Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

Кафедра телекоммуникаций и основ радиотехники (ТОР)

А. Л. Конюхов

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Методические указания по выполнению лабораторных работ

2016

Корректор: С. Д. Сарина

Конюхов А. Л.
Информационные технологии : методические указания по выполнению лабораторных работ / А. Л. Конюхов. – Томск : ФДО, ТУСУР, 2016. – 27 с.

СОДЕРЖАНИЕ

1 ЛАБОРАТОРНАЯ РАБОТА № 1. КОМАНДНАЯ СТРОКА. ГЛОБАЛЬНАЯ СЕТЬ ИНТЕРНЕТ. ПОИСКОВЫЕ СИСТЕМЫ

Цель работы: получение базовых навыков работы в командной строке и использование поисковых систем для нахождения нужных сетевых ресурсов и различной информации.

1.1 Вводная часть

Цель данной работы состоит в ознакомлении с командной строкой («текстовым интерфейсом» компьютера), в которой инструкции компьютеру даются путём ввода команд. Также необходимо задействовать поисковые системы и воспользоваться сетевыми сервисами, доступными в глобальной сети Интернет.

1.2 Описание рабочего места

Для успешного выполнения лабораторной работы необходимо воспользоваться персональным компьютером с установленной на нем ОС Windows. Допускается использование ПК с ОС семейства Linux и Mac OS, однако в этом случае студент должен сам найти и изучить синтаксис используемых в командной строке (консоли) команд. На ПК должен быть установлен интернет-браузер (для выполнения данной работы подойдет любой браузер). Кроме того, ПК должен иметь доступ в сеть Интернет.

1.3 Методика проведения эксперимента

При выполнении работы необходимо запустить командную строку и интернет-браузер (browse – просматривать). Необходимо получить базовые навыки работы в командной строке и обозревателе интернет-ресурсов.

1.4 Порядок выполнения работы

1.4.1 Использовать командную строку.

1.4.1.1 Запустить командную строку от имени администратора. Нажать Пуск – Все программы – Стандартные – Командная строка (кликнуть правой кнопкой, выбрать пункт «Запуск от имени администратора»).

1.4.1.2 Ввести команду «ipconfig», получить значения настроек сетевой карты ПК, сделать скриншот командной строки.

1.4.1.3 По полученным данным заполнить таблицу 1.1 (за исключением последней строки).

Таблица 1.1 – Пример

Параметр	Значение
IPv4 адрес	192.168.0.1
Маска подсети	255.255.255.0
Основной шлюз	192.168.0.254
Публичный адрес (если в домашней сети используется пограничный маршрутизатор)	88.204.75.155

1.4.1.4 Запустить интернет-браузер, войти на сайт 2ip.ru или аналогичный, установить свой публичный IP-адрес, присвоенный провайдером. Ресурс 2ip.ru при входе на него сразу же возвращает на главной странице публичный IP-адрес пользователя, обратившегося к ресурсу. По полученным данным заполнить последнюю строку таблицы 1.1, сделать скриншот веб-страницы.

1.4.2 Использовать интернет-браузер для работы с интернет-сервисами.

1.4.2.1 Войти на сайт google.ru.

1.4.2.2 С помощью поисковых запросов найти в глобальной сети Интернет информацию об истории создания глобальной сети Интернет, а также драйвер на материнскую плату своего ПК. Включить ссылки на найденную информацию в отчет.

1.5 Содержание отчета

1.5.1 Использование командной строки. По пункту 1.4.1.2 в отчете должен находиться скриншот, по пункту 1.4.1.3 в отчете должна находиться заполненная таблица 1.1, по пункту 1.4.1.4 в отчете должен находиться скриншот сайта 2ip.ru.

1.5.2 Использование интернет-браузера. По пункту 1.4.2.2 в отчете должны находиться ссылки на страницы об истории создания сети Интернет и драйвер материнской платы Вашего ПК.

1.5.3 Краткий вывод по каждому пункту выполненной работы.

1.6 Контрольные вопросы

1.6.1 Какую информацию можно получить в командной строке с помощью команды «ipconfig/displaydns»?

1.6.2 Чем отличаются команды «ipconfig» и «ipconfig/all»?

1.6.3 Какая информация предоставляется командной строкой по команде «nslookup google.ru»?

1.6.4 В чем отличие публичных и приватных IP-адресов?

2 ЛАБОРАТОРНАЯ РАБОТА № 2. АНАЛИЗ СЕТЕВОГО ТРАФИКА

Цель работы: изучение сетевого трафика, генерируемого сетевым устройством в сетях передачи данных при работе с различными сетевыми сервисами; анализ служебных заголовков часто используемых сетевых протоколов.

2.1 Вводная часть

Цель данной работы состоит в перехвате и анализе трафика, проходящего через сетевой интерфейс компьютера, используемого при выполнении данной лабораторной работы. Необходимо научиться определять, какому уровню модели OSI принадлежит тот или иной сетевой протокол, а также пользоваться служебной информацией, передающейся в служебных заголовках протоколов транспортного, сетевого и канального уровней модели OSI.

2.2 Описание рабочего места

Для успешного выполнения лабораторной работы необходимо воспользоваться персональным компьютером с установленной на нем ОС Windows. Допускается использование ПК с ОС семейства Linux и Mac OS, однако в этом случае студент должен сам найти и изучить синтаксис используемых в командной строке (консоли) команд. Кроме того, ПК должен иметь доступ в сеть Интернет.

Для анализа сетевого трафика, проходящего через сетевой интерфейс ПК, необходимо установить программный продукт Wireshark. Этот программный продукт распространяется под свободной лицензией GNU GPL. Существуют версии для Windows, Mac OS X, и большинства типов UNIX-систем.

Wireshark – это приложение, которое проводит анализ структуры самых различных сетевых протоколов, и позволяет «разобрать» блок передаваемых данных на составляющие, отображая значение каждого поля протокола любого уровня. Это делает Wireshark универсальным инструментом не только для обучения, но и выполнения различных задач по администрированию сетей передачи данных. Программный продукт Wireshark можно скачать на официальном сайте проекта www.wireshark.org.

2.3 Методика проведения эксперимента

Перед началом работы необходимо установить программный продукт WireShark на свой компьютер и настроить его. Выбор сетевого интерфейса, трафик которого будет подвергаться анализу, происходит в главном окне программы с помощью инструмента Capture. Если сетевых интерфейсов несколько, нужно выбрать тот, по которому осуществляется передача данных. Значение счетчика переданных пакетов у такого интерфейса постоянно растет (рис. 2.1).

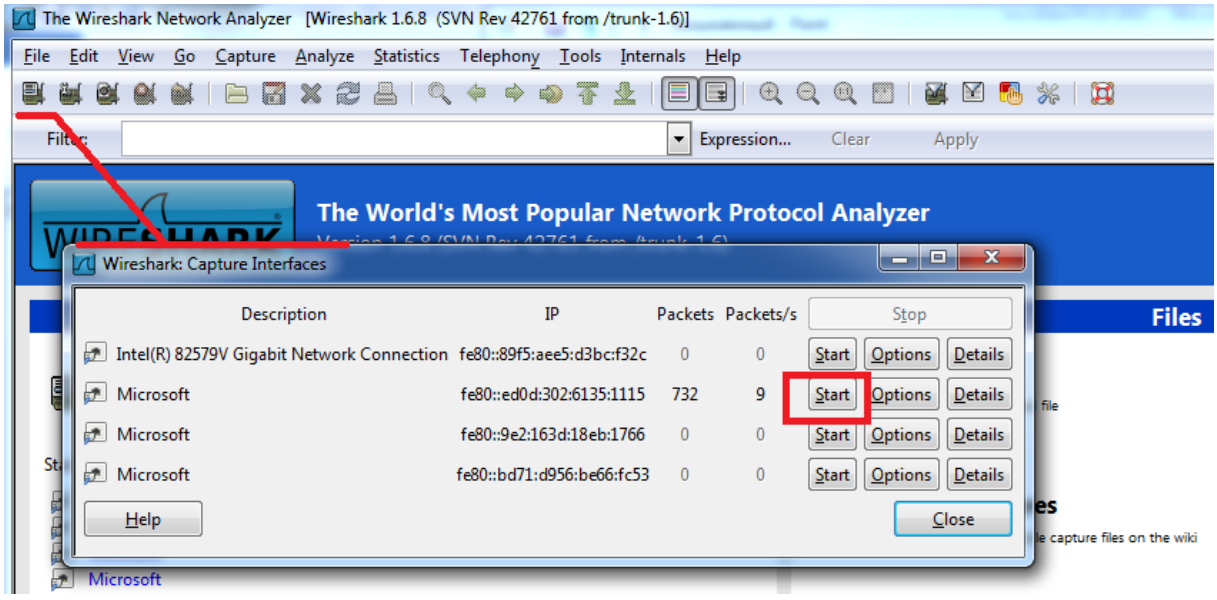

Рис. 2.1 – Выбор сетевого интерфейса

После запуска анализатора начинается процесс захвата сетевого трафика, проходящего через сетевой интерфейс ПК. Чтобы не перегружать поле вывода перехваченных блоков данных, после каждого обмена данными останавливайте захват трафика. Для каждого следующего задания по лабораторной работе – возобновляйте. Для фильтрации трафика и выделения нужных протоколов используйте быстрый фильтр: он выделяет трафик по типу протокола. Для выделения трафика после его захвата нужно набрать в строке фильтра название протокола, например tcp, arp, http (рис. 2.2).

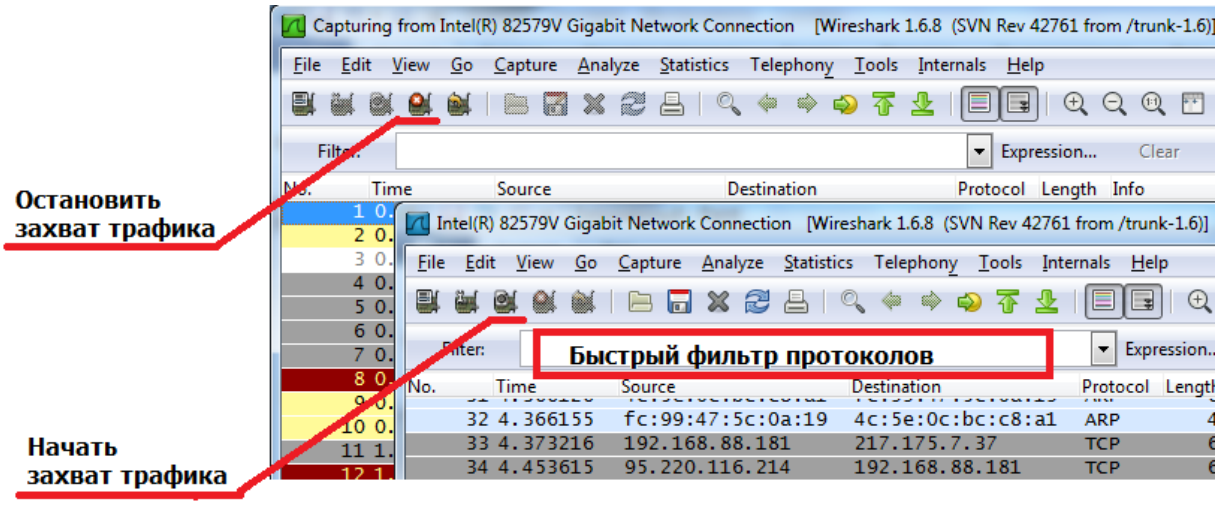

Рис. 2.2 – Захват трафика и быстрый фильтр

Для генерации необходимого трафика в данной работе будет использован интернет-браузер и командная строка. Командную строку можно запустить, набрав в поле Пуск – Выполнить команду «cmd», или найти ее в Пуск – Все программы – Стандартные. Команды для работы с протоколом ARP доступны по запросу arp, команды для работы с протоколом DNS – nslookup, команды для работы с протоколом ICMP – ping и tracert. Команды для работы с сетевым интерфейсом – ipconfig.

2.4 Порядок выполнения работы

2.4.1 Проанализировать работу протокола ARP.

2.4.1.1 Запустить анализатор трафика Wireshark. Включить захват трафика.

2.4.1.2 Запустить командную строку от имени администратора.

2.4.1.3 В командной строке выполнить команду ipconfig /all и на основе результата ее выполнения для используемого сетевого интерфейса начать заполнять таблицу 2.1 и приложить скриншот командной строки.

Таблица 2.1 – Пример

Параметр	Значение
Физический адрес	FC-99-47-5C-0A-19
DHCP включен	Да / Нет
IPv4-адрес	192.168.88.181
Маска подсети	255.255.255.0
Основной шлюз	192.168.88.254
DHCP-сервер	192.168.88.254
DNS-серверы	62.68.141.212, 62.68.144.253
Физический адрес основного шлюза	Заполнить по результату выполнения пункта 2.4.1.6
Производитель устройства, выступающего основным шлюзом	Заполнить по результату выполнения пункта 2.4.1.7

2.4.1.4 В командной строке выполнить команду «arp –d *» для очистки arp-таблицы сетевого интерфейса ПК.

2.4.1.5 Выполнить команду ping для своего Основного шлюза (например, «ping 192.168.88.254»).

2.4.1.6 В программе Wireshark выставить значение быстрого фильтра arp и выделить два кадра протокола ARP – arp-запрос и arp-ответ, открыть их, как показано на рисунке 2.3, сделать скриншот и внести в таблицу 2.1 значение MAC-адреса Основного шлюза. Проверить его, выполнив в командной строке команду «arp –a». Выключить захват трафика в программе Wireshark.

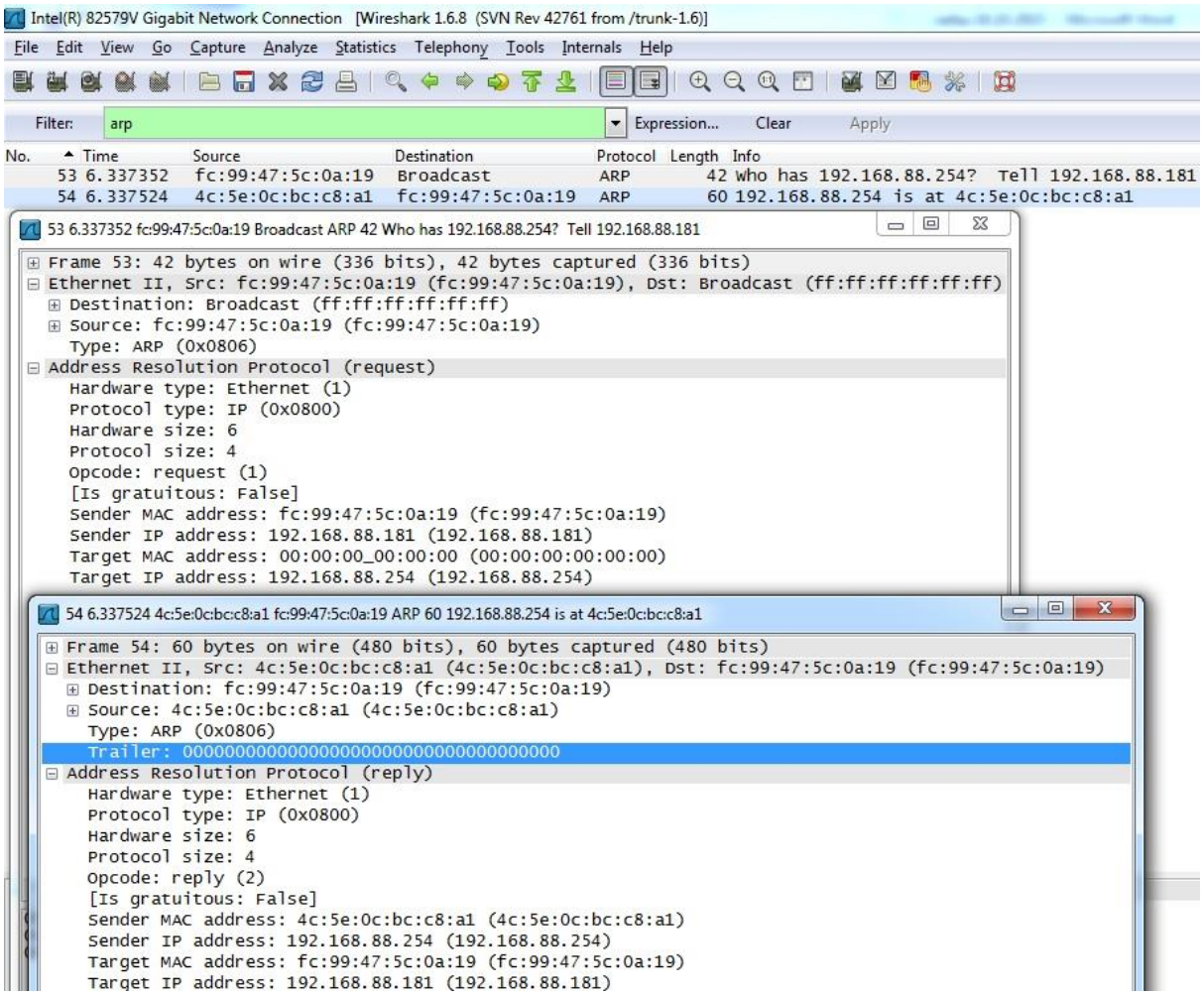

Рис. 2.3 – Результат анализа работы arp-протокола

2.4.1.7 В интернет-браузере, воспользовавшись поисковой системой yandex.ru или google.ru, выполнить поисковый запрос «MAC-address vendor», выбрать онлайн-сервис для установления производителя устройства,

выступающего основным шлюзом, ввести в онлайн-сервисе mac-адрес своего основного шлюза, полученные данные ввести в таблицу 2.1.

2.4.2 Проанализировать работу протокола ICMP.

2.4.2.1 Включить захват трафика в программе Wireshark.

2.4.2.2 В командной строке поочередно ввести команды «ping google.ru», «ping yandex.ru», «ping {ip-address основного шлюза}», «ping 8.8.8.8». Сделать скриншот командной строки. Выключить захват трафика в программе Wireshark.

2.4.2.3 Заполнить таблицу 2.2 на основе полученных данных.

Таблица 2.2 – Пример

Сетевой ресурс	Время отклика	Значение поля TTL
Google.ru		
Yandex.ru		
IP-адрес основного шлюза		
8.8.8.8		

2.4.2.4 В программе Wireshark выставить значение быстрого фильтра icmp, выбрать два пакета – icmp-request и icmp-reply – для одной из серий выполнения команды ping, сделать скриншот, как показано на рисунке 2.4.

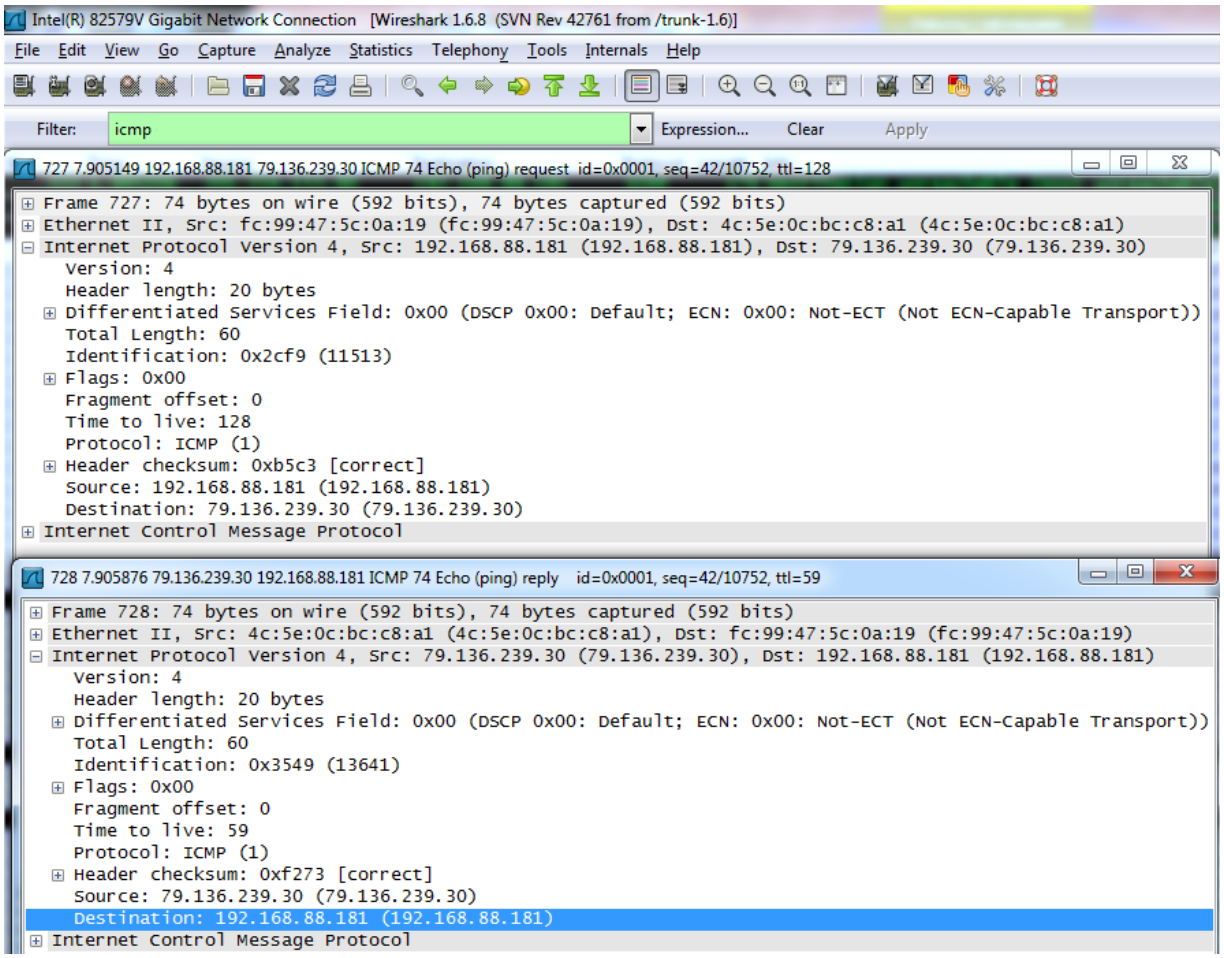

Рис. 2.4 – Результат анализа работы icmp-протокола

2.4.2.5 Включить захват трафика в программе Wireshark.

2.4.2.6 В командной строке поочередно ввести команду «tracert 8.8.8.8». Команда tracert определяет путь прохождения icmp-пакетов до пункта назначения, при этом запрашивая эхо-ответ у каждого промежуточного сетевого узла. В результате выполнения данной команды каждый промежуточный сетевой узел вернет отправителю эхо ответ. Таким образом, можно судить о примерном пути прохождения отправленных данных.

2.4.2.7 Дождаться окончания выполнения команды. Сделать скриншот командной строки. Выключить захват трафика в программе Wireshark.

2.4.2.8 В программе Wireshark выставить значение быстрого фильтра icmp, сделать скриншот, как показано на рисунке 2.5.

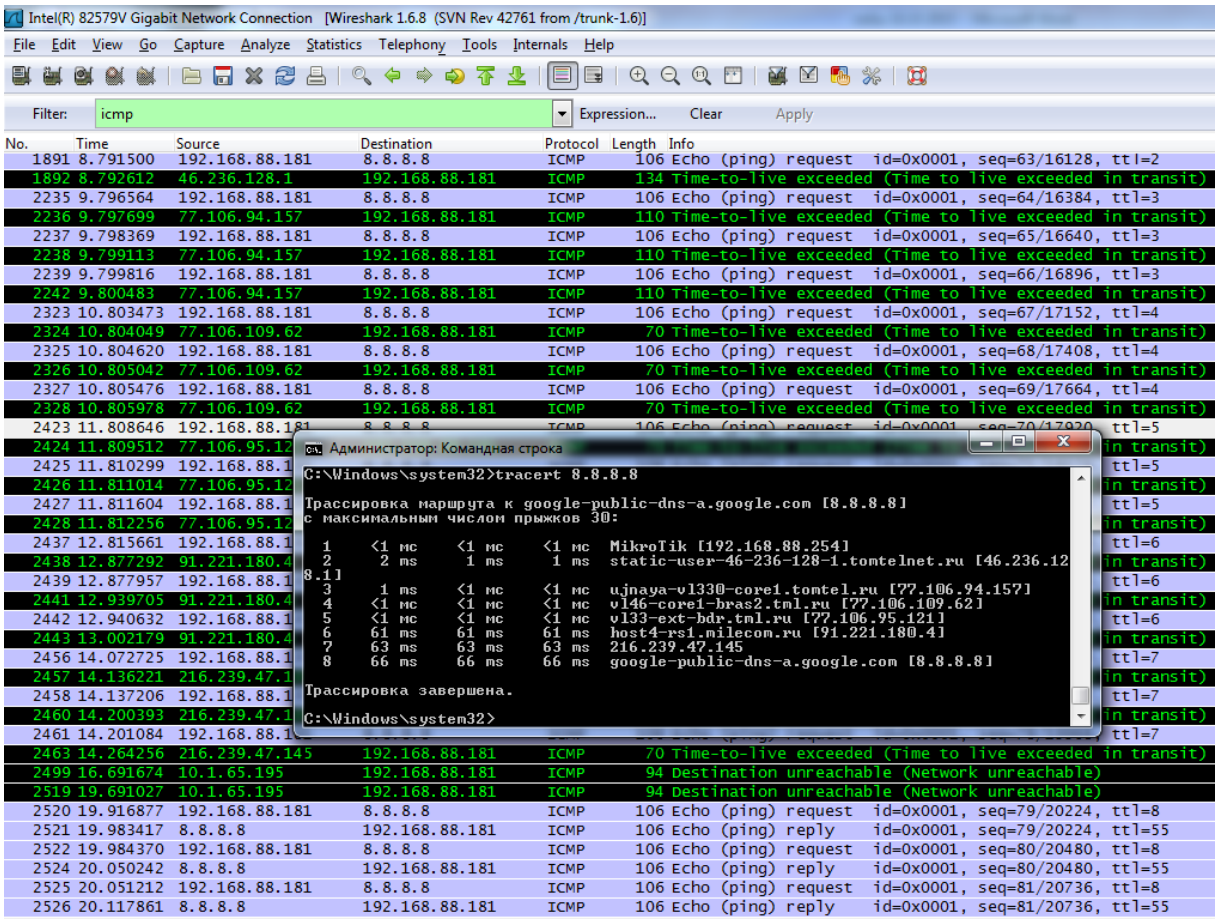

Рис. 2.5 – Результат выполнения команды tracert

2.4.3 Проанализировать работу протокола разрешения имен DNS и транспортного протокола UDP.

2.4.3.1 Включить захват трафика в программе Wireshark.

2.4.3.2 В командной строке поочередно ввести команды «ipconfig/ flushdns» для очистки DNS-кэша сетевого интерфейса, затем «nslookup ******.***» для получения IP-адреса произвольного сетевого ресурса (на Ваше усмотрение). Для успешного выполнения данного пункта не используйте популярные сетевые сервисы типа Яндекс, Google, официальный сайт ТУСУР, mail.ru. Выбранный Вами сайт не должен совпадать с сайтами из других студенческих работ. Сделать скриншот командной строки.

2.4.3.3 Выключить захват трафика в программе Wireshark. Выставить значение быстрого фильтра dns, сделать скриншот, аналогичный показанному

на рисунке 2.6. Обратить внимание, что сегменты запроса и ответа в программе Wireshark названы «Standart query A tusur.ru» и «Standart query response A» соответственно.

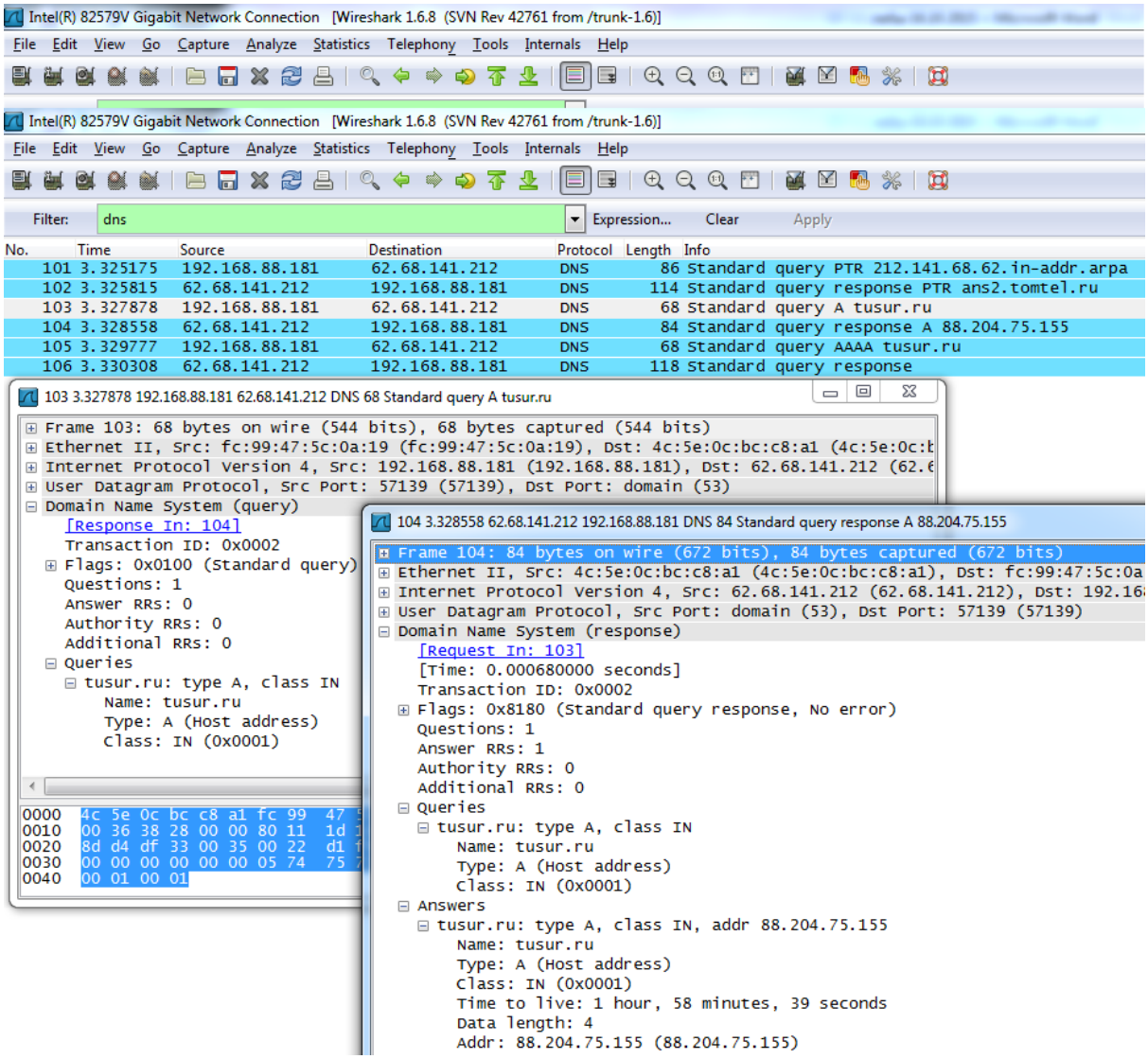

Рис. 2.6 – Анализ работы протокола DNS

2.4.3.4 На основе полученных данных использованных портов сегментов транспортного уровня заполнить таблицу 2.3. Речь идет об идентификации сетевого взаимодействия по сокету. Запрос отправляется DNS-серверу, который посылает отправителю ответ.

Таблица 2.3 – Пример

Инфо сегмента	Src Port	Dst Port	Src IP	Dst IP
Standart query A tusur.ru	57139 – произвольный порт	53 – порт, идентифицирующий протокол DNS	192.168.88.181	62.68.141.212 DNS-сервер провайдера
Standart query response A	53 – порт, идентифицирующий протокол DNS	57139	62.68.141.212 DNS-сервер провайдера	192.168.88.181

2.4.4 Проанализировать работу протокола HTTP и транспортного протокола TCP.

2.4.4.1 Включить захват трафика в программе Wireshark.

2.4.4.2 В интернет-браузере ввести имя интернет-ресурса, выбранного в пункте 2.4.3.2. Дождаться окончания загрузки веб-страницы.

2.4.4.3 Выключить захват трафика в программе Wireshark. Выставить значение быстрого фильтра http, сделать скриншот, как показано на рисунке 2.7. Обратить внимание, что требуемые для анализа сегменты – первый GET-запрос и следующий на него ответ.

2.4.4.4 На основе полученных данных использованных портов сегментов транспортного уровня заполнить таблицу 2.4. Речь идет об идентификации приложения по сокету.

2.4.4.5 Проанализировать значения счетчиков Seq, Ack, Len в заголовках транспортного уровня исследуемых сегментов. Len=303 сегмента, посланного отправителем, и Ack=304 сегмента, посланного сервером tusur.ru, говорит об установленной TCP-сессии и контроле доставки сегментов за счет обмена счетчиками и увеличения их на 1.

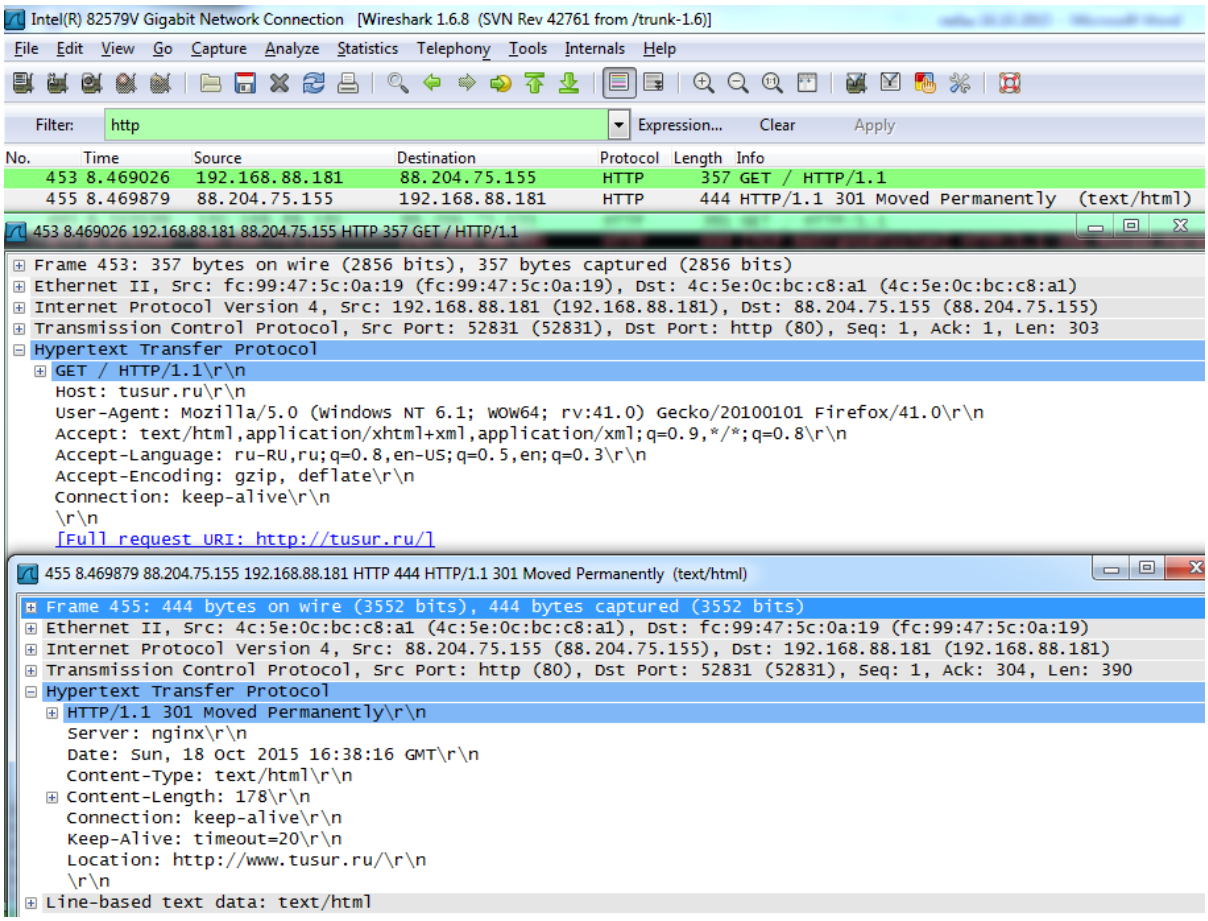

Рис. 2.7 – Анализ работы протокола HTTP

Таблица 2.4 – Пример

Инфо сегмента	Src Port	Dst Port	Src IP	Dst IP
GET	52831 – произвольный порт	80 – порт, идентифицирующий протокол HTTP	192.168.88.181	88.204.75.155 Сервер tu.tusur.ru
HTTP	80 – порт, идентифицирующий протокол HTTP	52831	88.204.75.155 Сервер tu.tusur.ru	192.168.88.181

2.5 Содержание отчета

2.5.1 Анализ протокола ARP. По пункту 2.4.1 в отчете должна находиться заполненная таблица 2.1 и два скриншота (п. 2.4.1.3 и п. 2.4.1.6).

2.5.2 Анализ протокола ICMP. По пункту 2.4.2 в отчете должна находиться заполненная таблица 2.2 и скриншоты по подпунктам 2.4.2.4 и 2.4.2.8.

2.5.3 Анализ протокола DNS. По пункту 2.4.3 в отчете должны находиться два скриншота по подпунктам 2.4.3.2 и 2.4.3.3, а так же заполненная таблица 2.3.

2.5.4 Анализ протокола HTTP. По пункту 2.4.4 в отчете должен находиться скриншот по пункту 2.4.4.3, а также заполненная таблица 2.4.

2.5.5 Краткий вывод по каждому пункту выполненной работы.

2.6 Контрольные вопросы

2.6.1 К какому уровню модели OSI относится протокол ARP? Почему?

2.6.2 К какому уровню модели OSI относится протокол ICMP? Почему?

2.6.3 Какова функция поля TTL? Какой вывод можно сделать, сравнивания значения поля TTL для результатов выполнения команд «ping {IP-адрес основного шлюза}» и «ping 8.8.8.8»?

2.6.4 Что такое сокет?

2.6.5 Какой номер порта транспортного уровня модели OSI идентифицирует протокол DNS?

2.6.6 Какой номер порта транспортного уровня модели OSI идентифицирует протокол HTTP?

3 ЛАБОРАТОРНАЯ РАБОТА № 3. ЭЛЕКТРОННАЯ ПОЧТА И НОВОСТНЫЕ ЛЕНТЫ

Цель работы: получение навыков использования мультимедиа-ресурсов, таких как электронная почта (E-Mail) и новостной ленты (RSS).

3.1 Вводная часть

Цель данной работы состоит в освоении программ, упорядочивающих доступ к различным мультимедиа-ресурсам. Необходимо научиться настраивать почтовый клиент и ленту новостей и получать с их помощью мультимедиа-контент.

3.2 Описание рабочего места

Для успешного выполнения данной работы необходимо выполнить требования, описанные в предыдущих лабораторных работах. Также необходимо завести (если еще нет) электронный почтовый ящик на любом общедоступном почтовом сервере.

Для доступа к мультимедиа-ресурсам необходимо установить программный продукт Mozilla Thunderbird. Этот программный продукт распространяется под свободной лицензией GNU GPL. Программный продукт можно скачать на официальном сайте проекта www.mozilla.org/ru/thunderbird/.

Для выполнения данной лабораторной работы можно использовать любой почтовый клиент, например The Bat! (также распространяется по лицензии GNU GPL) или MS Outlook (включен в состав ОС Windows). Но в этом случае изучение особенностей настройки доступа клиента к мультимедиа-ресурсам целиком ложится на обучающегося.

3.3 Методика проведения эксперимента

Перед началом работы необходимо установить программный продукт Mozilla Thunderbird на свой компьютер. После этого будет настроен доступ к электронной почте и новостной ленте.

3.4 Порядок выполнения работы

3.4.1 Настроить почтовый клиент.

3.4.1.1 Запустить программу Mozilla Thunderbird.

3.4.1.2 Инициировать подключение существующего почтового аккаунта (организацию доступа к почтовому ящику), как показано на рисунках 3.1 и 3.2. Для выполнения данного пункта лабораторной работы у учащегося должен быть в распоряжении зарегистрированный на любом почтовом сервере электронный почтовый ящик.

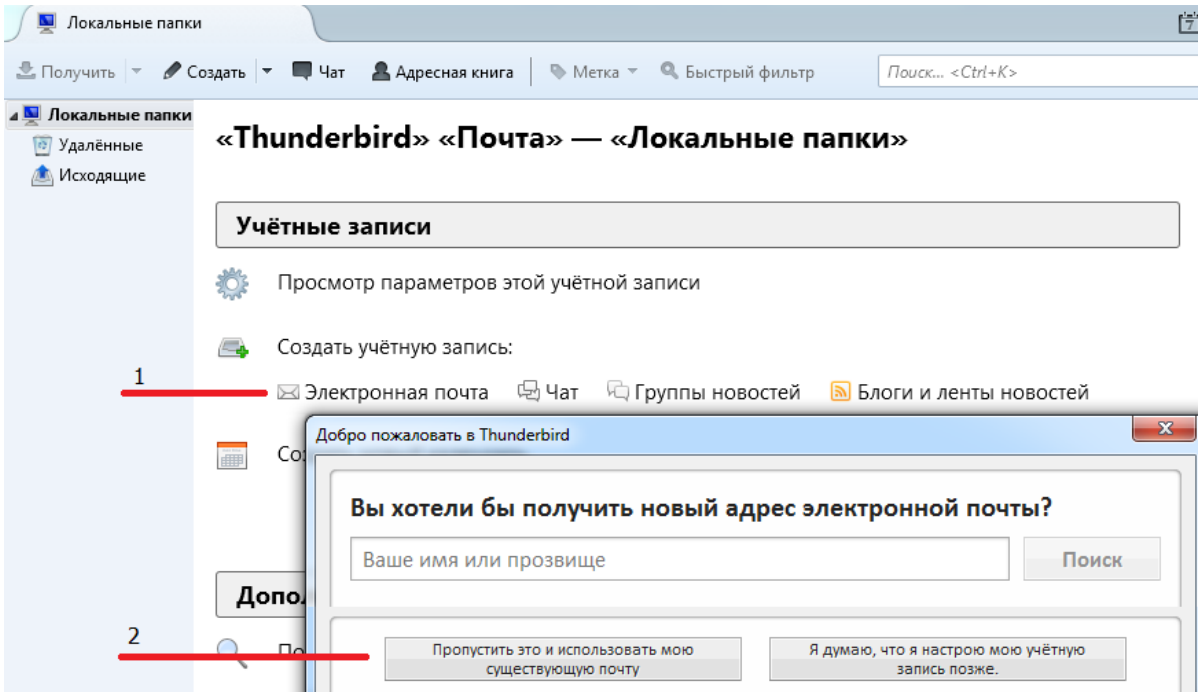

Рис. 3.1 – Подключение почтового ящика

На рисунке 3.1 почтовый клиент получает команду на подключение к почтовому ящику, на рисунке 3.2 – получает данные для аутентификации пользователя.

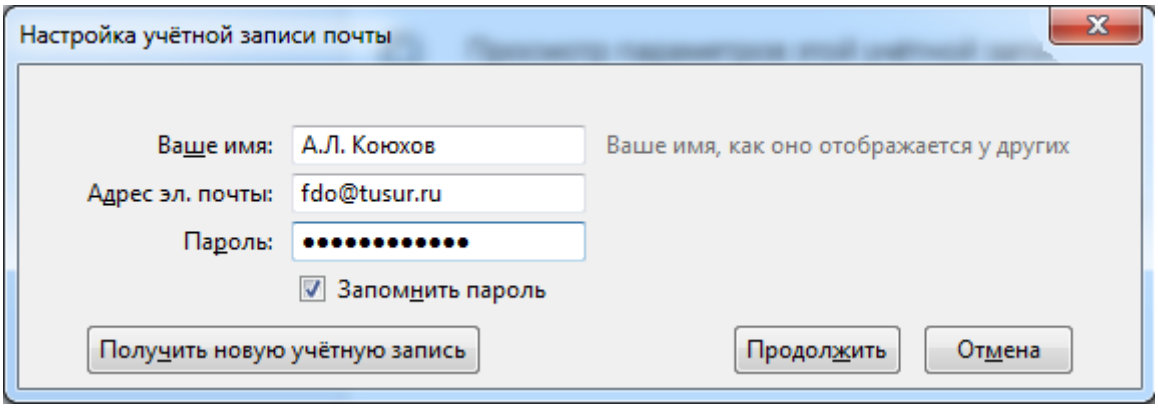

Рис. 3.2 – Ввод данных для аутентификации на почтовом сервере

После ввода корректных данных – существующего почтового ящика и пароля к нему – нажать кнопку «Продолжить», после того как произойдет подключение клиента к потовому ящику, нажать появившуюся кнопку «Готово».

3.4.1.3 В почтовом клиенте выбрать подключенный ящик, нажать кнопку «Получить» (см. рис. 3.3). Имеется в виду – получить почту, находящуюся в почтовом ящике, к которому почтовый клиент получил доступ.

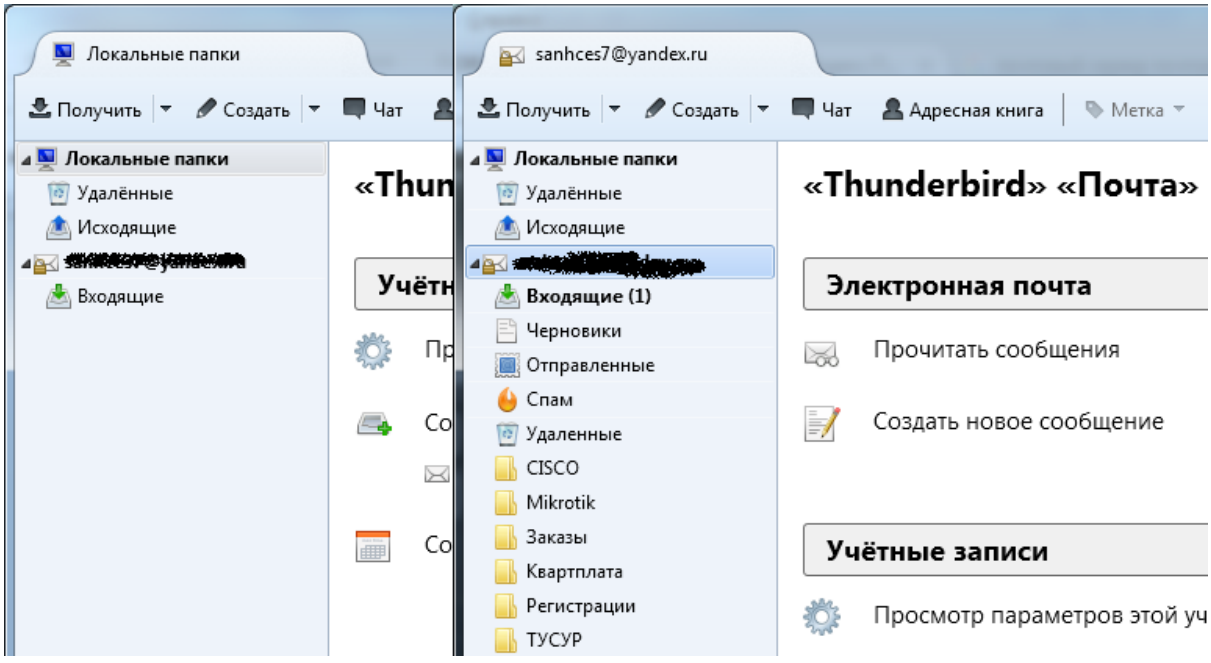

Рис. 3.3 – Получение писем почтовым клиентом

3.4.1.4 Написать и отправить тестовое письмо, содержащее ФИО учащегося, номер его группы и произвольное изображение, на электронный адрес alk@fdo.tusur.ru. Файл можно добавить к письму командой «Вложить». Ограничение на размер отправляемого файла для данной лабораторной работы – 2 Мб. Максимальный размер почтовых вложений зависит от конкретного почтового сервера.

3.4.1.5 Проанализировать свойства любого входящего письма. Открыть полученное письмо, нажать кнопку «Больше», в выпадающем меню выбрать пункт «Показать исходник» (рис. 3.4).

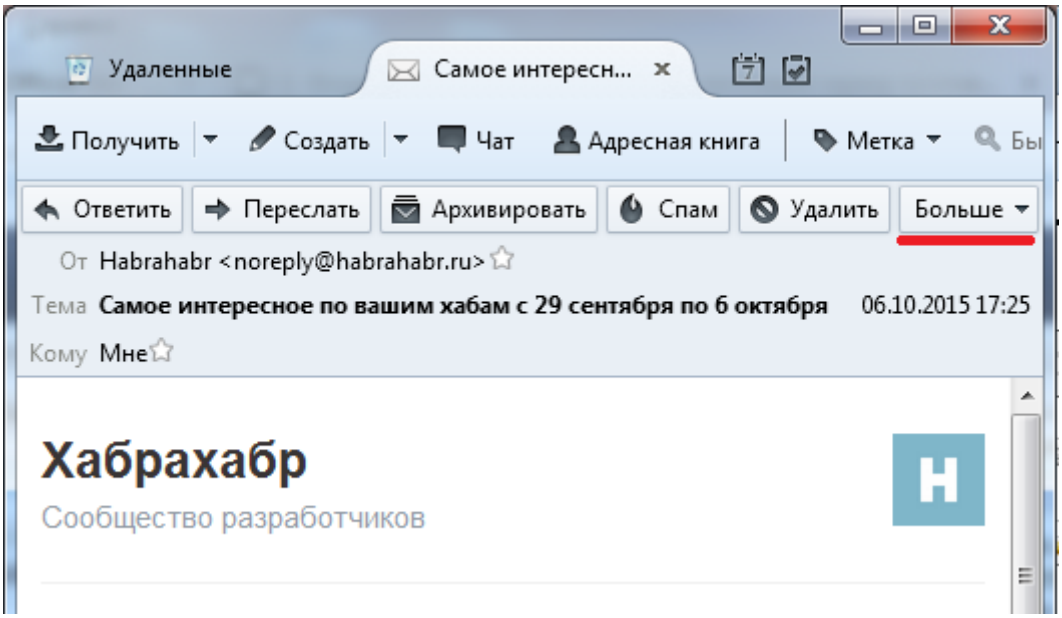

Рис. 3.4 – Открытие свойств письма

3.4.1.6 Воспользоваться сетевым онлайн сервисом, позволяющим анализировать заголовки электронных писем. В данном примере использован сервис ru.smart-ip.net, можно найти другие по поисковому запросу «Трассировка e-mail». Цель этого анализа – выяснить географическую привязку пути прохождения письма по глобальной сети передачи данных.

3.4.1.7 Скопировать из исходника письма заголовок (от начала кода до строки «X-Antivirus-Status: Clean», ориентироваться можно по семантическим названиям полей), и вставить в форму обработки запроса онлайн сервиса ru.smart-ip.net.

3.4.1.8 Проанализировать заголовок электронного письма, заполнить таблицу 3.1 на основе полученных данных:

Таблица 3.1 – Пример

Электронный адрес почтового ящика учащегося	Заключение сервиса ru.smart-ip.net (или любого другого онлайн сервиса)
xx111xxx@study.tusur.ru	**Заключение** Данное сообщение отправлено от noreply@habrahabr.ru к sanhces7@yandex.ru. Изначально оно было создано и отправлено в Вто, 06 Окт 2015 11:25:26 +0000 (UTC) и доставлено в почтовый ящик адресата через 2 минуты и 47 секунд. Нельзя утверждать достоверно, но с большой вероятностью, что сообщение было создано и отправлено с компьютера, имеющего IP-адрес 95.211.146.161, который находится в: Нидерланды. Во время пересылки к адресату сообщение пересылалось через следующие сервера: 1. 95.211.146.161, located in Нидерланды [whois | на карте | пинг | трассировка | проверка на спам] 2. 84.201.187.134, located in Россия [whois | на карте | пинг | трассировка | проверка на спам] 3. 84.201.186.19, located in Россия [whois | на карте | пинг | трассировка | проверка на спам] ← Анализировать другой заголовок

3.4.2 Настроить получение новостей с помощью ленты новостей**.**

3.4.2.1 Инициировать подключение существующей новостной ленты с целью получения новостей в виде электронных писем. В диспетчере учетных записей (левая колонка основного тела программы) почтового клиента выбрать пункт «Локальные папки» и создать еще одну учетную запись под названием «Блоги и ленты новостей».

3.4.2.3 Кликнуть по созданной учетной записи правой кнопкой мыши и войти во вкладку «Параметры».

3.4.2.4 В открывшемся меню нажать кнопку «Управление подписками». Откроется следующее окно (рис. 3.5).

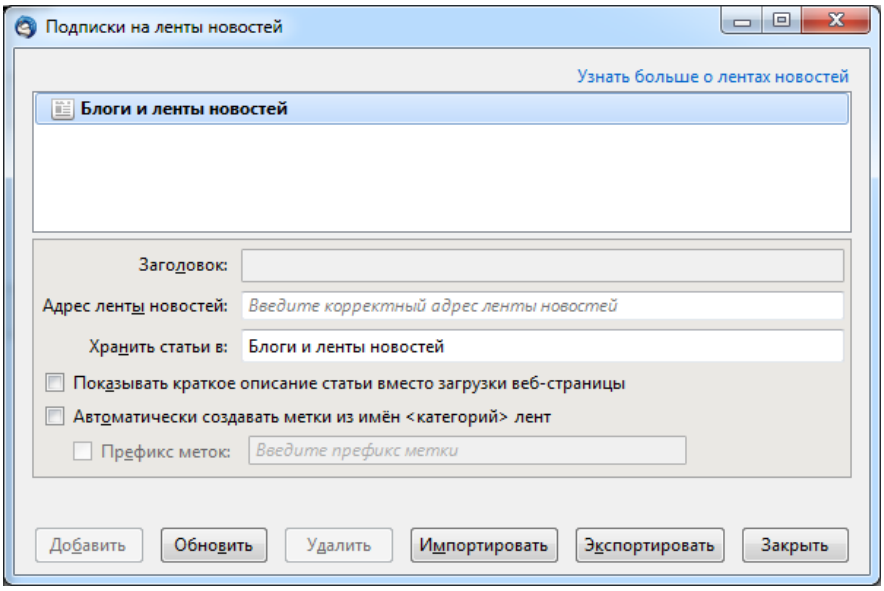

Рис. 3.5 – Окно управления подписками

3.4.2.5 В строку «Адрес ленты новостей» окна управления подписками необходимо вставить ссылку на подключаемую ленту новостей (RSS). Получить ее можно по адресу http://www.tusur.ru/ru/news/index.html или зайти на официальный сайт ТУСУР, кликнуть по любой новости и попасть в раздел новостей. Там скопировать URL-адрес гиперссылки RSS Feed и вставить ее в окно управления подписками. Нажать кнопку «Добавить». Если все сделано правильно, все новости отобразятся в списке полученных сообщений для этой учетной записи.

3.4.2.6 Сделать скриншот почтового клиента, как показано на рисунке 3.6:

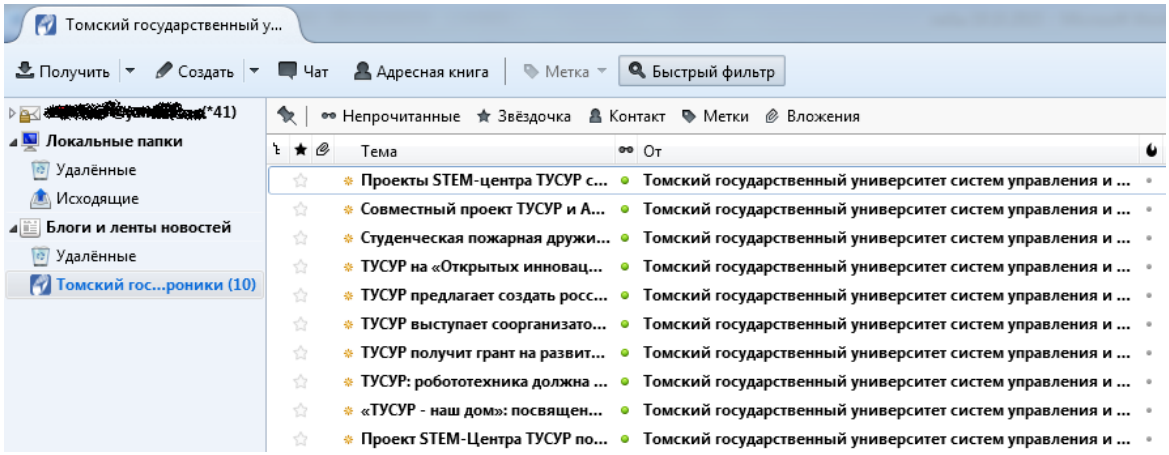

Рис. 3.6 – Скриншот почтового клиента с настроенными учетными записями для электронной почты и ленты новостей

3.5 Содержание отчета

3.5.1 Отправка электронной почты. По пункту 3.4.1.4 на электронный почтовый ящик alk@fdo.tusur.ru должно прийти письмо с Вашего почтового ящика, содержащее Ваши ФИО, номер группы и произвольное изображение (максимальный размер вложения – 2 Мб).

3.5.2 Анализ заголовка электронного письма, полученного от преподавателя. По пункту 3.4.1 в отчете должна находиться заполненная таблица 3.1. Допускается вставить скриншот заключения онлайн сервиса трассировки электронной почты.

3.5.3 Подключение ленты новостей. По пункту 3.4.2.6 в отчете должен находиться скриншот почтового клиента с настроенными учетными записями почтового ящика и новостной ленты.

3.5.4 Краткий вывод по каждому пункту выполненной работы.

3.6 Контрольные вопросы

3.6.1 Какой протокол используется для представления данных в формате RSS? (Подсказка: RSS не является протоколом передачи данных, а лишь инструментом форматирования передаваемого текста).

3.6.2 Какой номер порта транспортного уровня модели OSI идентифицирует протокол SMTP?

3.6.3 В чем отличие функций протоколов работы с электронной почтой SMTP и IMAP?

3.6.4 Каково назначение так называемого «коммерческого at» – @ в адресе электронного почтового ящика?

3.6.5 Какой протокол транспортного уровня, TCP или UDP, используется при передаче данных по протоколам SMTP и IMAP?

4 ТРЕБОВАНИЯ К ОТЧЕТАМ ПО ЛАБОРАТОРНЫМ РАБОТАМ

Отчет должен содержать титульный лист, требуемые к выполнению пункты лабораторных работ, необходимые таблицы и скриншоты и четкие выводы по проделанной работе.

При оформлении отчетов по лабораторным работам следует руководствоваться требованиями образовательного стандарта вуза – ОС ТУСУР 01-2013. Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления.

Форма изложения материала, дополнения, пояснения и необходимые скриншоты – на усмотрение обучающегося.

ЛИТЕРАТУРА

1. Конюхов А. Л. Информационные технологии : учеб. пособие / А. Л. Конюхов. – Томск : ФДО, ТУСУР, 2016. – 83 с.

2. ОС ТУСУР 01–2013. Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления. – Режим доступа: http://www.tusur.ru/export/sites/ru.tusur.new/ru/education/documents/inside/tech_01-2013_new.pdf