Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Факультет Программной инженерии и компьютерной техники

**Лабораторная работа №3**

по дисциплине «Сети ЭВМ и телекоммуникации»

**Выполнил**

Ореховский А.,

группа P3317

**Преподаватель**

Манаев Н.Ю.

Санкт-Петербург

2020

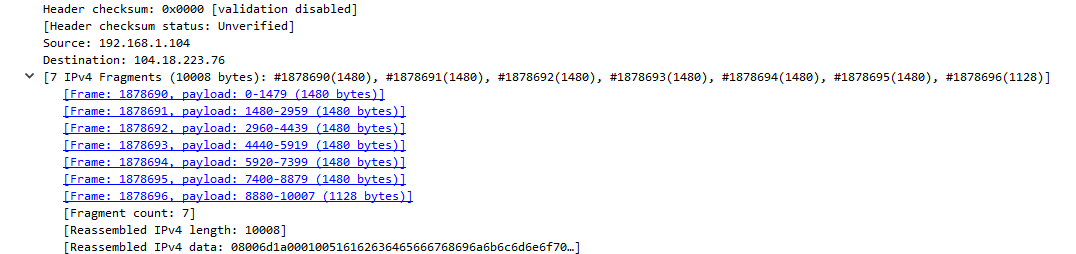
# Цель работы

Изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark.

# 1. Анализ трафика утилиты “ping”

1. **Имеет ли место фрагментация исходного пакета, какое поле на это указывает?**

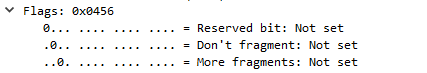
Если пакет фрагментирован, появляется поле под полем Destination, содержащее информацию о фрагментах.



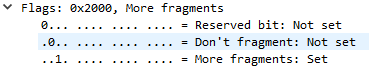
1. **Какая информация указывает, является ли фрагмент пакета последним или промежуточным?**

Флаг More fragments в заголовке ip пакета. Если установлен - пакет промежуточный, если не установлен - пакет последний.

*Пример отсутствия флага.*



*Пример присутствия флага.*



1. **Чему равно количество фрагментов при передаче ping-пакетов?**

MSS (Maximum Segment Size) - значение, которое определяет максимальный размер блока данных в байтах. В данном случае он равен 1480 байт (из них 8 байт на icmp заголовок). Соответственно, пакет будет фрагментироваться на фрагменты максимум по 1480 байт, откуда можно посчитать кол-во фрагментов для заданного размера пакета.



1. **Построить график, в котором на оси абсцисс находится размер\_пакета, а по оси ординат –количество фрагментов, на которое был разделён каждый ping-пакет.**
2. **Как изменить поле TTL с помощью утилиты ping?**

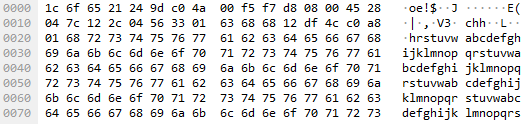
Указать параметр -i с числовым значением срока жизни пакетов.

*Пример команды ping с указанным TTL = 123*



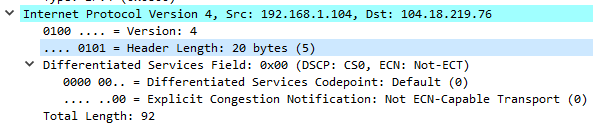
1. **Что содержится в поле данных ping-пакета?**

Данные для эхо-запроса и эхо-ответа, которые должны совпадать (заполняет циклически шестнадцатеричными числами от 61 до 77) .

****

# 2. Анализ графика утилиты “tracert”

1. **Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?**



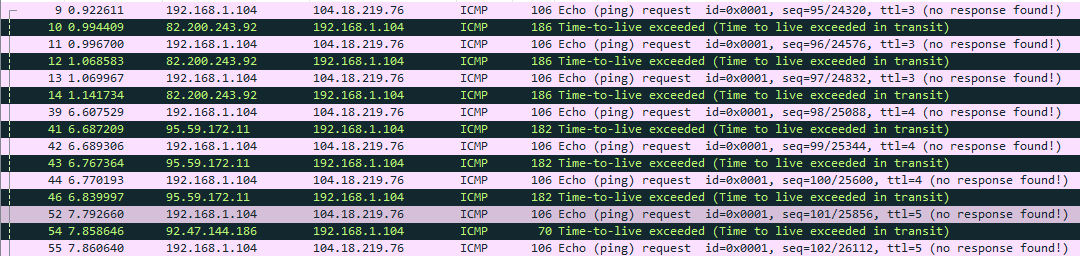
На данном скриншоте видно, что размер пакета равен 92 байта, из них 20 – размер заголовка IP пакета.



На этом скриншоте видно, что размер данных составляет 64 байта, и значит оставшиеся 8 байт — это заголовок ICMP.

1. **Как и почему изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.**

Для определения промежуточных маршрутизаторов tracert отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL («время жизни») на 1. Это поле указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение «time exceeded in transit», указывающее на невозможность доставки данных. Tracert фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем tracert повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает «time exceeded in transit». Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

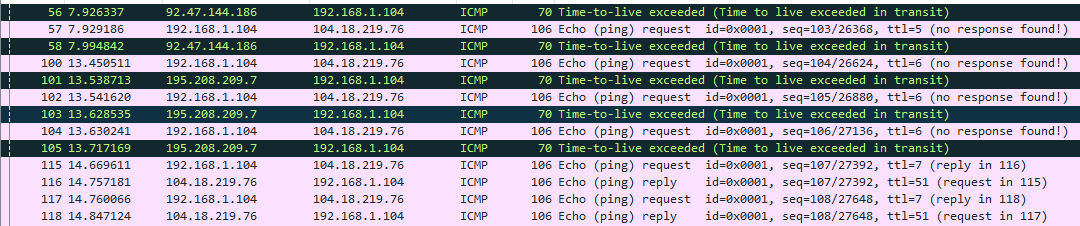


1. **Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание).**

Ping отправляет ICMP пакеты с типом echo с кодом 8, в ответ получает Echo reply с кодом 0. Tracert отправляет тоже Echo (code 8), но в ответ он получает Time exceeded (code 11).Также, утилита tracert заполняет поле данных нулями, в то время как ping заполняет циклически от 61 до 77(в шестнадцатеричной системе).

1. **Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?**

ICMP reply должен вернуть обратно пакет с исходными данными для того, чтобы удостовериться в целостности связи, в то время как ICMP error сигнализирует об ошибке, путем установления соответствующего типа и кода, и присылает пакет c пакетом внутри, с которым произошла проблема. Tracert использует ICMP-сообщения с типом 11 и т. о. фиксирует адрес маршрутизатора, который вернул такой пакет. Последний пакет с достаточным TTL, должен дойти до целевого узла и в ответ придет ICMP reply, таким образом работа программы завершится.

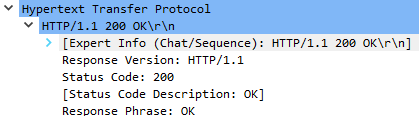


1. **Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться?**

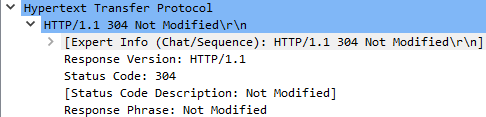
Параметр -d убирает вывод имен сетевых узлов(выводит только ip адреса).

# 3. Анализ HTTP графика

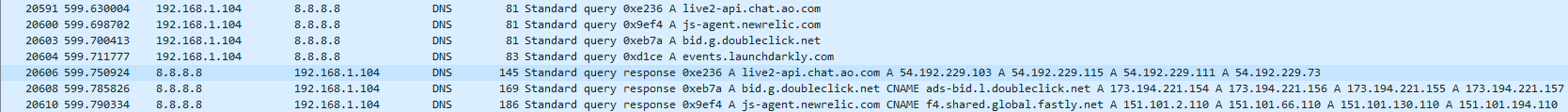
При первичном посещении приходит ответ с кодом 200:



При перезагрузке страницы приходит ответ с кодом 304. Это говорит браузеру о том, что некоторый элемент страницы не изменился:



# 4. Анализ DNS графика



1. **Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?**

Потому что до получения ответа на DNS-запроса адрес посещаемого сайта неизвестен, если сайт не посещался недавно.

1. **Какие бывают типы DNS-запросов?**

Рекурсивный запрос—это запрос, при котором клиент передает задание на поиск IP-адреса серверу.

Итеративный (не рекурсивный) запрос—это запрос, при котором клиент сам совершает опрос DNS-серверов

1. **В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?**

Если эти изображения находятся на сервере с другим доменным именем.

# 5. Анализ ARP графика



1. **Какие МАС-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют?**

Перед тем как передать пакет сетевого уровня через сегмент Ethernet, сетевой стек проверяет кэш ARP, чтобы выяснить, не зарегистрирована ли в нём уже нужная информация об узле-получателе. Если такой записи в кэше ARP нет, то выполняется широковещательный запрос ARP.

Этот запрос имеет следующий смысл: «Кто-нибудь знает физический адрес устройства, обладающего следующим IP-адресом?» Когда получатель с этим IP-адресом примет этот пакет, то должен будет ответить: «Да, это мой IP-адрес. Мой физический адрес следующий: …» После этого отправитель обновит свой кэш ARP и будет способен передать информацию получателю.

1. **Какие МАС-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса?** Что означают эти адреса? Какие устройства они идентифицируют?

MAC-адреса отправителя и получателя. Старшие 3 байта называются OUI (Organizational Unique Identifier) - уникальный идентификатор производителя. Младшие 3 байта называются номером интерфейса, их значение устанавливается на заводе и является уникальным для каждого устройства.

1. **Для чего ARP-запрос содержит IP-адрес источника?**

Для определения находятся ли адреса отправителя и получателя в одной подсети. Если это так, то вызывается протокол ARP и определяется физический адрес получателя, после чего IP-пакет отправляется по указанному физическому адресу, соответствующему IP-адресу назначения. Если нет, то определяется маршрут, и если он найден, то определяется физический адрес соответствующего маршрутизатора, и пакет отправляется по указанному физическому адресу. Если маршрут не найден, вызывается протокол ARP и определяется физический адрес маршрутизатора по умолчанию, после чего пакет оправляется по указанному физическому адресу.