

Санкт-Петербургский Политехнический Университет Петра Великого  
Институт компьютерных наук и технологий  
Кафедра компьютерных систем и программных технологий

# Защита информации

Отчет по лабораторной работе №1  
Исследование сетевого трафика

Работу выполнил:  
Раскин Андрей  
Группа: 43501/3  
Преподаватель:  
Новопашенный Андрей Гелиевич

Санкт-Петербург  
2017

## 1 Цель работы

Закрепление навыков работы в программе Wireshark и знаний о некоторых сетевых протоколах.

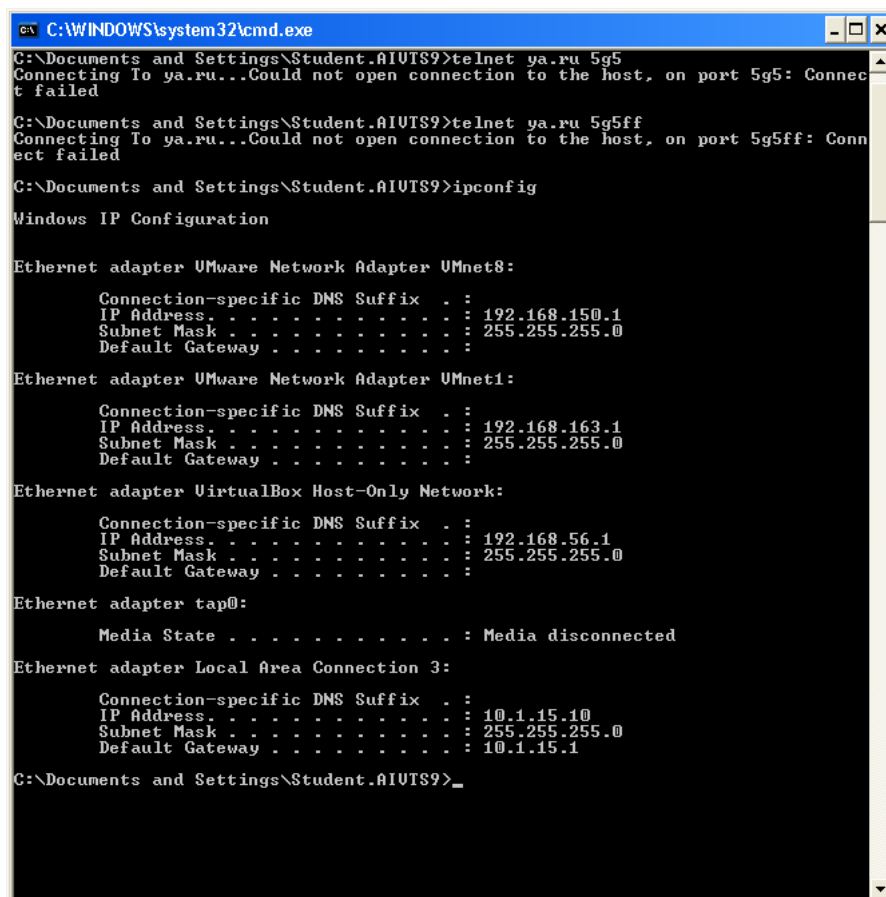
## 2 Программа работы

При помощи анализатора сетевого трафика Wireshark продемонстрировать в сети:

1. Работу утилиты ping
2. Работу утилиты tracert
3. Работу ICMP-протокола в следующих ситуациях:
  - Отправка фрагментированного ping'a,
  - Получение ошибки 3.1 (Destination host unreachable)
4. Работу ARP-протокола (запрос и ответ);
5. Работу протокола TCP в следующих ситуациях:
  - Установка соединения,
  - Разрыв соединения,
  - Попытка соединения на отсутствующий порт

## 3 Конфигурация компьютера в сети

1



```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Student.AIUTS9>telnet ya.ru 5g5
Connecting To ya.ru...Could not open connection to the host, on port 5g5: Connection failed

C:\Documents and Settings\Student.AIUTS9>telnet ya.ru 5g5ff
Connecting To ya.ru...Could not open connection to the host, on port 5g5ff: Connection failed

C:\Documents and Settings\Student.AIUTS9>ipconfig

Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.150.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.163.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.56.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

Ethernet adapter tap0:

    Media State . . . . .             : Media disconnected

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 10.1.15.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 10.1.15.1

C:\Documents and Settings\Student.AIUTS9>_

```

Рис. 1: Конфигурация сети

## 4 Ход работы

### 4.1 Работы утилиты ping

Ping — утилита для проверки целостности и качества соединений в сетях на основе TCP/IP, а также обходное наименование самого запроса. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). По умолчанию производится 4 попытки отправки запроса.

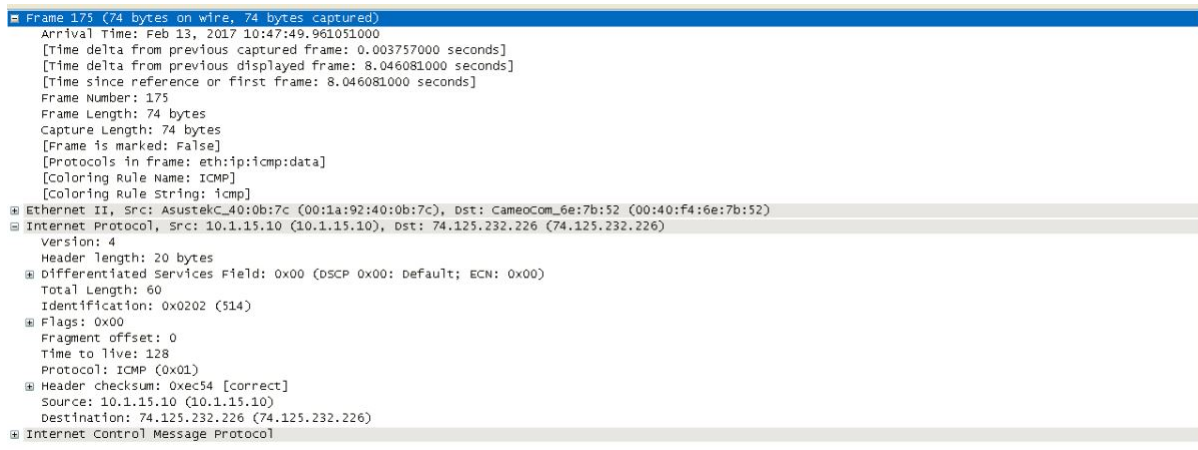


Рис. 2: ICMP эхо запрос

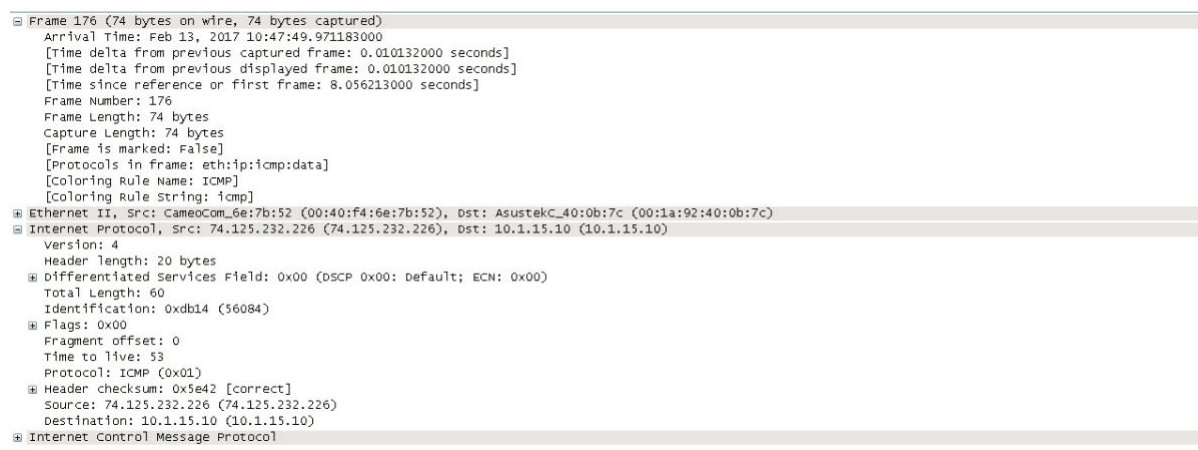


Рис. 3: ICMP эхо ответ

Как видно, в поле Destination указан IP-адрес google.com, поле Source показывает IP-адрес текущего компьютера.

### 4.2 Работа утилиты tracer

В основе работы данной утилиты лежит протокол icmp. Команда TRACERT определяет путь до точки назначения с помощью послыки в точку назначения эхо-сообщений протокола Control Message Protocol (ICMP) с постоянным увеличением значений срока жизни (Time to Live, TTL). Попробуем пронаблюдать трассировку маршрута пакетов до узла spbstu.ru при помощи протокола ICMP и утилиты tracer.

Первый пакет трассировки маршрута отправляется с TTL равным 1. Это значит, что на первом же маршрутизаторе пакет будет уничтожен и нам придет сообщение об ошибке.

В сообщении об ошибке указан тип ICMP-пакета — 11.0, что означает, что время жизни пакета истекло. Сообщение пришло от маршрутизатора сети, который имеет адрес 192.168.1.1. Аналогично продолжается трассировка маршрута дальше с постепенным инкрементом параметра TTL. Таким образом составляется примерный маршрут прохождения IP-пакета до узла с адресом spbstu.ru.

```
C:\Users\Georgiy>tracert spbstu.ru

Трассировка маршрута к spbstu.ru [195.209.230.198]
с максимальным числом прыжков 30:

 1      13 ms      5 ms      6 ms 192.168.1.1
 2      6 ms      6 ms     14 ms 192.168.25.2
 3      3 ms      4 ms      7 ms 1p-1.47.255.92.net.unnet.ru [92.255.47.1]
 4      3 ms     30 ms      5 ms 92.255.2.239
 5      7 ms      6 ms      4 ms 1p-51.97.104.89.net.unnet.ru [89.104.97.51]
 6      3 ms      3 ms      3 ms h16-1-gv.spb.runnet.ru [194.190.255.29]
 7     78 ms     123 ms      5 ms stu.spb.runnet.ru [194.85.36.238]
 8      4 ms      4 ms      6 ms 195.209.230.190
 9      4 ms      3 ms      4 ms cnd.spbstu.ru [195.209.230.198]
```

Рис. 4: Результат трассировки маршрута в консоли

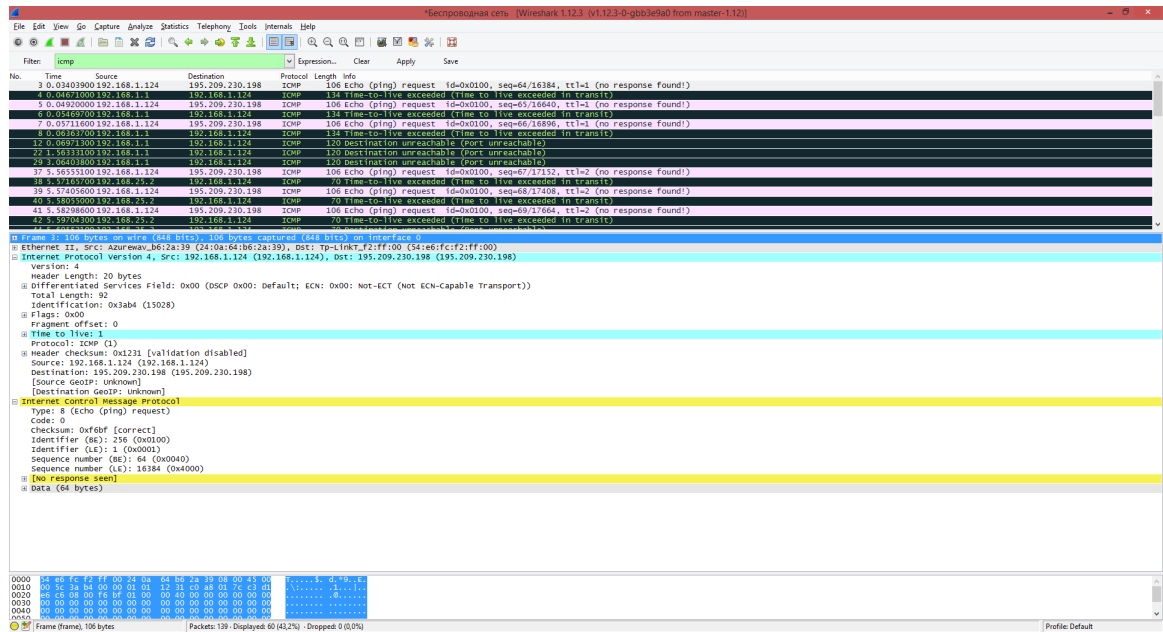


Рис. 5: Первый пакет трассировки маршрута

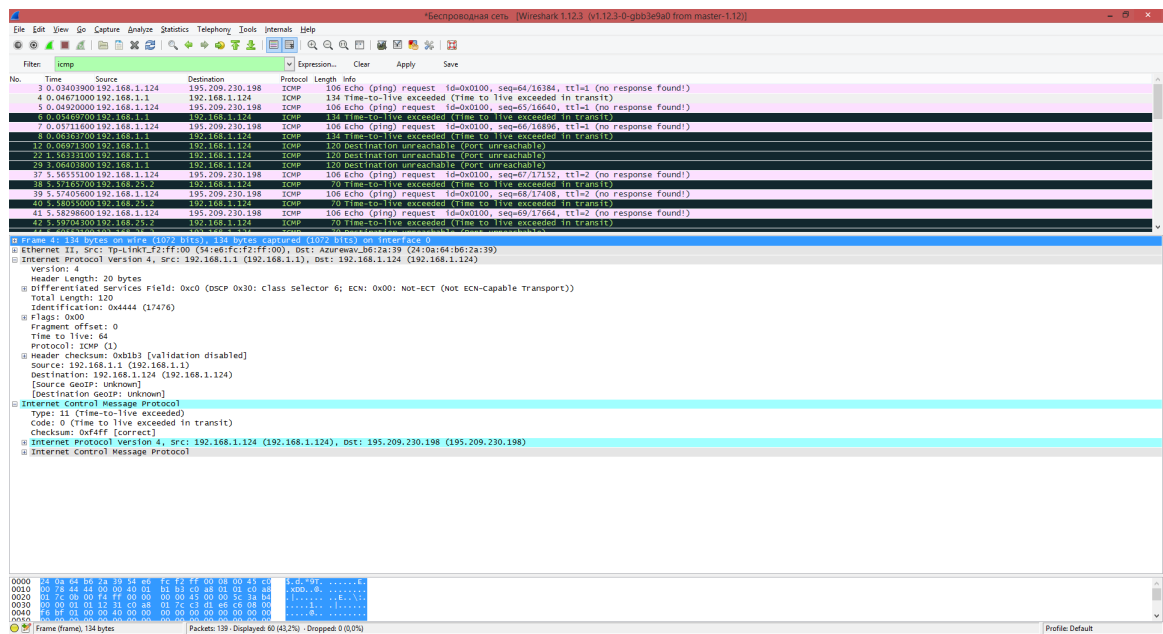


Рис. 6: Ответ на первый пакет трассировки

## 4.3 Протокол ICMP

### 4.3.1 Фрагментированный ping

Попробуем отослать фрагментированный ping-запрос. Данный вид запроса использует ICMP-протокол. Для фрагментации пакета необходимо указать его размер, превышающий MTU (maximum transmission

unit) - максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации. Для протокола Ethernet обычно это чуть больше 1500 байт. Для фрагментации пакета на 3 части укажем размер – 4000 байт.

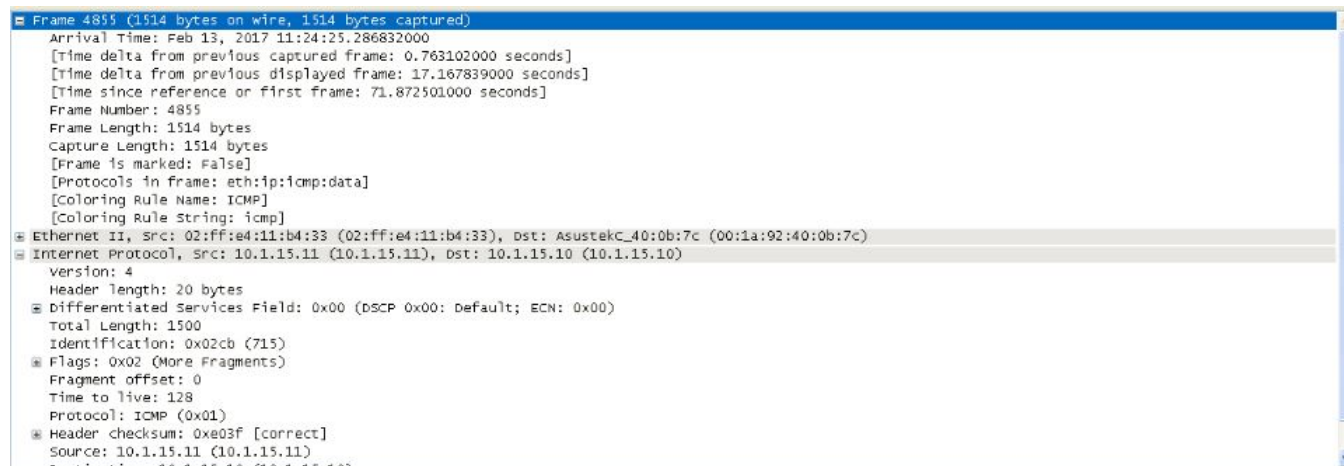


Рис. 7: Ответ на первый пакет трассировки

О фрагментированности пакета свидетельствуют флаги пакета IP (0x01 – имеются еще фрагменты). О том, что это первый пакет из фрагментированных, свидетельствует нулевое смещение фрагмента. При этом во всех трех IP пакетах содержится ICMP-пакет с одним и тем же идентификатором.

#### 4.3.2 Несуществующий хост

Попробуем пронаблюдать ошибку типа 3.1 (целевой узел недостижим). Для этого отправим ping-запрос на адрес, которого не существует. В пакете можно наблюдать типичный ping-запрос (ICMP-пакет типа 8.0).

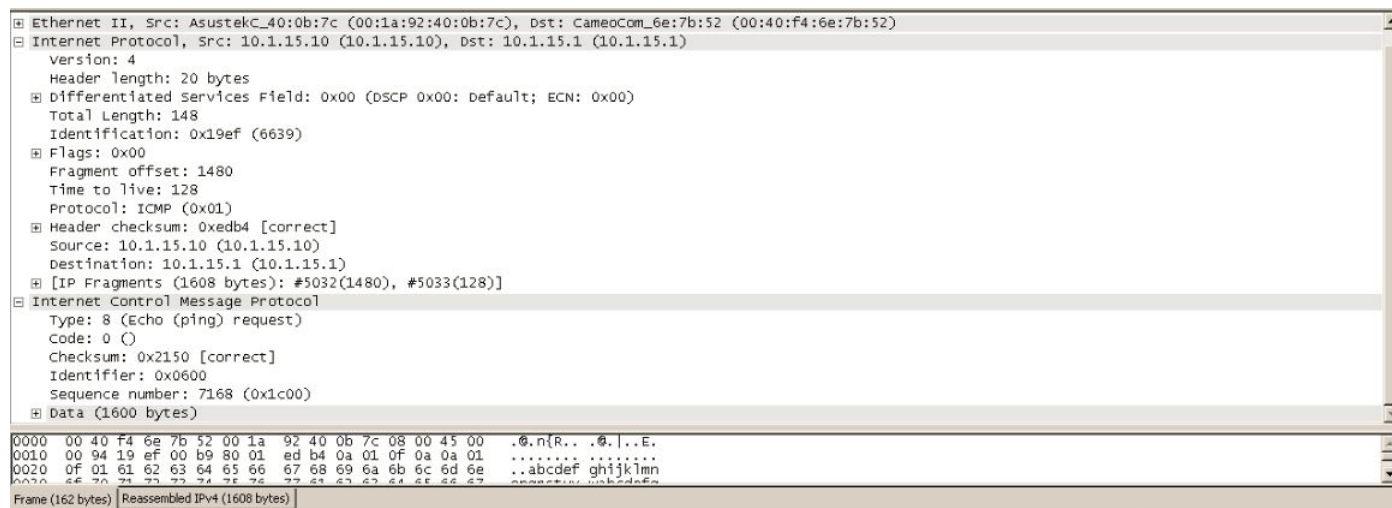


Рис. 8: Ping-запрос

А вот ответом на указанный выше запрос будет ICMP-пакет типа 3.1, свидетельствующий об ошибке «целевой узел недостижим». При этом, в ответе, в качестве данных пакета отправляется заголовок того пакета, на который пришел ответ.

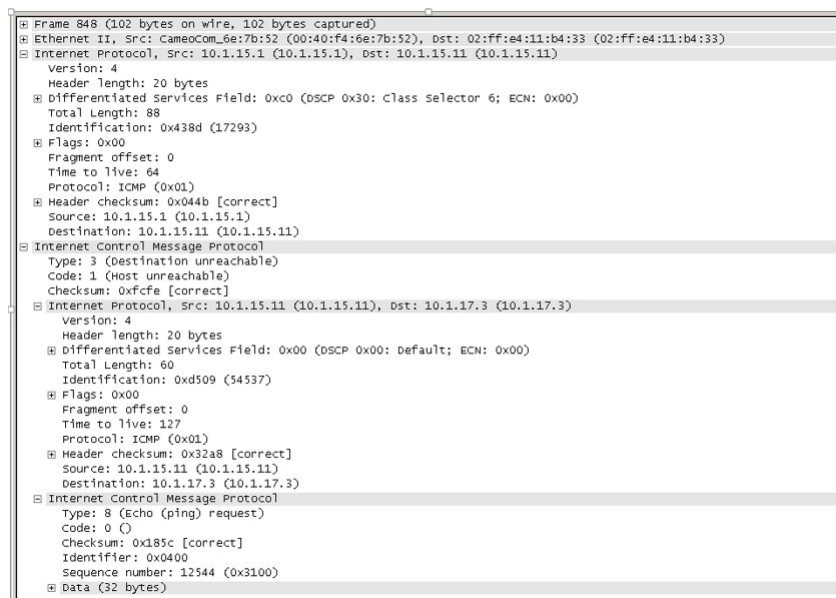


Рис. 9: ICMP-ответ

#### 4.4 ARP протокол

ARP-запрос выполняется по широковещательному адресу (ff:ff:ff:ff:ff:ff), для того, чтобы все узлы сети получили данный пакет. В пакете указывается его тип (поле Opcode) – запрос, а так же целевой IP-адрес для которого запрашивается MAC-адрес. MAC-адрес цели при этом обнулен.

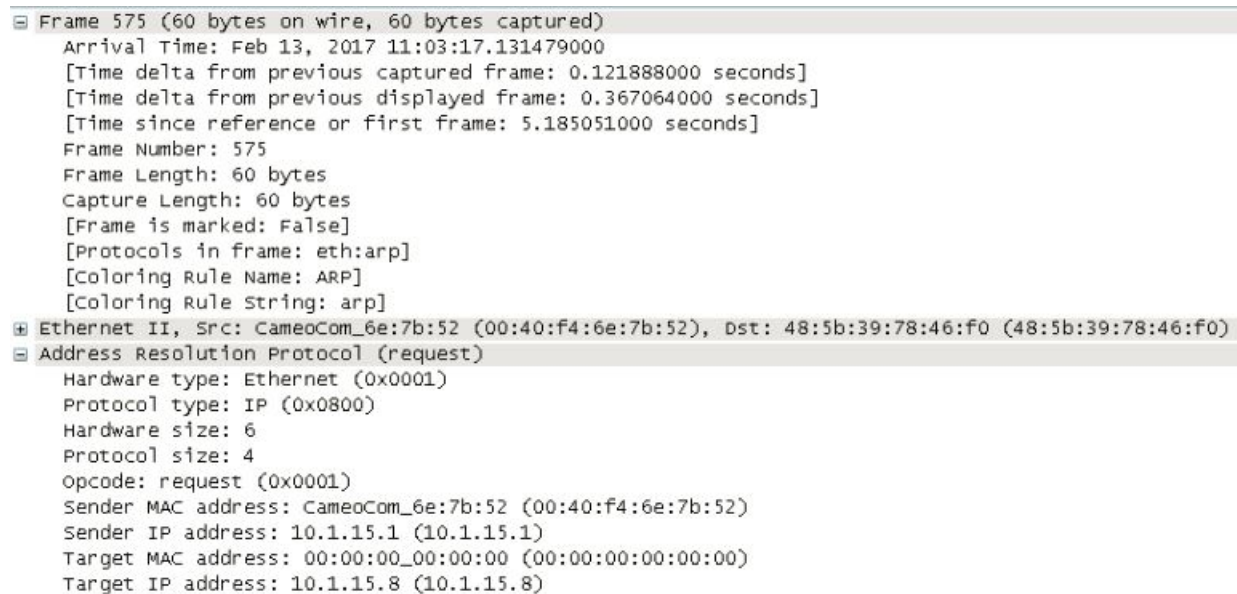


Рис. 10: Часть IP-пакета, содержащего ARP-запрос

ARP-ответ отправляется уже на тот адрес, с которого исходил ARP-запрос. В пакете указывается его тип (поле Opcode) – ответ, а так же заполненный MAC-адрес цели.

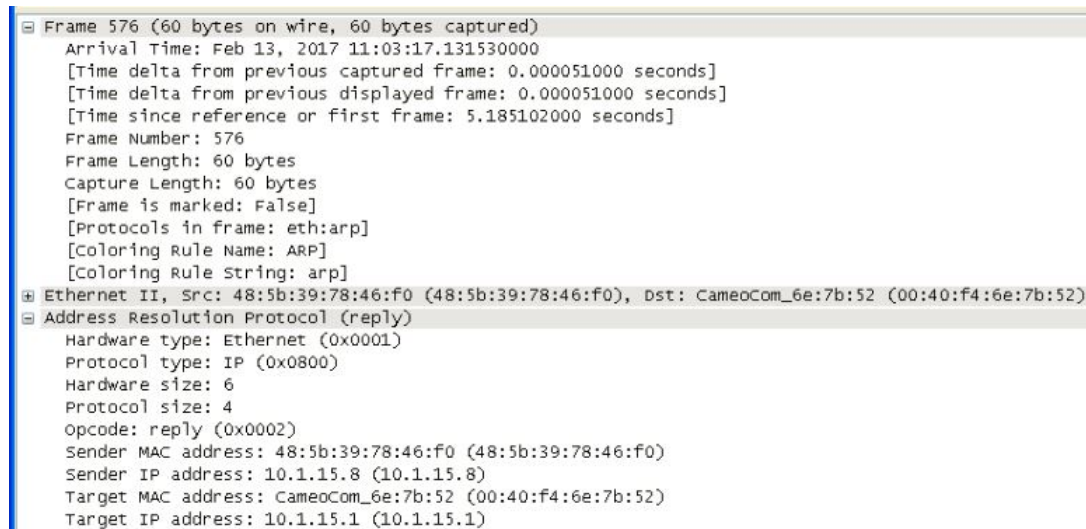


Рис. 11: Часть IP-пакета, содержащего ARP-ответ

## 4.5 TCP-протокол

### 4.5.1 Установление соединения

Эта операция происходит следующим образом: Клиент, посылает серверу сегмент с номером последовательности и флагом SYN. Сервер получает сегмент, запоминает номер последовательности и

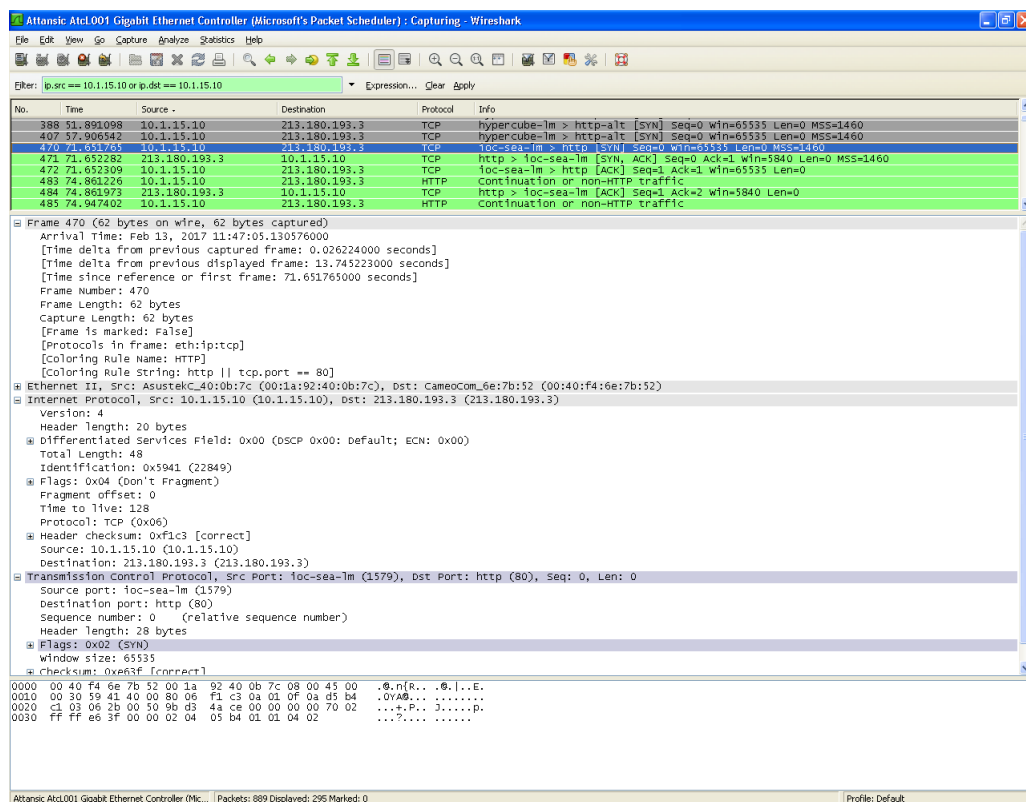


Рис. 12: TCP запрос на установление соединения SYN

посылает клиенту сегмент с номером последовательности и флагами SYN и ACK. Если клиент получает сегмент с флагом SYN, то он запоминает номер последовательности и посылает сегмент с флагом ACK.



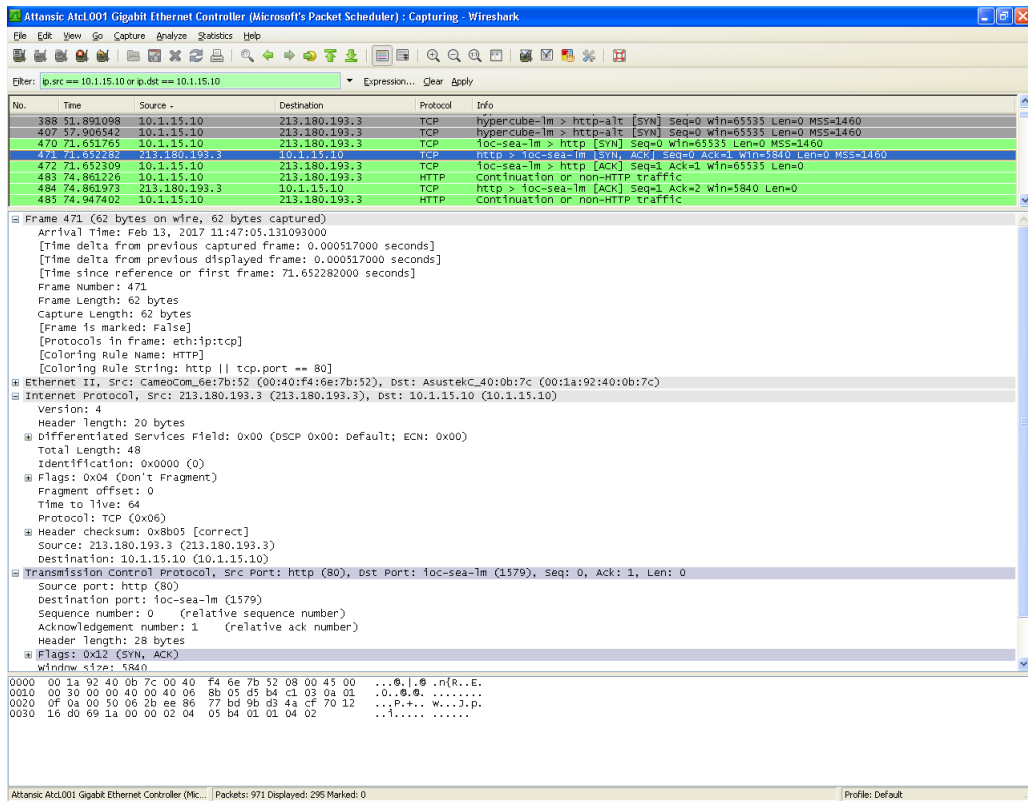


Рис. 13: Ответ сервера на установление TCP-соединения

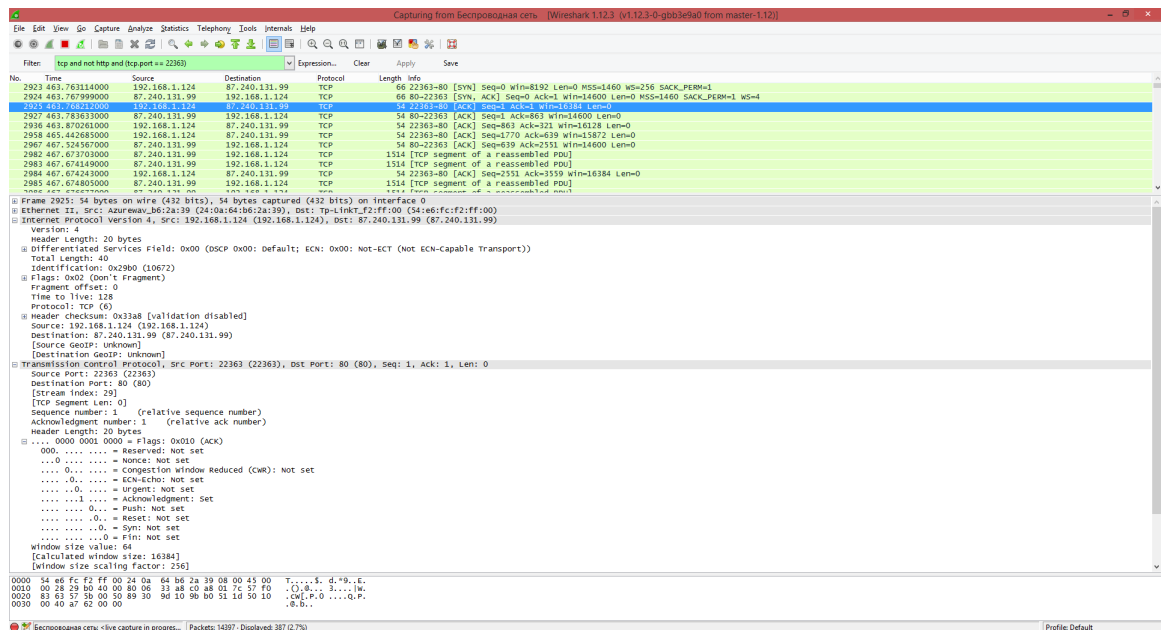


Рис. 14: Подтверждение от клиента о получении ответа

## 4.5.2 Разрыв соединения

При разрыве соединения сервер отправляет клиенту пакет с установленным флагом RST.



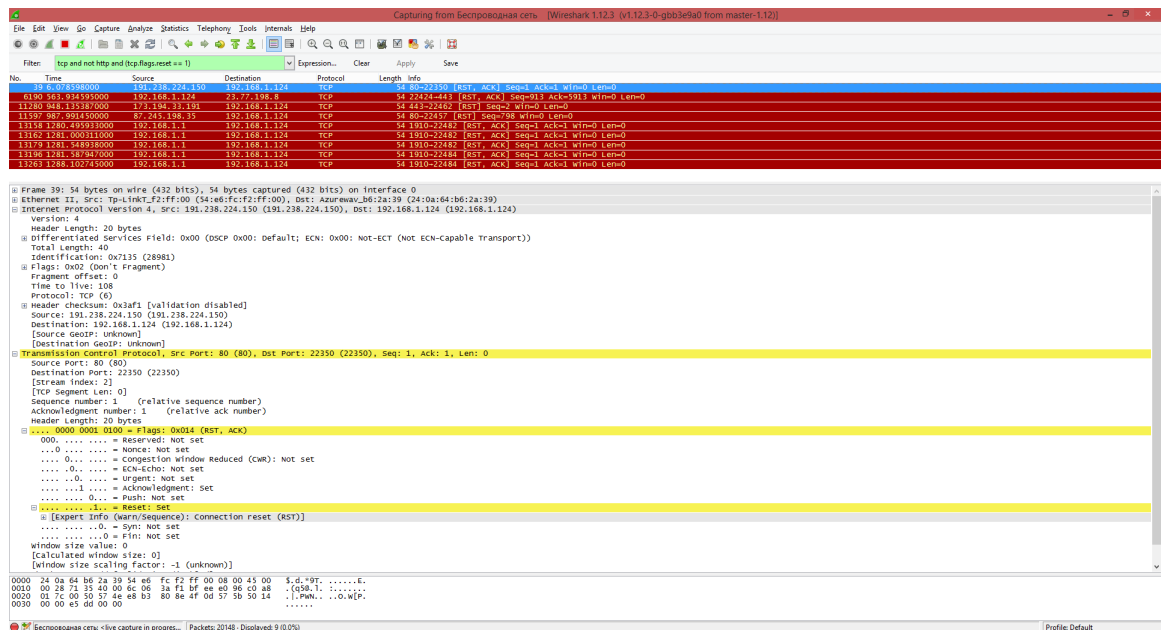


Рис. 15: Пример пакета с флагом RST

### 4.5.3 Установка соединения с отсутствующим портом

При попытке подключения к отсутствующему порту, не приходит ACK и RST, поэтому клиент находится в подвешенном состоянии и ожидает ответа.

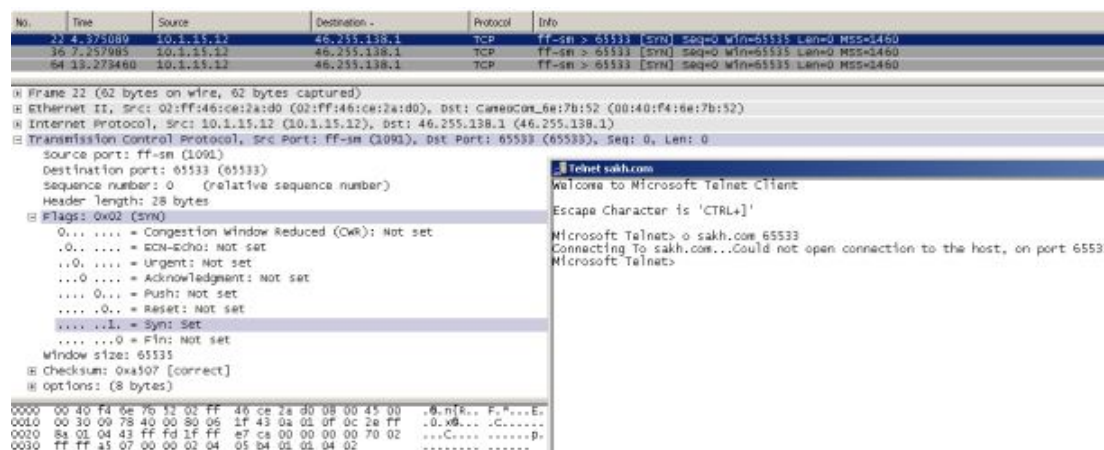


Рис. 16: Пример пакета с подвешенным состоянием

## 5 Выводы

В ходе работы были получены навыки работы в программе WireShark и закреплены знания о сетевых протоколах ARP, ICMP, TCP. Были рассмотрены:

1. работу утилит ping и tracertr;
2. работа ARP-протокола;
3. работа протокола ICMP, включая такие типовые случаи, как: отправка фрагментированного пакета, возникновение ошибки 3.1, трассировка маршрута;
4. установка, разрыв и завершение TCP соединения;