МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования «Санкт-Петербургский политехнический
университет Петра Великого»

Институт компьютерных наук и кибербезопасности

Высшая школа технологий искусственного интеллекта

Направление: 02.03.01 «Математика и компьютерные науки»

Лабораторная работа №2
«Анализ пакетного трафика»
по дисциплине «Сети ЭВМ и телекоммуникации компьютерных сетей»

Студент,
группы 5130201/20102 _____ Тищенко А. А.

Преподаватель _____ Мулюха В. А.

«_____»_____ 2025г.

Санкт-Петербург, 2025

1 Постановка задачи

Необходимо установить и запустить программу tcpdump (с соответствующими библиотеками). tcpdump лучше запускать с опциями -XX -s 128 -S -e. Вывод tcpdump можно перенаправить в файл.

Не останавливая tcpdump выполнить последовательно:

1. Команду ping того адреса, который написан;
2. Команду traceroute (или tracert) того адреса, который указан;
3. Войти через браузер на третий адрес.

Остановить tcpdump.

В отчёте привести трафик соответствующий проводимым действиям и уметь ответить на вопросы какая строчка вывода соответствует какому действию и что вообще делает. Где какое поле и т.п.

Если между действиями в tcpdump попал другой трафик, то часть вывода можно сократить, приведя только нужный.

Вариант	**ping**	**tracert**	**web-доступ**
34	myblog.jp	blogg.de	mega.cl

2 Ход работы

2.1 Подготовка

Вместо tcpdump был установлен его полный аналог для ОС Windows – WinDump (https://www.winpcap.org/windump/install/), в связке с библиотекой WinPcap. Исполняемый файл `WinDump.exe` был добавлен в PATH.

С помощью команды `windump -D`, которая выводит список сетевых интерфейсов и их номеров, был определён номер основного сетевого интерфейса, используемого ноутбуком. В частности это оказался интерфейс под номером 2, поэтому далее в работе в параметре `-i` будет указан именно он.

2.2 Команда ping

Открываем два окна консоли. В одном выполняем команду `windump -XX -s 128 -S -e -i 2 icmp`, с помощью которой будем отлавливать icmp пакеты. В другом выполняем команду `ping myblog.jp`. Выводы команд представлены в листингах 1 и 2.

Листинг 1. Вывод команды `ping myblog.jp`.

```
1  Обмен пакетами с myblog.jp [163.43.102.56] с 32 байтами данных:
2  Ответ от 163.43.102.56: число байт=32 времямс=206 TTL=40
3  Ответ от 163.43.102.56: число байт=32 времямс=204 TTL=40
4  Ответ от 163.43.102.56: число байт=32 времямс=212 TTL=40
5  Ответ от 163.43.102.56: число байт=32 времямс=210 TTL=40
6
7  Статистика Ping для 163.43.102.56:
8      Пакетов: отправлено = 4, получено = 4, потеряно = 0
9      (0% потерь)
10 Приблизительное время приемапередачи– в мс:
11     Минимальное = мсек204, Максимальное = 212 мсек, Среднее = 208 мсек
```

Листинг 2. windump -XX -s 128 -S -e -i 2 icmp.

```
1  windump: listening on \Device\NPF_{7B52B01B–3CC8–4A94–A3C3–E6EC1A52EE5B}
2  21:22:48.160122 7a:12:0e:01:fd:36 (oui Unknown) > ce:24:0b:a1:a4:fb (oui Unknown), ethertype IPv4
     (0x0800), length 74: artem > www3846.sakura.ne.jp: ICMP echo request, id 1, seq 62, length 40
3          0x0000:  ce24 0ba1 a4fb 7a12 0e01 fd36 0800 4500  .$....z....6..E.
4          0x0010:  003c 1cff 0000 8001 1b8a c0a8 382c a32b  .<..........8,.+
5          0x0020:  6638 0800 4d1d 0001 003e 6162 6364 6566  f8..M....>abcdef
6          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
7          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
8  21:22:48.366759 ce:24:0b:a1:a4:fb (oui Unknown) > 7a:12:0e:01:fd:36 (oui Unknown), ethertype IPv4
     (0x0800), length 74: www3846.sakura.ne.jp > artem: ICMP echo reply, id 1, seq 62, length 40
9          0x0000:  7a12 0e01 fd36 ce24 0ba1 a4fb 0800 4500  z....6.$......E.
10         0x0010:  003c 7341 0000 2801 1d48 a32b 6638 c0a8  .<sA..(..H.+f8..
11         0x0020:  382c 0000 551d 0001 003e 6162 6364 6566  8,..U....>abcdef
12         0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
13         0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
14 21:22:49.171976 7a:12:0e:01:fd:36 (oui Unknown) > ce:24:0b:a1:a4:fb (oui Unknown), ethertype IPv4
     (0x0800), length 74: artem > www3846.sakura.ne.jp: ICMP echo request, id 1, seq 63, length 40
15         0x0000:  ce24 0ba1 a4fb 7a12 0e01 fd36 0800 4500  .$....z....6..E.
```

```
16          0x0010:  003c 1d00 0000 8001 1b89 c0a8 382c a32b  .<..........8,.+
17          0x0020:  6638 0800 4d1c 0001 003f 6162 6364 6566  f8..M....?abcdef
18          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
19          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
20      21:22:49.375868 ce:24:0b:a1:a4:fb (oui Unknown) > 7a:12:0e:01:fd:36 (oui Unknown), ethertype IPv4
          (0x0800), length 74: www3846.sakura.ne.jp > artem: ICMP echo reply, id 1, seq 63, length 40
21          0x0000:  7a12 0e01 fd36 ce24 0ba1 a4fb 0800 4500  z....6.$......E.
22          0x0010:  003c 7343 0000 2801 1d46 a32b 6638 c0a8  .<sC..(..F.+f8..
23          0x0020:  382c 0000 551c 0001 003f 6162 6364 6566  8,..U....?abcdef
24          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
25          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
26      21:22:50.182542 7a:12:0e:01:fd:36 (oui Unknown) > ce:24:0b:a1:a4:fb (oui Unknown), ethertype IPv4
          (0x0800), length 74: artem > www3846.sakura.ne.jp: ICMP echo request, id 1, seq 64, length 40
27          0x0000:  ce24 0ba1 a4fb 7a12 0e01 fd36 0800 4500  .$....z....6..E.
28          0x0010:  003c 1d01 0000 8001 1b88 c0a8 382c a32b  .<..........8,.+
29          0x0020:  6638 0800 4d1b 0001 0040 6162 6364 6566  f8..M....@abcdef
30          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
31          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
32      21:22:50.394953 ce:24:0b:a1:a4:fb (oui Unknown) > 7a:12:0e:01:fd:36 (oui Unknown), ethertype IPv4
          (0x0800), length 74: www3846.sakura.ne.jp > artem: ICMP echo reply, id 1, seq 64, length 40
33          0x0000:  7a12 0e01 fd36 ce24 0ba1 a4fb 0800 4500  z....6.$......E.
34          0x0010:  003c 7345 0000 2801 1d44 a32b 6638 c0a8  .<sE..(..D.+f8..
35          0x0020:  382c 0000 551b 0001 0040 6162 6364 6566  8,..U....@abcdef
36          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
37          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
38      21:22:51.194625 7a:12:0e:01:fd:36 (oui Unknown) > ce:24:0b:a1:a4:fb (oui Unknown), ethertype IPv4
          (0x0800), length 74: artem > www3846.sakura.ne.jp: ICMP echo request, id 1, seq 65, length 40
39          0x0000:  ce24 0ba1 a4fb 7a12 0e01 fd36 0800 4500  .$....z....6..E.
40          0x0010:  003c 1d02 0000 8001 1b87 c0a8 382c a32b  .<..........8,.+
41          0x0020:  6638 0800 4d1a 0001 0041 6162 6364 6566  f8..M....Aabcdef
42          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
43          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
44      21:22:51.404994 ce:24:0b:a1:a4:fb (oui Unknown) > 7a:12:0e:01:fd:36 (oui Unknown), ethertype IPv4
          (0x0800), length 74: www3846.sakura.ne.jp > artem: ICMP echo reply, id 1, seq 65, length 40
45          0x0000:  7a12 0e01 fd36 ce24 0ba1 a4fb 0800 4500  z....6.$......E.
46          0x0010:  003c 7348 0000 2801 1d41 a32b 6638 c0a8  .<sH..(..A.+f8..
47          0x0020:  382c 0000 551a 0001 0041 6162 6364 6566  8,..U....Aabcdef
48          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
49          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
50
51      8 packets captured
52      69 packets received by filter
53      0 packets dropped by kernel
```

В выводе команды windump (листинг 2) представлена информация о восьми пакетах. Разберём первый из них (строки 2-7).

В строке 2 указана следующая информация о пакете:

1. `21:22:48.160122` – время, когда пакет был захвачен (чч:мм:сс.мс);

2. `7a:12:0e:01:fd:36 (oui Unknown)` – MAC-адрес отправителя (отправляющий хост), OUI – Organizationally Unique Identifier – код производителя устройства, в данном случае производителя по коду (первые три байта – `7a:12:0e`) определить не удалось;

3. `ce:24:0b:a1:a4:fb (oui Unknown)` – MAC-адрес получателя (маршрутизатор или шлюз);
4. `ethertype IPv4 (0x0800)` – кадр содержит IPv4-пакет;
5. `length 74` – длина Ethernet-кадра 74 байта;
6. `artem > www3846.sakura.ne.jp` – IPадрес отправителя (artem) и адрес получателя (www3846.sakura.ne.jp);
7. `ICMP echo request, id 1, seq 62, length 40` – содержит информацию об ICMP (Internet Control Message Protocol) запросе. `echo request` означает, что это запрос, а не ответ на ping (`echo reply`).

В строках 3-7 идёт непосредственно дамп пакета. По нему видно, что были переданы следующие байты:

1. `ce24 0ba1 a4fb 7a12 0e01 fd36 0800` – первые 14 байт это заголовок Ethernet-кадра.
    - `ce24 0ba1 a4fb` — MAC-адрес получателя.
    - `7a12 0e01 fd36` — MAC-адрес отправителя.
    - `0800` — Тип пакета, который завёрнут в Ethernet.`0800` — это тип протокола, который указывает, что данные в кадре Ethernet содержат пакет IPv4 (Internet Protocol version 4). Другие возможные типы:
        - `86DD` — IPv6.
        - `0806` — ARP (Address Resolution Protocol).
        - `8847` — MPLS (Multi-Protocol Label Switching).
        - `8848` — MPLS Multicast.
        - И другие.
2. `4500 003c 1cff 0000 8001 1b8a c0a8 382c a32b 6638` – следующие 20 байт это заголовок IPv4.
    - `45` — первый байт: версия и длина заголовка.
        - Первая цифра `4` — это версия протокола, что означает `IPv4`.
        - Вторая цифра `5` — это длина заголовка в 32-битных словах, где `5` означает 5 слов, то есть $5 \times 4 = 20$ байт (стандартная длина IPv4-заголовка).
    - `003c` — значение указывает на общий размер пакета (заголовок + данные), равный 60 байт.
    - `1cff` — идентификатор пакета.
        - Это поле используется для фрагментации пакета. Идентификатор `1cff` уникален для каждого фрагмента одного пакета, чтобы при получении фрагменты могли быть правильно собраны.
    - `0000` — флаги и смещение фрагмента.

  - Первая часть `0000` указывает на то, что фрагментация не используется (все биты флагов равны 0).
  - Сдвиг фрагмента также равен 0.
- `80` — TTL (Time to Live).
  - `80` в шестнадцатеричной системе равно `128` в десятичной системе.
  - Это значение определяет максимальное количество маршрутизаторов (хопов), через которые может пройти пакет, прежде чем он будет отброшен.
- `01` — протокол данных внутри IPv4. `01` указывает на протокол ICMP (Internet Control Message Protocol).
  - `01` — ICMP (Internet Control Message Protocol): используется для обмена сообщениями контроля и диагностики, например, команда `ping`.
  - `06` — TCP (Transmission Control Protocol).
  - `11` — UDP (User Datagram Protocol).
  - и некоторые другие.
- `1b8a` — контрольная сумма заголовка.
  - Это значение используется для проверки целостности заголовка IPv4. Контрольная сумма пересчитывается на каждом маршрутизаторе.
- `c0a8 382c` — IP-адрес источника.
  - `c0a8 382c` в шестнадцатеричной системе соответствует IP-адресу `192.168.56.44`.
- `a32b 6638` — IP-адрес назначения.
  - `a32b 6638` в шестнадцатеричной системе соответствует IP-адресу `163.43.102.56`.

3. `0800 4d1d 0001 003e` – заголовок ICMP (8 байт).
   - `08` — Тип ICMP сообщения.
     - `08` указывает на тип сообщения ICMP: Echo Request (запрос эхо), используемый в команде `ping`.
     - `00` – Echo Reply.
     - есть и другие типы.
   - `00` — Код ICMP сообщения. Может содержать информацию о типе ошибки. Для нормальных Echo Request и Echo Reply код 0 означает, что всё штатно.
   - `4d1d` — Контрольная сумма заголовка и данных ICMP.
   - `0001` — Идентификатор запроса.
   - `003e` — Номер последовательности (62 в десятичной системе).
4. `6162 6364 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 7576 7761 6263 6465 6667 6869` – данные внутри ICMP (32 байта). Просто буквы `abcdefghijklmnopqrstuvwabcdefghi`.

2.3 Команда tracert

Команда `tracert` (traceroute) — утилита для определения маршрута следования сетевых пакетов до указанного узла. Она:

- Отправляет серию ICMP-пакетов с увеличивающимся значением TTL (Time To Live).
- Фиксирует ответы от промежуточных маршрутизаторов (хостов) и время задержки.

Листинг 3. Вывод команды `tracert blogg.de`.

```
1  Трассировка маршрута к blogg.de [85.13.145.176] с максимальным числом прыжков 30:
2
3   1   <1 мс   <1 мс   <1 мс  192.168.56.20
4   2    *        *        *    Превышен интервал ожидания для запроса.
5   3   24 ms    26 ms    39 ms  10.226.12.85
6   4   15 ms    28 ms    20 ms  10.226.8.85
7   5   34 ms    24 ms    31 ms  10.226.8.98
8   6   21 ms    18 ms    16 ms  10.226.7.90
9   7    *        *        *    Превышен интервал ожидания для запроса.
10  8   18 ms    21 ms    15 ms  spb-ivc-cr2.ae2544-0.rascom.as20764.net [80.64.108.138]
11  9    *        *        *    Превышен интервал ожидания для запроса.
12  10   57 ms    58 ms    57 ms  80.81.192.39
13  11   62 ms    62 ms    78 ms  dd26736.kasserver.com [85.13.145.176]
14
15  Трассировка завершена.
```

- **1:** `<1 мс <1 мс <1 мс 192.168.56.20` Это первый шаг трассировки. Ответ от локального маршрутизатора (IP-адрес `192.168.56.20`), с минимальным временем отклика (менее 1 мс). Это IP-адрес в локальной сети, который является шлюзом по умолчанию.
- **2:** `* * * Превышен интервал ожидания для запроса.` На втором шаге не было получено ответа. Это может означать, что маршрутизатор не отвечает на ICMP-запросы (ping).
- **3-6:** Ответы от промежуточных маршрутизаторов с IP-адресами `10.226.12.85`, `10.226.8.85`, `10.226.8.98`, `10.226.7.90`. Скорее всего это маршрутизаторы внутри сети провайдера.
- **7:** `* * * Превышен интервал ожидания для запроса.` На этом шаге опять нет ответа. Это может означать, что промежуточное оборудование не отвечает на ICMP-запросы.
- **8:** `18 мс 21 мс 15 мс spb-ivc-cr2.ae2544-0.rascom.as20764.net [80.64.108.138]` Ответ от маршрутизатора `80.64.108.138` с именем `spb-ivc-cr2.ae2544-0.rascom.as20764.net`. Узел из сети Санкт-Петербургского провайдера РАСКОМ (https://ipinfo.io/ips/80.64.108.0/24).
- **10:** `57 мс 58 мс 57 мс 80.81.192.39` Ответ от маршрутизатора с IP-адресом `80.81.192.39`. Время отклика от 57 мс до 58 мс. Этот IP адресс находится

в сети немецкого провайдера *Neue Medien Muennich GmbH*. Само устройство, связанное с этим IP адресом, находится в дата-центре *DE-CIX* во Франкфурте. Данные с сайта https://bgp.he.net/exchange/DE-CIX%20Frankfurt.

- **11:** `62 мс 62 мс 78 мс dd26736.kasserver.com [85.13.145.176]` Ответ от целевого сервера `dd26736.kasserver.com` с IP-адресом `85.13.145.176`. Это последний маршрутизатор на пути, который принадлежит хостинг-платформе, на которой размещён сайт `blogg.de`. Время отклика варьируется от 62 мс до 78 мс.

Паралелльно с выполнением `tracert` была запущена команда `windump -XX -s 128 -S -e -i 2 -v icmp`. За время выполнения команды `tracert` было поймано 90 пакетов. Первый запрос с ttl 1 и ответ на него представлен в листинге 4. По нему видно, что ближайший маршрутизатор `192.168.56.20` вернул ICMP Time Exceeded. Также по выводу windump видно, что, в отличие от команды ping, tracert заполняет поле данных запроса нулями. В остальном это такой же ICMP Echo Request.

Листинг 4. Вывод windump во время выполнения tracert.

```
1  19:22:50.704303 96:48:79:96:d1:f6 (oui Unknown) > 8a:c4:3e:12:66:73 (oui Unknown), ethertype IPv4 (0
       x0800), length 106: (tos 0x0, ttl   1, id 50580, offset 0, flags [none], proto: ICMP (1), length: 92)
       artem > dd26736.kasserver.com: ICMP echo request, id 1, seq 148, length 72
2          0x0000:  8ac4 3e12 6673 9648 7996 d1f6 0800 4500  ..>.fs.Hy.....E.
3          0x0010:  005c c594 0000 0101 147b c0a8 382c 550d  .\.......{..8,U.
4          0x0020:  91b0 0800 f76a 0001 0094 0000 0000 0000  .....j..........
5          0x0030:  0000 0000 0000 0000 0000 0000 0000 0000  ................
6          0x0040:  0000 0000 0000 0000 0000 0000 0000 0000  ................
7          0x0050:  0000 0000 0000 0000 0000 0000 0000 0000  ................
8          0x0060:  0000 0000 0000 0000 0000                 ..........
9  19:22:50.704638 8a:c4:3e:12:66:73 (oui Unknown) > 96:48:79:96:d1:f6 (oui Unknown), ethertype IPv4 (0
       x0800), length 134: (tos 0xc0, ttl  64, id 36552, offset 0, flags [none], proto: ICMP (1), length: 120)
        192.168.56.20 > artem: ICMP time exceeded in-transit, length 100
10         (tos 0x0, ttl   1, id 50580, offset 0, flags [none], proto: ICMP (1), length: 92) artem > dd26736.
       kasserver.com: ICMP echo request, id 1, seq 148, length 72
11         0x0000:  9648 7996 d1f6 8ac4 3e12 6673 0800 45c0  .Hy.....>.fs..E.
12         0x0010:  0078 8ec8 0000 4001 f96b c0a8 3814 c0a8  .x....@..k..8...
13         0x0020:  382c 0b00 f4ff 0000 0000 4500 005c c594  8,........E..\..
14         0x0030:  0000 0101 147b c0a8 382c 550d 91b0 0800  .....{..8,U.....
15         0x0040:  f76a 0001 0094 0000 0000 0000 0000 0000  .j..............
16         0x0050:  0000 0000 0000 0000 0000 0000 0000 0000  ................
17         0x0060:  0000 0000 0000 0000 0000 0000 0000 0000  ................
18         0x0070:  0000 0000 0000 0000 0000 0000 0000 0000  ................
```

2.4 Открытие сайта в браузер

Для выполнения последней задачи необходимо было открыть сайт `mega.cl` в браузере с включённым windump, для запуска которого использовалась команда `windump -i 2 -v host mega.cl`.

Первые три пакета (листинг 5) используются для установки TCP соединения между клиентом и сервером.

Листинг 5. Первые три пакета.

```
1 19:41:58.828210 IP (tos 0x0, ttl 128, id 20148, offset 0, flags [DF], proto: TCP (6), length: 52) artem
    .61628 > as5300-c4-139.cpc.entelchile.net.443: S, cksum 0xee91 (correct),
    1029066177:1029066177(0) win 8760 <mss 1460,nop,wscale 8,nop,nop,sackOK>
2 19:41:59.074184 IP (tos 0x0, ttl 238, id 5828, offset 0, flags [DF], proto: TCP (6), length: 52) as5300-
    c4-139.cpc.entelchile.net.443 > artem.61628: S, cksum 0x889f (correct), 1631908201:1631908201(0)
     ack 1029066178 win 14000 <mss 1400,nop,wscale 0,sackOK,eol>
3 19:41:59.074345 IP (tos 0x0, ttl 128, id 20150, offset 0, flags [DF], proto: TCP (6), length: 40) artem
    .61628 > as5300-c4-139.cpc.entelchile.net.443: ., cksum 0xfebb (correct), ack 1 win 34
```

Рассмотрим каждый пакет по отдельности:

1. Клиент (ноутбук artem) с порта 61628 отправляет TCP-пакет (упакованный в IP пакет) с флагом S (SYN) для инициализации соединения с сервером as5300-c4-139.cpc.entelchile.net по порту 443 (HTTPS). Отправляется также номер последовательности – 1029066177.

2. Сервер отвечает пакетом с флагом S (SYN) и ACK (windump не выводит его явно, но можно понять, что он передаётся по наличию поля ack). В поле ack сервер указывает 1029066178, то есть увеличенный на единицу номер последовательности, который передал клиент при установке соединения. Также сервер отправляет новый номер последовательности – 1631908201.

3. Клиент отправляет пакет с флагом ACK (выводится как .), подтверждая получения SYN-ACK пакета.

После установки соединения начинается передача данных. В листинге 6 видно, как клиент отправляет пакет с флагом P (PUSH) и передаёт 317 байт данных. Клиент указывает диапазон переданных байтов – 1401:1718. За ним следует ответ от сервера с флагом ACK (.). В поле ack сервер указывает конец диапазона байтов, получение которых он подтверждает (ack 1718). Скорее всего в этом пакете клиент делает HTTP запрос.

Листинг 6. Клиент делает запрос.

```
1 19:41:59.075165 IP (tos 0x0, ttl 128, id 20152, offset 0, flags [DF], proto: TCP (6), length: 357) artem
    .61628 > as5300-c4-139.cpc.entelchile.net.443: P 1401:1718(317) ack 1 win 34
2 19:41:59.336245 IP (tos 0x0, ttl 238, id 6571, offset 0, flags [DF], proto: TCP (6), length: 40) as5300-
    c4-139.cpc.entelchile.net.443 > artem.61628: ., cksum 0xbac3 (correct), ack 1718 win 15717
```

Затем сервер начинает передавать клиенту ответные данные (листинг 7). Клиент отвечает и подтверждает, что принял данные. Последний пакет сервер отправляет с флагом P (PUSH), чтобы клиент начал обработку пришёдших данных. На этот пакет клиент также отвечает подтверждением.

Листинг 7. Сервер отвечает.

```
1 19:41:59.341484 IP (tos 0x0, ttl 238, id 6602, offset 0, flags [DF], proto: TCP (6), length: 206) as5300-
    c4-139.cpc.entelchile.net.443 > artem.61628: . 1:167(166) ack 1718 win 15717
2 19:41:59.341647 IP (tos 0x0, ttl 238, id 6603, offset 0, flags [DF], proto: TCP (6), length: 1440) as5300
    -c4-139.cpc.entelchile.net.443 > artem.61628: . 167:1567(1400) ack 1718 win 15717
3 19:41:59.341683 IP (tos 0x0, ttl 128, id 20154, offset 0, flags [DF], proto: TCP (6), length: 40) artem
    .61628 > as5300-c4-139.cpc.entelchile.net.443: ., cksum 0xf1e8 (correct), ack 1567 win 34
```

```
4  19:41:59.341727 IP (tos 0x0, ttl 238, id 6604, offset 0, flags [DF], proto: TCP (6), length: 1440) as5300
       −c4−139.cpc.entelchile.net.443 > artem.61628: . 1567:2967(1400) ack 1718 win 15717
5  19:41:59.341757 IP (tos 0x0, ttl 238, id 6605, offset 0, flags [DF], proto: TCP (6), length: 1268) as5300
       −c4−139.cpc.entelchile.net.443 > artem.61628: P 2967:4195(1228) ack 1718 win 15717
6  19:41:59.341771 IP (tos 0x0, ttl 128, id 20155, offset 0, flags [DF], proto: TCP (6), length: 40) artem
       .61628 > as5300−c4−139.cpc.entelchile.net.443: ., cksum 0xe7a4 (correct), ack 4195 win 34
```

Завершение соединения (листинг 8) происходит в три этапа:

- 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.

Листинг 8. Закрытие соединения.

```
1  19:43:04.183260 IP (tos 0x0, ttl 128, id 20206, offset 0, flags [DF], proto: TCP (6), length: 40) artem
       .61651 > as5300−c4−139.cpc.entelchile.net.443: F, cksum 0xe3cf (correct), 1786:1786(0) ack 4195
       win 34
2  19:43:04.452987 IP (tos 0x0, ttl 238, id 45873, offset 0, flags [DF], proto: TCP (6), length: 40) as5300−
       c4−139.cpc.entelchile.net.443 > artem.61651: ., cksum 0xa648 (correct), ack 1787 win 15785
3  19:43:04.453042 IP (tos 0x0, ttl 238, id 45874, offset 0, flags [DF], proto: TCP (6), length: 40) as5300−
       c4−139.cpc.entelchile.net.443 > artem.61651: F, cksum 0xa647 (correct), 4195:4195(0) ack 1787
       win 15785
4  19:43:04.453067 IP (tos 0x0, ttl 128, id 20208, offset 0, flags [DF], proto: TCP (6), length: 40) artem
       .61651 > as5300−c4−139.cpc.entelchile.net.443: ., cksum 0xe3ce (correct), ack 4196 win 34
```