**Министерство цифрового развития связи и массовых коммуникаций Российской Фередации**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«санкт-петербургский государственный университет телекоммуникаций им. проф. м. а. бонч-бруевича»**

**(СПбГУТ)**

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

ЛАБОРАТОРАЯ РАБОТА №1

IP-телефония в сценарии клиент-клиент. Протоколы обеспечения безопасности IP-телефонии

Студенты:

Громов А. А. ИКТЗ-83

(ФИО, № группы)

Жиляков Г. В. ИКТЗ-83

(ФИО, № группы)

Мазеин Д. С. ИКТЗ-83

(ФИО, № группы)

Миколаени М. С. ИКТЗ-83

(ФИО, № группы)

Научный руководитель:

Ассистент каф. ЗСС, Поляничева А. В.

(учетная степень, учетное звание, ФИО)

(подпись)

Санкт-Петербург

2021

Задание:

1. Изучить основы работы с сетевым анализатором Wireshark;
2. Установить программное обеспечение Phoner, реализующее функционал VoIP клиента, на два компьютера;
3. Настроить взаимодействие между VoIP терминалами пользователя и создать дампы звонков с использованием сетевого анализатора;
4. Настроить протокол ZRTP на клиентах и изучить его функционирование;
5. Настроить протокол SDES на клиентах и изучить его функционирование;
6. Создать дампы звонков с использованием сетевого анализатора Wireshark при включенных протоколах обеспечение безопасности IP-телефонии.

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ: 4](#_Toc82361012)

[ОСНОВНАЯ ЧАСТЬ: 5](#_Toc82361013)

[Схема лабораторной установки: 5](#_Toc82361014)

[Выполнение работы: 5](#_Toc82361015)

[Часть 1 – сетевой анализатор трафика Wireshark 5](#_Toc82361016)

[Часть 2 – установка и настройка программных клиентов IP-телефонии 6](#_Toc82361017)

[Часть 3 – Настройка соединения в топологии точка-точка в незащищенном режиме 8](#_Toc82361018)

[Часть 4 – Настройка протоколов защищенной IP-телефонии (ZRTP/SRTP и SDES/SRTP) 11](#_Toc82361019)

[ЗАКЛЮЧЕНИЕ: 14](#_Toc82361020)

# ВВЕДЕНИЕ:

В данной лабораторной работе мы познакомимся с IP-телефонией в сценарии клиент-клиент. Получим первичные навыки работы в таких программных обеспечениях, как Phoner (приложение для многопротокольной телефонии, поддерживающее телефонию через CAPI, TAPI) и Wireshark (сетевым анализатором). Цель данной лабораторной работы - осуществить соединение между двумя терминалами пользователя по протоколу SIP. Изучить и настроить протоколы обеспечения безопасности IP-телефонии на терминале пользователя и убедится в их функционировании.

# ОСНОВНАЯ ЧАСТЬ:

## Схема лабораторной установки:

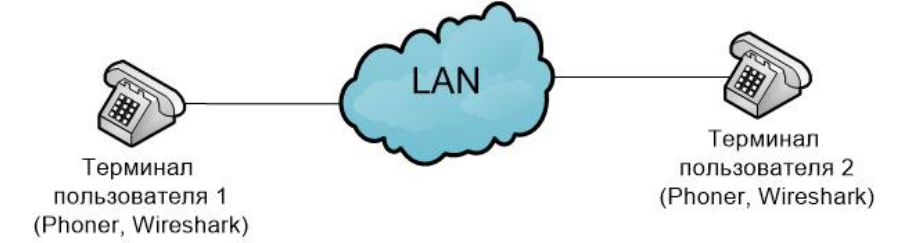


Рис. 1.1 Схема лабораторной установки

## Выполнение работы:

### Часть 1 – сетевой анализатор трафика Wireshark

Установили Wireshark – анализатор сетевых протоколов, который позволяет перехватывать и интерактивно просматривать трафик, протекающий в компьютерной сети.

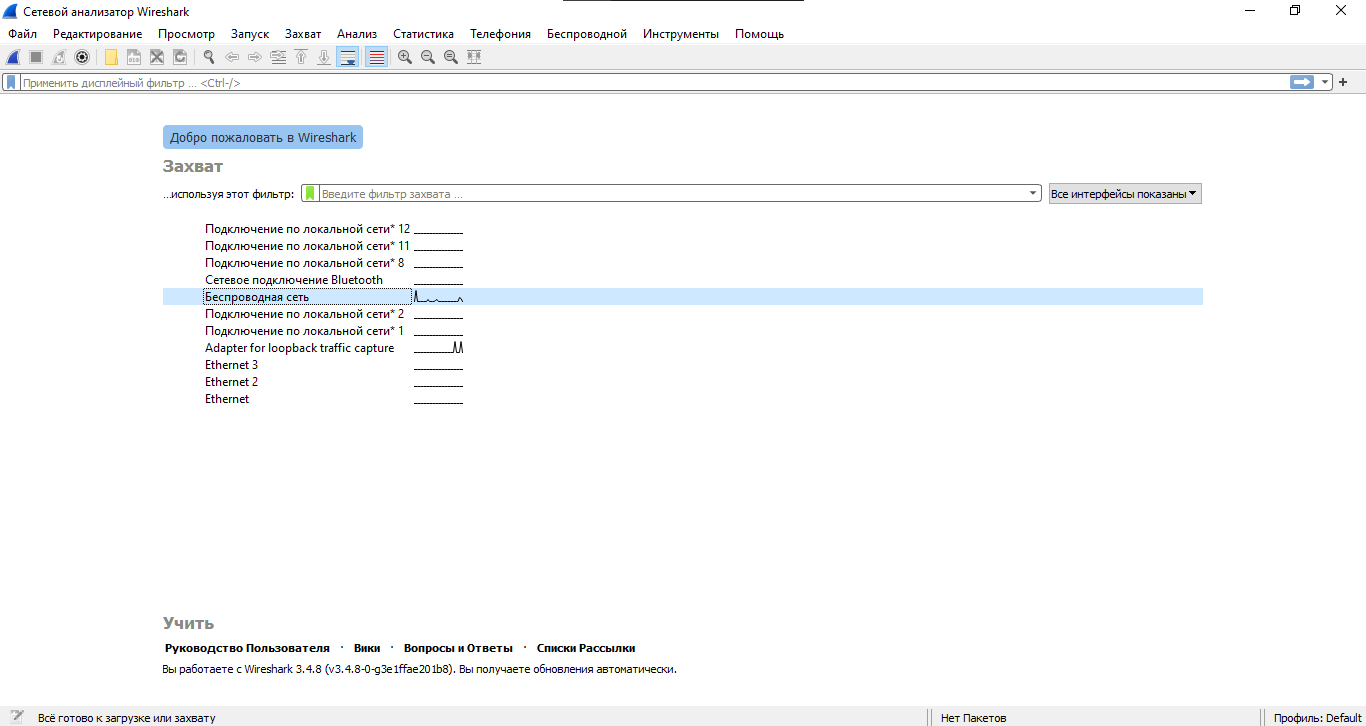


Рис. 1.2 Главный экран Wireshark

Проверяем доступность на [www.mail.ru](http://www.mail.ru) и сохраняем дамп протоколов.

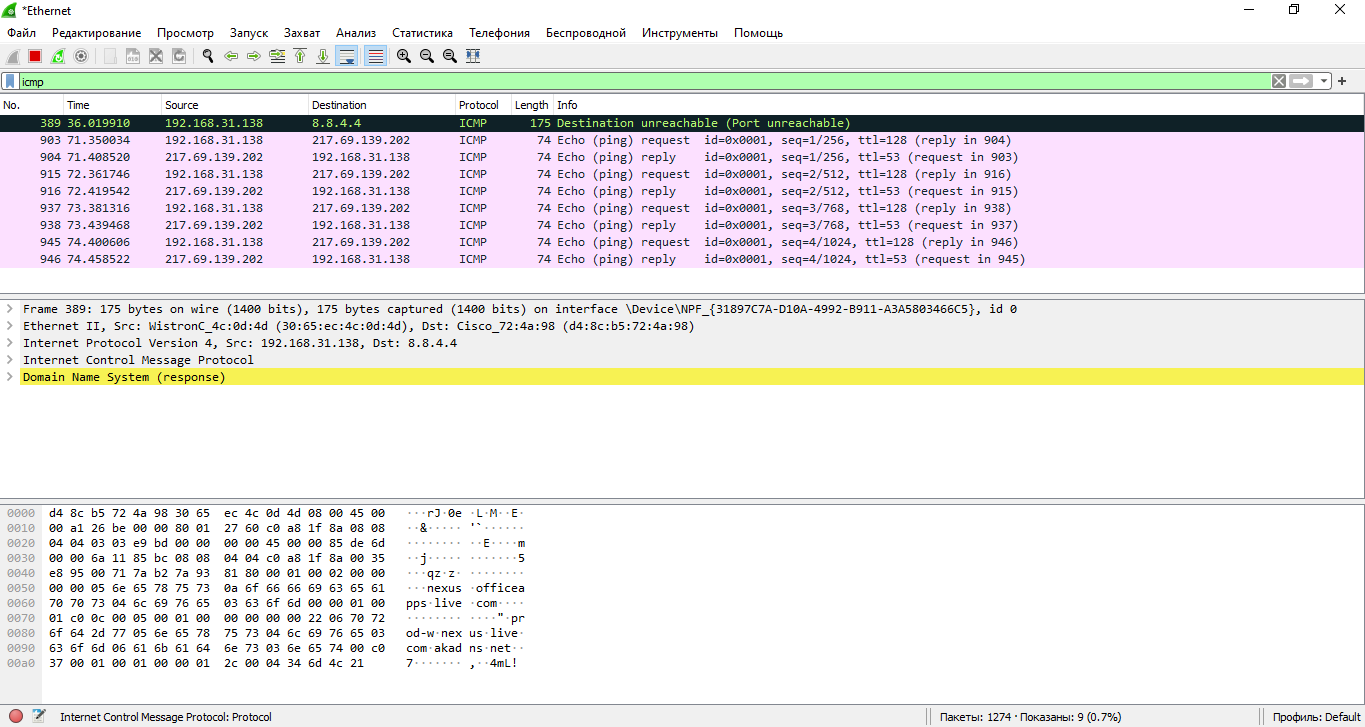


Рис. 1.3 Скриншот ICMP запросов и ответов

### Часть 2 – установка и настройка программных клиентов IP-телефонии

Установили программное обеспечение Phoner

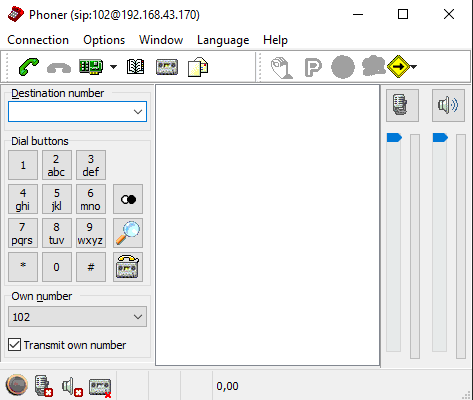


Рис. 2.1 Главный экран ПО Phoner

Настроили SIP профиль

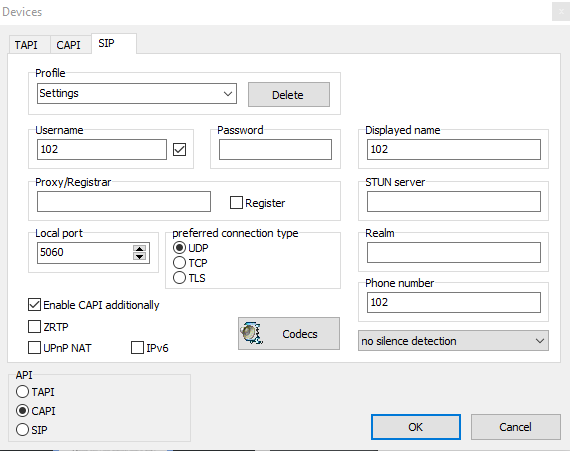


Рис. 2.2 Окно настройки SIP профиля

Выполнили звонок с одного устройства на другой

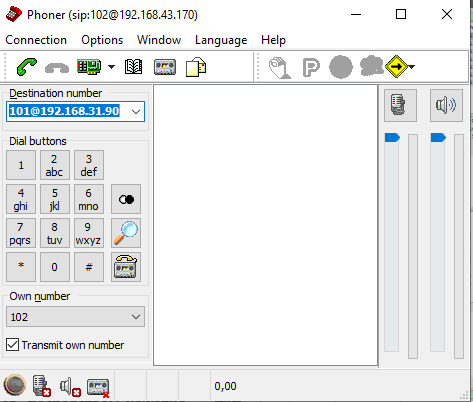


Рис. 2.3 IP звонка

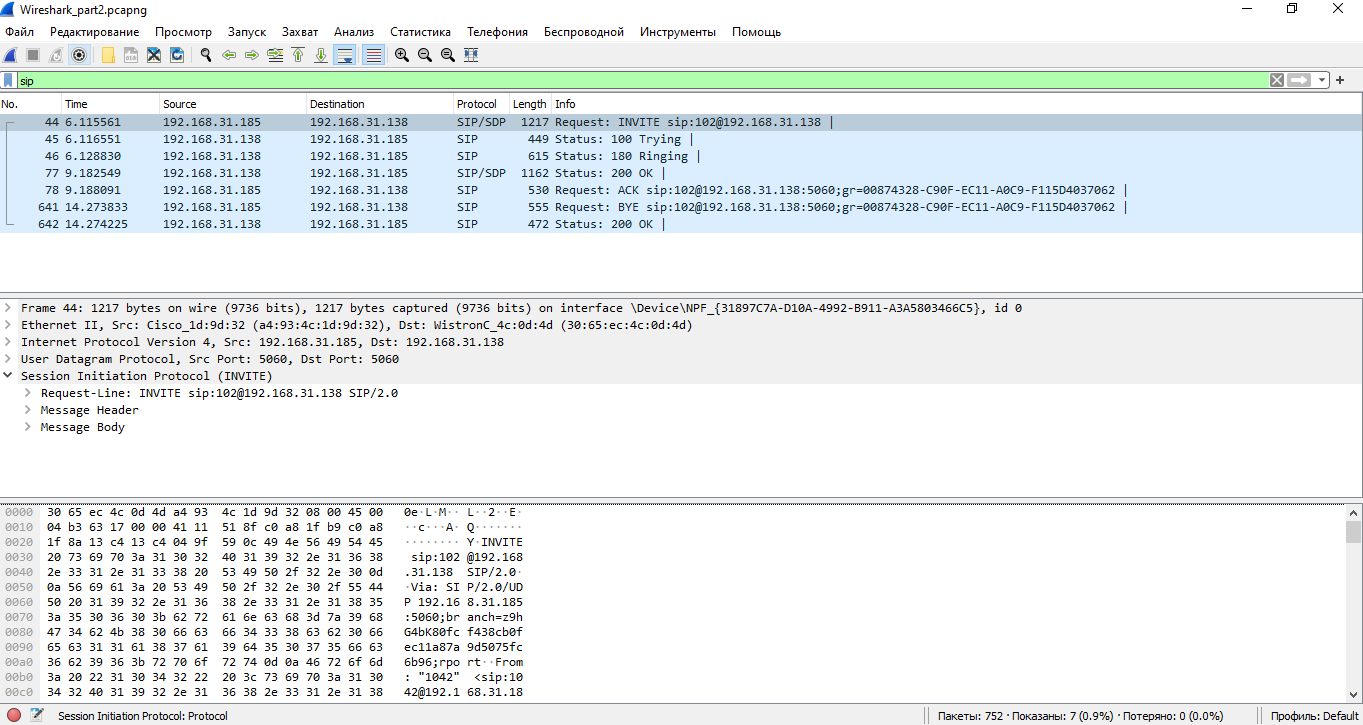


Рис. 2.4 Скриншот Invite пакета SIP

### Часть 3 – Настройка соединения в топологии точка-точка в незащищенном режиме

|  |  |  |
| --- | --- | --- |
| Настройка | Терминал пользователя 1 | Терминал пользователя 2 |
| IP-адрес | 192.168.31.138 | 192.168.31.186 |
| MAC-адрес | 30:65:ec:4c:0d:4d | a4:93:4c:1d:9d:32 |
| SIP-номер | 102@192.168.31.137:5060 | 1042@192.168.31.186:1720 |

Таблица 1 Настройки терминалов IP-телефонии

Позвонили с терминала пользователя 1 на терминал пользователя 2 и дождались срабатывание автоответчика. Записали дамп пакет в Wireshark.

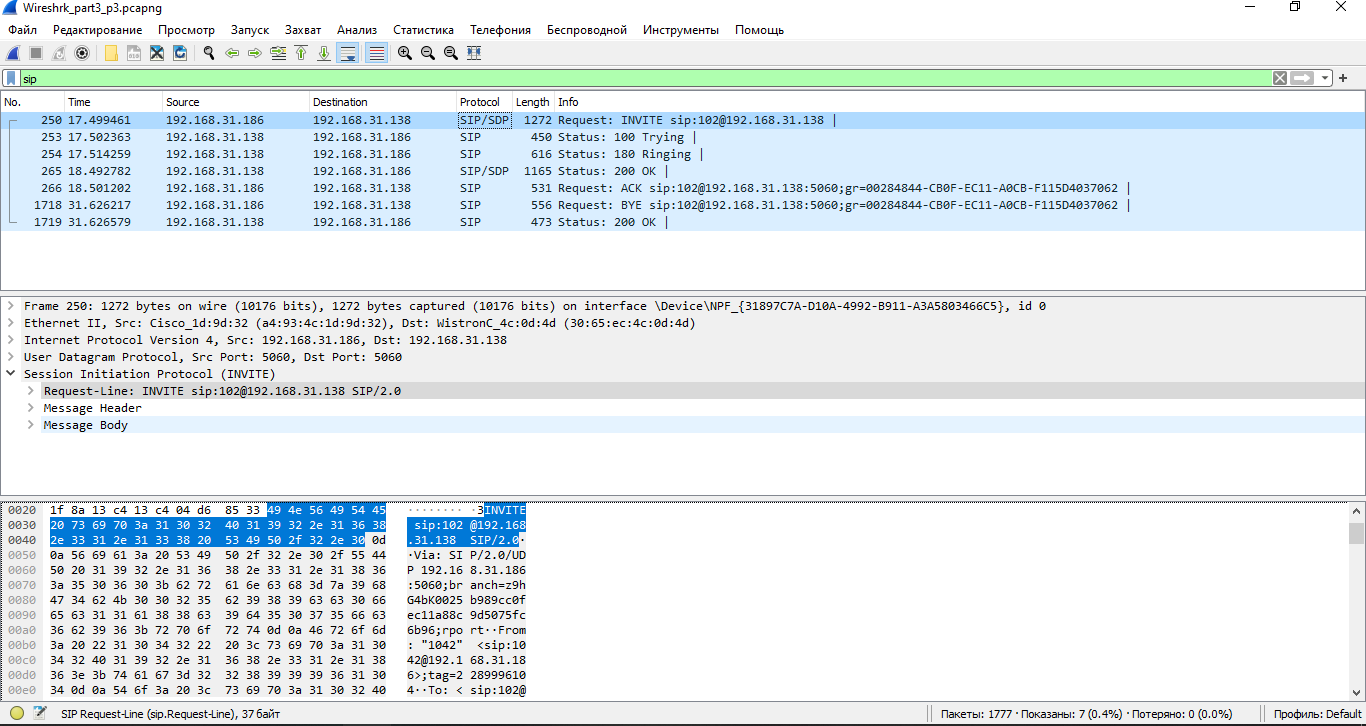


Рис. 3.1 Скриншот SIP пакетов

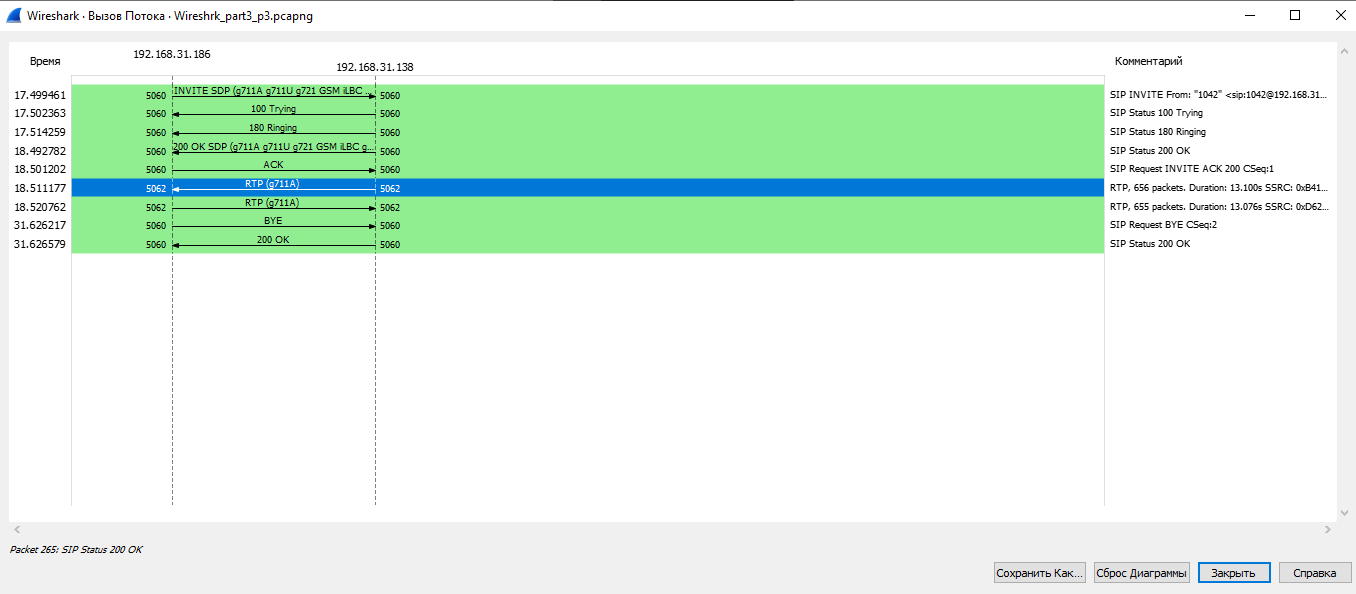


Рис. 3.2 Скриншот обмена SIP сообщениями

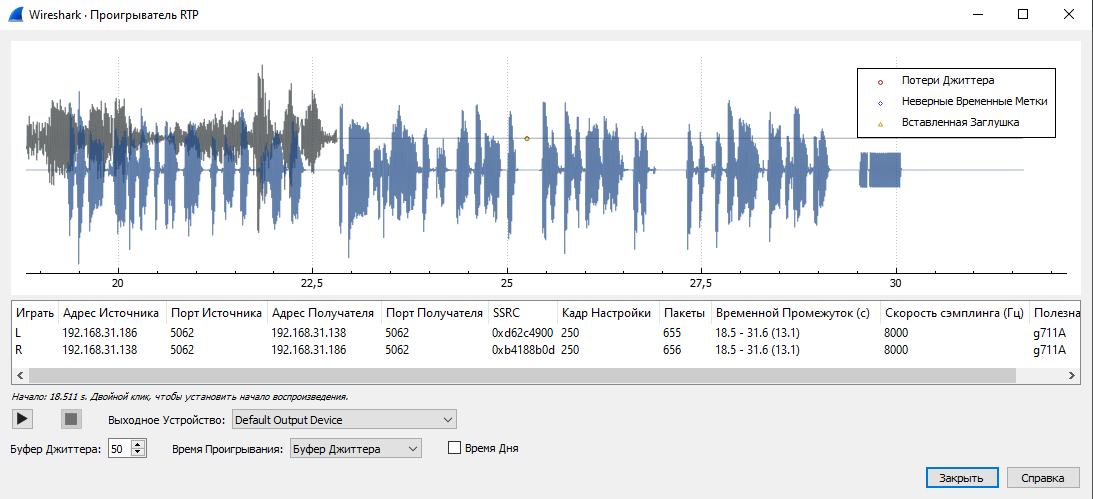


Рис. 3.3 Скриншот записанного звонка

Настроили SIP протокол для работы поверх TCP на обоих терминалах

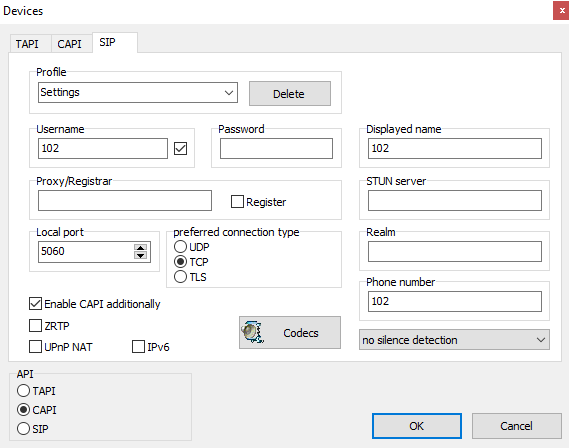


Рис. 3.4 Настройка работы SIP поверх протокола TCP

Сделали звонок с терминала пользователя 1 на терминал пользователя 2 и записали дамп файл с помощью Wireshak.

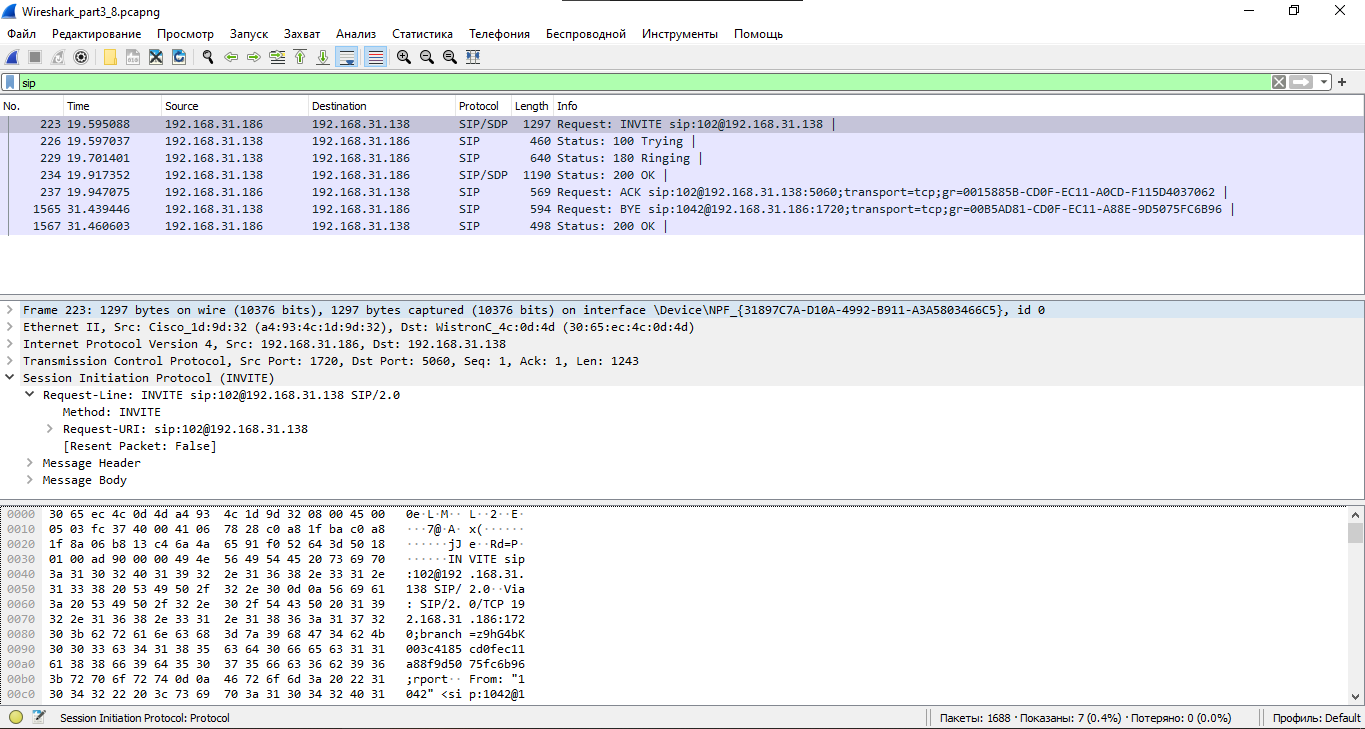


Рис. 3.5 Скриншот Invite пакета (TCP)

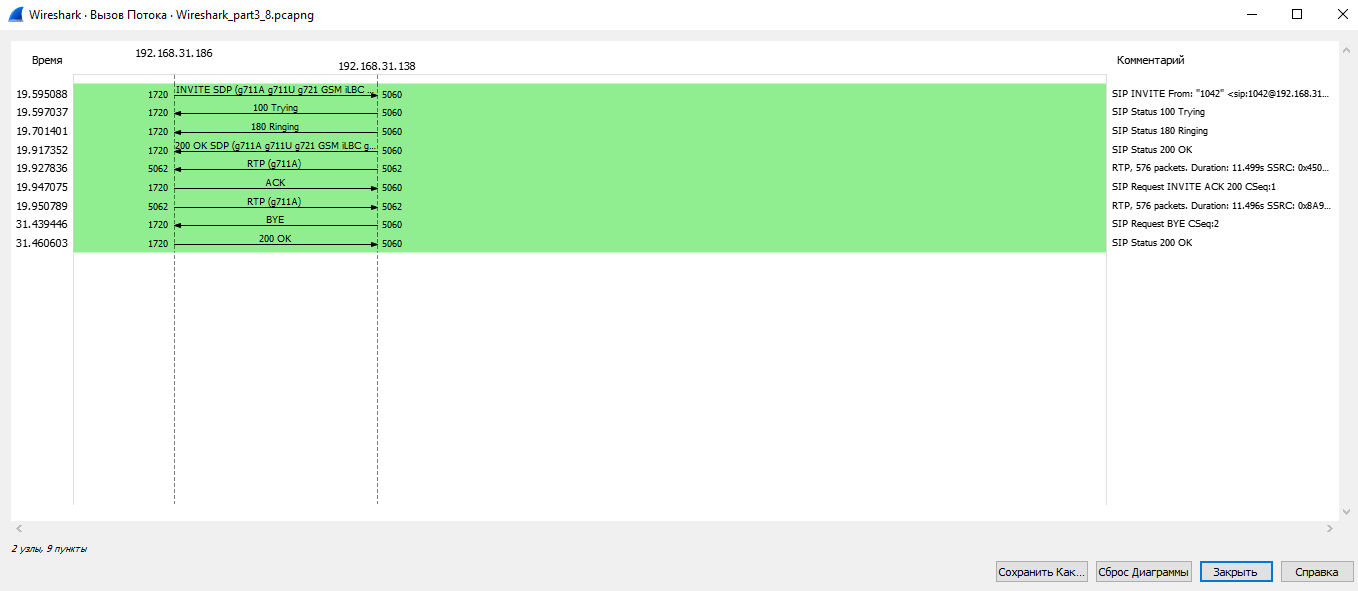


Рис. 3.6 Обмен SIP сообщениями (TCP)

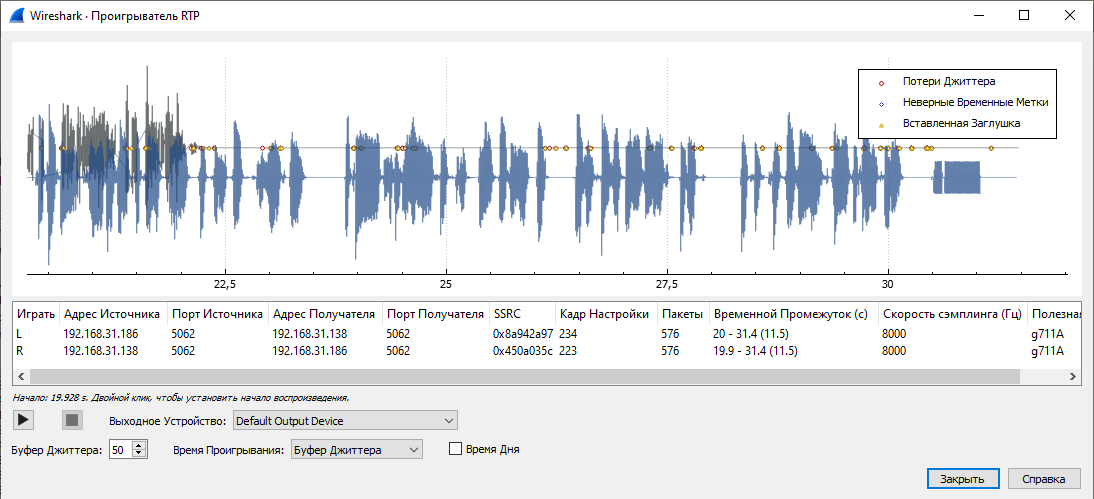


Рис. 3.7 Скриншот записанного звонка (TCP)

### Часть 4 – Настройка протоколов защищенной IP-телефонии (ZRTP/SRTP и SDES/SRTP)

Активация протокола ZRTP

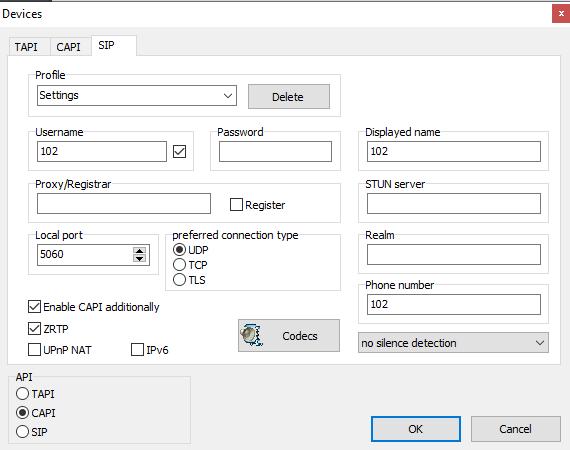


Рис. 4.1 Скриншот настроек (ZRTP)

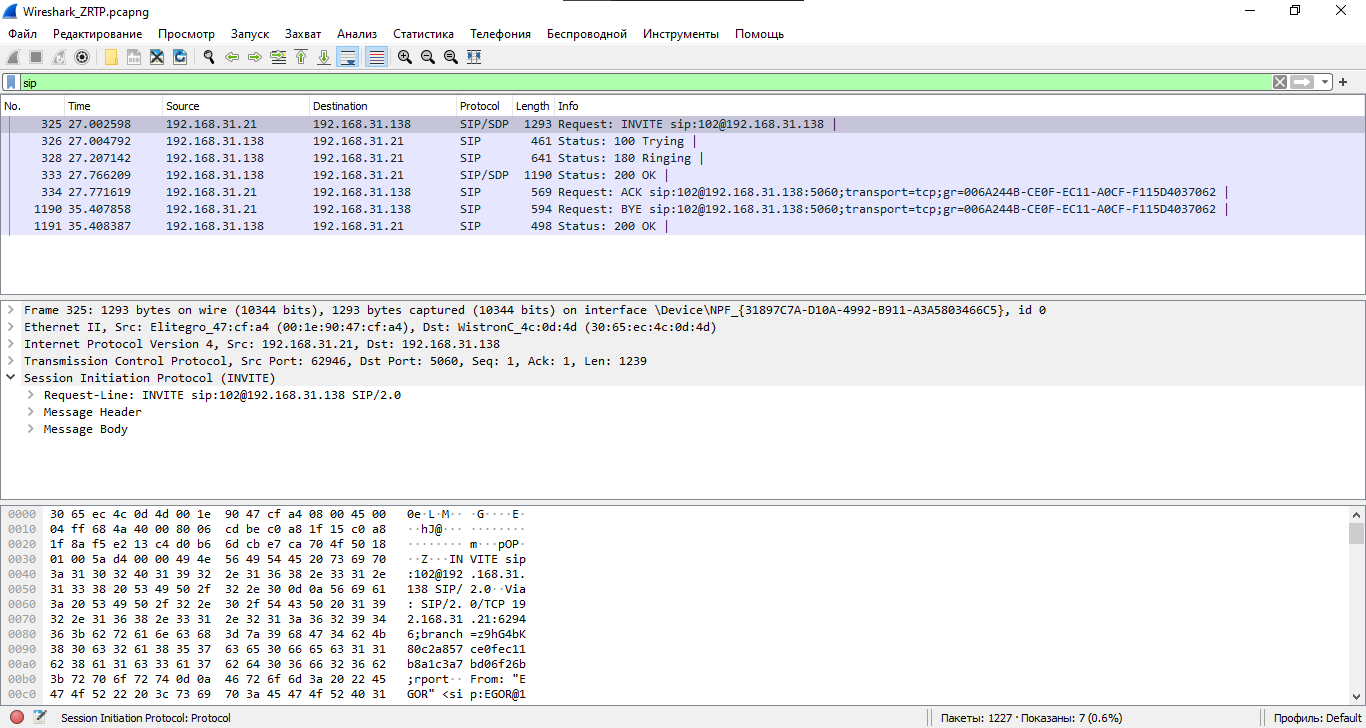


Рис.4.2 Скриншот Invite пакета (ZRTP)

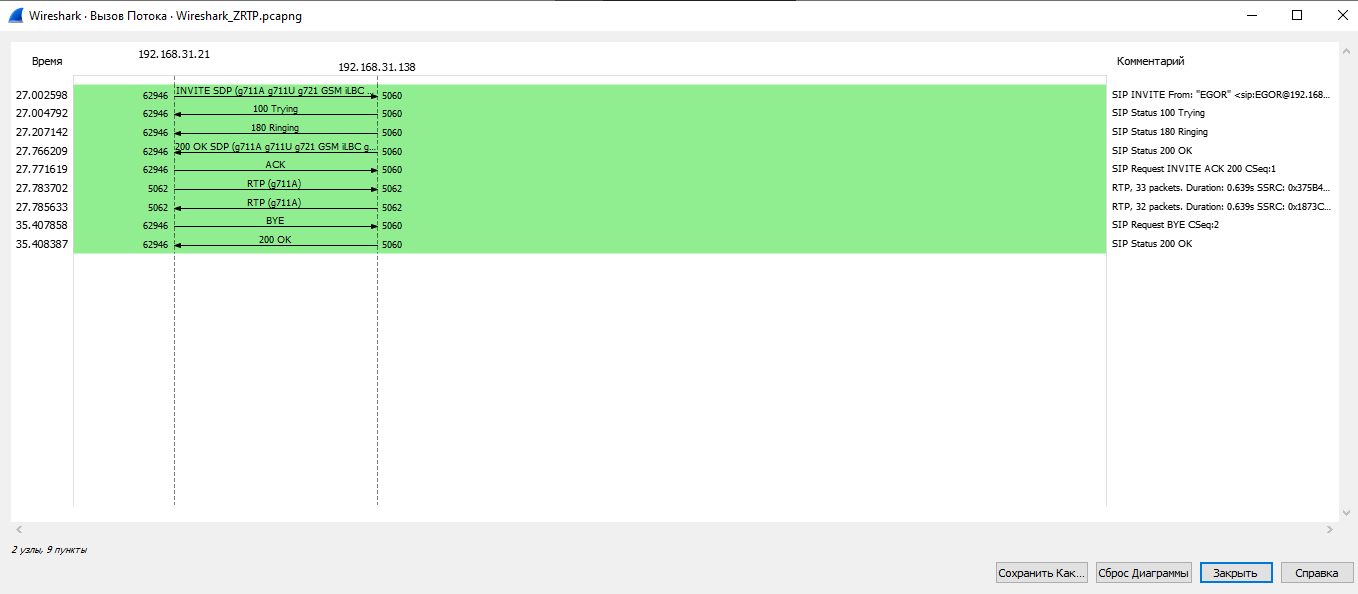


Рис. 4.3 Скриншот обмена SIP сообщениями (ZRTP)

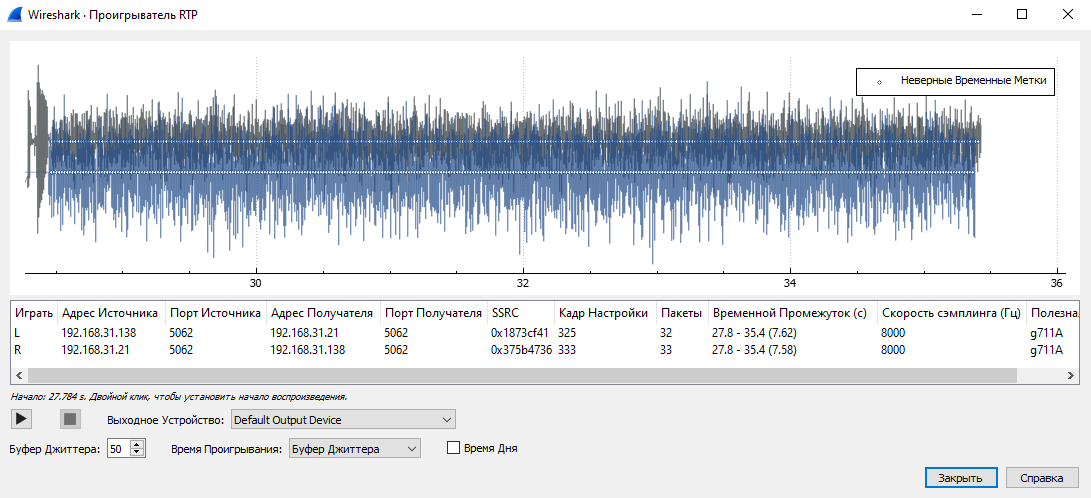


Рис. 4.4 Скриншот записанного звука (ZRTP)

Активация протокола SDES

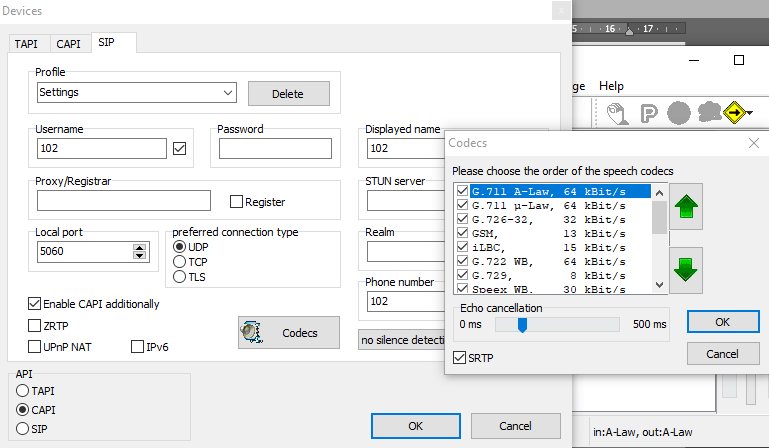


Рис. 4.5 Скриншот настроек (SDES)

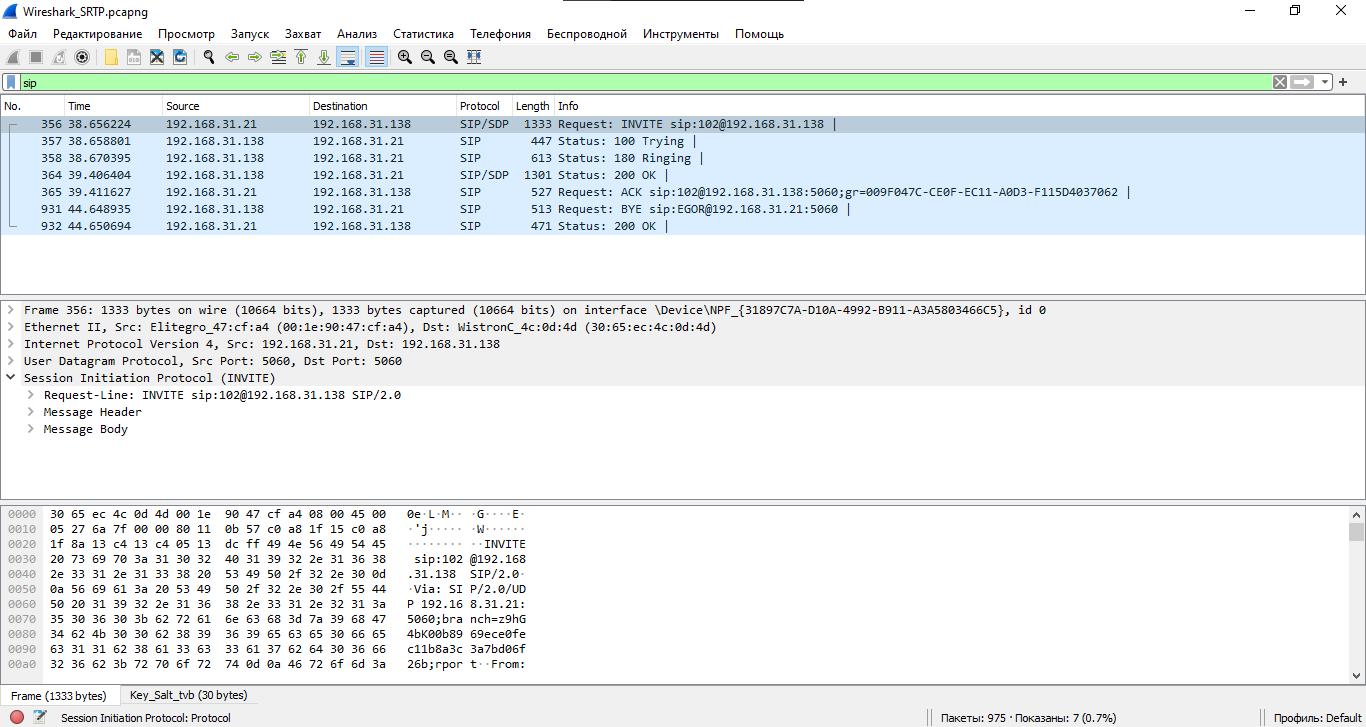


Рис. 4.6 Скриншот Invite пакета (SDES)

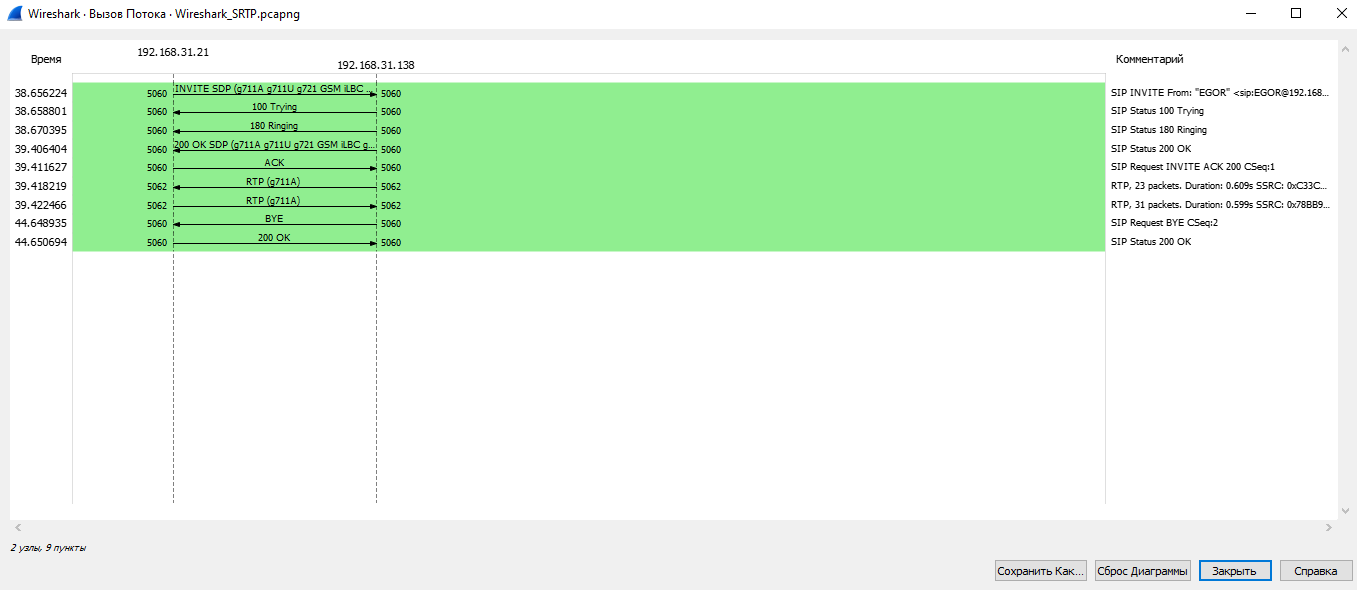


Рис. 4.7 Скриншот обмена SIP сообщениями (SDES)

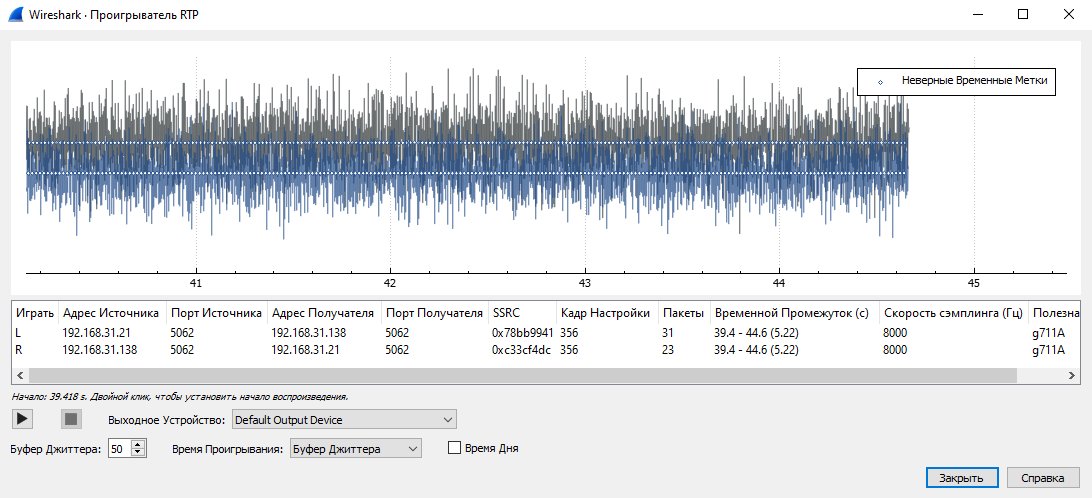


Рис. 4.8 Скриншот записанного звука (SDES)

# ЗАКЛЮЧЕНИЕ:

По итогу проделанной работы, представленной выше, можно сделать следующий вывод. Мы познакомились с основами IP-телефонии в сценарии клиент-клиент. Получили первичные основные навыки работы с ПО Phoner и Wireshark, а также узнали основные протоколы безопасности IP-телефонии.

Защищенные протоколы:

* SIP (Session Initiation Protocol) – протокол передачи данных, предназначен для организации, изменения и завершения сеансов связи, включающие обмен мультимедийным содержимым;
* SRTP (Secure Real-time Transport Protocol) – безопасный протокол передачи данных в реальном времени, определяет профиль RTP и предназначен для шифрования, установления подлинности сообщения, целостности, защиту от замены данных RTP в UNICAST и MULTICAST передачах медиа.

Протоколы согласования ключей:

* ZRTP – криптографический протокол согласования ключей шифрования, описывает метод получения ключей по алгоритму Диффи-Хелмана для SRTP, а также согласует ключи в том же потоке RTP, где передаются медиапотоки, и не требует отдельного канала;
* DTLS (Datagram Transport Layer Security) – обеспечивает защищенность соединений для протоколов, использующих датаграммы, предотвращает перехват, прослушивание, вмешательство, не нарушая защиты целостности данных или подделку содержимого сообщения;
* MIKEY (Multimedia Internet KEYing) – протокол обмена ключами, разработанный специально для мультимедийных приложений, работающих в реальном времени. Используется для обмена ключами для шифрования голосовых сессий протоколов SRTP.

TCP/UDP для SIP:

* TCP – используется в электронной почте, передаче файлов и т.д., т.к. передача каждого пакета квитируется, это гарантирует доставку каждого пакета в нужной последовательности, сохраняя целостность данных;
* UDP – чаще всего используется в IP-телефонии для передачи голоса или видео, т.к. скорость передачи гораздо важнее, некоторых потерь.