WebRTC

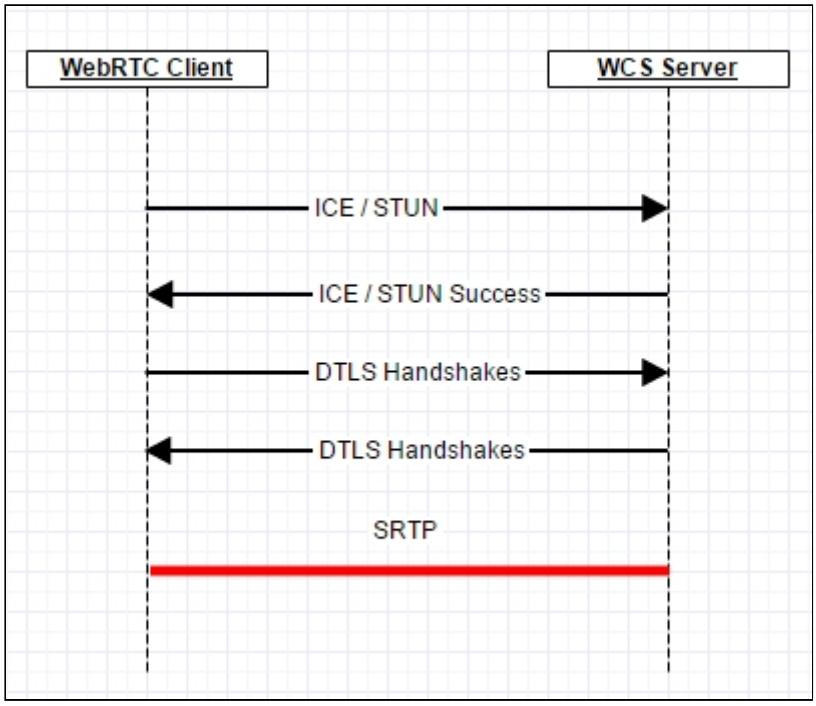
Общие сведения

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

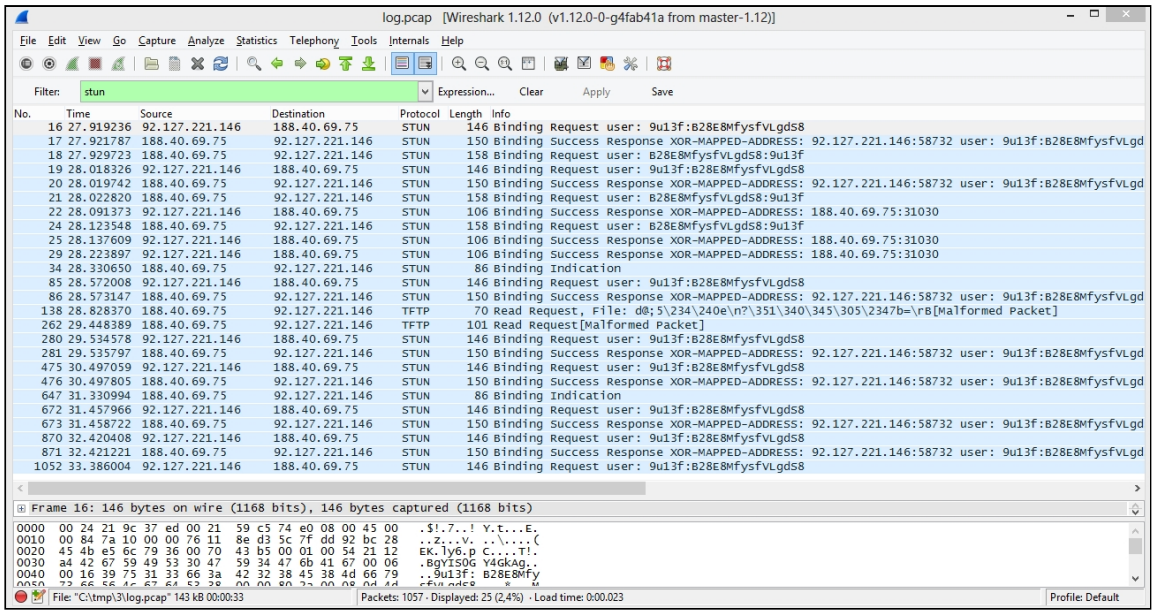
В большинстве случаев неполадки связаны с непрохождением UDP трафика ICE, STUN, DTLS, SRTP между участниками системы.

Устранение неполадок

Убедитесь, что весь трафик при установке WebRTC сессии и передаче медиа данных беспрепятственно проходит между участниками. 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.

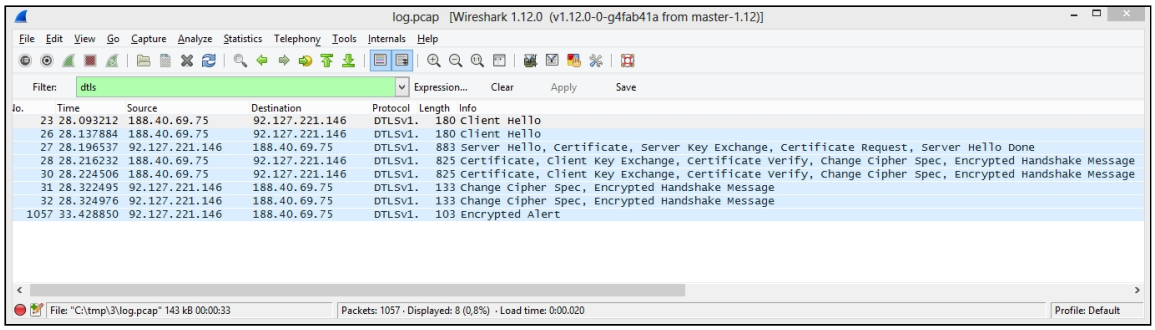
ICE и STUN трафик

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



DTLS Трафик

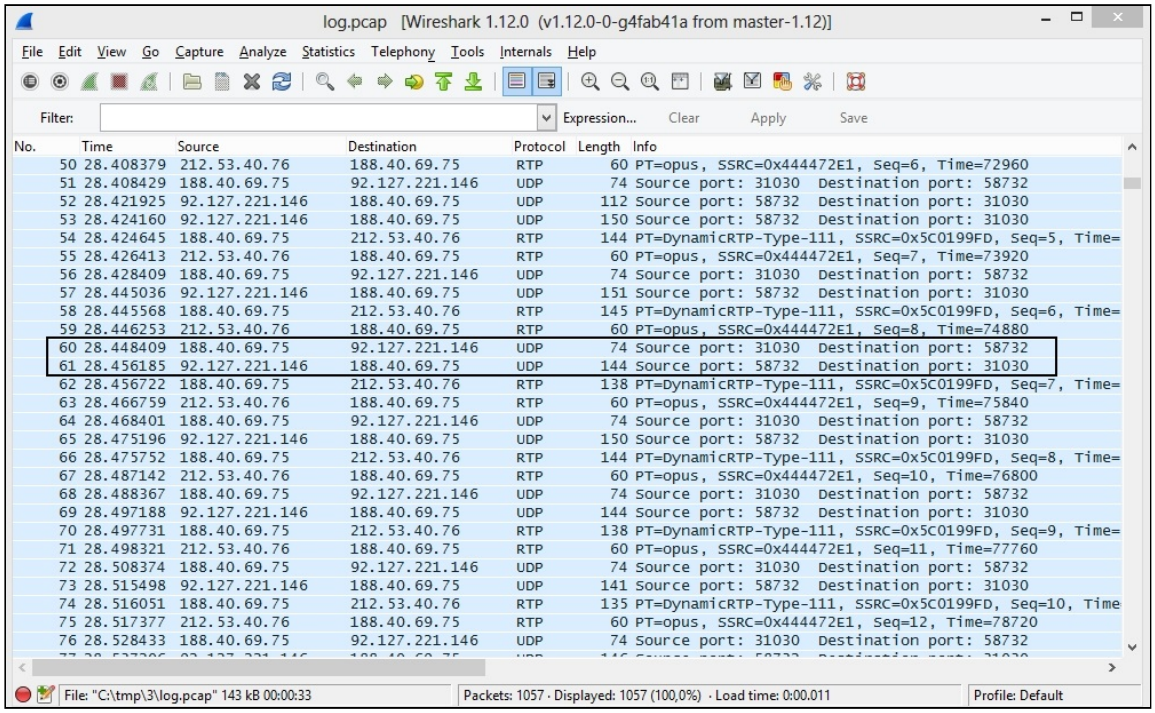
DTLS начинает работать сразу после того, как ICE установил соединение. Обмен сертификатами представляет собой несколько Handshake-сообщений, в результате чего устанавливается защищенное соединение для передачи медиа данных.



SRTP Трафик

Определение SRTP пакетов

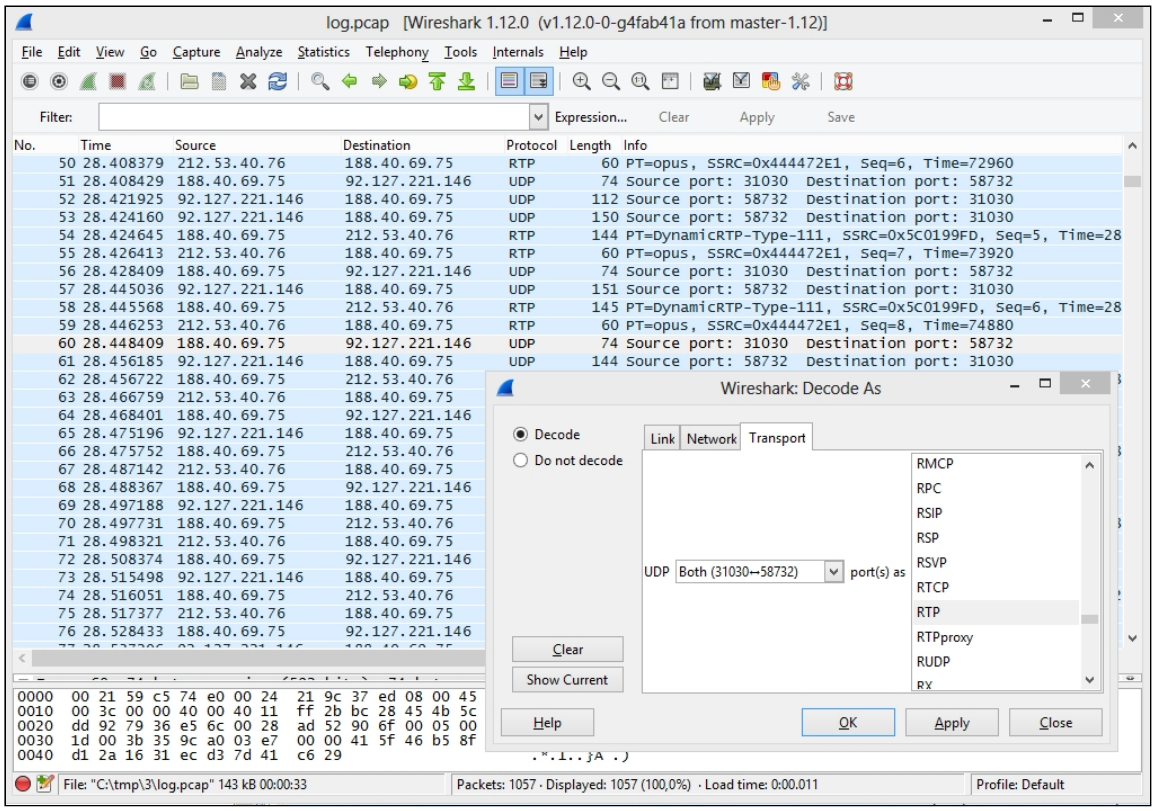
При передаче данных по SRTP, Wireshark может не распознать SRTP пакеты. Найти эти пакеты достаточно просто. WCS по умолчанию использует диапазон портов 31000-32000 для передачи WebRTC медиа трафика. В дампе ниже мы нашли два неопознанных UDP-пакета, один из которых отправлен с порта 31030, а второй принят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



Декодирование SRTP-пакетов

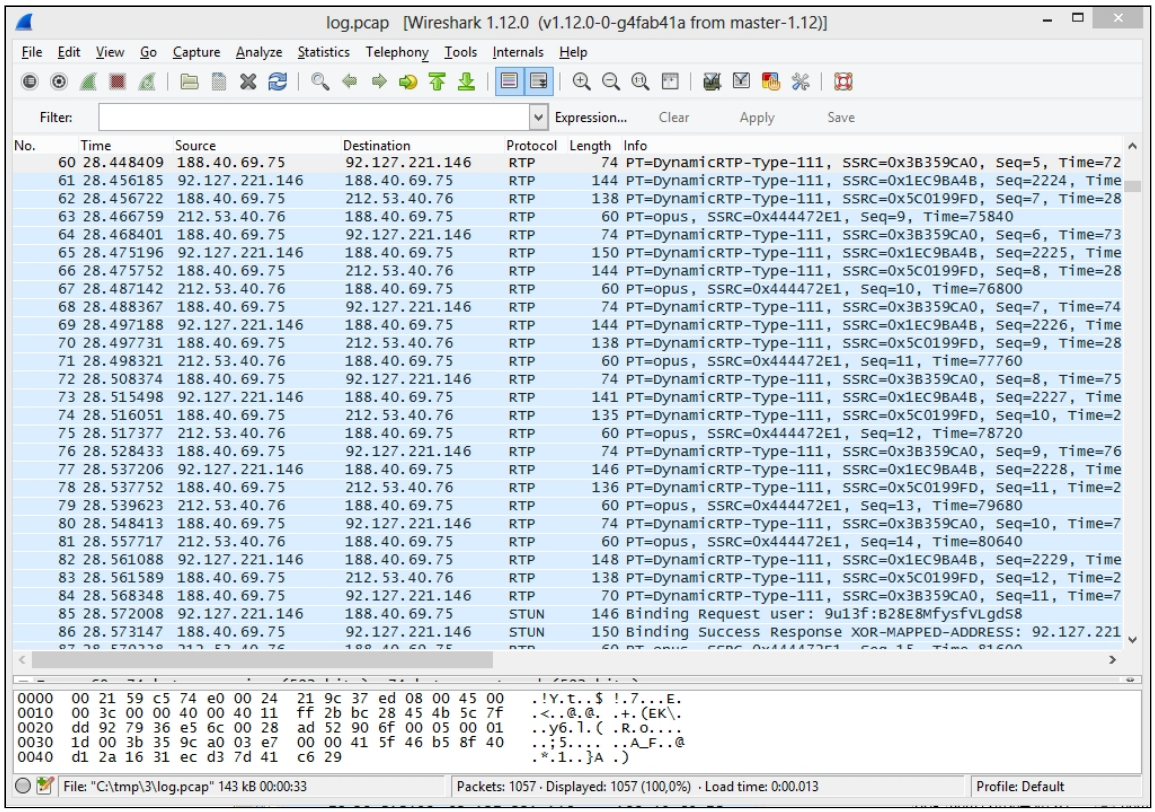
Wireshark сможет разобрать найденные UDP пакеты, если мы укажем ему протокол. В свойствах пакета выберите 'Decode As..' и далее выберите RTP протокол для всех пакетов, которые идут между браузером на порту 31030 и WCS сервером на порту

58732. Эти порты выделяются динамически и в конкретном случае будут использоватся другие значения.



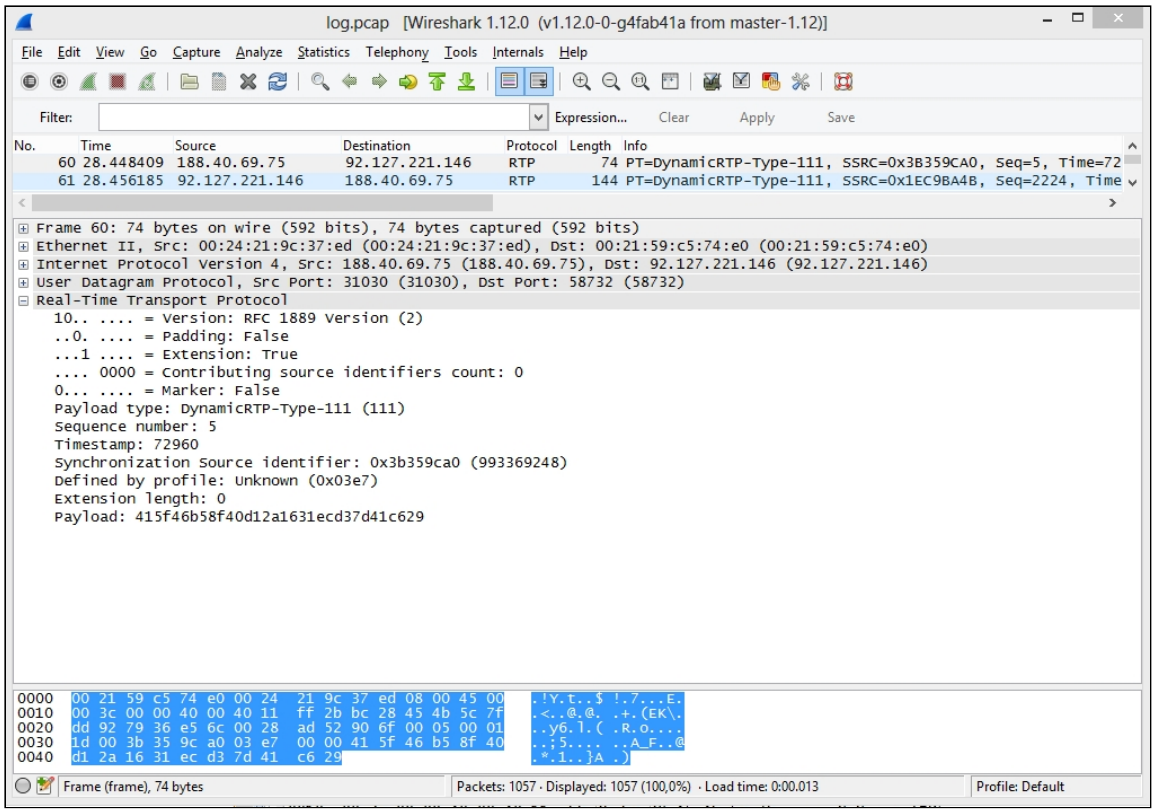
Разобранный SRTP-трафик

В результате декодирования протокола, Wireshark отобразит разобранный SRTP трафик:



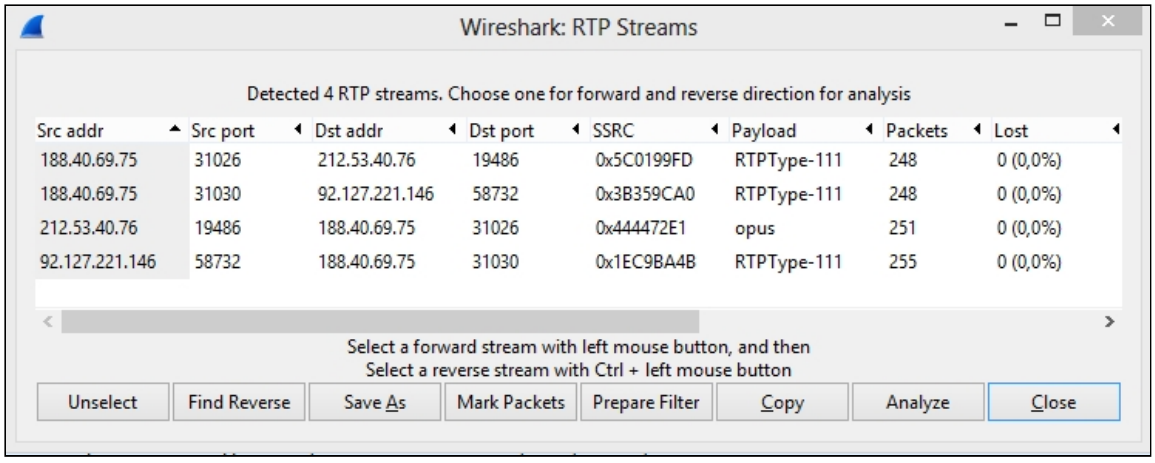
Заголовки SRTP-пакета

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: