федеральное государственное автономное образовательное учреждение высшего образования

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

**Факультет программной инженерии и компьютерной техники**

**Кафедра информатики и прикладной математики**

**ЛАБОРАТОРНАЯ РАБОТА № 3**

**ПО ДИСЦИПЛИНЕ «СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ»**

Выполнили: Баев Д.В., Съестов Д.В.

Группа: P3317

Преподаватель: Шинкарук Д.Н.

\

Санкт-Петербург

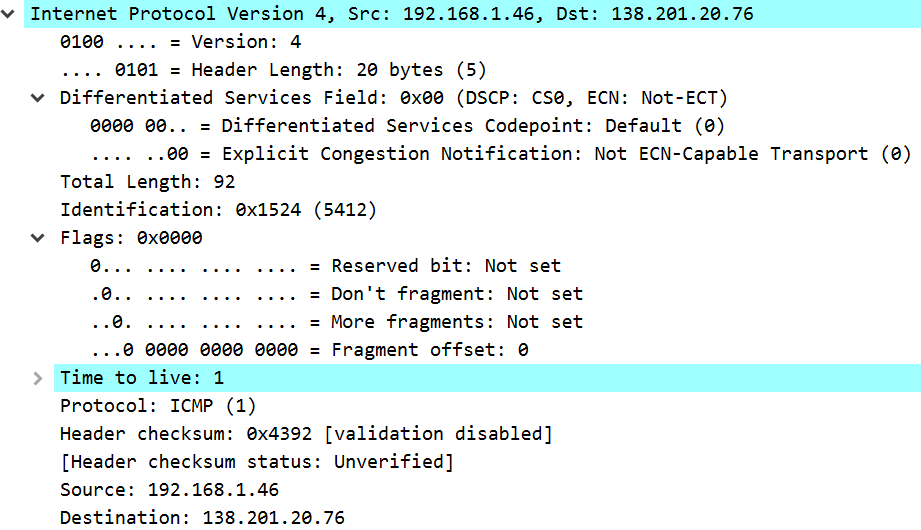
2018/2019

**Цель работы:**

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

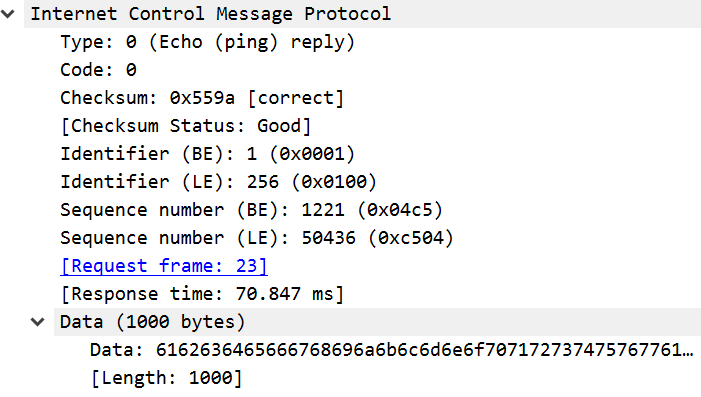
**Структура наблюдаемых PDU:**

**IP-пакет IPv4:**

****

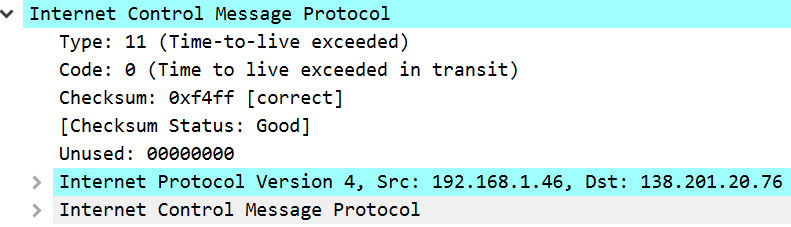
* Версия — для IPv4 значение поля должно быть равно 4.
* IHL — (Internet Header Length) длина заголовка IP-пакета в 32-битных словах (dword). Именно это поле указывает на начало блока данных в пакете. Минимальное корректное значение для этого поля равно 5.
* Длина пакета — (Total Length) длина пакета в [октетах](https://ru.wikipedia.org/wiki/%D0%9E%D0%BA%D1%82%D0%B5%D1%82_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), включая заголовок и данные. Минимальное корректное значение для этого поля равно 20, максимальное — 65 535.
* Идентификатор — (Identification) значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета. Для фрагментированного пакета все фрагменты имеют одинаковый идентификатор.
* 3 бита флагов. Первый бит должен быть всегда равен нулю, второй бит DF (don’t fragment) определяет возможность фрагментации пакета и третий бит MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов.
* Смещение фрагмента — (Fragment Offset) значение, определяющее позицию фрагмента в потоке данных. Смещение задается количеством восьмибайтовых блоков, поэтому это значение требует умножения на 8 для перевода в байты.
* Время жизни ([TTL](https://ru.wikipedia.org/wiki/Time_to_live)) — число маршрутизаторов, которые может пройти этот пакет. При прохождении маршрутизатора это число уменьшается на единицу.
* Протокол — идентификатор интернет-протокола следующего уровня указывает, данные какого протокола содержит пакет, например, TCP, UDP, или ICMP.
* Контрольная сумма заголовка

**ICMP-пакет для эхо-сообщения**



* Тип пакета
* Код пакета
* Контрольная сумма (для проверки целостности данных)
* Идентификатор(для соотнесения эхо-сообщений)
* Номер последовательности(для соотнесения эхо-сообщений)
* Данные

**ICMP-пакет для сообщения о превышении контрольного времени**

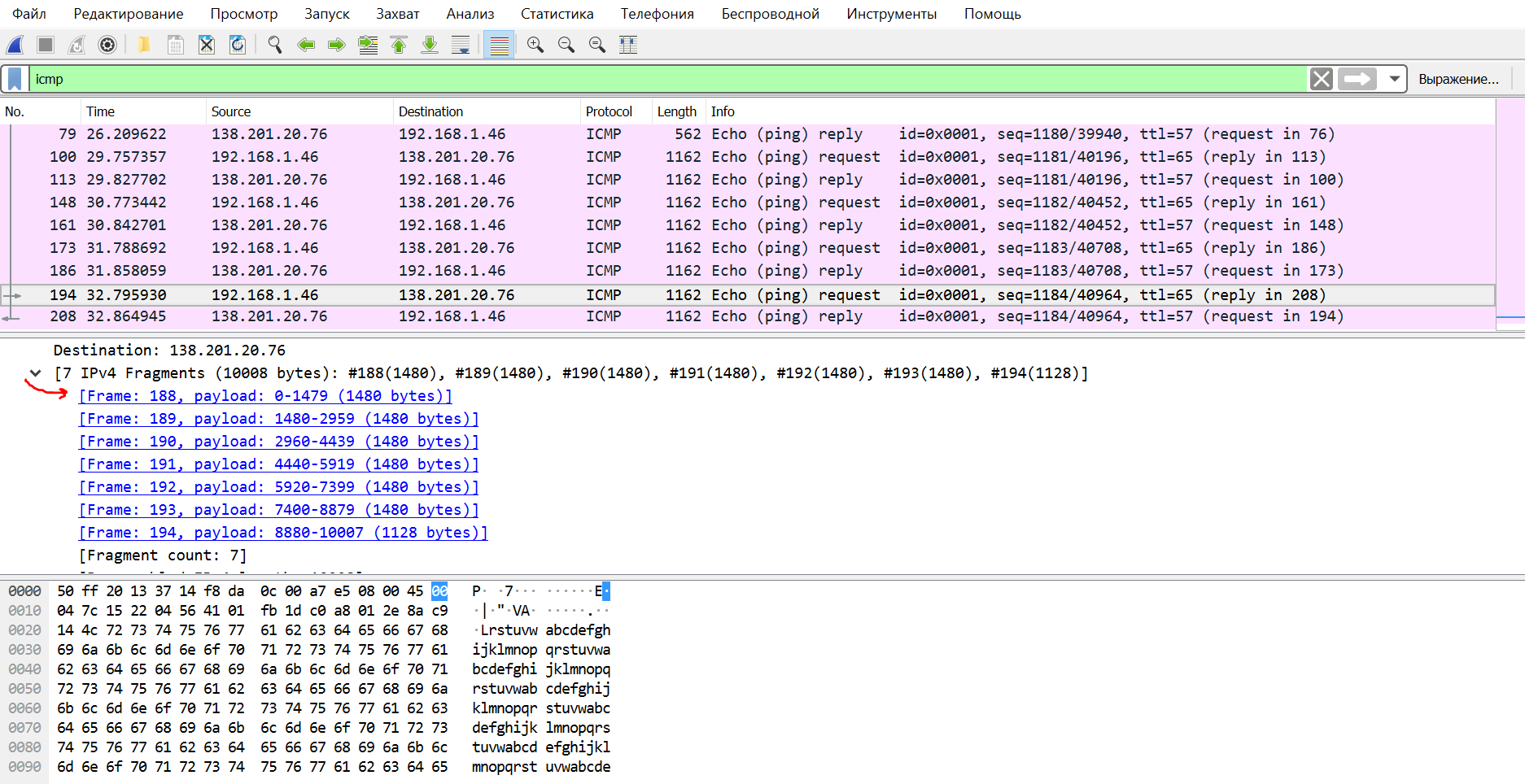


* Тип пакета
* Код пакета
* Контрольная сумма (для проверки целостности данных)
* Информация об исходном пакете

**Ping**

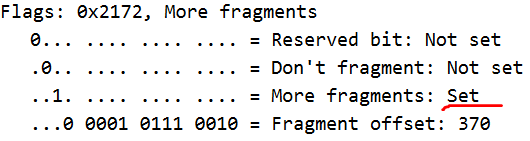
*1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?*

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



*2. 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.

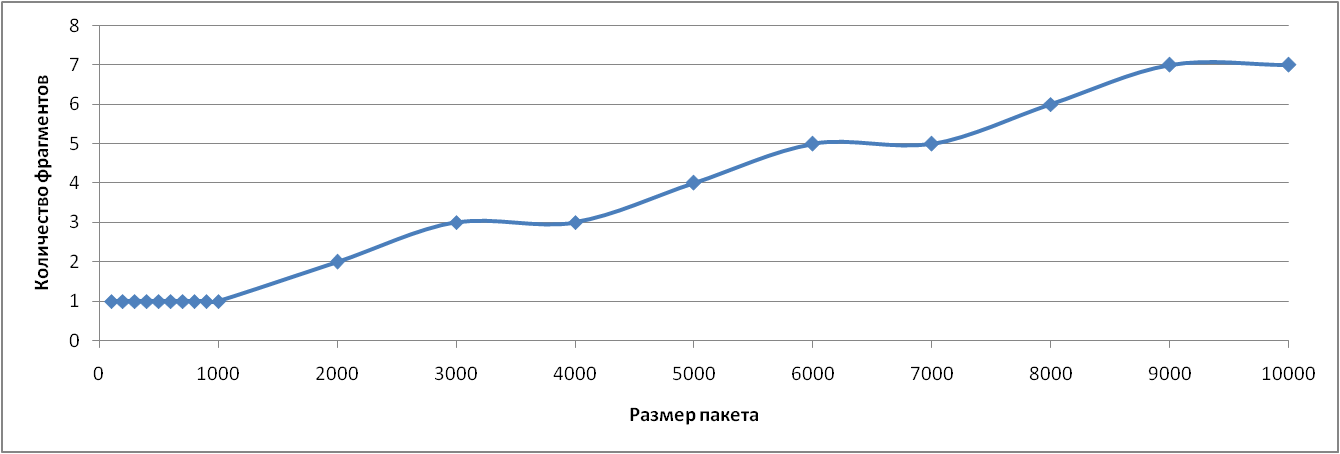


*3. Чему равно количество фрагментов при передаче ping-пакетов?*

MSS (Maximum Segment Size) - значение, которое определяет максимальный размер блока данных в байтах. В нашем 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.



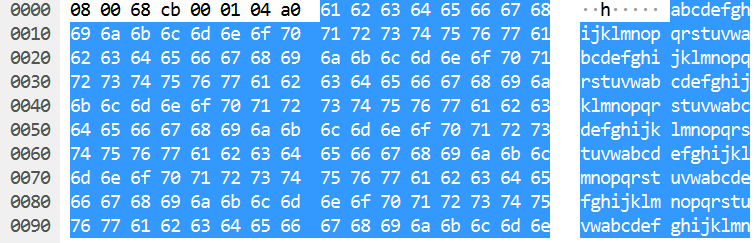
*4. Построить график, в котором на оси абсцисс находится размер пакета, а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет.*

**

*5. Как изменить поле TTL с помощью утилиты ping?*

Указать параметр -i с числовым значением срока жизни пакетов.

*6. 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) .

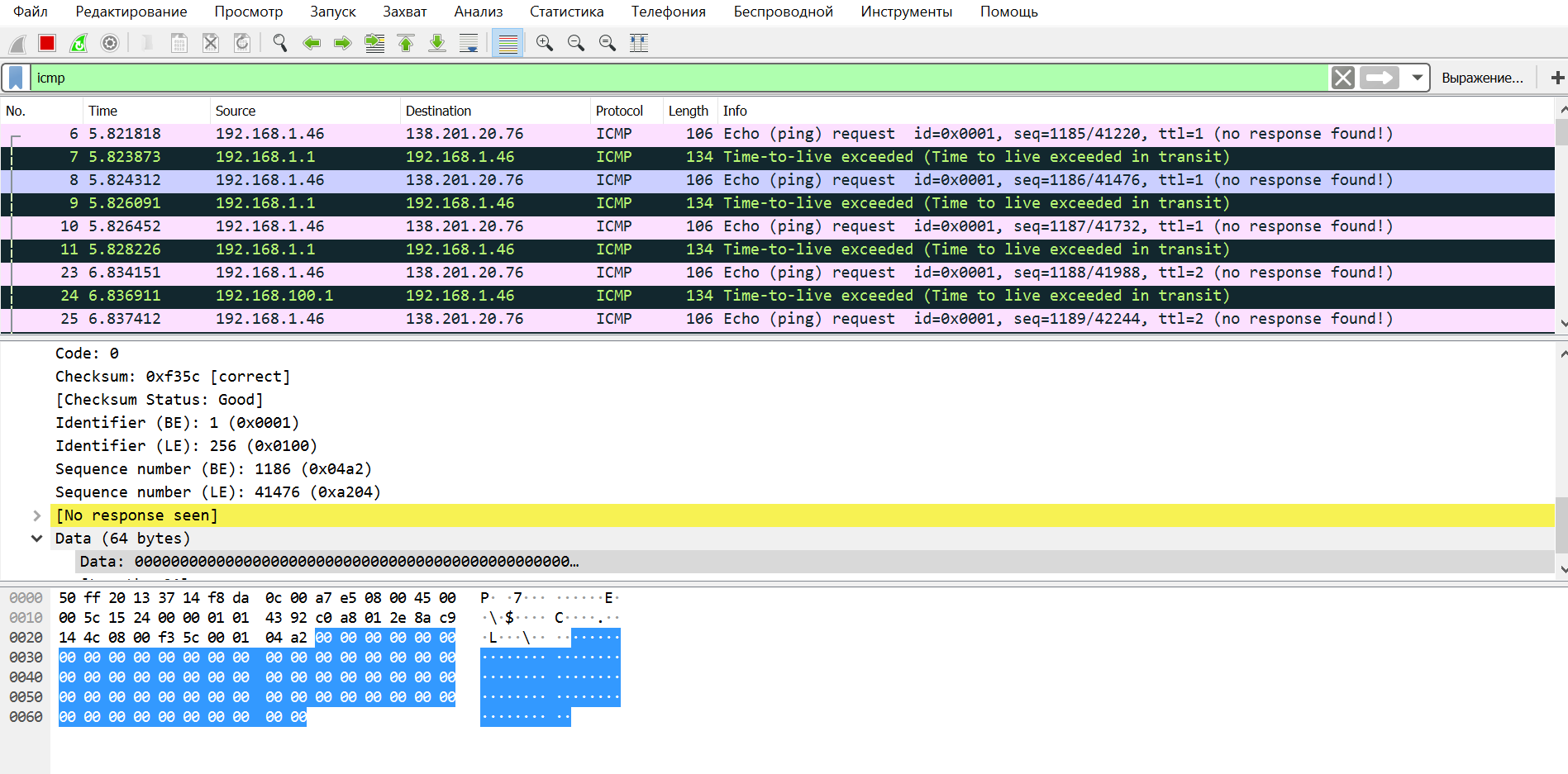
**Tracert**

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

В заголовке IP содержится 20 байт. В поле данных содержится 72 байта icmp-пакета(64 байта данных и 8 байт заголовка).

*2. 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.

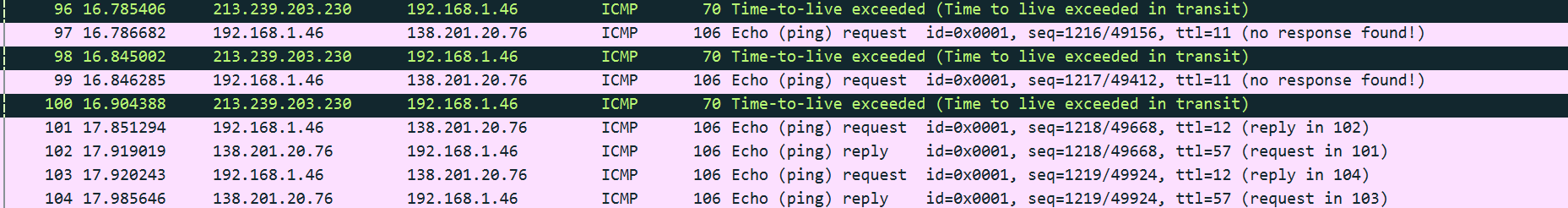


*3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание).*

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 шестнадцатиричной системе).

*4. 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.



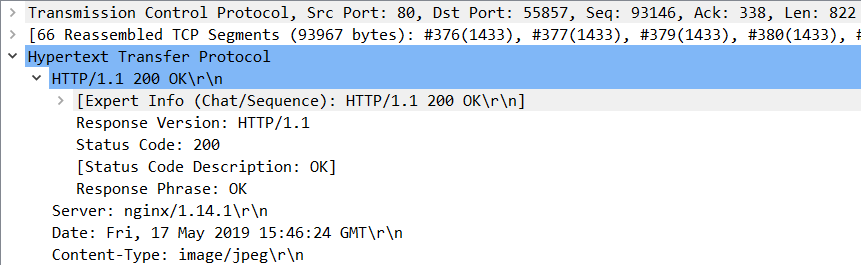
*5. Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться?*

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

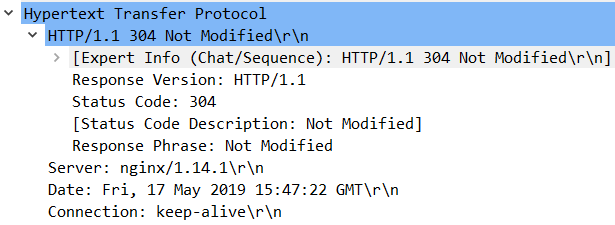
**HTTP**

*По результатам анализа собранной трассы покажите, каким образом протокол HTTP передавал содержимое страницы при первичном посещении страницы и при вторичном запросе-обновлении от браузера (т.е. при различных видах GET-запросов).*

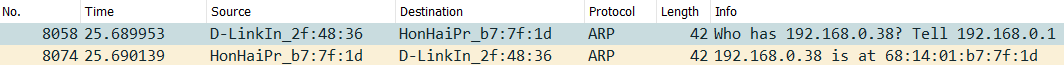
При первичном посещении приходит ответ с кодом 200, в теле которого находится содержимое:



При перезагрузке страницы приходит ответ с кодом 304. Это говорит браузеру о том, что страница не изменилась:



**ARP**



*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.

*2. 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.

*3. 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.

**DNS**

**Изображение выглядит как снимок экрана

Автоматически созданное описание**

*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.

*2. 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

Обратный запрос—это запрос, при котором необходимо по IP адресу вернуть имя домена

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

Если эти изображения находятся на сервере с другим доменным именем.