Московский государственный технический университет им. Н.Э. Баумана

Факультет «Информатика и системы управления»

Кафедра «Системы обработки информации и управления»



**Отчет**

**Лабораторная работа № 8**

**По курсу «Сети и телекоммуникации»**

**«Исследование протоколов сетевого и транспортного уровней IP-сетей с помощью анализатора протоколов NetInfo, Wireshark»**

**ИСПОЛНИТЕЛЬ:**

Группа ИУ5-55Б

\_Финк Д.Д.

"29"\_декабря\_\_2021 г.

**ПРЕПОДАВАТЕЛЬ:**

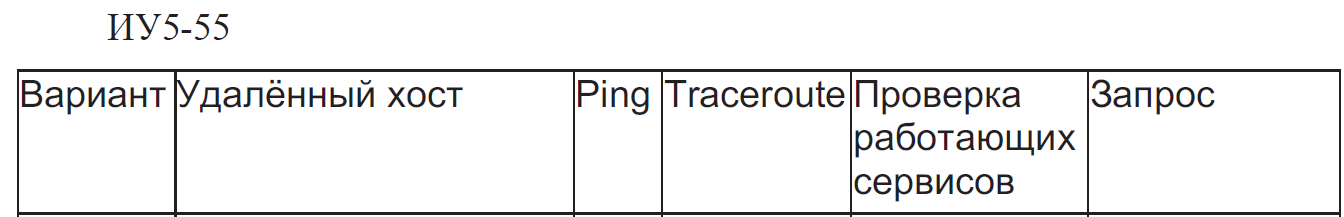
\_\_\_Канев А.И.\_\_\_\_

"\_\_"\_\_\_\_\_\_\_\_\_\_2021 г.

Москва 2021

1. Цель работы

Развитие практических навыков работы с протоколами TCP/IP и исследование возможностей протоколов ICMP, UDP, TCP.

1. Задание  
   



Инициировать ТСР сеанс с хостом, указанным в варианте, и проанализировать его открытие, поддержку и закрытие при помощи пакетного анализатора. Перенести в отчет описание процедур открытия, поддержания и закрытия ТСР соединения посредством обмена заголовками протокола ТСР для этого сеанса. Найти и перенести в отчет все пакеты, отвечающие за вышеуказанные события.

1. Ход работы.

Установлю фильтрацию пакетов.

Зайду на ресурс <https://gmail.com> через браузер.

Для анализа понадобится сделующая информация:

Поля флагов. Указаны в 4м слове заголовка: URD, ACKNOWLADGE, PUSH, RESET, SYNCHRONIZE и FINISH.

URG – пометка того, что пакет содержит важные данные. Подробная информация о важности содержится в поле с данными.

ACK – указывает, что в пакет с номером, указанным в номере подтверждения и все предыдущие получены.

PSH – данные в TCР пакете должны быть немедленно переданы прикладной программе, которая их ожидает.

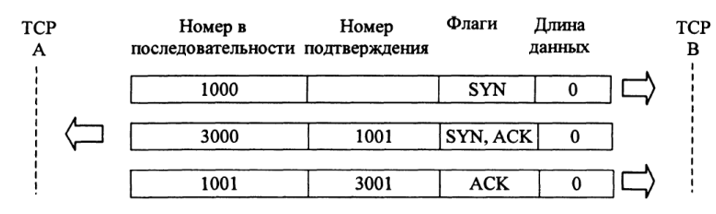
ACK & PSH – все предыдущие пакеты доставлены программе.

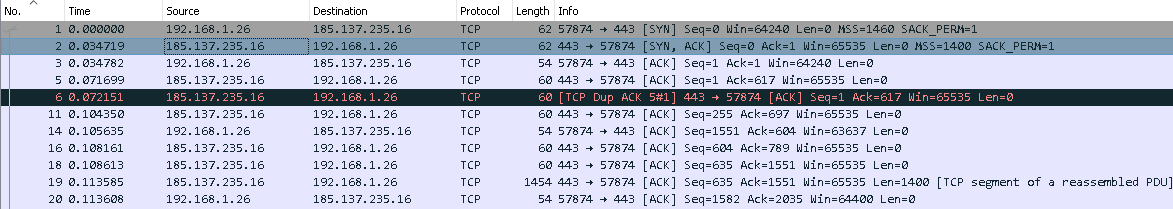
RST == 1 – отправляется в ответ на получение ошибочного TCP-пакета. Также используется как запрос на переустановление соединения.

SYN == 1 – говорит о том, что данный TCP-пакет – это запрос на установление соединения. Передаются суммы для синхронизации.

FIN – запрос на закрытие логического соединения.

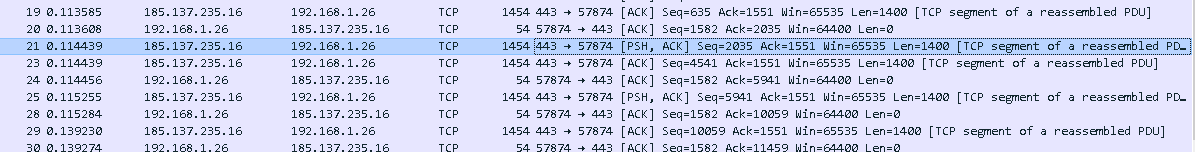
Рассмотрю начало хода пакетов. Самые первые пакеты – запрос на установление соединения по схеме тройного рукопожатия



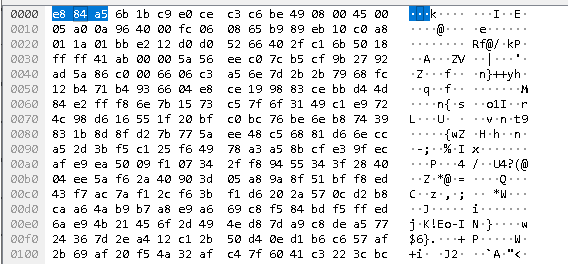


Первый запрос – запрос моего компьютера на установление соединения (флаг SYN), передача ключа для синхронизации. Второй – ответ сервера SYN, ACK – подтверждение готовности, передача сервером своего ключа для синхронизации. Третий пакет – HTTPS-запрос (TSL скрыт фильтром) на получение документа / от ресурса. Посмотрим, что в нем и последующих.

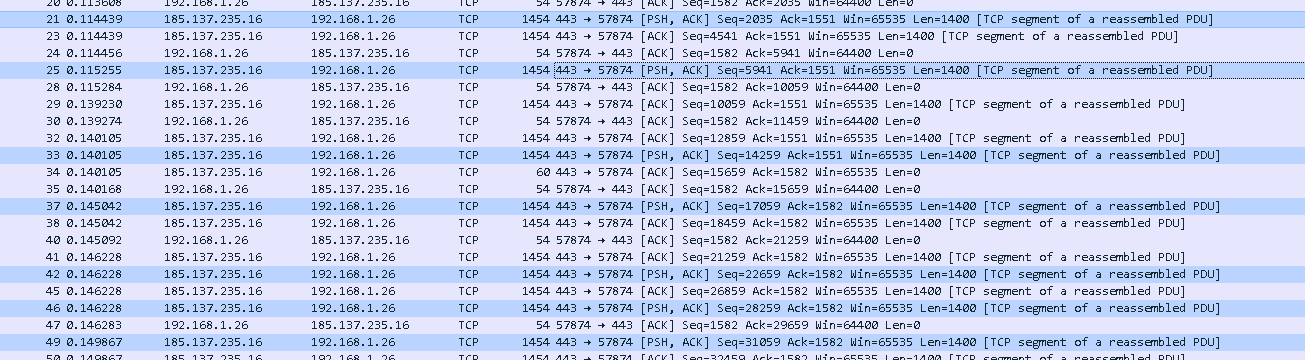
После рукопожатия Сервер шлет мне подряд несколько пакетов с информационным полем длины 1400 байт. А мой компьютер шлет ему в ответ флаги ACK, говорящие о том, что данные приняты:



Содержимое пакетов нечитаемо. Возможно, из-за разности кодировок, ведь с сайта возвращается много кириллицы.

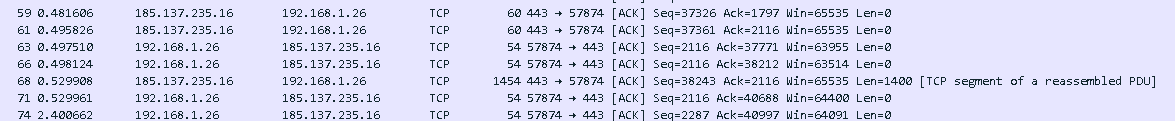


Несколько раз встречается флаг PSH, говорящий о том, что информация предназначена для прикладной программы, т.е. браузеру.



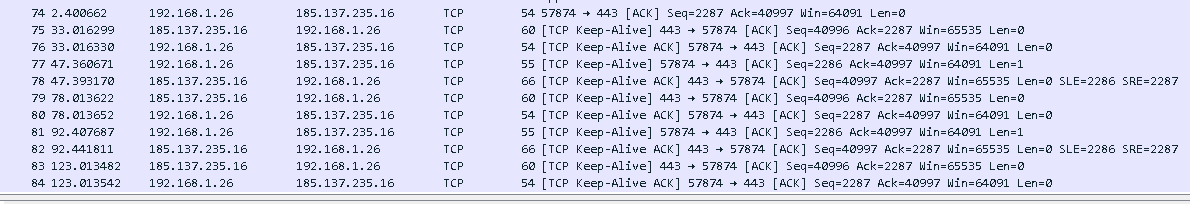
Можно предположить, что именно здесь идет копирование html-документа в кэш браузера.

Загрузка заканчивается, когда начинают идти пакеты с длиной информационной части 0.

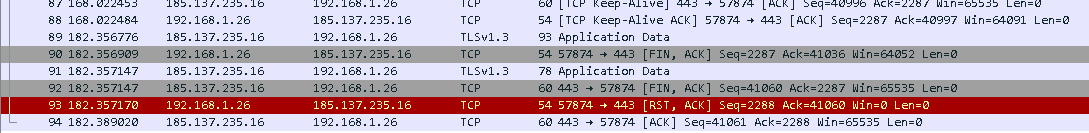


1 пакет 1400 байт – это скорее всего какая-то из картинок, загрузившаяся последней. До этого я сделал какой-то TCP-запрос.

По мере ожидания появляются новые пакеты. Это TCP-запросы на продление соединения.



Закрою вкладку браузера



Моим компьютером были посланы запросы на разрыв соединения – пакет FIN, после чего прошла передача еще нескольких пакетов от сервера мне.

В конце произошел интересный случай. При закрытии соединения не дошел какой-то пакет, и сетевая карта моего компьютера запросила его еще раз, и сервер мне этот пакет предоставил уже после подтверждения закрытия соединения.

1. Вывод.

Мне удалось пронаблюдать теоретические сведения о работе TCP на практике.