Лабораторная работа № 1. IP-телефония в сценарии клиент-клиент. Протоколы обеспечения безопасность IP-телефонии.

Цель работы: осуществить соединение между двумя терминалами пользователя по протоколу SIP. Освоить основы работы с сетевым анализатором Wireshark. Настроить протоколы обеспечения безопасности на терминале пользователя и убедиться в их функционировании.

Задание:

Изучить основы работы с сетевым анализатором Wireshark;

Установить программное обеспечение Phoner, реализующее функционал VoIP клиента, на два компьютера;

Настроить взаимодействие между VoIP терминалами пользователя и создать дампы звонков с использованием сетевого анализатора;

Настроить протокол ZRTP на клиентах и изучить его функционирование;

Настроить протокол SDES на клиентах и изучить его функционирование;

Создать дампы звонков с использованием сетевого анализатора Wireshark при включенных протоколах обеспечение безопасности IP-телефонии.

Схема лабораторной установки

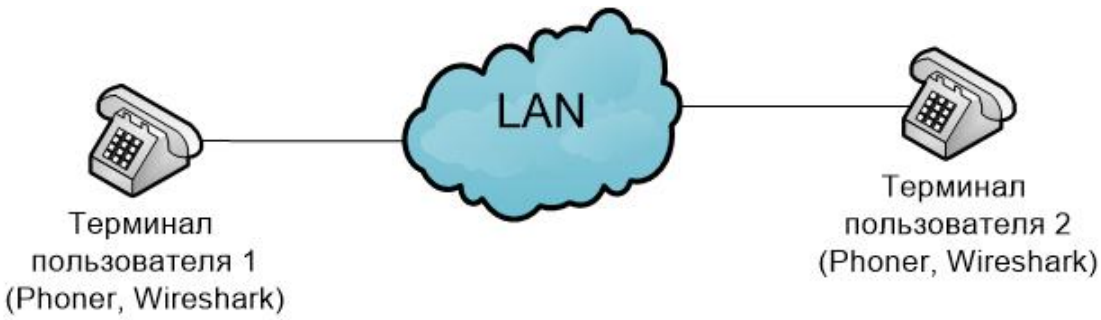

Рисунок 1.1 – Схема лабораторной установки.

Руководство:

Часть 1 –сетевой анализатор трафика Wireshark

1. Установить Wireshark (https://www.wireshark.org/download.html) на компьютер с операционной системой Windows или Linux.

   Wireshark® – это анализатор сетевых протоколов. Он позволяет перехватывать и интерактивно просматривать трафик, протекающий в

компьютерной сети. У приложения богатый набор возможностей, и оно является одним из популярных в мире среди анализаторов протоколов.

2. Изучить основы работы с Wireshark: создание дампа трафика, остановка записи дампа трафика, изменение используемого сетевого интерфейса, открытие дампа, применение фильтрации протоколов при анализе ранее созданного дампа.

3. Проверить на доступность сайт www.mail.ru и получите дамп пакетов протокола ICMP. Добавить скриншот ICMP запросов и ответов к отчёту по лабораторной работе.

Часть 2 – установка и настройка программных клиентов IP-телефонии

1. Установить программное обеспечение Phoner (программный клиент IP-телефонии) версии не ниже 2.90 на оба компьютера. Запустить установленное приложение. Настроить SIP профиль в Phoner на каждом из компьютеров. Для этого открыть Option/Communication, как показано на рисунке 1.2, и выполнить настройки, как показано на рисунке 1.3, где XY – порядковый номер студента в списке группы.

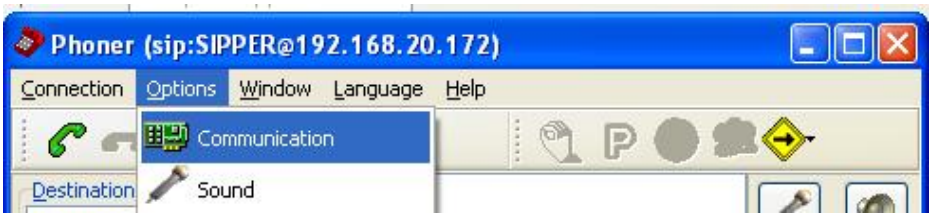

Рисунок 1.2 – Настройка SIP профиля

Сделать скриншот выполненных настроек.

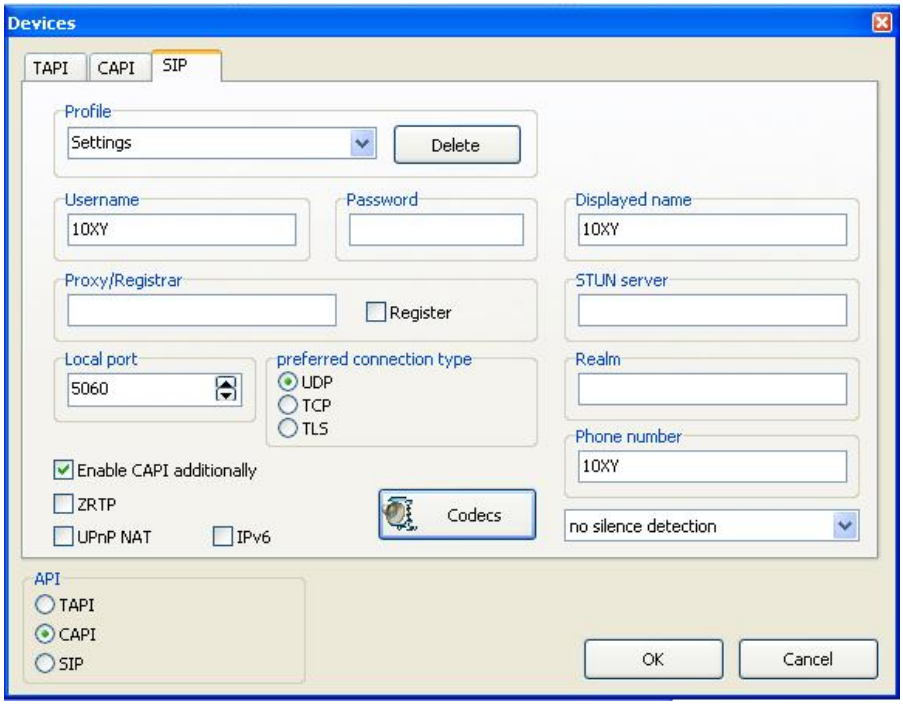

Рисунок 1.3 – Окно настройки SIP профиля

2. Выполнить звонок с одного программного клиента на другой в соответствии с рисунком 1.4.

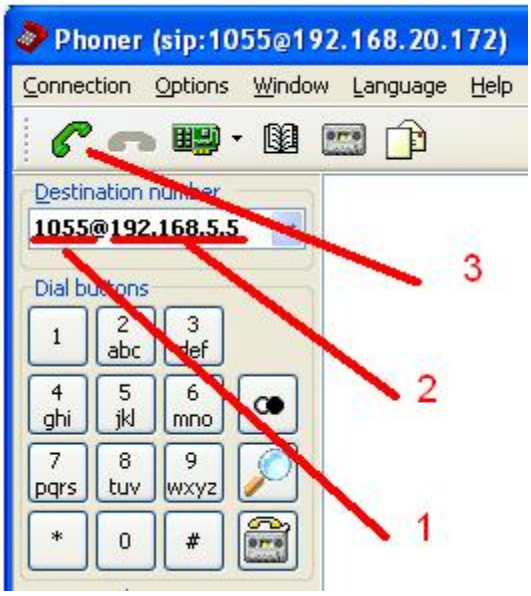

Рисунок 1.4 – Реализация вызова на программном клиенте

Для этого в поле Destination number вводится номер вызываемого пользователя, а через символ @ вводится IP-адрес вызываемого пользователя. После этого осуществляется вызов, посредством нажатия кнопки вызова.

3. Создать дамп трафика для вызова точка-точка.

Для этого необходимо:

a) В программе Wireshark включить создание дампа трафика
b) Осуществить вызов между двумя пользователями
c) Остановить создание дампа трафика
d) Сохранить данный дамп трафика для будущего анализа
e) Сделать скриншота Invite пакета SIP

4. Изучить основы обмена SIP сообщениями (сценарий обмена сообщениями SIP потока, декодирование голоса).

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

Компьютеры соединены по топологии точка-точка, как показано на рисунке 1.1. Необходимо указать настройки сетевых интерфейсов в таблице 1, которую следует включить в отчет.

Таблица 1.1. Настройки терминалов IP-телефонии

Настройка	Терминал пользователя 1	Терминал пользователя 2
IP-адрес		
MAC-адрес		
SIP-номер		

1. Включить запись дампа в Wireshark.

2. Включить автоответчик, нажав на кнопку, как показано на рисунке 1.5.

Рисунок 1.5 – Активация автоответчика

Сделать звонок с терминала пользователя 1 на терминал пользователя 2, используя программу Phoner. Дождаться срабатывания автоответчика. Завершить срединение.

3. Остановить запись дампа, сохранить дамп в файл.

4. Сделать скриншот SIP пакетов.

Используя меню Wireshark Telephony/VoIP Calls проверить запись звонка в дампе. Используя кнопку «Flow» – проверить обмен SIP сообщениями. Так же необходимо сделать скриншот для отчета. Используя клавишу «Player »- прослушать запись звонка и сделать скриншот записанного звонка.

5. Настроить SIP протокол для работы поверх TCP на обоих терминалах пользователя, как показано на рисунке 1.6.

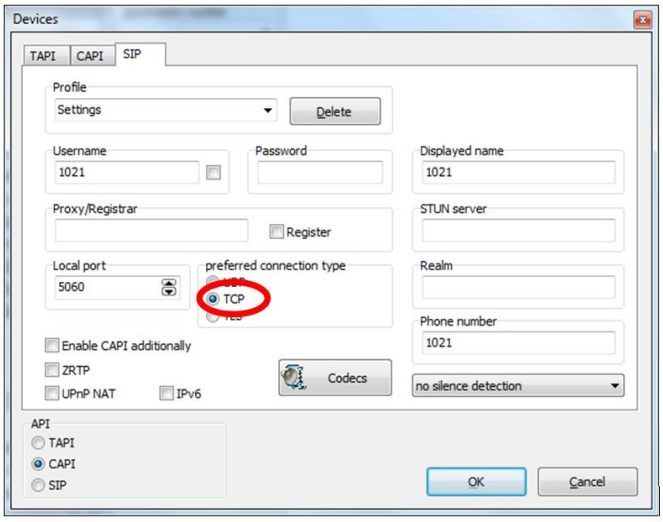

Рисунок 1.6 – Настройка работы SIP поверх протокола TCP

6. Начать запись дампа в Wireshark.

7. Сделать звонок с терминала пользователя 1 на терминал пользователя 2.

8. Сохранить дамп в файл.

9. Сделать скриншот обмена SIP сообщениями (Flow graph), скриншот раскрытого пакета INVITE. Используя меню Wireshark Telephony/VoIP Calls, проверить запись VoIP звонка в дампе. Используя кнопку «Flow» – проверить обмен SIP-сообщениями, а также сделать скриншот данного окна. Используя клавишу «Player» – прослушать запись звонка и сделать скриншот записанного звонка.

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

1. Изучить протоколы защиты IP-телефонии: протокол защиты сигнализации SIP (SIP-S), протокол защиты медиаданных (SRTP), протоколы согласования ключей (ZRTP, DTLS, SDES, MIKEY).

2. **ZRTP**

   Активировать протокол ZRTP и SRTP на программных клиентах IP-телефонии. Для этого установить галочку ZRTP в окне настроек, как показано на рисунке 1.7, а также установить UDP в качестве предпочитаемого протокола для SIP.Убедиться, что в настройках Codecs снята галочка SRTP, так как она отвечает за включение протокола SDES. Сделать скриншот персональных настроек.

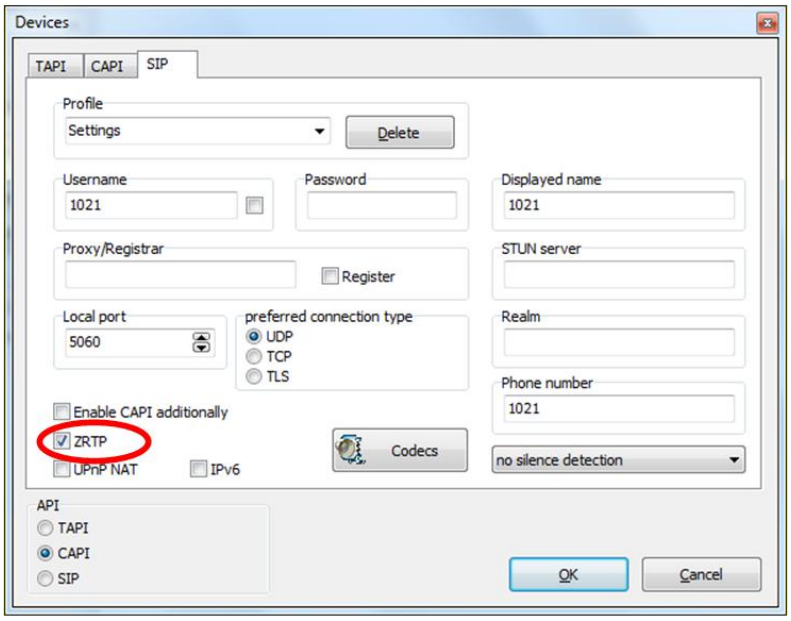

Рисунок 1.7 – Настройка работы SIP поверх работы протокола TCP

3. Повторить пункты 6-9 части 3.

4. Подготовить скриншоты обмена ZRTP и скриншот SRTP пакета.

5. **SDES**

   Активировать протокол SDES и SRTP на программных клиентах IP-телефонии. Для этого выключить установленный ранее флажок ZRTP, зайти в настройки Codecs и установить флаг SRTP, как показано на рисунке 1.8. Сделать скриншот введенных настроек

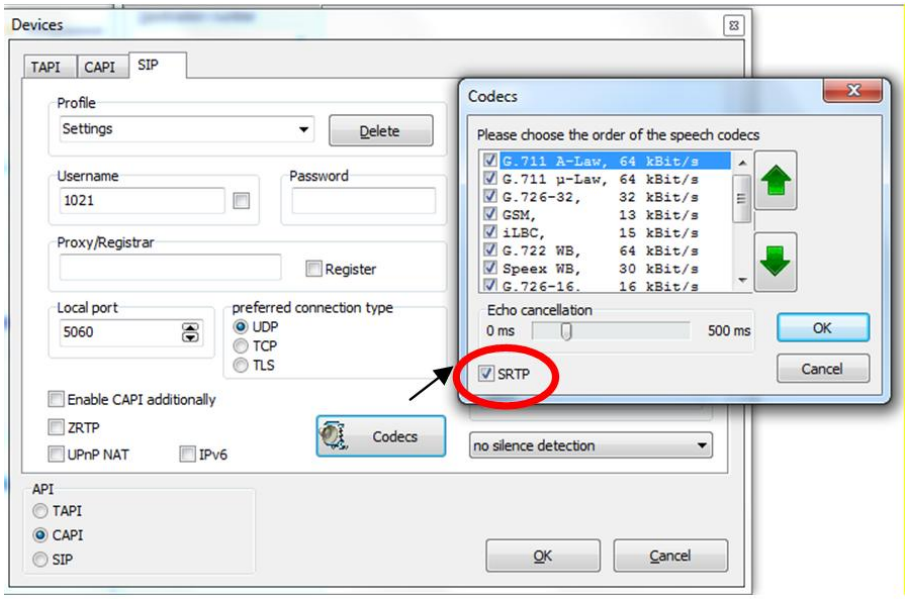

Рисунок 1.8 – Активация протокола SDES и SRTP

6. Повторить пункты 6-9 части 3.

7. Подготовить скриншоты обмена SDES-SRTP и скриншот SRTP пакета. Используя меню Wireshark Telephony/VoIP Calls, проверить запись VoIP звонка в дампе. Используя кнопку «Flow», проверить обмен SIP сообщениями. Используя клавишу «Player», прослушать запись звонка и сделать скриншот записанного звонка. Сделать скриншот вышеописанных окон для отчета. Сделать скриншот SIP пакетов (Flow graph) и раскрытого SIP сообщения INVITE, чтобы отображались параметры шифрования в заголовке SDP.

Проверка выполнения работы

Вы выполнили работу, если

1. При звонке с программного клиента ПК 1 на программный клиент на ПК 2 звонок состоялся без использования протоколов защиты и у вас есть дамп этого звонка.

2. При звонке с программного клиента ПК 1 на программный клиент на ПК 2 и активированном протоколе ZRTP разговор состоялся и у вас есть дамп этого звонка, а также подготовлены все необходимые скриншоты.

3. При звонке с программного клиента ПК 1 на программный клиент на ПК 2 и активированном протоколе SDES разговор состоялся и у вас есть дамп этого звонка, а также подготовлены все необходимые скриншоты.

4. В каждом из дампов вы можете посмотреть SIP Flow.

Требования к отчёту по лабораторной работе

- Отчет должен содержать скришоты, сделанные по пунктам заданий.
- Отчет должен содержать скриншот выполнения команд «ipconfig – all» и «arp –a» в консоли терминала пользователя.
- обмен SIP-сообщениями (SIP Flow)
- Дать краткую характеристику протоколам: защищенный протокол SIP (SIP-S), защищенный протокол передачи мультимедиа (SRTP), протоколы согласования ключей (ZRTP, DTLS, SDES, MIKEY);
- Описать особенности использования TCP / UDP для SIP.

Вопросы для самоподготовки

- Какие инструменты Wireshark особенно удобно использовать для анализа протоколов IP-телефонии?
- Описать назначение протоколов SIP, RTP, RTCP.
- Дать определение терминалу пользователя IP-телефонии и его функциям на примере программного обеспечения Phoner.
- Привести сценарий установления соединения в IP-телефонии, порядок обмена SIP-сообщениями, а также алгоритм выбора кодека и механизм передачи голосовых данных поверх IP.
- Привести краткую характеристику протоколов SIPS, SRTP, SRTCP, ZRTP, DTLS, SDES, MIKEY.
- В чем отличие протоколов SIP-S, SRTP, ZRTP, DTLS, SDES, MIKEY? Каково назначение этих протоколов?