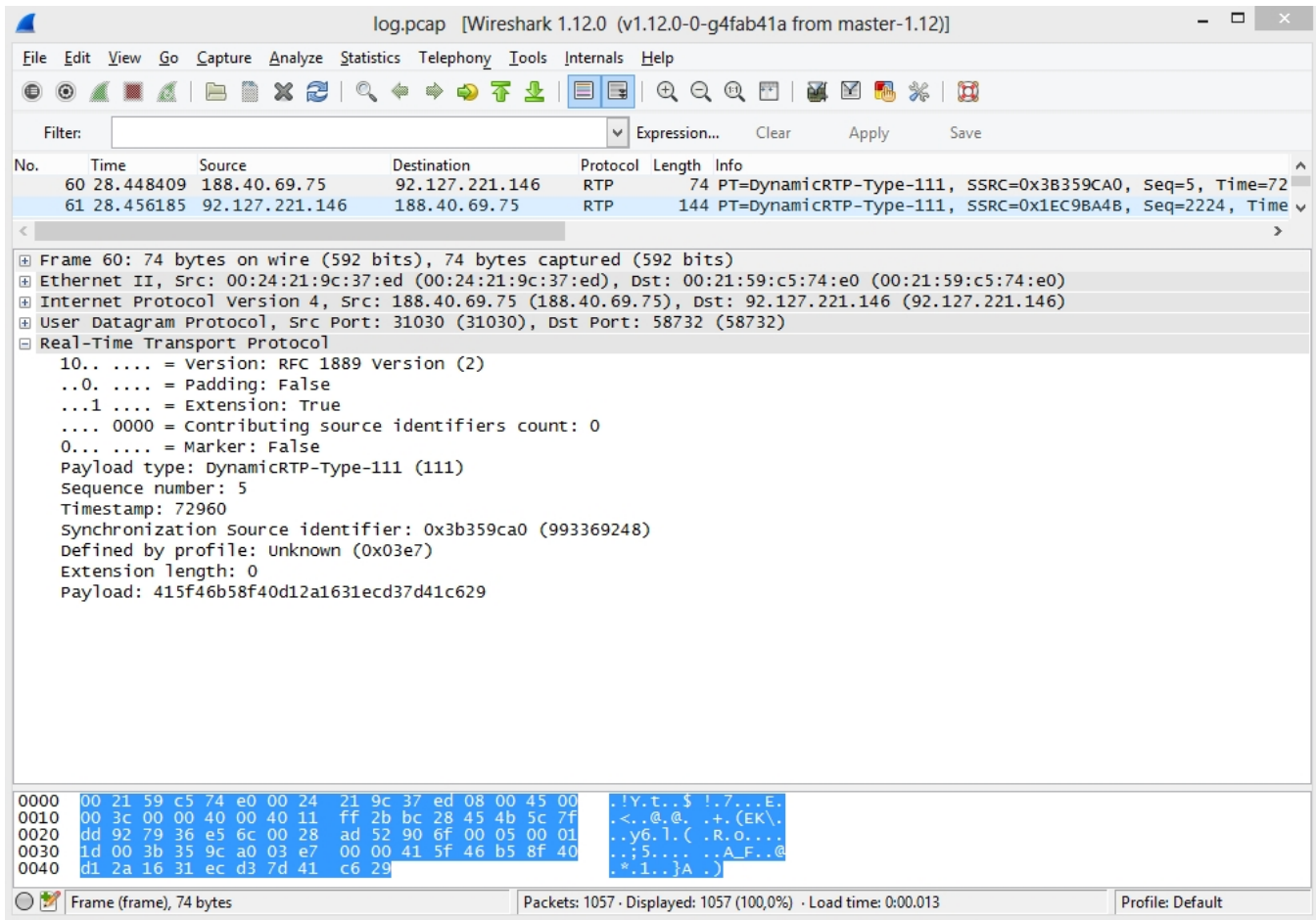
| No. | Time      | Source         | Destination    | Protocol | Length | Info  |
|-----|-----------|----------------|----------------|----------|--------|---|
| 60  | 28.448409 | 188.40.69.75   | 92.127.221.146 | RTP      | 74     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=5, Time=72     |
| 61  | 28.456185 | 92.127.221.146 | 188.40.69.75   | RTP      | 144    | PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2224, Time=72  |
| 62  | 28.456722 | 188.40.69.75   | 212.53.40.76   | RTP      | 138    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=7, Time=28     |
| 63  | 28.466759 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=9, Time=75840                 |
| 64  | 28.468401 | 188.40.69.75   | 92.127.221.146 | RTP      | 74     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=6, Time=73     |
| 65  | 28.475196 | 92.127.221.146 | 188.40.69.75   | RTP      | 150    | PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2225, Time=73  |
| 66  | 28.475752 | 188.40.69.75   | 212.53.40.76   | RTP      | 144    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=8, Time=28     |
| 67  | 28.487142 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=10, Time=76800                |
| 68  | 28.488367 | 188.40.69.75   | 92.127.221.146 | RTP      | 74     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=7, Time=74     |
| 69  | 28.497188 | 92.127.221.146 | 188.40.69.75   | RTP      | 144    | PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2226, Time=74  |
| 70  | 28.497731 | 188.40.69.75   | 212.53.40.76   | RTP      | 138    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=9, Time=28     |
| 71  | 28.498321 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=11, Time=77760                |
| 72  | 28.508374 | 188.40.69.75   | 92.127.221.146 | RTP      | 74     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=8, Time=75     |
| 73  | 28.515498 | 92.127.221.146 | 188.40.69.75   | RTP      | 141    | PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2227, Time=75  |
| 74  | 28.516051 | 188.40.69.75   | 212.53.40.76   | RTP      | 135    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=10, Time=2     |
| 75  | 28.517377 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=12, Time=78720                |
| 76  | 28.528433 | 188.40.69.75   | 92.127.221.146 | RTP      | 74     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=9, Time=76     |
| 77  | 28.537206 | 92.127.221.146 | 188.40.69.75   | RTP      | 146    | PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2228, Time=76  |
| 78  | 28.537752 | 188.40.69.75   | 212.53.40.76   | RTP      | 136    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=11, Time=2     |
| 79  | 28.539623 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=13, Time=79680                |
| 80  | 28.548413 | 188.40.69.75   | 92.127.221.146 | RTP      | 74     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=10, Time=7     |
| 81  | 28.557717 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=14, Time=80640                |
| 82  | 28.561088 | 92.127.221.146 | 188.40.69.75   | RTP      | 148    | PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2229, Time=7   |
| 83  | 28.561589 | 188.40.69.75   | 212.53.40.76   | RTP      | 138    | PT=DynamicRTP-Type-111, SSRC=0x5C0199FD, Seq=12, Time=2     |
| 84  | 28.568348 | 188.40.69.75   | 92.127.221.146 | RTP      | 70     | PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=11, Time=7     |
| 85  | 28.572008 | 92.127.221.146 | 188.40.69.75   | STUN     | 146    | Binding Request user: 9u13f:B28E8mfysfVLgdS8                |
| 86  | 28.573147 | 188.40.69.75   | 92.127.221.146 | STUN     | 150    | Binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146 |
| 87  | 28.573228 | 212.53.40.76   | 188.40.69.75   | RTP      | 60     | PT=opus, SSRC=0x444472E1, Seq=15, Time=81600                |

0000 00 21 59 c5 74 e0 00 24 21 9c 37 ed 08 00 45 00 .!Y.t..\$ !.7...E.  
0010 00 3c 00 00 40 00 40 11 ff 2b bc 28 45 4b 5c 7f .<..@.@. .+(EK).  
0020 dd 92 79 36 e5 6c 00 28 ad 52 90 6f 00 05 00 01 ..y6.l.(.R.o....  
0030 1d 00 3b 35 9c a0 03 e7 00 00 41 5f 46 b5 8f 40 ..;5... ..A.F..@  
0040 d1 2a 16 31 ec d3 7d 41 c6 29 \*.1..}A.)

File: "C:\tmp\3\log.pcap" 143 kB 00:00:33 Packets: 1057 · Displayed: 1057 (100,0%) · Load time: 0:00.013 Profile: Default

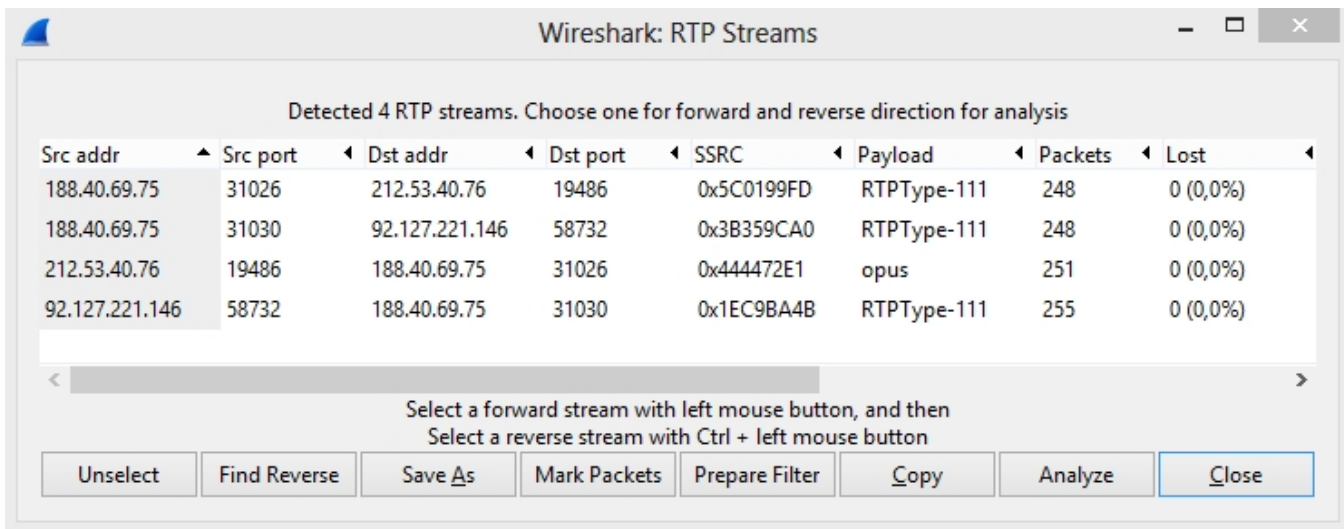
## SRTP packet header

SRTP traffic is encrypted. This means if you try to play it, you will hear noises instead of normal speech. But only the content traffic is encrypted. The main RTP headers remain non-encrypted and they can be seen in the RTP packet. This is handy to analyze SRTP traffic parameters. The below example shows an SRTP packet with Payload Type, Sequence Number, Timestamp, SSRC.



## The list of SRTP and RTP streams taking part in a WebRTC session

SRTP and RTP streams can be analyzed using Wireshark. To do this, use the 'Telephony - RTP - Show All Streams' menu.



In this case, streams with SSRC 0x3B359CA0 and 0x1EC9BA4B are SRTP streams between the web browser and WCS, because the source and destination address is the IP address of the web client (we know it beforehand). The other two streams, specifically, the first and the third ones from the top, are RTP streams between WCS and the SIP server (we know addresses of the WCS server and the SIP server too).

## SRTP stream analysis

As described above, SRTP packet headers are not encrypted, so the SRTP stream is available for analysis of quality, losses, jitter, latency just like a conventional RTP stream:

Wireshark: RTP Streams

Wireshark: RTP Stream Analysis

Forward Direction

Reversed Direction

Analysing stream from 188.40.69.75 port 31030 to 92.127.221.146 port 58732 SSRC = 0x3B359CA0

| Packet | Sequence | Delta(ms) | Filtered Jitter(ms) | Skew(ms) | IP BW(kbps) | Marker | Status |
|--------|----------|-----------|---------------------|----------|-------------|--------|--------|
| 44     | 1        | 0,00      | 0,00                | 0,00     | 0,48        |        | [ Ok ] |
| 46     | 2        | 0,00      | 0,00                | 0,00     | 0,96        |        | [ Ok ] |
| 51     | 3        | 0,00      | 0,00                | 0,00     | 1,44        |        | [ Ok ] |
| 56     | 4        | 0,00      | 0,00                | 0,00     | 1,92        |        | [ Ok ] |
| 60     | 5        | 0,00      | 0,00                | 0,00     | 2,40        |        | [ Ok ] |
| 64     | 6        | 0,00      | 0,00                | 0,00     | 2,88        |        | [ Ok ] |
| 68     | 7        | 0,00      | 0,00                | 0,00     | 3,36        |        | [ Ok ] |
| 72     | 8        | 0,00      | 0,00                | 0,00     | 3,84        |        | [ Ok ] |

Max delta = 0,00 ms at packet no. 0

Max jitter = 0,00 ms. Mean jitter = 0,00 ms.

Max skew = 0,00 ms.

Total RTP packets = 248 (expected 248) Lost RTP packets = 0 (0,00%) Sequence errors = 0

Duration 4,88 s (0 ms clock drift, corresponding to 1 Hz (+0,00%))

Save payload...

Save as CSV...

Refresh

Jump to

Graph

Player

Next non-Ok

Close

Src addr

188.40.69.75

188.40.69.75

212.53.40.76

92.127.221.146

Unselect