МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

Институт компьютерных наук и технологий

Направление **02.03.01** : Математика и компьютерные науки

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

Исполнитель: _____ Яшнова Дарья Михайловна
группа 5130201/20002

Руководитель: _____ Мулюха Владимир Александрович

«___»_____ 2025г

Санкт-Петербург, 2025

1 Вариант 36

Задание:

В процессе снятия дампа, выполнить следующие команды:

1. пропинговать blogg.de,
2. выполнить трассировку к mega.cl,
3. выполнить вход на rnz.co.nz.

Остановить снятие дампа. В отчете привести фрагменты дампа, содержащие запросы с объяснениями, почему именно такие фрагменты привели.

Привести схему сети, на которой выполнялась работа (свой ip-адрес, mac-адрес; mac-адрес и ip-адрес шлюза по умолчанию, а также ip-адреса всех серверов, к которым обращаетесь).

Вариант	Ping	tracert / traceroute	web-доступ
36	blogg.de	mega.cl	rnz.co.nz

1.1 Необходимые адреса

С помощью команды ipconfig были выявлены следующие адреса:

IPv4-адрес. . . . . : 192.168.83.44
Маска подсети . . . . . : 255.255.255.0
Физический адрес. . . . . : C8-09-A8-C4-B5-3A
Основной шлюз. . . . . : 192.168.83.2
IP адрес маршрутизатора: 192.168.83.44
MAC - адрес маршрутизатора: 20:3b:34:3f:86:7c

Чтобы узнать ip-адреса серверов, была использована команда (Resolve-DnsName mega.cl).IPAddress. Получились следующие ip-адреса:

```
>(Resolve-DnsName blogg.de).IPAddress
 85.13.145.176
>(Resolve-DnsName mega.cl).IPAddress
 164.77.67.149
> (Resolve-DnsName rnz.co.nz).IPAddress

 151.101.194.133
```

1.2 Схема сети

На рис.1 представлена схема сети.

1.3 Начало работы Wireshark

1. В главном окне Wireshark был выбран сетевой интерфейс (Wi-Fi), через который идёт интернет-трафик.

2. Был начат захват пакетов.

Существует аналогичный способ захвата через WSL - tcpdump. Для этого можно ввести команду:

sudo tcpdump -XX -s 128 -S -e -w results2.pcap

-XX: Опция, которая указывает tcpdump выводить содержимое каждого пакета в шестнадцатеричном формате (hexadecimal) и в формате ASCII. Это полезно для детального анализа данных.

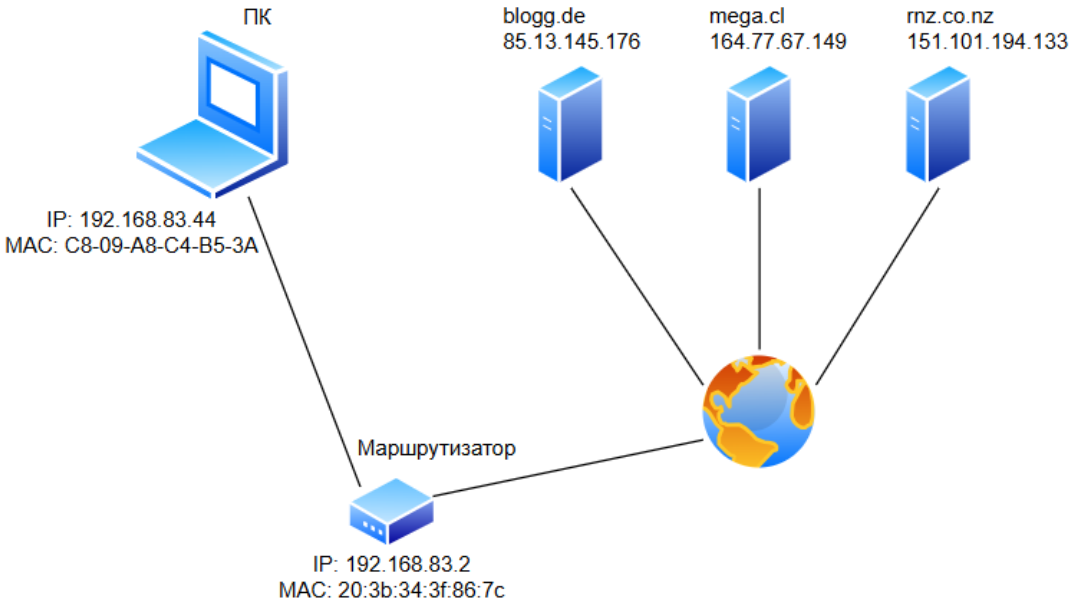

Рис. 1: Схема сети

-s 128: Опция -s (snaplen) определяет максимальное количество байтов каждого пакета, которое будет захвачено. В данном случае, 128 означает, что будут захвачены только первые 128 байтов каждого пакета. Ограничение размера захватываемых данных полезно для экономии места на диске и для уменьшения нагрузки на процессор, если вам не нужна полная информация о каждом пакете.

-S: Опция включает вывод абсолютных номеров последовательностей TCP. Это полезно при анализе TCP-соединений для отслеживания порядка пакетов.

-e: Опция -e (print data link header) указывает tcpdump выводить информацию заголовка канального уровня (например, MAC-адреса Ethernet).

-w results2.pcap: Опция -w указывает tcpdump сохранять захваченные пакеты в файл с именем results2.pcap.

1.4 Создание трафика в сети

В консоли были выполнены следующие команды и получены соответствующие результаты:

```
PS C:\Users\User> ping -n 4 blogg.de

Обмен пакетами с blogg.de [85.13.145.176] с 32 байтами данных:
Ответ от 85.13.145.176: число байт=32 время=86мс TTL=51
Ответ от 85.13.145.176: число байт=32 время=78мс TTL=51
Ответ от 85.13.145.176: число байт=32 время=89мс TTL=51
Ответ от 85.13.145.176: число байт=32 время=76мс TTL=51

Статистика Ping для 85.13.145.176:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 76мсек, Максимальное = 89 мсек, Среднее = 82 мсек

```

```
PS C:\Users\User> tracert -h 8 mega.cl

Трассировка маршрута к mega.cl [190.96.7.123]
с максимальным числом прыжков 8:

  1     *        *        *     Превышен интервал ожидания для запроса.
  2    49 ms    33 ms    36 ms  10.10.177.129
  3     *        *        *     Превышен интервал ожидания для запроса.
  4    48 ms    44 ms    38 ms  10.10.189.1
  5    71 ms    30 ms    45 ms  195.222.167.239
  6    65 ms    36 ms    39 ms  195.222.167.238
  7    68 ms     *        *     mx01.Stockholm.gldn.net [79.104.235.78]
  8   105 ms    92 ms    85 ms  8-2-4-102.ear2.Stockholm2.Level3.net
     [62.140.24.21]

Трассировка завершена.


PS C:\Users\User> curl rnz.co.nz


StatusCode        : 200
StatusDescription : OK
....
```

1.5 Пакеты ICMP при ping blogg.de

На рис.2 показан захват пакетов ICMP (ping) трафика между двумя IP-адресами: 192.168.83.44 и 85.13.145.176. Перехват фильтруется так, чтобы отображались только пакеты, содержащие 85.13.145.176, как указано фильтром «ip.addr == 85.13.145.176».

```
$ tcpdump -r final.pcap icmp and host 85.13.145.176 -XX -n


reading from file final.pcap, link-type EN10MB (Ethernet), snapshot
   length 262144
10:37:12.353759 IP 192.168.83.44 > 85.13.145.176: ICMP echo request, id
   1, seq 300, length 40
        0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
           .
        0x0010:  003c 7b2f 0000 4101 0000 c0a8 532c 550d  .<{/..A.....S,U
           .
        0x0020:  91b0 0800 4c2f 0001 012c 6162 6364 6566  ....L/...,
           abcdef
        0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
           ghijklmnopqrstuv
        0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
10:37:12.440628 IP 85.13.145.176 > 192.168.83.44: ICMP echo reply, id 1,
   seq 300, length 40
        0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
           EP
        0x0010:  003c 5878 0000 3301 3467 550d 91b0 c0a8  .<Xx..3.4gU
           .....
        0x0020:  532c 0000 542f 0001 012c 6162 6364 6566  S,..T/...,
           abcdef
        0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
           ghijklmnopqrstuv
```

```
17          0x0040:  7761 6263 6465 6667 6869                  wabcdefghi
18  10:37:13.374972 IP 192.168.83.44 > 85.13.145.176: ICMP echo request, id
       1, seq 301, length 40
19          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
20          0x0010:  003c 7b30 0000 4101 0000 c0a8 532c 550d  .<{0..A.....S,U
               .
21          0x0020:  91b0 0800 4c2e 0001 012d 6162 6364 6566  ....L....-
               abcdef
22          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
               ghijklmnopqrstuv
23          0x0040:  7761 6263 6465 6667 6869                  wabcdefghi
24  10:37:13.453266 IP 85.13.145.176 > 192.168.83.44: ICMP echo reply, id 1,
       seq 301, length 40
25          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
               EP
26          0x0010:  003c 595d 0000 3301 3382 550d 91b0 c0a8  .<Y]..3.3.U
               .....
27          0x0020:  532c 0000 542e 0001 012d 6162 6364 6566  S,..T....-
               abcdef
28          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
               ghijklmnopqrstuv
29          0x0040:  7761 6263 6465 6667 6869                  wabcdefghi
30  10:37:14.397208 IP 192.168.83.44 > 85.13.145.176: ICMP echo request, id
       1, seq 302, length 40
31          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
32          0x0010:  003c 7b31 0000 4101 0000 c0a8 532c 550d  .<{1..A.....S,U
               .
33          0x0020:  91b0 0800 4c2d 0001 012e 6162 6364 6566  ....L-....
               abcdef
34          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
               ghijklmnopqrstuv
35          0x0040:  7761 6263 6465 6667 6869                  wabcdefghi
36  10:37:14.486105 IP 85.13.145.176 > 192.168.83.44: ICMP echo reply, id 1,
       seq 302, length 40
37          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
               EP
38          0x0010:  003c 597b 0000 3301 3364 550d 91b0 c0a8  .<Y{..3.3dU
               .....
39          0x0020:  532c 0000 542d 0001 012e 6162 6364 6566  S,..T-....
               abcdef
40          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
               ghijklmnopqrstuv
41          0x0040:  7761 6263 6465 6667 6869                  wabcdefghi
42  10:37:15.417292 IP 192.168.83.44 > 85.13.145.176: ICMP echo request, id
       1, seq 303, length 40
43          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
44          0x0010:  003c 7b32 0000 4101 0000 c0a8 532c 550d  .<{2..A.....S,U
               .
45          0x0020:  91b0 0800 4c2c 0001 012f 6162 6364 6566  ....L,.../
               abcdef
46          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
               ghijklmnopqrstuv
47          0x0040:  7761 6263 6465 6667 6869                  wabcdefghi
48  10:37:15.493901 IP 85.13.145.176 > 192.168.83.44: ICMP echo reply, id 1,
       seq 303, length 40
49          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
               EP
```

```
50          0x0010:  003c 59fb 0000 3301 32e4 550d 91b0 c0a8  .<Y...3.2.U
                .....
51          0x0020:  532c 0000 542c 0001 012f 6162 6364 6566  S,..T,.../
                abcdef
52          0x0030:  6768 696a 6b6c 6d6e 6f70 7172 7374 7576
                ghijklmnopqrstuv
53          0x0040:  7761 6263 6465 6667 6869                 wabcdefghi
```

Объяснение одного из пакетов:

1. Ethernet-заголовок (14 байт)

   ```
   0x0000: f627 6152 4350 c809 a8c4 b53a 0800
   ```

   - MAC назначения (6 байт): f6:27:61:52:43:50
   - MAC отправителя (6 байт): c8:09:a8:c4:b5:3a
   - Тип протокола (2 байта): 0800 — IPv4.

2. IP-заголовок (20 байт)

   ```
   0x000E: 4500 003c 7b2f 0000 4101 0000 c0a8 532c 550d 91b0
   ```

   - Версия и длина заголовка (1 байт): 45 — версия IPv4 (4), длина заголовка: $5 \times 4 = 20$ байт.
   - DSCP/ECN (1 байт): 00 — приоритет по умолчанию.
   - Общая длина (2 байта): 003c — 60 байт (включая IP-заголовок и данные).
   - Идентификатор (2 байта): 7b2f — уникальный ID пакета (31535 в десятичной).
   - Флаги и смещение (2 байта): 0000 — пакет не фрагментирован.
   - TTL (1 байт): 41 — Time To Live: 65 (максимум 65 переходов через маршрутизаторы).
   - Протокол (1 байт): 01 — ICMP.
   - Контрольная сумма (2 байта): 0000.
   - IP отправителя (4 байта): c0a8532c — 192.168.83.44.
   - IP получателя (4 байта): 550d91b0 — 85.13.145.176.

3. ICMP-заголовок (8 байт)

   ```
   0x0022: 0800 4c2f 0001 012c
   ```

   - Тип (1 байт): 08 — Echo Request (запрос пинга).
   - Код (1 байт): 00 — стандартный код для Echo Request.
   - Контрольная сумма (2 байта): 4c2f — проверка целостности ICMP-пакета.
   - Идентификатор (2 байта): 0001 — ID процесса, отправившего запрос.

4. Данные ICMP (32 байта)

   ```
   0x002A: 6162 6364 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 7576 7761 6263 6465 666
   ```

   Номер последовательности (2 байта): 012c — 300 в десятичной (порядковый номер пакета).

1.6 Пакеты при tracert mega.cl

Traceroute - это инструмент, который отправляет серию пакетов с увеличивающимися значениями времени жизни (TTL) для определения пути от одного сетевого устройства к другому. В данном случае мы имеем перехват пакета, который показывает попытку отследить путь к IP-адресу 190.96.7.123 от хоста с IP-адресом 192.168.83.44.

```
1   $ tcpdump -r final.pcap icmp and not host 85.13.145.176 -c 4 -XX -n
2  reading from file final.pcap, link-type EN10MB (Ethernet), snapshot
       length 262144
3  10:37:34.496964 IP 192.168.83.44 > 190.96.7.123: ICMP echo request, id 1,
       seq 304, length 72
4          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
5          0x0010:  005c 6b2d 0000 0101 0000 c0a8 532c be60  .\k-........S
               ,.`
6          0x0020:  077b 0800 f6ce 0001 0130 0000 0000 0000
               .{.......0......
7          0x0030:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
8          0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
9          0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
10         0x0060:  0000 0000 0000 0000 0000                 ..........
11 10:37:38.270150 IP 192.168.83.44 > 190.96.7.123: ICMP echo request, id 1,
       seq 305, length 72
12         0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
13         0x0010:  005c 6b2e 0000 0101 0000 c0a8 532c be60  .\k.........S
               ,.`
14         0x0020:  077b 0800 f6cd 0001 0131 0000 0000 0000
               .{.......1......
15         0x0030:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
16         0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
17         0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
18         0x0060:  0000 0000 0000 0000 0000                 ..........
19 10:37:42.272937 IP 192.168.83.44 > 190.96.7.123: ICMP echo request, id 1,
       seq 306, length 72
20         0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
21         0x0010:  005c 6b2f 0000 0101 0000 c0a8 532c be60  .\k/........S
               ,.`
22         0x0020:  077b 0800 f6cc 0001 0132 0000 0000 0000
               .{.......2......
23         0x0030:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
24         0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
25         0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
26         0x0060:  0000 0000 0000 0000 0000                 ..........
27 10:37:46.265156 IP 192.168.83.44 > 190.96.7.123: ICMP echo request, id 1,
       seq 307, length 72
28         0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
29         0x0010:  005c 6b30 0000 0201 0000 c0a8 532c be60  .\k0........S
```

```
            ,.‘
30          0x0020:  077b 0800 f6cb 0001 0133 0000 0000 0000
               .{.......3......
31          0x0030:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
32          0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
33          0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
               ................
34          0x0060:  0000 0000 0000 0000 0000                 ..........
35  10:37:46.314320 IP 10.10.177.129 > 192.168.83.44: ICMP time exceeded in-
       transit, length 36
36          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.’aRCP..
               EP
37          0x0010:  0038 f205 0000 fe01 fb0e 0a0a b181 c0a8
               .8..............
38          0x0020:  532c 0b00 f4ff 0000 0000 4548 005c 6b30  S,........EH.\k
               0
39          0x0030:  0000 0101 7479 c0a8 532c be60 077b 0800  ....ty..S
               ,.‘.{..
40          0x0040:  f6cb 0001 0133                           .....3
```

Объяснение одной из строк:
- IP 192.168.83.44 > 190.96.7.123: IP-адреса источника и назначения.
- ICMP echo request: Тип пакета.
- id 1, seq 304, length 72: Идентификатор, номер последовательности, размер.
- 0x0000: f627 6152 4350 c809 a8c4 b53a 0800 4500 ...: Шестнадцатеричное представление данных пакета. Значение в 0x0010 указывает на TTL = 1 (Time To Live), который важен для traceroute.

1.7 Пакеты при curl rnz.co.nz

На рис.2 представлены пакеты, при вводе команды curl rnz.co.nz.

```
1   $ tcpdump -r final.pcap -n port http -S
2
3   10:39:00.995600 IP 192.168.83.44.61935 > 151.101.194.133.80: Flags [S],
       seq 2444111603, win 64240, options [mss 1460,nop,wscale 8,nop,nop,
       sackOK], length 0
4           0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .’aRCP.....:..E
               .
5           0x0010:  0034 9261 4000 4106 0000 c0a8 532c 9765  .4.a@.A.....S,.
               e
6           0x0020:  c285 f1ef 0050 91ae 2ef3 0000 0000 8002  .....P
               ..........
7           0x0030:  faf0 6de6 0000 0204 05b4 0103 0308 0101  ..m
               ............
8           0x0040:  0402                                     ..
9   10:39:01.084198 IP 151.101.194.133.80 > 192.168.83.44.61935: Flags [S.],
       seq 3639419375, ack 2444111604, win 65535, options [mss 1240,nop,nop,
       sackOK,nop,wscale 9], length 0
10          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.’aRCP..
               EP
11          0x0010:  0034 0000 4000 3906 d3b4 9765 c285 c0a8  .4..@.9....e
               ....
12          0x0020:  532c 0050 f1ef d8ed 21ef 91ae 2ef4 8012  S,.P
               ....!.......
13          0x0030:  ffff 545c 0000 0204 04d8 0101 0402 0103  ..T
               \...........
```

```
14          0x0040:  0309                                           ..
15  10:39:01.084319 IP 192.168.83.44.61935 > 151.101.194.133.80: Flags [.],
       ack 1, win 513, length 0
16          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
17          0x0010:  0028 9262 4000 4106 0000 c0a8 532c 9765  .(.b@.A.....S,.
               e
18          0x0020:  c285 f1ef 0050 91ae 2ef4 d8ed 21f0 5010  .....P......!.P
               .
19          0x0030:  0201 6dda 0000                           ..m...
20  10:39:01.088914 IP 192.168.83.44.61935 > 151.101.194.133.80: Flags [P.],
       seq 1:155, ack 1, win 513, length 154: HTTP: GET / HTTP/1.1
21          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
               .
22          0x0010:  00c2 9263 4000 4106 0000 c0a8 532c 9765  ...c@.A.....S,.
               e
23          0x0020:  c285 f1ef 0050 91ae 2ef4 d8ed 21f0 5018  .....P......!.P
               .
24          0x0030:  0201 6e74 0000 4745 5420 2f20 4854 5450  ..nt..GET./.
               HTTP
25          0x0040:  2f31 2e31 0d0a 5573 6572 2d41 6765 6e74  /1.1..User-
               Agent
26          0x0050:  3a20 4d6f 7a69 6c6c 612f 352e 3020 2857  :.Mozilla/5.0.(
               W
27          0x0060:  696e 646f 7773 204e 543b 2057 696e 646f  indows.NT;.
               Windo
28          0x0070:  7773 204e 5420 3130 2e30 3b20 7275 2d52  ws.NT.10.0;.ru-
               R
29          0x0080:  5529 2057 696e 646f 7773 506f 7765 7253  U).
               WindowsPowerS
30          0x0090:  6865 6c6c 2f35 2e31 2e31 3930 3431 2e35  hell
               /5.1.19041.5
31          0x00a0:  3438 360d 0a48 6f73 743a 2072 6e7a 2e63  486..Host:.rnz.
               c
32          0x00b0:  6f2e 6e7a 0d0a 436f 6e6e 6563 7469 6f6e  o.nz..
               Connection
33          0x00c0:  3a20 4b65 6570 2d41 6c69 7665 0d0a 0d0a  :.Keep-Alive
               ....
34  10:39:01.171170 IP 151.101.194.133.80 > 192.168.83.44.61935: Flags [.],
       ack 155, win 288, length 0
35          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
               EP
36          0x0010:  0028 8c93 4000 3906 472d 9765 c285 c0a8  .(..@.9.G-.e
               ....
37          0x0020:  532c 0050 f1ef d8ed 21f0 91ae 2f8e 5010  S,.P....!.../.P
               .
38          0x0030:  0120 929a 0000                           ......
39  10:39:01.171170 IP 151.101.194.133.80 > 192.168.83.44.61935: Flags [P.],
       seq 1:486, ack 155, win 288, length 485: HTTP: HTTP/1.1 301 Moved
       Permanently
40          0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
               EP
41          0x0010:  020d 8c94 4000 3906 4547 9765 c285 c0a8  ....@.9.EG.e
               ....
42          0x0020:  532c 0050 f1ef d8ed 21f0 91ae 2f8e 5018  S,.P....!.../.P
               .
43          0x0030:  0120 6c4b 0000 4854 5450 2f31 2e31 2033  ..lK..HTTP
               /1.1.3
44          0x0040:  3031 204d 6f76 6564 2050 6572 6d61 6e65  01.Moved.
               Permane
```

```
45          0x0050:  6e74 6c79 0d0a 436f 6e6e 6563 7469 6f6e  ntly..Connection
46          0x0060:  3a20 636c 6f73 650d 0a43 6f6e 7465 6e74  :.close..Content
47          0x0070:  2d4c 656e 6774 683a 2030 0d0a 5365 7276  -Length:.0..Serv
48          0x0080:  6572 3a20 5661 726e 6973 680d 0a52 6574  er:.Varnish..Ret
49          0x0090:  7279 2d41 6674 6572 3a20 300d 0a68 7474  ry-After:.0..htt
50          0x00a0:  702e 4361 6368 652d 436f 6e74 726f 6c3a  p.Cache-Control:
51          0x00b0:  206e 6f2d 6361 6368 652c 206e 6f2d 7374  .no-cache,.no-st
52          0x00c0:  6f72 652c 206d 7573 742d 7265 7661 6c69  ore,.must-revali
53          0x00d0:  6461 7465 2c20 6d61 782d 6167 653d 3336  date,.max-age=36
54          0x00e0:  3030 0d0a 4c6f 6361 7469 6f6e 3a20 6874  00..Location:.ht
55          0x00f0:  7470 733a 2f2f 7777 772e 726e 7a2e 636f  tps://www.rnz.co
56          0x0100:  2e6e 7a2f 0d0a 4163 6365 7074 2d52 616e  .nz/..Accept-Ran
57          0x0110:  6765 733a 2062 7974 6573 0d0a 4461 7465  ges:.bytes..Date
58          0x0120:  3a20 5765 642c 2031 3220 4d61 7220 3230  :.Wed,.12.Mar.20
59          0x0130:  3235 2030 373a 3339 3a30 3220 474d 540d  25.07:39:02.GMT.
60          0x0140:  0a56 6961 3a20 312e 3120 7661 726e 6973  .Via:.1.1.varnis
61          0x0150:  680d 0a58 2d53 6572 7665 642d 4279 3a20  h..X-Served-By:.
62          0x0160:  6361 6368 652d 6672 612d 6564 6466 3832  cache-fra-eddf82
63          0x0170:  3330 3033 362d 4652 410d 0a58 2d43 6163  30036-FRA..X-Cac
64          0x0180:  6865 3a20 4849 540d 0a58 2d43 6163 6865  he:.HIT..X-Cache
65          0x0190:  2d48 6974 733a 2030 0d0a 582d 5469 6d65  -Hits:.0..X-Time
66          0x01a0:  723a 2053 3137 3431 3736 3531 3433 2e35  r:.S1741765143.5
67          0x01b0:  3037 3136 312c 5653 302c 5645 300d 0a58  07161,VS0,VE0..X
68          0x01c0:  2d50 6f77 6572 6564 2d42 793a 204f 6e65  -Powered-By:.One
69          0x01d0:  2073 6d61 6c6c 2070 6965 6365 206f 6620  .small.piece.of.
70          0x01e0:  6661 6972 7920 6361 6b65 0d0a 5374 7269  fairy.cake..Stri
71          0x01f0:  6374 2d54 7261 6e73 706f 7274 2d53 6563  ct-Transport-Sec
72          0x0200:  7572 6974 793a 206d 6178 2d61 6765 3d33  urity:.max-age=3
73          0x0210:  3135 3537 3630 300d 0a0d 0a              1557600....
74  10:39:01.175006 IP 192.168.83.44.61935 > 151.101.194.133.80: Flags [F.], seq 155, ack 486, win 511, length 0
75          0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
```

```
                .
76              0x0010:  0028 9264 4000 4106 0000 c0a8 532c 9765  .(.d@.A.....S,.
                   e
77              0x0020:  c285 f1ef 0050 91ae 2f8e d8ed 23d5 5011  .....P../...#.P
                   .
78              0x0030:  01ff 6dda 0000                           ..m...
79    10:39:01.175256 IP 151.101.194.133.80 > 192.168.83.44.61935: Flags [F.],
         seq 486, ack 155, win 288, length 0
80              0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
                   EP
81              0x0010:  0028 8c95 4000 3906 472b 9765 c285 c0a8  .(..@.9.G+.e
                   ....
82              0x0020:  532c 0050 f1ef d8ed 23d5 91ae 2f8e 5011  S,.P....#.../.P
                   .
83              0x0030:  0120 90b4 0000                           ......
84    10:39:01.175276 IP 192.168.83.44.61935 > 151.101.194.133.80: Flags [.],
         ack 487, win 511, length 0
85              0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
                   .
86              0x0010:  0028 9265 4000 4106 0000 c0a8 532c 9765  .(.e@.A.....S,.
                   e
87              0x0020:  c285 f1ef 0050 91ae 2f8f d8ed 23d6 5010  .....P../...#.P
                   .
88              0x0030:  01ff 6dda 0000                           ..m...
89    10:39:01.475561 IP 192.168.83.44.61935 > 151.101.194.133.80: Flags [F.],
         seq 155, ack 487, win 511, length 0
90              0x0000:  f627 6152 4350 c809 a8c4 b53a 0800 4500  .'aRCP.....:..E
                   .
91              0x0010:  0028 9266 4000 4106 0000 c0a8 532c 9765  .(.f@.A.....S,.
                   e
92              0x0020:  c285 f1ef 0050 91ae 2f8e d8ed 23d6 5011  .....P../...#.P
                   .
93              0x0030:  01ff 6dda 0000                           ..m...
94    10:39:01.560377 IP 151.101.194.133.80 > 192.168.83.44.61935: Flags [.],
         ack 156, win 288, length 0
95              0x0000:  c809 a8c4 b53a f627 6152 4350 0800 4550  .....:.'aRCP..
                   EP
96              0x0010:  0028 0000 4000 3906 d3c0 9765 c285 c0a8  .(..@.9....e
                   ....
97              0x0020:  532c 0050 f1ef d8ed 23d6 91ae 2f8f 5010  S,.P....#.../.P
                   .
98              0x0030:  0120 90b3 0000                           ......
```

No.	Time	Source	Destination	Protocol	Length	Info
3288	112.850507	192.168.83.44	151.101.194.133	TCP	66	61935 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3289	112.939105	151.101.194.133	192.168.83.44	TCP	66	80 → 61935 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1240 SACK_PERM WS=512
3290	112.939226	192.168.83.44	151.101.194.133	TCP	54	61935 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
3291	112.943821	192.168.83.44	151.101.194.133	HTTP	208	GET / HTTP/1.1
3292	113.026077	151.101.194.133	192.168.83.44	TCP	54	80 → 61935 [ACK] Seq=1 Ack=155 Win=147456 Len=0
3293	113.026077	151.101.194.133	192.168.83.44	HTTP	539	HTTP/1.1 301 Moved Permanently
3294	113.029913	192.168.83.44	151.101.194.133	TCP	54	61935 → 80 [FIN, ACK] Seq=155 Ack=486 Win=130816 Len=0
3295	113.030163	151.101.194.133	192.168.83.44	TCP	54	80 → 61935 [FIN, ACK] Seq=486 Ack=155 Win=147456 Len=0
3296	113.030183	192.168.83.44	151.101.194.133	TCP	54	61935 → 80 [ACK] Seq=156 Ack=487 Win=130816 Len=0
3310	113.330468	192.168.83.44	151.101.194.133	TCP	54	[TCP Retransmission] 61935 → 80 [FIN, ACK] Seq=155 Ack=487 Win=130816 Len=0
3315	113.415284	151.101.194.133	192.168.83.44	TCP	54	80 → 61935 [ACK] Seq=487 Ack=156 Win=147456 Len=0

Рис. 2: Пакеты, при вводе команды curl rnz.co.nz

Разбор некоторых пакетов:

1. Временная метка (Timestamp)

   10:39:00.995600 – точное время отправки пакета.

2. IP-заголовок (IPv4)

   IP – указывает, что используется протокол IPv4.

   192.168.83.44 – исходный IP-адрес (отправитель, клиент).

   151.101.194.133 – целевой IP-адрес (получатель, сервер).

   Это публичный IP, например, сервер reddit.com или CDN (Fastly).

   61935 – исходный порт (клиентский, выбран случайно ОС).

   80 – целевой порт (HTTP-сервер, стандартный для веб-трафика).

3. TCP-заголовок

   Flags [S] – флаг SYN (Synchronize). Это первый шаг трёхэтапного рукопожатия TCP:

   - Клиент -> Сервер: SYN
   - Сервер -> Клиент: SYN-ACK
   - Клиент -> Сервер: ACK

   seq 2444111603 – начальный номер последовательности (ISN). Используется для контроля порядка и целостности данных.

   win 64240 – размер окна приёма (буфер клиента, 64 240 байт).

   options [...] – дополнительные параметры TCP:

   - mss 1460 – Maximum Segment Size (макс. размер сегмента без фрагментации).
   - nop – "No Operation"(выравнивание опций).
   - wscale 8 – Window Scaling (масштабирование окна, множитель $2^8 = 256$).

sackOK – Selective Acknowledgment (поддержка выборочных подтверждений).

Позволяет подтверждать не только последовательные данные, но и фрагментированные.

- length 0 – нет данных (только заголовок, так как это SYN).

2 Заключение

В ходе лабораторной работы были изучены команды для определения параметров сети, проверки наличия подключения (ping) и трассировки маршрутов (traceroute), а также получены навыки работы с программой сбора и анализа трафика wireshark и tcpdump. Для решения поставленых задач были использованы команды curl, tracert, ping. Затем сохраненный в файл дамп прочитан и отфильтрован с помощью программы tcpdump.