

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ПРОГРАММНЫХ ТЕХНОЛОГИЙ

**Отчёт по лабораторной работе №1**

**Курс: «Защита информации»**

**Тема: «Исследование сетевого трафика»**

Выполнил студент:

Ерниязов Тимур Ертлеуевич

Группа: 43501/3

Проверил:

Новопашенный Андрей Гелиевич

Санкт-Петербург  
2018 г.

# Оглавление

<b>1</b>	<b>Лабораторная работа №1</b>	<b>2</b>
1.1	Цель работы . . . . .	2
1.2	Конфигурация сети . . . . .	2
1.3	Ход работы . . . . .	3
1.3.1	Утилита Ping . . . . .	3
1.3.2	Утилита Tracert . . . . .	10
1.3.3	Протокол ICMP . . . . .	12
1.3.4	Протокол ARP . . . . .	13
1.3.5	Протокол TCP . . . . .	15
1.4	Вывод . . . . .	24

# Лабораторная работа №1

## 1.1 Цель работы

Получение навыков по исследованию сетевого трафика при помощи программы WireShark

## 1.2 Конфигурация сети

```
Настройка протокола IP для Windows

Ethernet adapter Сетевое подключение Bluetooth:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::98dc:a34b:531a:e304%13
    IPv4-адрес. . . . . : 192.168.0.102
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.0.1

Туннельный адаптер isatap.{7E82D5E7-222B-409B-8509-795D76264FD9}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 12:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Туннельный адаптер isatap.{068CDEC0-51A9-44F3-8865-6D5FFB3DF026}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

C:\Users\Lorismelik>
```

Рис. 1.1: Сетевые параметры компьютера

## 1.3 Ход работы

### 1.3.1 Утилита Ping

Утилита Ping отправляет ICMP запрос, после чего, в случае успеха должен прийти эхо-ответ ICMP. Если пакет не пришел за некоторое время, то сервер считается недостижимым. По умолчанию производится четыре попытки.

#### **Ping без фрагментации**

Трафик утилиты Ping со стандартными параметрами.

Пакеты были распознаны как ICMP с пометкой "Echo (ping) reply/request". Поле Destination показывает IP адрес удаленного сервера, который мы пингуем, Source показывает IP адрес текущего компьютера.

Поля "Identifier" и "Sequence number" присутствуют только в эхо запросе/ответе (ICMP типы 0 и 8) и необходимы для сопоставления ответа и запроса.

```

# Frame 369: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  ▸ Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 11, 2018 00:27:18.439122000 Московское время (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1523392038.439122000 seconds
    [Time delta from previous captured frame: 0.003740000 seconds]
    [Time delta from previous displayed frame: 0.004650000 seconds]
    [Time since reference or first frame: 54.291584000 seconds]
    Frame Number: 369
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
  # Destination: 64:70:02:91:26:1c
    Address: 64:70:02:91:26:1c
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0 .... = IG bit: Individual address (unicast)
  # Source: c8:0a:a9:d0:5c:0a
    Address: c8:0a:a9:d0:5c:0a
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0 .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
# Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: google.com (108.177.14.138)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x14dc (5340)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.102 (192.168.0.102)
    Destination: google.com (108.177.14.138)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
# Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d5a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Response frame: 370]
  ▸ Data (32 bytes)

```

Рис. 1.2: ICMP эхо-запрос

```

Frame 370: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 11, 2018 00:27:18.443732000 Московское время (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1523392038.443732000 seconds
    [Time delta from previous captured frame: 0.004610000 seconds]
    [Time delta from previous displayed frame: 0.004610000 seconds]
    [Time since reference or first frame: 54.296194000 seconds]
    Frame Number: 370
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: 64:70:02:91:26:1c, Dst: c8:0a:a9:d0:5c:0a
  Destination: c8:0a:a9:d0:5c:0a
    Address: c8:0a:a9:d0:5c:0a
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  Source: 64:70:02:91:26:1c
    Address: 64:70:02:91:26:1c
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: clients.l.google.com (108.177.14.138), Dst: 192.168.0.102 (192.168.0.102)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0000 (0)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 48
    Protocol: ICMP (1)
    Header checksum: 0x4e78 [validation disabled]
    [Header checksum status: Unverified]
    Source: clients.l.google.com (108.177.14.138)
    Destination: 192.168.0.102 (192.168.0.102)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x555a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Request frame: 369]
  [Response time: 4.610 ms]

```

Рис. 1.3: ICMP эхо-ответ

## Ping с фрагментацией

Для фрагментации пакета необходимо явно указать его размер, превышающий MTU (maximum transmission unit) - максимальный размер полезного блока данных одного пакета, который может быть передан без фрагментации. Установим с помощью флага `-l` увеличенную длину пакета.

Запустим Ping с измененными параметрами (*bytes* = 4096).

Была произведена фрагментация на 3 пакета:

193	6.261297	192.168.0.102	yandex.ru	ICMP	1514 Echo (ping) request id=0x0
194	6.261303	192.168.0.102	yandex.ru	IPv4	1514 Fragmented IP protocol (pro
195	6.261309	192.168.0.102	yandex.ru	IPv4	1178 Fragmented IP protocol (pro
196	6.277587	yandex.ru	192.168.0.102	ICMP	1514 Echo (ping) reply id=0x0
197	6.277707	yandex.ru	192.168.0.102	IPv4	1514 Fragmented IP protocol (pro
198	6.277810	yandex.ru	192.168.0.102	IPv4	1178 Fragmented IP protocol (pro

Рис. 1.4: Последовательность фрагментированных пакетов

```

# Frame 193: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
  ▸ Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 19, 2018 07:38:22.726986000 Московское время (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1524109102.726986000 seconds
    [Time delta from previous captured frame: 0.148920000 seconds]
    [Time delta from previous displayed frame: 0.148920000 seconds]
    [Time since reference or first frame: 6.261297000 seconds]
    Frame Number: 193
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
  ▸ Destination: 64:70:02:91:26:1c
  ▸ Source: c8:0a:a9:d0:5c:0a
    Type: IPv4 (0x0800)
# Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: yandex.ru (77.88.55.66)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x0685 (1669)
  # Flags: 0x01 (More Fragments)
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.102 (192.168.0.102)
    Destination: yandex.ru (77.88.55.66)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
# Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x9f99 [unverified] [fragmented datagram]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 12 (0x000c)
  Sequence number (LE): 3072 (0x0c00)
  [Response frame: 196]
# Data (1472 bytes)
  Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
  [Length: 1472]

```

Рис. 1.5: Фрагментированный эхо-запрос (первый фрагмент)



```

  Frame 194: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
    Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 19, 2018 07:38:22.726992000 Московское время (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1524109102.726992000 seconds
    [Time delta from previous captured frame: 0.000006000 seconds]
    [Time delta from previous displayed frame: 0.000006000 seconds]
    [Time since reference or first frame: 6.261303000 seconds]
    Frame Number: 194
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
  Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
    Destination: 64:70:02:91:26:1c
    Source: c8:0a:a9:d0:5c:0a
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: yandex.ru (77.88.55.66)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0x0685 (1669)
  Flags: 0x01 (More Fragments)
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.102 (192.168.0.102)
    Destination: yandex.ru (77.88.55.66)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  Data (1480 bytes)
    Data: 61626364656666768696a6b6c6d6e6f707172737475767761...
    [Length: 1480]

```

Рис. 1.6: Фрагментированный эхо-запрос (второй фрагмент)

```

4 Frame 195: 1178 bytes on wire (9424 bits), 1178 bytes captured (9424 bits) on interface 0
  ▸ Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 19, 2018 07:38:22.726998000 Московское время (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1524109102.726998000 seconds
    [Time delta from previous captured frame: 0.000006000 seconds]
    [Time delta from previous displayed frame: 0.000006000 seconds]
    [Time since reference or first frame: 6.261309000 seconds]
    Frame Number: 195
    Frame Length: 1178 bytes (9424 bits)
    Capture Length: 1178 bytes (9424 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
4 Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
  ▸ Destination: 64:70:02:91:26:1c
  ▸ Source: c8:0a:a9:d0:5c:0a
    Type: IPv4 (0x0800)
4 Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: yandex.ru (77.88.55.66)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  4 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1164
  Identification: 0x0685 (1669)
  4 Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 2960
  Time to live: 128
  Protocol: ICMP (1)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.102 (192.168.0.102)
  Destination: yandex.ru (77.88.55.66)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
4 Data (1144 bytes)
  Data: 696a6b6c6d6e6f7071727374757677616263646566676869...
  [Length: 1144]

```

Рис. 1.7: Фрагментированный эхо-запрос (последний фрагмент)

### 1.3.2 Утилита Tracert

Tracert базируется на использовании поля TTL протокола ICMP. Первый пакет имеет TTL=1, для каждого последующего пакета TTL инкрементируется. Это продолжается до тех пор пока не придет эхо-ответ, а не ошибка истечения TTL. Трафик tracert это набор ICMP пакетов с типом "Time-to-live exceeded"(код 0x11) и в случае успеха, последний успешный эхо-ответ.

```
Encapsulation type: Ethernet (1)
Arrival Time: Apr 11, 2018 00:51:52.256742000 Московское время (зима)
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1523393512.256742000 seconds
[Time delta from previous captured frame: 0.005985000 seconds]
[Time delta from previous displayed frame: 0.006873000 seconds]
[Time since reference or first frame: 0.554910000 seconds]
Frame Number: 6
Frame Length: 106 bytes (848 bits)
Capture Length: 106 bytes (848 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
  # Destination: 64:70:02:91:26:1c
    Address: 64:70:02:91:26:1c
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  # Source: c8:0a:a9:d0:5c:0a
    Address: c8:0a:a9:d0:5c:0a
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
# Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: yandex.ru (77.88.55.88)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0x4459 (17497)
  ▸ Flags: 0x00
  Fragment offset: 0
  ▸ Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.102 (192.168.0.102)
  Destination: yandex.ru (77.88.55.88)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
# Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7ed [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 17 (0x0011)
  Sequence number (LE): 4352 (0x1100)
# [No response seen]
  ▸ [Expert Info (Warning/Sequence): No response seen to ICMP request]
  ▸ Data (64 bytes)
```

Рис. 1.8: Процесс трассировки yandex.ru (первый ICMP эхо-запрос)

Видно, что первый эхо-запрос имеет TTL равный единице, это означает, что на первом же маршрутизаторе, проверяющем значение TTL пакет будет уничтожен и вернется сообщение об ошибке.

Как и ожидалось, первая остановка это сетевой шлюз. В этом узле TTL стало равным нулю и был отправлен ICMP пакет с ошибкой типа "Time-to-live exceeded".

```

# Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.102 (192.168.0.102)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
# Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 120
  Identification: 0x47b5 (18357)
# Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: ICMP (1)
  Header checksum: 0xb058 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.1 (192.168.0.1)
  Destination: 192.168.0.102 (192.168.0.102)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
# Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  [Checksum Status: Good]
# Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: yandex.ru (77.88.55.66)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
# Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 92
  Identification: 0x33ce (13262)
# Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x402b [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.102 (192.168.0.102)
  Destination: yandex.ru (77.88.55.66)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
# Internet Control Message Protocol

```

Рис. 1.9: Процесс трассировки yandex.ru (сообщение об ошибке Time-to-live exceeded)

### 1.3.3 Протокол ICMP

ICMP ошибка о недоступности хоста (host unreachable) отправляется маршрутизатором, когда он получает IP датаграмму, которую невозможно перенаправить. Данная ошибка была получена в лаборатории.

```
Настройка протокола IP для Windows

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . : icc.spbstu.ru
Локальный IPv6-адрес канала . . . . : fe80::ad49:7421:c409:5d3%13
IPv4-адрес. . . . . : 10.1.99.121
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 10.1.99.1
```

Рис. 1.10: Конфигурация системы в лаборатории

В результате, на каждый посылаемый ICMP эхо запрос, вернулись ICMP пакеты с ошибкой "Destination unreachable (Host unreachable)" с типом 0x3 и кодом 0x1. Особенностью данной ошибки является то, что она посылается от плюза, а не от узла назначения.

No.	Time	Source	Destination	Protocol	Length	Info
18102	273.587699	10.1.99.121	10.1.17.2	ICMP	74	Echo (ping) request id=0x0001, seq=484/58369,
18115	276.588718	10.1.99.1	10.1.99.121	ICMP	102	Destination unreachable (Host unreachable)

Рис. 1.11: Запрос недостижимого хоста

```
> Frame 18102: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: HewlettP_06:90:84 (40:a8:f0:06:90:84), Dst: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52)
> Internet Protocol Version 4, Src: 10.1.99.121, Dst: 10.1.17.2
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4b77 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 484 (0x01e4)
  Sequence number (LE): 58369 (0xe401)
> [No response seen]
> Data (32 bytes)
```

Рис. 1.12: ICMP запрос

```
> Frame 18115: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52), Dst: HewlettP_06:90:84 (40:a8:f0:06:90:84)
> Internet Protocol Version 4, Src: 10.1.99.1, Dst: 10.1.99.121
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 1 (Host unreachable)
  Checksum: 0xfcf6 [correct]
  [Checksum Status: Good]
  Unused: 00000000
> Internet Protocol Version 4, Src: 10.1.99.121, Dst: 10.1.17.2
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4b77 [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 484 (0x01e4)
```

Рис. 1.13: Ответ с ошибкой Host unreachable

### 1.3.4 Протокол ARP

Рассмотрим пару ARP пакетов, которая демонстрирует работу протокола.

```

# Frame 63: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  ▸ Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 11, 2018 01:39:15.611018000 Московское время (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1523396355.611018000 seconds
    [Time delta from previous captured frame: 0.093517000 seconds]
    [Time delta from previous displayed frame: 0.508052000 seconds]
    [Time since reference or first frame: 15.345170000 seconds]
    Frame Number: 63
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: ff:ff:ff:ff:ff:ff
  # Destination: ff:ff:ff:ff:ff:ff
    Address: ff:ff:ff:ff:ff:ff
    .... ..1. .... .. = LG bit: Locally administered address (this is NO
    .... ..1 .... .. = IG bit: Group address (multicast/broadcast)
  # Source: c8:0a:a9:d0:5c:0a
    Address: c8:0a:a9:d0:5c:0a
    .... ..0. .... .. = LG bit: Globally unique address (factory default
    .... ..0 .... .. = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
# Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: c8:0a:a9:d0:5c:0a
  Sender IP address: 192.168.0.102 (192.168.0.102)
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.0.101 (192.168.0.101)
```

Рис. 1.14: ARP запрос

Был отправлен широковещательный ARP запрос с заданным полем IP адресом и нулевым полем "Target MAC Address".

На запрос получен ARP ответ, в котором поле "Sender MAC Address" содержит искомый MAC адрес. Тип ARP пакета указывается в поле Opcode (запрос 0x1, ответ 0x2).



```

# Frame 65: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
  ▸ Interface id: 0 (\Device\NPF_{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 11, 2018 01:39:15.638426000 Московское время (зима)
      [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1523396355.638426000 seconds
      [Time delta from previous captured frame: 0.021103000 seconds]
      [Time delta from previous displayed frame: 0.027408000 seconds]
      [Time since reference or first frame: 15.372578000 seconds]
    Frame Number: 65
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
# Ethernet II, Src: 40:b8:37:d4:d2:f7, Dst: c8:0a:a9:d0:5c:0a
  # Destination: c8:0a:a9:d0:5c:0a
    Address: c8:0a:a9:d0:5c:0a
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0. .... = IG bit: Individual address (unicast)
  # Source: 40:b8:37:d4:d2:f7
    Address: 40:b8:37:d4:d2:f7
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0. .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 0000000000000000000000000000000000000000
# Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: 40:b8:37:d4:d2:f7
  Sender IP address: 192.168.0.101 (192.168.0.101)
  Target MAC address: c8:0a:a9:d0:5c:0a
  Target IP address: 192.168.0.102 (192.168.0.102)

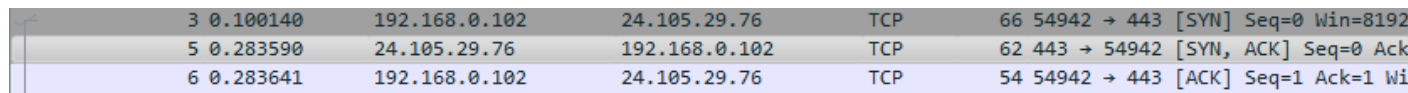
```

Рис. 1.15: ARP ответ

### 1.3.5 Протокол TCP

#### Установление соединения

Попробуем установить TCP соединение с помощью утилиты telnet.



3	0.100140	192.168.0.102	24.105.29.76	TCP	66	54942 → 443	[SYN] Seq=0 Win=8192
5	0.283590	24.105.29.76	192.168.0.102	TCP	62	443 → 54942	[SYN, ACK] Seq=0 Ack=
6	0.283641	192.168.0.102	24.105.29.76	TCP	54	54942 → 443	[ACK] Seq=1 Ack=1 Wi

Рис. 1.16: TCP запрос на установление соединения SYN

Для установления соединения посылается TCP пакет с управляющим битом SYN (синхронизация номеров последовательности) и номером последовательности. Сервер получает сегмент, запоминает номер последовательности и пытается создать сокет для обслуживания нового клиента. В случае успеха сервер посылает клиенту сегмент с номером последовательности и флагами SYN и ACK. В случае неудачи сервер посылает клиенту сегмент с флагом RST.

В данном случае на сервер был отправлен пакет с флагом SYN и ISN=0. Был получен пакет с установленным флагом ACK и номером последовательности ACK=1, что означает, что пакет с ISN=0 был успешно получен. Также в этом пакете установлен флаг SYN и ISN=0, что означает, что ожидается ACK со стороны клиента. Последний пакет содержит только ACK=1 для сервера.



```

# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
# Destination: 64:70:02:91:26:1c
  Address: 64:70:02:91:26:1c
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
# Source: c8:0a:a9:d0:5c:0a
  Address: c8:0a:a9:d0:5c:0a
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
# Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: 24.105.29.76 (24.105.29.76)
  0100 .... = Version: 4
  ....0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x76f4 (30452)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.102 (192.168.0.102)
    Destination: 24.105.29.76 (24.105.29.76)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
# Transmission Control Protocol, Src Port: 54942, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 54942
  Destination Port: 443
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0xf6e9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  # Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP)
    ▸ TCP Option - Maximum segment size: 1460 bytes
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Window scale: 8 (multiply by 256)
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - SACK permitted

```

Рис. 1.17: Запрос на установку TCP соединения

```

└─ Ethernet II, Src: 64:70:02:91:26:1c, Dst: c8:0a:a9:d0:5c:0a
  └─ Destination: c8:0a:a9:d0:5c:0a
    Address: c8:0a:a9:d0:5c:0a
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  └─ Source: 64:70:02:91:26:1c
    Address: 64:70:02:91:26:1c
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
└─ Internet Protocol Version 4, Src: 24.105.29.76 (24.105.29.76), Dst: 192.168.0.102 (192.168.0.102)
└─ Transmission Control Protocol, Src Port: 443, Dst Port: 54942, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 54942
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  0111 .... = Header Length: 28 bytes (7)
└─ Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... 0... = ECN-Echo: Not set
  .... 0... = Urgent: Not set
  .... 1... = Acknowledgment: Set
  .... 0... = Push: Not set
  .... 0... = Reset: Not set
└─ .... 1. = Syn: Set
  └─ [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 443]
    [Connection establish acknowledge (SYN+ACK): server port 443]
    [Severity level: Chat]
    [Group: Sequence]
    .... 0 = Fin: Not set
    [TCP Flags: .....A..S.]
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x3cb8 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
└─ Options: (8 bytes), Maximum segment size, SACK permitted, End of Option List (EOL)
  └─ TCP Option - Maximum segment size: 1460 bytes
  └─ TCP Option - SACK permitted
  └─ TCP Option - End of Option List (EOL)
└─ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 3]
  [The RTT to ACK the segment was: 0.183450000 seconds]
  [iRTT: 0.183501000 seconds]

```

Рис. 1.18: Удачная установка TCP соединения (ответ с сервера)

Ответ содержит установленные биты SYN и ACK, что свидетельствует об успешной установке соединения.

```

# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
# Destination: 64:70:02:91:26:1c
  Address: 64:70:02:91:26:1c
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
# Source: c8:0a:a9:d0:5c:0a
  Address: c8:0a:a9:d0:5c:0a
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
# Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: 24.105.29.76 (24.105.29.76)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x76f5 (30453)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.102 (192.168.0.102)
    Destination: 24.105.29.76 (24.105.29.76)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
# Transmission Control Protocol, Src Port: 54942, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 54942
  Destination Port: 443
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
# Flags: 0x010 (ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....A....]
  Window size value: 64240
  [Calculated window size: 64240]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0xf6dd [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
```

Рис. 1.19: Удачная установка TCP соединения (последний ACK)

Последний этап это отправка на сервер пакета с установленным флагом ACK.

### Неудачное соединение

Рассмотрим попытку неудачного соединения. Клиент посылает пакет с управляющим битом SYN (запрос на установление соединения рассмотрен в предыдущем пункте).

Сервер посылает пакет с установленным управляющим битом RST. После чего клиент уже не пытается установить соединение.

```

Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 192.168.0.102 (192.168.0.102)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xb8e1 (47329)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xffcf [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.104 (192.168.0.104)
    Destination: 192.168.0.102 (192.168.0.102)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 55255, Seq: 1, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 55255
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
  ▸ .... .... .1.. = Reset: Set
    ▸ [Expert Info (Warning/Sequence): Connection reset (RST)]
      [Connection reset (RST)]
      [Severity level: Warning]
      [Group: Sequence]
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: .....A·R··]
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5d60 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 6]
    [The RTT to ACK the segment was: 0.051542000 seconds]
    [iRTT: 0.051542000 seconds]

```

Рис. 1.20: Неудачная попытка TCP соединения

## Завершение соединения

Данный опыт был проведен с конфигурацией:

```

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::98dc:a34b:531a:e304%13
    IPv4-адрес . . . . . : 192.168.0.105
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 192.168.0.1

Туннельный адаптер isatap.{068CDEC0-51A9-44F3-8865-6D5FFB3DFA26}:

    Состояние среды . . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

Туннельный адаптер Подключение по локальной сети* 12:

    Состояние среды . . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

Туннельный адаптер isatap.{7E82D5E7-222B-409B-8509-795D76264FD9}:

    Состояние среды . . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

```

Рис. 1.21: Сетевые параметры

Рассмотрим процесс завершения соединения:

290	58.534488	192.168.0.105	tiger.ftk.spbstu.ru	TCP	54 61030 → 80 [FIN, ACK] Seq=25
291	58.536389	tiger.ftk.spbstu.ru	192.168.0.105	TCP	60 80 → 61030 [FIN, ACK] Seq=25
292	58.536407	192.168.0.105	tiger.ftk.spbstu.ru	TCP	54 61030 → 80 [ACK] Seq=25

Рис. 1.22: Последовательность пакетов при завершении TCP соединения

```

Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
  Destination: 64:70:02:91:26:1c
  Source: c8:0a:a9:d0:5c:0a
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.105 (192.168.0.105), Dst: tiger.ftk.spbstu.ru (194.190.225.54)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x50a1 (20641)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.105 (192.168.0.105)
  Destination: tiger.ftk.spbstu.ru (194.190.225.54)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 61030, Dst Port: 80, Seq: 24, Ack: 1, Len: 0
  Source Port: 61030
  Destination Port: 80
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 24 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x011 (FIN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...1 = Fin: Set
    ▸ [Expert Info (Chat/Sequence): Connection finish (FIN)]
    [TCP Flags: .....A....F]
  Window size value: 258
  [Calculated window size: 66048]
  [Window size scaling factor: 256]
  Checksum: 0x6521 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0

```

Рис. 1.23: Посылка FIN

```

# Ethernet II, Src: 64:70:02:91:26:1c, Dst: c8:0a:a9:d0:5c:0a
  > Destination: c8:0a:a9:d0:5c:0a
  > Source: 64:70:02:91:26:1c
    Type: IPv4 (0x0800)
    Padding: 000000000000
# Internet Protocol Version 4, Src: tiger.ftk.spbstu.ru (194.190.225.54), Dst: 192.168.0.105 (192.168.0.105)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x3dcb (15819)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 54
    Protocol: TCP (6)
    Header checksum: 0xa1fe [validation disabled]
    [Header checksum status: Unverified]
    Source: tiger.ftk.spbstu.ru (194.190.225.54)
    Destination: 192.168.0.105 (192.168.0.105)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
# Transmission Control Protocol, Src Port: 80, Dst Port: 61030, Seq: 1, Ack: 25, Len: 0
  Source Port: 80
  Destination Port: 61030
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 25 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
# Flags: 0x011 (FIN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
# .... .... ...1 = Fin: Set
  > [Expert Info (Chat/Sequence): Connection finish (FIN)]
  [TCP Flags: .....A...F]
  Window size value: 46
  [Calculated window size: 5888]
  [Window size scaling factor: 128]
  Checksum: 0xbceb [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
# [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 290]
  [The RTT to ACK the segment was: 0.001901000 seconds]
  [iRTT: 0.002508000 seconds]

```

Рис. 1.24: Ответный FIN/ACK

```

# Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
  ▸ Destination: 64:70:02:91:26:1c
  ▸ Source: c8:0a:a9:d0:5c:0a
  Type: IPv4 (0x0800)
# Internet Protocol Version 4, Src: 192.168.0.105 (192.168.0.105), Dst: tiger.ftk.spbstu.ru (194.190.225.54)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x50a2 (20642)
  ▸ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.105 (192.168.0.105)
  Destination: tiger.ftk.spbstu.ru (194.190.225.54)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
# Transmission Control Protocol, Src Port: 61030, Dst Port: 80, Seq: 25, Ack: 2, Len: 0
  Source Port: 61030
  Destination Port: 80
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 25 (relative sequence number)
  Acknowledgment number: 2 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  # Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A.....]
  Window size value: 258
  [Calculated window size: 66048]
  [Window size scaling factor: 256]
  Checksum: 0x6521 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  # [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 291]
    [The RTT to ACK the segment was: 0.000018000 seconds]
    [iRTT: 0.002508000 seconds]

```

Рис. 1.25: Завершение TCP соединения



Если соединение уже было установлено, то завершение соединения производится следующим образом:

- Посылка серверу от клиента флага FIN на завершение соединения.
- Сервер посылает клиенту флаги ответа ACK , FIN, что соединение закрыто.
- После получения этих флагов клиент закрывает соединение и в подтверждение отправляет серверу ACK, что соединение закрыто.

## UDP

Рассмотрим содержимое пакета UDP

```
┌ Ethernet II, Src: c8:0a:a9:d0:5c:0a, Dst: 64:70:02:91:26:1c
└─▶ Destination: 64:70:02:91:26:1c
    └─▶ Source: c8:0a:a9:d0:5c:0a
        Type: IPv4 (0x0800)
┌ Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: 192.168.0.1 (192.168.0.1)
└─▶ 0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    └─▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 74
        Identification: 0x1f9c (8092)
        └─▶ Flags: 0x00
            Fragment offset: 0
            Time to live: 128
            Protocol: UDP (17)
            Header checksum: 0x0000 [validation disabled]
            [Header checksum status: Unverified]
            Source: 192.168.0.102 (192.168.0.102)
            Destination: 192.168.0.1 (192.168.0.1)
            [Source GeoIP: Unknown]
            [Destination GeoIP: Unknown]
┌ User Datagram Protocol, Src Port: 57859, Dst Port: 53
└─▶ Source Port: 57859
    Destination Port: 53
    Length: 54
    Checksum: 0x81ff [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
┌ Domain Name System (query)
└─▶ [Response In: 92]
    Transaction ID: 0x88b5
    └─▶ Flags: 0x0100 Standard query
        Questions: 1
        Answer RRs: 0
        Authority RRs: 0
        Additional RRs: 0
    └─▶ Queries
```

Рис. 1.26: udp

## 1.4 Вывод

В ходе работы был исследован сетевой трафик и просмотрено содержимое ICMP, ARP, TCP и UDP пакетов. В ходе работы был использован анализатор трафика Wireshark, как мы выяснили, он имеет широкие возможности для фильтрации трафика.