

WebRTC

- Общие сведения
 - Возможные неполадки
 - Устранение неполадок
- ICE и STUN трафик
- DTLS Трафик
- SRTP Трафик
 - Определение SRTP пакетов
 - Декодирование SRTP-пакетов
 - Разобранный SRTP-трафик
 - Заголовки SRTP-пакета
 - Список SRTP и RTP потоков, участвующих в WebRTC сессии
 - Анализ SRTP-потока

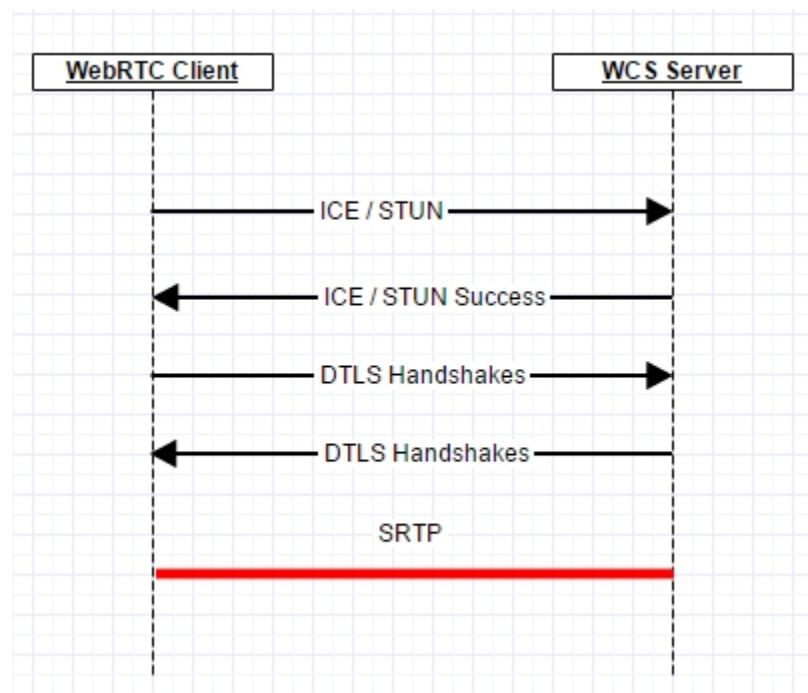
Общие сведения

Технология WebRTC при работе с сетью опирается на три основных спецификации:

- ICE и STUN
- DTLS
- SRTP

Для установки WebRTC - соединения используется ICE. Web-клиент отправляет STUN - запросы WCS серверу, WCS сервер отвечает на эти запросы и тем самым подтверждает что готов к установке соединения.

Следующим шагом происходит обмен SSL сертификатами через DTLS и установка зашифрованного канала между Web-клиентом и WCS-сервером. После того, как соединение установлено, начинает идти SRTP - трафик.



Возможные неполадки

В большинстве случаев неполадки связаны с непрохождением UDP трафика ICE, STUN, DTLS, SRTP между участниками системы.

Устранение неполадок

Убедитесь, что весь трафик, который участвует в установке WebRTC сессии и в передаче медиа данных беспрепятственно проходит между участниками звонка. Медиа порты WCS сервера в диапазоне [31000-32000] по умолчанию, должны быть открыты для приема входящего UDP трафика. Если WCS-сервер находится за NAT и имеет внешний IP-адрес, убедитесь что UDP пакеты, отправленные на этот внешний адрес будут корректно маршрутизированы на соответствующие порты WCS сервера, который находится за NAT.

ICE и STUN трафик

Так выглядит обмен ICE - транзакциями перед установкой соединения. В дампе это обычные STUN запросы и ответы. После того, как соединение установлено ICE продолжает работать для мониторинга установленного соединения. Если в результате мониторинга ICE перестал проходить, то звонок будет прерван.

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

Filter: **stun** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	27.919236	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8
17	27.921787	188.40.69.75	92.127.221.146	STUN	150	binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
18	27.929723	188.40.69.75	92.127.221.146	STUN	158	binding Request user: B28E8mfysfVLgds8:9u13f
19	28.018326	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8
20	28.019742	188.40.69.75	92.127.221.146	STUN	150	binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
21	28.022820	188.40.69.75	92.127.221.146	STUN	158	binding Request user: B28E8mfysfVLgds8:9u13f
22	28.091373	92.127.221.146	188.40.69.75	STUN	106	binding Success Response XOR-MAPPED-ADDRESS: 188.40.69.75:31030
24	28.123548	188.40.69.75	92.127.221.146	STUN	158	binding Request user: B28E8mfysfVLgds8:9u13f
25	28.137609	92.127.221.146	188.40.69.75	STUN	106	binding Success Response XOR-MAPPED-ADDRESS: 188.40.69.75:31030
29	28.223897	92.127.221.146	188.40.69.75	STUN	106	binding Success Response XOR-MAPPED-ADDRESS: 188.40.69.75:31030
34	28.330650	188.40.69.75	92.127.221.146	STUN	86	binding Indication
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: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
138	28.828370	188.40.69.75	92.127.221.146	TFTP	70	Read Request, File: d8;5\234\240e\n?\351\340\345\305\2347b=\rB[Malformed Packet]
262	29.448389	188.40.69.75	92.127.221.146	TFTP	101	Read Request[Malformed Packet]
280	29.534578	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8
281	29.535797	188.40.69.75	92.127.221.146	STUN	150	binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
475	30.497059	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8
476	30.497805	188.40.69.75	92.127.221.146	STUN	150	binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
647	31.330994	188.40.69.75	92.127.221.146	STUN	86	binding Indication
672	31.457966	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8
673	31.458722	188.40.69.75	92.127.221.146	STUN	150	binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
870	32.420408	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8
871	32.421221	188.40.69.75	92.127.221.146	STUN	150	binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146:58732 user: 9u13f:B28E8mfysfVLgds8
1052	33.386004	92.127.221.146	188.40.69.75	STUN	146	binding Request user: 9u13f:B28E8mfysfVLgds8

Frame 16: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)

0000 00 24 21 9c 37 ed 00 21 59 c5 74 e0 08 00 45 00 .\$.!7..! Y.t...E.
0010 00 84 7a 10 00 00 76 11 8e d3 5c 7f dd 92 bc 28 ..Z...V.(.
0020 45 4b e5 6c 79 36 00 70 43 b5 00 01 00 54 21 12 EK.ly6.p C...Tl.
0030 a4 42 67 59 49 53 30 47 59 34 47 6b 41 67 00 06 .BgYISOG y4GkAg..
0040 00 16 39 75 31 33 66 3a 42 32 38 45 38 4d 66 79 ..9u13f: B28E8mfy
0050 72 66 56 4c 67 64 53 28 00 00 80 22 00 08 0d 4d cFvuGds8 *m

File: "C:\tmp\3\log.pcap" 143 kB 00:00:33 Packets: 1057 - Displayed: 25 (2,4%) - Load time: 0:00.023 Profile: Default

DTLS Трафик

DTLS начинает работать сразу после того, как ICE установил соединение. Обмен сертификатами представляет собой несколько Handshake - сообщений, в результате чего устанавливается защищенное соединение для передачи медиа данных.

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

Filter: **dtls** Expression... Clear Apply Save

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

File: "C:\tmp\3\log.pcap" 143 kB 00:00:33 Packets: 1057 - Displayed: 8 (0,8%) - Load time: 0:00.020 Profile: Default

SRTP Трафик

Определение SRTP пакетов

При передаче данных по SRTP, Wireshark может не распознать SRTP пакеты. Найти эти пакеты достаточно просто. WCS по умолчанию использует диапазон портов [31000-32000] для передачи медиа трафика, в том числе и WebRTC. В дампе ниже мы нашли два неопознанных UDP-пакета, один из которых отправлен с порта 31030, а второй принят на этом порту. Для таких пакетов нужно явно указать используемый протокол.

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

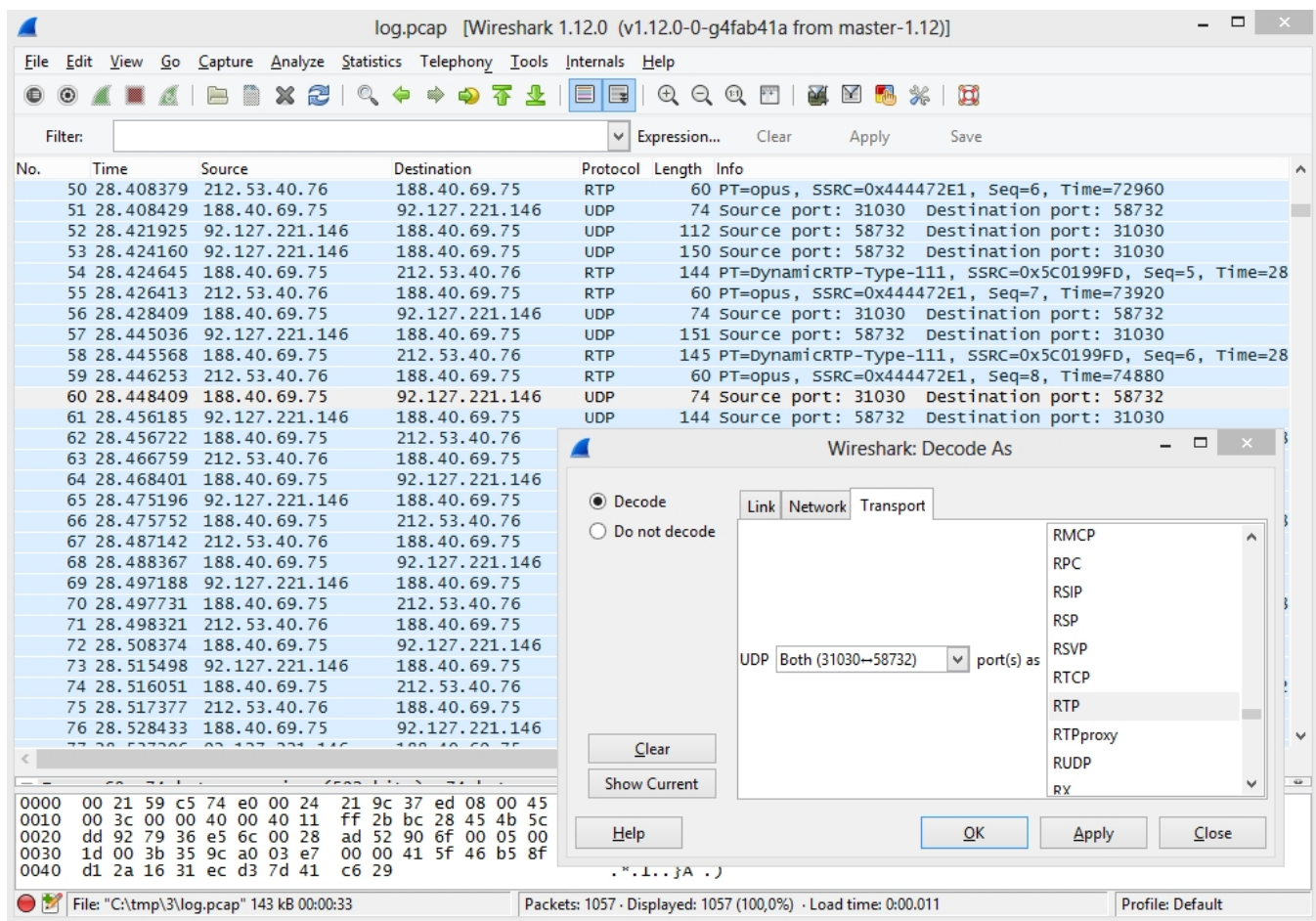
Filter: Expression... Clear Apply Save

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=73920
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=74880
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=75840
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=76800
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=77760
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=78720
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
77	28.537306	92.127.221.146	188.40.69.75	UDP	146	Source port: 58732 Destination port: 31030

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

Декодирование SRTP-пакетов

Wireshark сможет разобрать найденные UDP пакеты, если мы укажем ему протокол. В свойствах пакета выберите 'Decode As..' и далее выберите RTP протокол для всех пакетов, которые идут между браузером на порту 31030 и WCS сервером на порту 58732. Эти порты выделяются динамически и в вашем случае будут использоваться другие значения.



Разобранный SRTP-трафик

В результате декодирования протокола, Wireshark отобразит разобранный SRTP трафик:

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

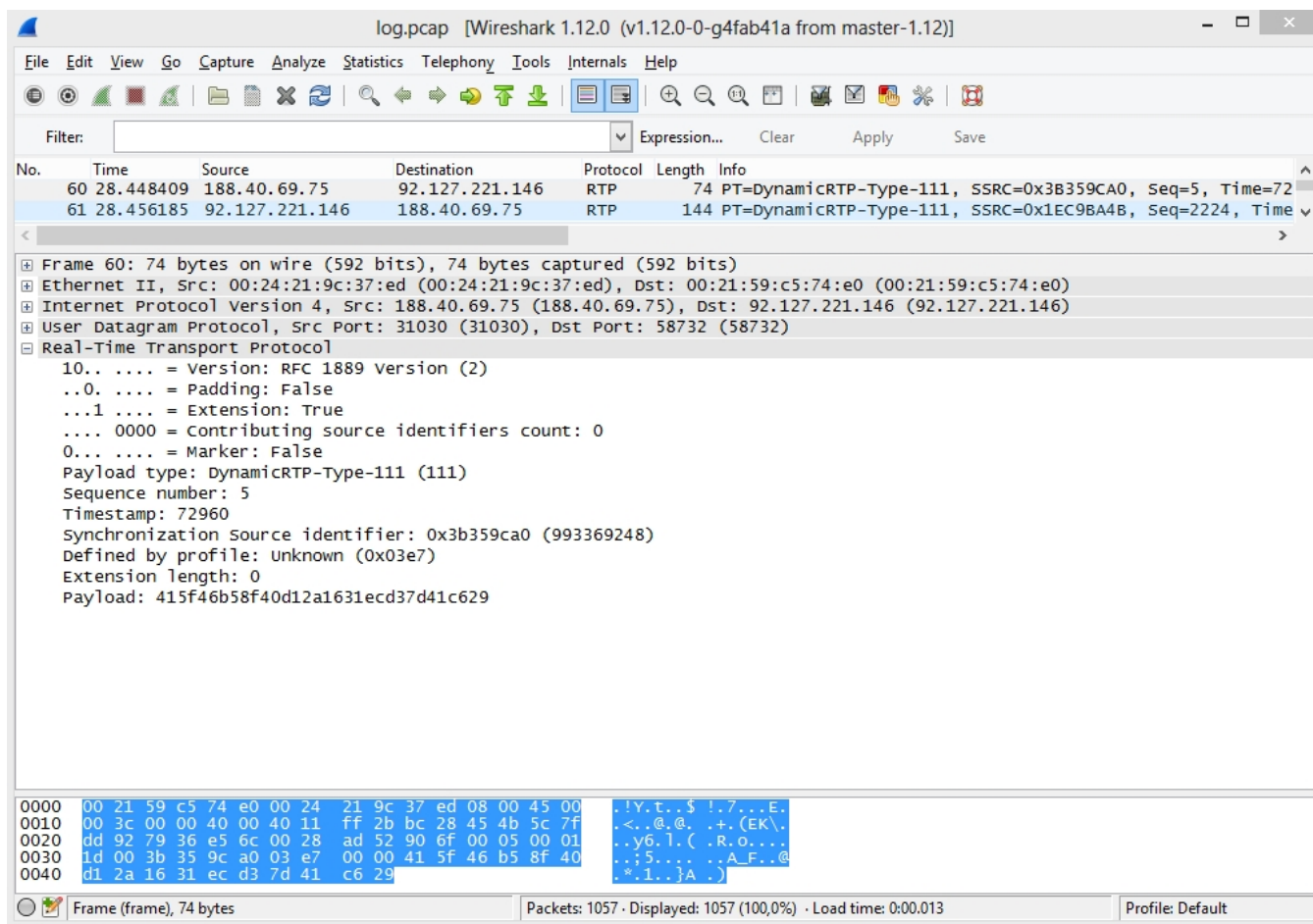
No.	Time	Source	Destination	Protocol	Length	Info
60	28.448409	188.40.69.75	92.127.221.146	RTP	74	PT=DynamicRTP-Type-111, SSRC=0x3B359CA0, Seq=5, Time=72
61	28.456185	92.127.221.146	188.40.69.75	RTP	144	PT=DynamicRTP-Type-111, SSRC=0x1EC9BA4B, Seq=2224, Time=72
62	28.456722	188.40.69.75	212.53.40.76	RTP	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	188.40.69.75	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:B28E8mfysfvLgd58
86	28.573147	188.40.69.75	92.127.221.146	STUN	150	Binding Success Response XOR-MAPPED-ADDRESS: 92.127.221.146

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

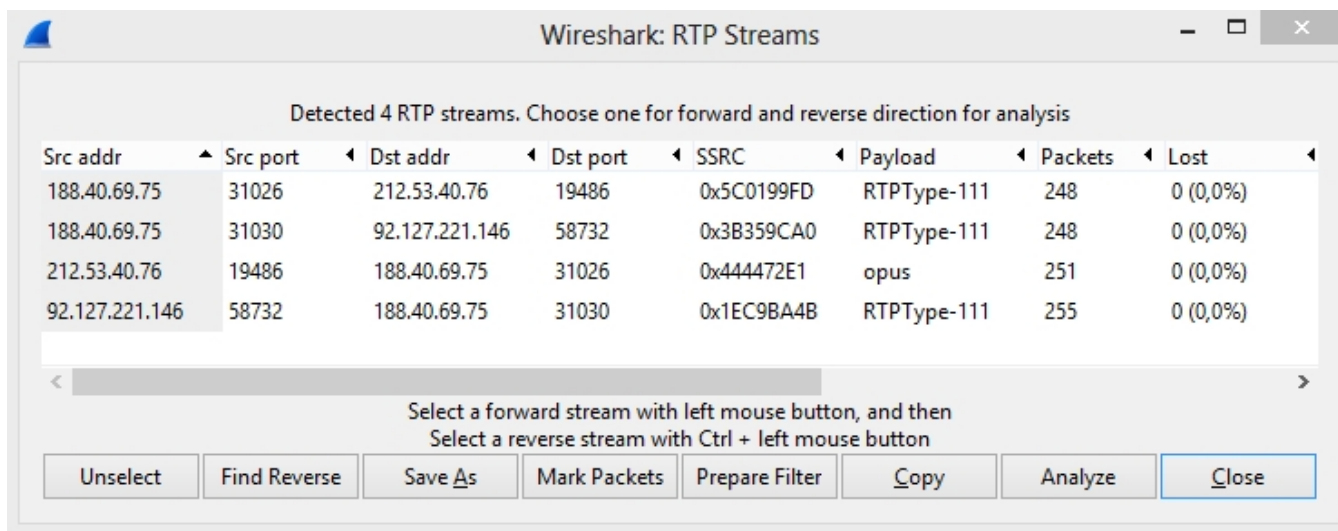
Заголовки SRTP-пакета

SRTP трафик зашифрован. Это означает что если попытаться его проиграть, вместо нормальной речи будут шумы. Но зашифровано только содержание трафика. Основные RTP-заголовки не зашифрованы и их видно в RTP пакете. Это удобно для анализа характеристик SRTP трафика. В примере ниже показан SRTP пакет с Payload Type, Sequence Number, Timestamp, SSRC.



Список SRTP и RTP потоков, участвующих в WebRTC сессии

SRTP и RTP потоки можно проанализировать с помощью Wireshark. Для этого нужно использовать меню 'Telephony - RTP - Show All Streams'.



В данном случае потоки с SSRC 0x3B359CA0 и 0x1EC9BA4B являются SRTP-потоками между Web-браузером и WCS, т.к. их источником и адресом назначения является IP-адрес веб-клиента (он нам заранее известен). Остальные два потока - первый и третий сверху это RTP потоки между WCS и SIP сервером (адреса WCS сервера и SIP сервера нам также известны заранее).

Анализ SRTP-потока

Как описывалось выше, заголовки SRTP-пакета не шифруются и поэтому SRTP поток полностью доступен для анализа качества, потерь, джиттера и задержок, как обычный RTP поток:

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