

Министерство образования и науки
Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа искусственного интеллекта
Направление: 02.03.01 Математика и компьютерные науки

ЛАБОРАТОРНАЯ РАБОТА №2

по дисциплине «Сети ЭВМ и телекоммуникации компьютерных сетей»

Анализ пакетного трафика

Вариант № 39

Студент, гр. 5130201/20102

Салимли А.

Преподаватель, к.т.н.

Мулюха В. А.

«____» _____ 20____.

Санкт-Петербург
2025

1 Постановка задачи

Установить tcpdump, в последствие, снять дамп и в процессе снятия выполнить команды:

- Пропинговать указанный адрес
- Выполнить трассировку к указанному адресу
- Выполнить вход на указанный сайт

Далее остановить снятие дампа, и привести в отчете фрагменты дампа, с запросами.

tcpdump - утилита позволяющая перехватывать и анализировать трафик.

В системах UNIX, она установлена по умолчанию. Так как ОС MacOS - является UNIX-подобной системой, она так же установлена по умолчанию. Можно так же обновить или переустановить утилиту командой:

```
brew reinstall tcpdump
```

После можно отследить версию с командой:

```
tcpdump --version
```

Выполнять tcpdump, нужно с ключами -xx, иначе будет мало данных что бы понять какие пакеты вывелись в консоль.

Нужно привести схему, на которой выполнялась работа (ip, mac, ip и mac шлюза по умолчанию, ip - серверов к которым обращались)

Вариант № 39:

ping	tracet/traceroute	web-доступ
<u>newzealand.com</u>	<u>immigration.govt.nz</u>	<u>skykiwi.com</u>

2 Схема сети

Для того что бы узнать требуемые адреса в локальной сети, можно прописать команду

```
% ifconfig -a :
```

Она выведет информацию о всех интерфейсах: en0, lo0.

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
    ether 16:d6:de:e2:e0:27
    inet6 fe80::1477:ed37:e18f:e3f4%en0 prefixlen 64 secured scopeid 0xb
    inet 192.168.0.27 netmask 0xffffffff broadcast 192.168.0.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
```

Тут:

inet - мой адрес IPv4

inet6 - мой адрес IPv6 (Link-local)

ether - MAC-адрес

Так как в моей системе нет иных физических и виртуальных сетей достаточно прописать en0.

Для того что бы просмотреть роутер/шлюз по умолчанию можно вписать команду:

```
% arp -a
```

```
? (192.168.0.1) at 58:f8:5c:22:27:5d on en0 ifscope [ethernet]
? (192.168.0.5) at a2:cf:89:49:69:23 on en0 ifscope [ethernet]
? (192.168.0.22) at 20:15:82:26:81:1 on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent
[ethernet]
```

Тут:

- 192.168.0.1 - роутер/шлюз
- 58:f8:5c:22:27:5d - MAC адрес устройства который работает по 192.168.0.1.
- mdns.mcast.net - мультикаст-адрес для mDNS.

Для того что бы узнать список IP-адресов на которые резолвится сайт можно прописать команду:

```
% dig +short
```

То есть для нашего варианта:

```
% dig +short newzealand.com
```

```
% dig +short immigration.govt.nz
```

```
% dig +short skykiwi.com
```

Результат:

```
(base) ayzek@MacBook-Air-Gore-programmist ~ % dig +short newzealand.com
198.54.117.242
(base) ayzek@MacBook-Air-Gore-programmist ~ % dig +short immigration.govt.nz
103.241.84.81
(base) ayzek@MacBook-Air-Gore-programmist ~ % dig +short skykiwi.com
47.84.176.250
```

Графическое описание сети:

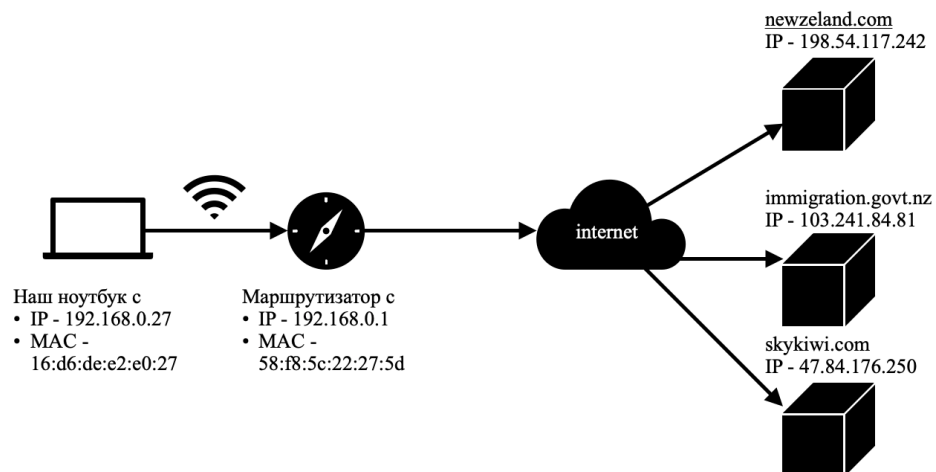


Рис. 1 Схема сети

3 Запуск скриптов

Запуск tcpdump (так как -w дает запись в бинарном формате):

```
% sudo tcpdump -i en0 -XX -s 128 -S -e > zapisDampa.txt
```

Результат:

```
tcpdump: listening on en0, link-type EN10MB (Ethernet), snapshot length 128 bytes
```

Теперь не прерывая tcpdump в новом терминале:

```
%ping newzealand.com
```

```
PING newzealand.com (2.21.205.159): 56 data bytes
64 bytes from 2.21.205.159: icmp_seq=0 ttl=57 time=20.026 ms
64 bytes from 2.21.205.159: icmp_seq=1 ttl=57 time=19.490 ms
64 bytes from 2.21.205.159: icmp_seq=2 ttl=57 time=19.534 ms
64 bytes from 2.21.205.159: icmp_seq=3 ttl=57 time=19.560 ms
64 bytes from 2.21.205.159: icmp_seq=4 ttl=57 time=20.513 ms
64 bytes from 2.21.205.159: icmp_seq=5 ttl=57 time=25.858 ms
64 bytes from 2.21.205.159: icmp_seq=6 ttl=57 time=19.713 ms
64 bytes from 2.21.205.159: icmp_seq=7 ttl=57 time=19.654 ms
64 bytes from 2.21.205.159: icmp_seq=8 ttl=57 time=19.171 ms
64 bytes from 2.21.205.159: icmp_seq=9 ttl=57 time=19.410 ms
64 bytes from 2.21.205.159: icmp_seq=10 ttl=57 time=25.846 ms
64 bytes from 2.21.205.159: icmp_seq=11 ttl=57 time=20.007 ms
64 bytes from 2.21.205.159: icmp_seq=12 ttl=57 time=19.293 ms
64 bytes from 2.21.205.159: icmp_seq=13 ttl=57 time=19.942 ms
64 bytes from 2.21.205.159: icmp_seq=14 ttl=57 time=27.341 ms
^C
--- newzealand.com ping statistics ---
15 packets transmitted, 15 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.171/21.024/27.341/2.700 ms
```

```
%tracert immigration.govt.nz
```

```
tracert to immigration.govt.nz (103.241.84.81), 64 hops max, 40 byte packets
 1  rt.homelan (192.168.0.1)  4.677 ms  3.788 ms  3.805 ms
 2  92.101.243.1 (92.101.243.1)  22.306 ms  6.660 ms  7.002 ms
 3  xe-1-1-3-10g.tl600-2-210.nwtelecom.ru (212.48.194.252)  14.315 ms
13.054 ms  7.170 ms
 4  217.107.120.119 (217.107.120.119)  47.443 ms  48.743 ms  47.633 ms
 5  bbr01.eq01.fra03.networklayer.com (80.81.194.244)  47.236 ms
    bbr01.xn01.fra01.networklayer.com (80.81.194.167)  49.886 ms
    bbr01.eq01.fra03.networklayer.com (80.81.194.244)  47.825 ms
 6  ae5.cbs02.eq01.fra03.networklayer.com (169.53.16.34)  48.472 ms
    ae5.cbs01.xn01.fra01.networklayer.com (169.45.18.166)  48.161 ms
    ae5.cbs02.eq01.fra03.networklayer.com (169.53.16.34)  48.221 ms
 7  ae0.cbs02.ic01.mil02.networklayer.com (50.97.19.173)  52.006 ms
54.868 ms
    ae9.cbs01.xn01.fra01.networklayer.com (169.53.16.42)  48.454 ms
 8  ae7.cbs01.ic01.mil02.networklayer.com (169.45.19.124)  59.352 ms
```

```

    ae0.cbs02.ic01.mil02.networklayer.com (50.97.19.173) 52.895 ms
    ae7.cbs01.ic01.mil02.networklayer.com (169.45.19.124) 57.917 ms
  9  ae7.cbs01.ic01.mil02.networklayer.com (169.45.19.124) 57.482 ms *
62.674 ms
10  * ae7.cbs02.eq01.sng02.networklayer.com (169.45.19.155) 214.753 ms
    ae1.cbs01.eq01.sng02.networklayer.com (169.45.19.97) 210.747 ms
11  ae7.cbs01.vz01.osl02.networklayer.com (50.97.17.126) 310.010 ms
312.521 ms
    ae7.cbs02.eq01.sng02.networklayer.com (169.45.19.155) 209.779 ms
12  ae7.bbr02.ng01.per01.networklayer.com (50.97.19.233) 302.871 ms
    ae7.cbs01.vz01.osl02.networklayer.com (50.97.17.126) 310.602 ms
313.551 ms
13  ae2.bbr01.eq01.syd02.networklayer.com (50.97.19.239) 309.829 ms
    ae7.bbr02.ng01.per01.networklayer.com (50.97.19.233) 303.303 ms
    ae2.bbr01.eq01.syd02.networklayer.com (50.97.19.239) 308.471 ms
14  ae2.bbr01.eq01.syd02.networklayer.com (50.97.19.239) 318.276 ms
    ae5.cbs02.eq02.syd02.networklayer.com (169.45.18.248) 303.866 ms
    ae2.bbr01.eq01.syd02.networklayer.com (50.97.19.239) 310.412 ms
15  1b.13.2da9.ip4.static.sl-reverse.com (169.45.19.27) 309.141 ms
    19.13.2da9.ip4.static.sl-reverse.com (169.45.19.25) 302.874 ms
    ae5.cbs02.eq02.syd02.networklayer.com (169.45.18.248) 304.033 ms
16  89.76.c682.ip4.static.sl-reverse.com (130.198.118.137) 315.448 ms^C

```

После чего открываем в браузере (в нашем случае safari) сайт skykiwi.com. И ждем пока сайт загрузится.

После чего можно прервать изначальный терминал в котором прописывали tcpdump с помощью control+C.

В директории где был запущен терминал создается файл zapisDampa.txt, в которой будет находиться фильтрация захваченного трафика.

4 Фильтрация захваченного трафика

Пакеты ICMP echo request/reply (ping)

Командой % tcpdump -n -r lab.pcap host newzealand.com -XX:

```
16:23:43.733760 IP 192.168.0.27 > 2.21.205.159: ICMP echo request, id 2808, seq 0,
length 64
    0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
    0x0010:  0054 c2e0 0000 4001 2751 c0a8 001b 0215  .T....@.'Q.....
    0x0020:  cd9f 0800 2ed9 0af8 0000 67d0 395f 000b  .....g.9_..
    0x0030:  31f1 0809 0a0b 0c0d 0e0f 1011 1213 1415  1.....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!\"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                         67
16:23:43.753636 IP 2.21.205.159 > 192.168.0.27: ICMP echo reply, id 2808, seq 0,
length 64
    0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 4500  ....'X.\"']..E.
    0x0010:  0054 8cf8 0000 3901 6439 0215 cd9f c0a8  .T....9.d9.....
    0x0020:  001b 0000 36d9 0af8 0000 67d0 395f 000b  ....6.....g.9_..
    0x0030:  31f1 0809 0a0b 0c0d 0e0f 1011 1213 1415  1.....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!\"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                         67
16:23:44.738968 IP 192.168.0.27 > 2.21.205.159: ICMP echo request, id 2808, seq 1,
length 64
    0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
    0x0010:  0054 bc76 0000 4001 2dbb c0a8 001b 0215  .T.v..@.-.....
    0x0020:  cd9f 0800 1abe 0af8 0001 67d0 3960 000b  .....g.9`..
    0x0030:  460a 0809 0a0b 0c0d 0e0f 1011 1213 1415  F.....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!\"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                         67
16:23:44.758256 IP 2.21.205.159 > 192.168.0.27: ICMP echo reply, id 2808, seq 1,
length 64
    0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 4500  ....'X.\"']..E.
    0x0010:  0054 8f7d 0000 3901 61b4 0215 cd9f c0a8  .T.}..9.a.....
    0x0020:  001b 0000 22be 0af8 0001 67d0 3960 000b  ....\".....g.9`..
    0x0030:  460a 0809 0a0b 0c0d 0e0f 1011 1213 1415  F.....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!\"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                         67
16:23:45.744211 IP 192.168.0.27 > 2.21.205.159: ICMP echo request, id 2808, seq 2,
length 64
    0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
    0x0010:  0054 c606 0000 4001 242b c0a8 001b 0215  .T....@.$+.....
    0x0020:  cd9f 0800 0651 0af8 0002 67d0 3961 000b  ....Q....g.9a..
    0x0030:  5a75 0809 0a0b 0c0d 0e0f 1011 1213 1415  Zu.....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!\"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                         67
16:23:45.763509 IP 2.21.205.159 > 192.168.0.27: ICMP echo reply, id 2808, seq 2,
length 64
    0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 4500  ....'X.\"']..E.
    0x0010:  0054 9287 0000 3901 5eaa 0215 cd9f c0a8  .T....9.^.....
    0x0020:  001b 0000 0e51 0af8 0002 67d0 3961 000b  ....Q....g.9a..
    0x0030:  5a75 0809 0a0b 0c0d 0e0f 1011 1213 1415  Zu.....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!\"#$%
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637                                         67
16:23:46.749478 IP 192.168.0.27 > 2.21.205.159: ICMP echo request, id 2808, seq 3,
length 64
    0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
    0x0010:  0054 8dab 0000 4001 5c86 c0a8 001b 0215  .T....@.\.....
    0x0020:  cd9f 0800 flad 0af8 0003 67d0 3962 000b  .....g.9b..
```

```

0x0030:  6f16 0809 0a0b 0c0d 0e0f 1011 1213 1415  o.....
0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....! "$%
0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
0x0060:  3637                                     67
16:23:46.768823 IP 2.21.205.159 > 192.168.0.27: ICMP echo reply, id 2808, seq 3,
length 64
0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 4500  ....'X.\"']..E.
0x0010:  0054 95bd 0000 3901 5b74 0215 cd9f c0a8  .T....9.[t.....
0x0020:  001b 0000 f9ad 0af8 0003 67d0 3962 000b  .....g.9b..
0x0030:  6f16 0809 0a0b 0c0d 0e0f 1011 1213 1415  o.....
0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....! "$%
0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
0x0060:  3637                                     67

```

Пакеты traceroute:

Кратко по всем пакетам из traceroute:

Командой % tcpdump -r lab.pcap icmp and not host newzealand.com -n

```

reading from PCAP-NG file lab.pcap
16:23:33.274866 IP 192.168.0.27 > 17.253.14.169: ICMP 192.168.0.27 udp port 54065 unreachable,
length 36
0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
0x0010:  0038 18fd 0000 4001 805f c0a8 001b 11fd  .8....@.._.....
0x0020:  0ea9 0303 27c3 0000 0000 4500 0061 0000  ....'.....E..a..
0x0030:  4000 3b11 5e23 11fd 0ea9 c0a8 001b 01bb  @.;.^#.....
0x0040:  d331 004d 0000                          .1.M..
16:23:33.274916 IP 192.168.0.27 > 17.253.14.169: ICMP 192.168.0.27 udp port 54065 unreachable,
length 36
0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
0x0010:  0038 d9a3 0000 4001 bfb8 c0a8 001b 11fd  .8....@.....
0x0020:  0ea9 0303 27e2 0000 0000 4500 0042 0000  ....'.....E..B..
0x0030:  4000 3b11 5e42 11fd 0ea9 c0a8 001b 01bb  @.;.^B.....
0x0040:  d331 002e 0000                          .1....
16:23:44.248262 IP 192.168.0.27 > 17.253.14.169: ICMP 192.168.0.27 udp port 54065 unreachable,
length 36
0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
0x0010:  0038 7c61 0000 4001 1cfb c0a8 001b 11fd  .8|a..@.....
0x0020:  0ea9 0303 27c3 0000 0000 4500 0061 0000  ....'.....E..a..
0x0030:  4000 3b11 5e23 11fd 0ea9 c0a8 001b 01bb  @.;.^#.....
0x0040:  d331 004d 0000                          .1.M..
16:23:44.248372 IP 192.168.0.27 > 17.253.14.169: ICMP 192.168.0.27 udp port 54065 unreachable,
length 36
0x0000:  58f8 5c22 275d 16d6 dee2 e027 0800 4500  X.\"'].....'..E.
0x0010:  0038 3673 0000 4001 62e9 c0a8 001b 11fd  .86s..@.b.....
0x0020:  0ea9 0303 27e2 0000 0000 4500 0042 0000  ....'.....E..B..
0x0030:  4000 3b11 5e42 11fd 0ea9 c0a8 001b 01bb  @.;.^B.....
0x0040:  d331 002e 0000                          .1....
16:24:25.986786 IP 192.168.0.1 > 192.168.0.27: ICMP time exceeded in-transit, length 48
0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 45c0  ....'X.\"']..E.
0x0010:  0044 d23b 0000 4001 2651 c0a8 0001 c0a8  .D.;..@.&Q.....
0x0020:  001b 0b00 722b 0000 0000 4500 0028 f969  ....r+....E..(.i
0x0030:  0000 0111 4356 c0a8 001b 67f1 5451 f968  ....CV....g.TQ.h
0x0040:  829b 0014 06bc 0000 0000 0000 0000 0000  .....
0x0050:  0000                                     ..
16:24:25.997120 IP 192.168.0.1 > 192.168.0.27: ICMP time exceeded in-transit, length 48
0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 45c0  ....'X.\"']..E.
0x0010:  0044 d23c 0000 4001 2650 c0a8 0001 c0a8  .D.<..@.&P.....
0x0020:  001b 0b00 722b 0000 0000 4500 0028 f96a  ....r+....E..(.j
0x0030:  0000 0111 4355 c0a8 001b 67f1 5451 f968  ....CU....g.TQ.h
0x0040:  829c 0014 06bb 0000 0000 0000 0000 0000  .....
0x0050:  0000                                     ..
16:24:26.000974 IP 192.168.0.1 > 192.168.0.27: ICMP time exceeded in-transit, length 48
0x0000:  16d6 dee2 e027 58f8 5c22 275d 0800 45c0  ....'X.\"']..E.
0x0010:  0044 d23d 0000 4001 264f c0a8 0001 c0a8  .D.=..@.&O.....
0x0020:  001b 0b00 722b 0000 0000 4500 0028 f96b  ....r+....E..(.k
0x0030:  0000 0111 4354 c0a8 001b 67f1 5451 f968  ....CT....g.TQ.h
0x0040:  829d 0014 06ba 0000 0000 0000 0000 0000  .....

```



```

0x0050: 0000
16:24:26.023202 IP 92.101.243.1 > 192.168.0.27: ICMP time exceeded in-transit, length 36
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 .....X.\"]..E.
0x0010: 0038 0000 0000 fe01 ac9a 5c65 f301 c0a8 .8.....\e....
0x0020: 001b 0b00 722b 0000 0000 4500 0028 f96c ....r+...E..(.l
0x0030: 0000 0111 4353 c0a8 001b 67f1 5451 f968 ....CS....g.TQ.h
0x0040: 829e 0014 06b9 .....
16:24:26.039601 IP 92.101.243.1 > 192.168.0.27: ICMP time exceeded in-transit, length 36
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 .....X.\"]..E.
0x0010: 0038 0000 0000 fe01 ac9a 5c65 f301 c0a8 .8.....\e....
0x0020: 001b 0b00 722b 0000 0000 4500 0028 f96d ....r+...E..(.m
0x0030: 0000 0111 4352 c0a8 001b 67f1 5451 f968 ....CR....g.TQ.h
0x0040: 829f 0014 06b8 .....
16:24:26.046610 IP 92.101.243.1 > 192.168.0.27: ICMP time exceeded in-transit, length 36
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 .....X.\"]..E.
0x0010: 0038 0000 0000 fe01 ac9a 5c65 f301 c0a8 .8.....\e....
0x0020: 001b 0b00 722b 0000 0000 4500 0028 f96e ....r+...E..(.n
0x0030: 0000 0111 4351 c0a8 001b 67f1 5451 f968 ....CQ....g.TQ.h
0x0040: 82a0 0014 06b7 .....
16:24:26.060951 IP 212.48.194.252 > 192.168.0.27: ICMP time exceeded in-transit, length 36
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 .....X.\"]..E.
0x0010: 0038 0000 0000 fd01 65d4 d430 c2fc c0a8 .8.....e..0....
0x0020: 001b 0b00 722b 0000 0000 4500 0028 f96f ....r+...E..(.o
0x0030: 0000 0111 4350 c0a8 001b 67f1 5451 f968 ....CP....g.TQ.h
0x0040: 82a1 0014 06b6 .....
16:24:26.084061 IP 212.48.194.252 > 192.168.0.27: ICMP time exceeded in-transit, length 36
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 .....X.\"]..E.
0x0010: 0038 0000 0000 fd01 65d4 d430 c2fc c0a8 .8.....e..0....
0x0020: 001b 0b00 722b 0000 0000 4500 0028 f970 ....r+...E..(.p
0x0030: 0000 0111 434f c0a8 001b 67f1 5451 f968 ....CO....g.TQ.h
0x0040: 82a2 0014 06b5 .....

```

Пакеты web-доступа:

Можно командой:

% tcpdump -r lab.pcap -n port http -XX (так как через браузер на 80 порту http):

```

reading from PCAP-NG file lab.pcap
16:29:08.571323 IP 192.168.0.27.58625 > 2.17.251.18.80: Flags [S], seq 323534951, win 0, options [mss
1460,nop,wscale 6,nop,nop,TS val 2120316617 ecr 0,sackOK,eol], length 0
0x0000: 58f8 5c22 275d 16d6 dee2 e027 0800 4500 X.\"].....E.
0x0010: 0040 0000 4000 4006 7cd1 c0a8 001b 0211 .@..@..|.....
0x0020: fb12 e501 0050 1348 c067 0000 0000 b002 .....P.H.g.....
0x0030: 0000 cae8 0000 0204 05b4 0103 0306 0101 .....
0x0040: 080a 7e61 76c9 0000 0000 0402 0000 ..~av.....
16:29:08.603509 IP 2.17.251.18.80 > 192.168.0.27.58625: Flags [S], seq 1267293982, ack 323534952, win
65160, options [mss 1452,sackOK,TS val 3279975958 ecr 2120316617,nop,wscale 7], length 0
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 .....X.\"]..E.
0x0010: 003c 0000 4000 3906 83d5 0211 fb12 c0a8 <..@.9.....
0x0020: 001b 0050 e501 4b89 5f1e 1348 c068 a012 ...P..K..H.h..
0x0030: fe88 f91b 0000 0204 05ac 0402 080a c380 .....
0x0040: 7616 7e61 76c9 0103 0307 v..~av....
16:29:08.604185 IP 192.168.0.27.58625 > 2.17.251.18.80: Flags [.], ack 1, win 45, options [nop,nop,TS val
2120316650 ecr 3279975958], length 0
0x0000: 58f8 5c22 275d 16d6 dee2 e027 0800 4500 X.\"].....E.
0x0010: 0034 0000 4000 4006 7cdd c0a8 001b 0211 .4..@..|.....
0x0020: fb12 e501 0050 1348 c068 4b89 5f1f 8010 .....P.H.hK._...
0x0030: 002d 261b 0000 0101 080a 7e61 76ea c380 .-&.....~av...
0x0040: 7616 v.
16:29:08.604185 IP 192.168.0.27.58625 > 2.17.251.18.80: Flags [P.], seq 1:154, ack 1, win 45, options
[nop,nop,TS val 2120316650 ecr 3279975958], length 153: HTTP: CONNECT proxy-safebrowsing.googleapis.com:443
HTTP/1.1
0x0000: 58f8 5c22 275d 16d6 dee2 e027 0800 4500 X.\"].....E.
0x0010: 00cd 0000 4000 4006 7c44 c0a8 001b 0211 ....@..|D.....
0x0020: fb12 e501 0050 1348 c068 4b89 5f1f 8018 .....P.H.hK._...
0x0030: 002d ccaf 0000 0101 080a 7e61 76ea c380 .-.....~av...
0x0040: 7616 434f 4e4e 4543 5420 7072 6f78 792d v.CONNECT.proxy-
0x0050: 7361 6665 6272 6f77 7369 6e67 2e67 6f6f safebrowsing.goo
0x0060: 676c 6561 7069 732e 636f 6d3a 3434 3320 gleapis.com:443.
0x0070: 4854 5450 2f31 2e31 0d0a 486f 7374 3a20 HTTP/1.1..Host:.
0x0080: 7072 6f78 792d 7361 6665 6272 6f77 7369 proxy-safebrowsi
0x0090: 6e67 2e67 6f6f 676c 6561 7069 732e 636f ng.googleapis.co

```

```

0x00a0: 6d0d 0a50 726f 7879 2d43 6f6e 6e65 6374 m..Proxy-Connect
0x00b0: 696f 6e3a 206b 6565 702d 616c 6976 650d ion:.keep-alive.
0x00c0: 0a43 6f6e 6e65 6374 696f 6e3a 206b 6565 .Connection:.kee
0x00d0: 702d 616c 6976 650d 0a0d 0a p-alive....
16:29:08.634873 IP 2.17.251.18.80 > 192.168.0.27.58625: Flags [.], ack 154, win 508, options [nop,nop,TS val
3279975990 ecr 2120316650], length 0
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 ..... 'X.\'']..E.
0x0010: 0034 56d9 4000 3906 2d04 0211 fb12 c0a8 .4V.@.9.-.....
0x0020: 001b 0050 e501 4b89 5f1f 1348 c101 8010 ...P..K._..H....
0x0030: 01fc 2393 0000 0101 080a c380 7636 7e61 ..#.....v6~a
0x0040: 76ea v.
16:29:08.634876 IP 2.17.251.18.80 > 192.168.0.27.58625: Flags [P.], seq 1:40, ack 154, win 508, options
[nop,nop,TS val 3279975991 ecr 2120316650], length 39: HTTP: HTTP/1.0 200 Connection established
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 ..... 'X.\'']..E.
0x0010: 005b 56da 4000 3906 2cdc 0211 fb12 c0a8 .[V.@.9.,.....
0x0020: 001b 0050 e501 4b89 5f1f 1348 c101 8018 ...P..K._..H....
0x0030: 01fc 19ab 0000 0101 080a c380 7637 7e61 .....v7~a
0x0040: 76ea 4854 5450 2f31 2e30 2032 3030 2043 v.HTTP/1.0.200.C
0x0050: 6f6e 6e65 6374 696f 6e20 6573 7461 626c onnection.establ
0x0060: 6973 6865 640d 0a0d 0a ished....
16:29:08.635959 IP 192.168.0.27.58625 > 2.17.251.18.80: Flags [.], ack 40, win 45, options [nop,nop,TS val
2120316681 ecr 3279975991], length 0
0x0000: 58f8 5c22 275d 16d6 dee2 e027 0800 4500 X.\''].....'..E.
0x0010: 0034 0000 4000 4006 7cdd c0a8 001b 0211 .4..@.@.|.....
0x0020: fb12 e501 0050 1348 c101 4b89 5f46 8010 .....P.H..K._F..
0x0030: 002d 251b 0000 0101 080a 7e61 7709 c380 .-%.....~aw...
0x0040: 7637 v7
16:29:08.635960 IP 192.168.0.27.58625 > 2.17.251.18.80: Flags [P.], seq 154:671, ack 40, win 45, options
[nop,nop,TS val 2120316681 ecr 3279975991], length 517: HTTP
0x0000: 58f8 5c22 275d 16d6 dee2 e027 0800 4500 X.\''].....'..E.
0x0010: 0239 0000 4000 4006 7ad8 c0a8 001b 0211 .9..@.@.z.....
0x0020: fb12 e501 0050 1348 c101 4b89 5f46 8018 .....P.H..K._F..
0x0030: 002d 52f7 0000 0101 080a 7e61 7709 c380 .-R.....~aw...
0x0040: 7637 1603 0102 0001 0001 fc03 034e 23f5 v7.....N#.
0x0050: 5eee 7674 c9d9 0f33 8fa0 334c af18 a623 ^.vt...3..3L...#
0x0060: ac1f 9c2c bd19 3099 4a3c b32d c820 bfcd ...,..0.J<.-....
0x0070: 109e 829e de92 c95c 5f16 07fa ab34 64df .....\_....4d.
0x0080: 46a9 e407 7045 57d7 4e8b 255f 3dbb 002a F...pEW.N._=...*
0x0090: eaea 1301 1302 1303 c02c c02b cca9 c030 .....+,...0
0x00a0: c02f cca8 c00a c009 c014 c013 009d 009c ./.....
0x00b0: 0035 002f c008 c012 000a 0100 0189 fafa .5./.....
0x00c0: 0000 0000 0026 0024 0000 2170 726f 7879 .....&.$..!proxy
0x00d0: 2d73 6166 6562 726f 7773 696e 672e 676f -safebrowsing.go
0x00e0: 6f67 6c65 6170 6973 2e63 6f6d 0017 0000 ogleapis.com....
0x00f0: ff01 0001 0000 0a00 0c00 0aaa aa00 1d00 .....
0x0100: 1700 1800 1900 0b00 0201 0000 1000 0e00 .....
0x0110: 0c02 6832 0868 7474 702f 312e 3100 0500 ..h2.http/1.1...
0x0120: 0501 0000 0000 000d 0016 0014 0403 0804 .....
0x0130: 0401 0503 0805 0805 0501 0806 0601 0201 .....
0x0140: 0012 0000 0033 002b 0029 aaaa 0001 0000 .....3.+.).....
0x0150: 1d00 201c 97df afc7 e412 3525 8cfa 5775 .....5%..Wu
0x0160: 4845 b584 afc7 90e1 c4ea c0c4 2dee 77d8 HE.....-w.
0x0170: 68d8 1a00 2d00 0201 0100 2b00 0b0a baba h...-.....+....
0x0180: 0304 0303 0302 0301 001b 0003 0200 016a .....j
0x0190: 6a00 0100 0015 00af 0000 0000 0000 0000 j.....
0x01a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0200: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0210: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0220: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0230: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0240: 0000 0000 0000 00 .....
16:29:08.667172 IP 2.17.251.18.80 > 192.168.0.27.58625: Flags [.], ack 671, win 504, options [nop,nop,TS val
3279976022 ecr 2120316681], length 0
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 ..... 'X.\'']..E.
0x0010: 0034 56db 4000 3906 2d02 0211 fb12 c0a8 .4V.@.9.-.....
0x0020: 001b 0050 e501 4b89 5f46 1348 c306 8010 ...P..K._F.H....
0x0030: 01f8 212c 0000 0101 080a c380 7656 7e61 ..!,.....vV~a

```

```

0x0040: 7709 w.
16:29:08.676780 IP 2.17.251.18.80 > 192.168.0.27.58625: Flags [.], seq 40:1480, ack 671, win 504, options
[nop,nop,TS val 3279976032 ecr 2120316681], length 1440: HTTP
0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 ..... 'X. \ ' ] ..E.
0x0010: 05d4 56dc 4000 3906 2761 0211 fb12 c0a8 ..V.@.9.'a.....
0x0020: 001b 0050 e501 4b89 5f46 1348 c306 8010 ...P..K._F.H....
0x0030: 01f8 2f93 0000 0101 080a c380 7660 7e61 .. / .....V`~a
0x0040: 7709 1603 0300 7a02 0000 7603 031c 3b17 w.....z...v...;
0x0050: c961 b360 3904 17ac fef9 f7bd c2d1 c999 ..a.`9.....
0x0060: 41c1 2d07 5640 512a 5913 9fbd 4620 bfcd A.-.V@Q*Y...F...
0x0070: 109e 829e de92 c95c 5f16 07fa ab34 64df ..... \_....4d.
0x0080: 46a9 e407 7045 57d7 4e8b 255f 3dbb 1301 F...pEW.N.%_=...
0x0090: 0000 2e00 3300 2400 1d00 206d 43da e287 .....3.$....mC...
0x00a0: 0952 d14b fcd0 21d8 3ea8 45a5 ef90 1c6a .R.K..!>.E....j
0x00b0: 44c0 e9ec 36ad 1668 68dc 7800 2b00 0203 D...6..hh.x.+...
0x00c0: 0414 0303 0001 0117 0303 1103 ae79 42df .....yB.
0x00d0: cbb8 3127 220a 9f4b eca3 5165 af11 a025 ..1'"..K..Qe...%
0x00e0: af71 c9a6 a3fb 4613 8b8f b50b bf85 a006 .q....F.....
0x00f0: 29c1 5d9f 92f8 608e 6e1c ad1a e15b 74ff ).]...`.n....[t.
0x0100: 57a7 ba02 f6ef 7754 8d6a be44 3a53 c9dc W.....wT.j.D:S..
0x0110: c072 80f0 de3f bba9 df91 f773 b244 16dc .r...?.....s.D..
0x0120: cbe3 f16c 280d 0e11 2df2 9fb1 8fbf 4bb6 ....l(....-....K.
0x0130: 93f7 5d12 a3c2 b3b7 4c63 7436 a322 ecfa ..].....Lct6."..
0x0140: b9a5 d01f 16e7 b6e3 9440 945c ac77 f082 .....@.\.w...
0x0150: 2b95 1a39 1170 61a2 96da 82a9 68f7 9ceb +..9.pa.....h...
0x0160: 3c4f a25f f666 b37a 5ebc beae 07aa 8b26 <O._.f.z^.....&
0x0170: 2cec 686d 71b5 a987 3bdc 5545 99e6 0317 ,.hmq....;UE....
0x0180: 7a6e 1f47 ad86 42f6 a8dd 2374 259d 1694 zn.G..B...#t%...
0x0190: d39f 0dc8 34f7 f939 40ba fled 3b70 4dc6 ....4..9@...;pM.
0x01a0: 4884 ab6e 8f3e 10bd c2f3 b292 16ca 3e72 H..n.>.....>r
0x01b0: 6557 8f1e ded1 6aa3 7d7c 0f06 07d2 4e95 eW....j.}|...N.
0x01c0: 36a6 c812 6a25 dbb6 3870 3729 117d 7a43 6...j%.8p7).}zC
0x01d0: 16d9 8811 2b32 e7e3 8336 ee24 9e8b e38b ....+2...6.$....
0x01e0: b4c5 b8cc 8e31 9cb9 09d5 e008 b6c5 a7c2 .....1.....
0x01f0: 33d2 826a a042 00df a84d 849a 0283 a67f 3..j.B...M.....
0x0200: 96cb b358 258d 83b4 126c ddac 7c30 193d ...X%....l..|0.=
0x0210: 6eb2 d045 62eb 95cc 2e11 5f8e 1311 e80b n..Eb....._.....
0x0220: ff0c 9dd6 d739 ea04 eff7 6048 436d 9a75 .....9....`HCm.u
0x0230: 3342 34c6 ebc0 d064 e597 1aa3 d0c4 f5da 3B4....d.....
0x0240: 4d29 7c9d 6304 b7e0 3452 e08b 40bd f038 M)|.c...4R...@..8
0x0250: c50e 45ec 4156 f7d7 8a43 493d ee9c 246d ..E.AV...CI=..$m
0x0260: 4878 e037 629d 4e2a 7191 0a6a 53d6 7c80 Hx.7b.N*q...jS.|.
0x0270: cca3 04c3 12a3 167e 20ee e302 c765 c0b1 .....~.....e..
0x0280: 8556 8d34 60c8 99b3 d44b 13fe 84ba 8893 .V.4`....K.....
0x0290: b417 f2fb dd3d 4f65 e633 8aaf 0d80 a171 .....=Oe.3.....q
0x02a0: 895f 4907 bd72 a979 5a77 42a6 e946 ad28 ._I..r.yZwB..F.(
0x02b0: 5516 7d52 4ec8 bb7a 1948 0e0a bd94 7a59 U.}RN..z.H....zY
0x02c0: 6a1e 7ab0 f4a2 a25a e9ee 1bd7 de29 6031 j.z....Z.....)`1
0x02d0: bce6 d297 2a4c aa57 abc4 743c df7e 157b ....*L.W..t<..~.{
0x02e0: 9d2f 6858 49eb b2b3 a148 bfca bf4a f650 ./hXI....H...J.P
0x02f0: 15f8 e453 6178 2048 16d8 8616 4de0 9574 ...Sax.H....M..t
0x0300: 4ba0 9f43 feb3 ec3a 139a 3a80 81ac 4d57 K..C.....:...MW
0x0310: ce38 7874 288d e0e5 54f3 a92d 751d 4f17 .8xt(...T..-u.O.
0x0320: 8a3c 3230 920a 6c0d 6a41 d2c8 593a 7914 .<20...l.jA..Y:y.
0x0330: f94d 5d58 9c91 6645 734c 821b aa3f c605 .M]X...fEsL...?..
0x0340: c0bc 0d91 d309 319c c258 c748 8e2e 556e .....1..X.H..Un
0x0350: fe2c bfc6 1ff4 a72e 1f3f 4837 6b2f ca86 ,.....?H7k/..
0x0360: 71df 77de d05f 0721 2622 bc13 20a0 2bd8 q.w..._!&".....+.
0x0370: 7878 c2fa b934 c19d 1c11 c1c6 fd7b 164d xx...4.....{.M
0x0380: 290f 6b25 c634 0728 0119 60ff f4c3 d436 ).k%.4.(..`....6
0x0390: a90e 8805 0b78 6f5e f6bc bf36 99c3 cd67 .....xo^....6...g
0x03a0: 7b37 190f 0ef9 6155 5c1a ca9e 6245 c938 {7....aU\...bE.8
0x03b0: d92c 9982 0d7b f073 e5a6 c16f 4a10 daab ,....{.s....oJ...
0x03c0: 3267 a24a 80e0 ced5 a27b 590c 4988 5582 2g.J.....{Y.I.U.
0x03d0: 8edc 7d4a 2f5f a139 afac 03c4 5661 b08b ..}J/_..9....Va..
0x03e0: a96d 723e 98b9 7261 ee99 814d d313 cb5c .mr>...ra...M...\
0x03f0: 0621 d7af 1eaf a2fc 0b54 1dfa 6d40 8ba1 .!.....T..m@..
0x0400: 3de1 a3c2 9d2b 2fb3 23b4 a6d7 57b5 15ab =....+/.#...W...
0x0410: 9e8a ab9d 7bdf 16f8 0b7a 0353 6528 a6c1 ....{....z.Se(..
0x0420: 3da8 e355 aa23 a38a 4a87 49a2 7a02 ae1b =..U.#...J.I.z...
0x0430: 8f89 8ebf 0221 66da 5d1c 8cdd 783a 37eb .....!f.]....x:7.
0x0440: 8e40 6b9a 710a b6bd 3556 5752 b3dd 3031 .@k.q...5VWR..01

```

```

0x0450: 1c2d aeb1 753b 3479 6b0b e462 57a2 a6e9 .-.u;4yk..bW...
0x0460: 7acf 2f09 7926 df8e 6fd1 b118 c6fd 5c48 z./y&..o.....\H
0x0470: 408d a8f1 b922 4245 21a8 8517 38c6 2e08 @...."BE!...8...
0x0480: 4f9f ac67 6955 5a8f c1db 30bc 566b d15d O..giUZ...0.Vk.]
0x0490: 0088 9af5 aa57 1543 f812 9549 a218 d28d .....W.C...I....
0x04a0: 3f6a 76a7 3fbb 3d3e 0980 72c3 52d6 89ac ?jv.?.=>..r.R...
0x04b0: 010f df51 5d9f 46df 4c8b 3574 24c7 e8b6 ...Q].F.L.5t$....
0x04c0: d769 86be edb5 a2ae 4824 61e0 63ca efe5 .i.....H$A.c...
0x04d0: 41af f6d1 c037 9945 3e37 2dc4 54f1 7888 A....7.E>7-.T.x.
0x04e0: fb53 8fe6 540b d105 f37a bd44 d25d fd7f .S..T....z.D.].
0x04f0: 967d 7ed1 5034 db88 0d79 1eab c793 99d9 .}~.P4...y.....
0x0500: b1aa 8cef 92b8 47bb a49a ae5e 5b4d 2383 .....G....^[M#.
0x0510: 2e8e 5ac4 93dd 7f73 55da 3625 b88a d5f8 ..Z....sU.6%.
0x0520: 81b9 e9c6 46d5 d347 75a0 903f 36ce f6ad ....F..Gu.?6...
0x0530: 43f7 ffee cc0b 77d2 d7ab 5758 507b 2dc7 C.....w...WXP{-
0x0540: d16f 28f3 8b06 139f 569f 86e0 d0e7 f270 .o(.....V.....p
0x0550: d425 dd6d 549a c55a ad76 351c be2b c364 .%.mT..Z.v5..+.d
0x0560: c0dc 3f88 9117 4da1 5170 0332 3b19 f890 ..?...M.Qp.2;...
0x0570: 224a 4677 10b3 f2f2 41fc 721b 87fb 369b "JFw....A.r...6.
0x0580: 837b bf1e 9f79 e843 a0fb a345 20e2 b3fd .{...y.C...E....
0x0590: a26b b163 ad0e 2dfd 0e0f 83e7 76f6 10ed .k.c.b-.....v...
0x05a0: 1a3e df0f 5d3e e24a 6766 156a 40a9 228a .>..]>.Jgf.j@.".
0x05b0: 11b9 ff88 bdf0 72bb 0d04 be96 3746 ba36 .....r.....7F.6
0x05c0: 2441 23e4 e26a bd46 59f8 7d06 70d0 3aee $A#..j.FY.}.p...
0x05d0: d1f3 c427 6d02 2528 fc72 5168 8cec da48 ...'m.%(rQh...H
0x05e0: bff8 ..

```

16:29:08.676782 IP 2.17.251.18.80 > 192.168.0.27.58625: Flags [P.], seq 1480:2920, ack 671, win 504, options [nop,nop,TS val 3279976032 ecr 2120316681], length 1440: HTTP

```

0x0000: 16d6 dee2 e027 58f8 5c22 275d 0800 4500 ..... 'X.\'']..E.
0x0010: 05d4 56dd 4000 3906 2760 0211 fb12 c0a8 ..V.@.9.'^.....
0x0020: 001b 0050 e501 4b89 64e6 1348 c306 8018 ...P..K.d..H....
0x0030: 01f8 a9d6 0000 0101 080a c380 7660 7e61 .....v~a
0x0040: 7709 79f3 a7b4 1e2b 9a7c e07b f7a1 9678 w.y.....+|. {...x
0x0050: f2f0 7c58 e46a cff3 1b3a 3568 76a7 c8ea ..|X.j....:5hv...
0x0060: 0d2d f487 0d90 d03d 9482 874b 9aa4 4f14 .-.....=...K..O.
0x0070: 0f81 a049 7ee0 48d0 2ba3 5862 97c2 ab08 ...I~.H.+Xb....
0x0080: 03a0 ce67 50d0 0ed5 6537 08f6 5aa1 ed22 ...gP...e7..Z.."
0x0090: e8ef 5c49 6234 261b 4f33 a8c2 2f0e 94a2 ..\Ib4&.O3../...
0x00a0: 89df 0aa5 1fdd 8cc2 5326 bc7f 9ada 12f2 .....S&.....
0x00b0: af91 faa4 ef30 888d 604e f9c8 4bb5 b5ee .....0..`N..K...
0x00c0: c88e 27ce 0e67 f57a 450e bbc4 4c13 1516 ..'.g.zE...L...
0x00d0: be1c 167d 3222 31f9 e3fd b6b0 9e20 7bf5 ...}2"1.....{.
0x00e0: e3ce cac6 5800 4bb8 0a35 b587 4454 7331 ...X.K..5..DTs1
0x00f0: dd40 a45b 5dfd 50e9 129f a944 d6ab 14b5 .@.[.].P....D....
0x0100: 7ef3 4692 2730 8e5f 0cfd 33d6 727c 180d ~.F.'0._...3.r|.
0x0110: a3d8 bf5d a544 4300 06f1 71f2 5345 e542 ...].DC...q.SE.B
0x0120: 382b d714 3070 2c4f 1b17 eed0 e5b2 63bf 8+..0p,O.....c.
0x0130: c11b 8d0e 7501 98d8 7dc2 7d18 ea80 49f3 ....u....}....I.
0x0140: 7050 e170 11b6 10ae d52a 0bd8 ce50 f8b9 pP.p.....*...P..
0x0150: 8e98 8bfd 4ed9 99f9 db33 a407 0c5f 0bbe ....N....3...._..
0x0160: c57b 7139 92db 8e85 d301 b981 7c86 3942 .{q9.....|.9B
0x0170: 5c6a 264d 24c1 4d5a b972 8436 8b3e 2a03 \j&M$.Mz.r.6.>*.
0x0180: e6bb 2bf4 607e 7c25 37fb 5126 bbed 2e9c ..+.`~|7.Q&....
0x0190: 8dee 0533 7c32 5949 93f3 af47 3019 bf42 ...3|2YI...G0..B
0x01a0: 9d51 4aff 8290 767e 26ef bda4 941d 7d85 .QJ...v~&.....}.
0x01b0: 94e7 1695 2574 5716 c66d f484 cbbb 9774 ....%tW..m.....t
0x01c0: f6e8 07e3 6e7e b7ac 1560 fef4 b3eb 46b0 ....n~....`....F.
0x01d0: 121f 29a3 9989 5166 e0a7 fbd6 3f43 f42c ..)...Qf....?C.,
0x01e0: 01a7 6551 c0df ae26 7009 94a8 2f4a 8b71 ..eQ...&p.../J.q
0x01f0: 88ed 0eb0 c77b ce01 dd52 62bb c35d c774 .....{...Rb..}.t
0x0200: c288 9eac 37ac f8d9 d82f 233f 6d46 ec18 ....7..../#?mF..
0x0210: 15d3 0100 7583 c9e9 f7da 5453 7da1 a858 ....u.....TS}.X
0x0220: c10a baae 2135 7faa 708d d48f 475e 486b ....!5..p...G^Hk
0x0230: f9f8 9a9f e20b 20da 48ff fa9e 7a10 d9f1 .....H...z....
0x0240: e52d b465 cd80 6e66 cc5a 2b00 ae9d 1550 .-.e..nf.Z+....P
0x0250: 7f64 1939 f184 27d7 8171 f808 b1a1 e980 .d.9...'.q.....
0x0260: 9f07 ab1a a3b8 0338 55fa 85b4 f614 0e2e .....8U.....
0x0270: cc06 a4ed 87d4 lcec 367b 73db 642d cc0e .....6{s.d-..
0x0280: c194 8c48 5135 4625 a862 c844 3354 02d6 ...HQ5F%.b.D3T..
0x0290: 965a 5724 716b 2279 01ea a56c 9a19 489b .ZW$gk"y...l..H.
0x02a0: d861 e273 925e 3948 0ca3 25e3 0cb4 74ad .a.s.^9H..%...t.
0x02b0: 80bc cfc7 b4c8 572c 18d8 e4b9 effc 9093 .....W,.....

```

```

0x02c0: f4e1 95a3 9eaa 9b03 d678 d165 3a46 da9d .....x.e:F..
0x02d0: 934a 16aa b10d cf76 3c9f 3c71 8e0b 20bd .J.....v<.<q....
0x02e0: 23b6 97df 1bda ad72 bcb3 45b2 f8df c263 #.....r..E....c
0x02f0: 1514 0960 fe51 b54e 2ff1 1866 e936 6093 ...`.Q.N/..f.6`.
0x0300: 8432 3af5 f801 fe1c 1df4 28b2 8c79 5b1e .2:.....(.y[.
0x0310: a765 4dc0 0e4b 6333 2536 1a1a e3b1 ac66 .eM..Kc3%6.....f
0x0320: 2d20 848f 0988 7045 e7f1 8d0d 443d 4b11 ~.....pE....D=K.
0x0330: 8f4d 550d 647c c296 2e81 67c4 afce 273a .MU.d|....g...':
0x0340: d41d a5cd 761b 2ead ed4c 3778 eb9b e430 ....v....L7x...0
0x0350: 2b68 9851 12bc c94c c854 2ae2 cec6 a4bb +h.Q...L.T*.....
0x0360: 6120 386b 6931 4260 82d5 602f 580a 154f a.8ki1B`..`/X..O
0x0370: d145 74f2 58cd d02f 746a 5ff4 4d5e a31e .Et.X../tj_.M^..
0x0380: 2153 0627 c134 23b0 3452 4d3f bcbf 71b2 !S.'.4#.4RM?...q.
0x0390: 14d9 c515 131f faf8 b140 2f54 344b c7fb .....@/T4K..
0x03a0: b5c1 e154 868f 6107 70e5 3242 7d68 1b19 ...T..a.p.2B}h..
0x03b0: 5076 cb4f 0e50 4ad3 3dec 16c5 61e1 0edf Pv.O.PJ.=...a...
0x03c0: f96a 41fc 7b4c 8ada f9e7 b177 9164 a781 .jA.{L.....w.d..
0x03d0: f3b9 79db ebbf 834a fa54 63f4 73a1 e4b9 ..y....J.Tc.s...
0x03e0: 5da4 6b04 8ede 269f 1056 7c36 9106 e51d ].k...&..V|6....
0x03f0: 3ec9 0bc7 2079 81df 8d0a ab42 5ddf 7217 >....y.....B].r.
0x0400: 1362 118e 5d16 bfe2 47f9 204a 6417 03b4 .b..]...G..Jd...
0x0410: 3b72 693a 6d26 cc58 8417 a79f 7010 db6e ;ri:m&X....p..n
0x0420: 4722 e9ad 8afd 694b 54b3 764c 304f 1876 G"....iKT.vL0O.v
0x0430: 4fe5 09c0 4b08 ab5f 1660 b830 723b a775 O...K...`.0r;u
0x0440: 5643 c312 4b6d 863f 1f31 a52e b62a 7ae3 VC..Km.?.1...*z.
0x0450: 4057 44c0 7878 122c f7ba 369e f1c3 b3b2 @WD.xx.,.6.....
0x0460: 94fd fb9f cb4b 56d1 60fa 7a8a 901f 8a86 .....KV.`.z.....
0x0470: 006f 664a f934 89c3 9037 61ab 8902 c8f6 .ofJ.4...7a.....
0x0480: 0c0a 1039 d965 aed8 200c 7ac2 5184 8719 ...9.e....z.Q...
0x0490: 1a3b b9c0 abd7 c5a0 1406 765e 5732 6f32 .;.....v^W2o2
0x04a0: 00db 567d 1510 23b2 6e48 5e81 800c b9ca ..V}...#.nH^.....
0x04b0: f5b5 0efe 54fb ab80 d696 a678 101d 8ea8 ....T.....x....
0x04c0: 8939 4c15 20e8 836a 48d3 6b89 f999 da77 .9L....jH.k....w
0x04d0: 7bda d3a8 7507 ac8c 7359 514c 616b 20a2 {...u....sYQLak..
0x04e0: e81e f84c 963e 7568 8f75 1a97 c241 301a ...L.>uh.u...A0.
0x04f0: b0fc 4204 82dd da34 8b45 8d74 6a34 c7dc ..B....4.E.tj4..
0x0500: ef16 20dc 389b 6a7c f9ca cc61 5930 9d31 ....8.j|...aY0.1
0x0510: bb5f d760 703e 026f e96a e49b 9527 7b79 ._.`p>.o.j...'{y
0x0520: cdac 0374 09f9 025c 8a71 3a76 36ec c799 ...t...\.q:v6...
0x0530: d4bf 707a cd8c 5efe 77c6 cf14 cbb2 f94e ..pz...^..w.....N
0x0540: 31e0 e974 0070 1840 e38d cf6b 6da7 e566 1..t.p.@...km..f
0x0550: 915d 6f5f f2a0 9748 b7ae 687b 5a02 780b .]o_...H..h{Z.x.
0x0560: b6c7 f5cb 01c9 8ffe adbc eb4f 90cd f2b5 .....O.....
0x0570: c9b7 71c1 4003 f5db 6eb6 da45 bcfa f9eb ..q.@...n..E....
0x0580: acb6 15d4 91ec 40fd f5a2 0453 6c91 8d19 .....@....Sl...
0x0590: d6d7 800d e096 982c 974a 690c c741 d422 .....,.Ji..A."
0x05a0: 3427 f348 9e7e 3695 34f1 5707 f456 cbce 4'.H.-6.4.W..V..
0x05b0: dfba 8296 a6c4 71fa 03ed d01b 27b6 572b .....q.....'.W+
0x05c0: 84a1 5225 8c52 7ecf 8efe 06bf 3192 0102 ..R%.R~.....l...
0x05d0: aa51 7442 74fd 38fb 2cf1 eaeb 5eab 729a .QtBt.8.,...^..r.
0x05e0: 2f19 /

```

16:29:08.677361 IP 192.168.0.27.58625 > 2.17.251.18.80: Flags [.] , ack 2920, win 45, options [nop,nop,TS val

Флаги:

- SYN (Synchronize): Используется для инициирования соединения. При установлении соединения между клиентом и сервером один из них отправляет пакет с флагом SYN.
- ACK (Acknowledgment): Указывает на подтверждение получения пакета. Каждый раз, когда одно устройство получает пакет, оно отправляет обратно ответ с установленным флагом ACK.
- FIN (Finish): Указывает на завершение соединения. Устройство, желающее закрыть соединение, отправляет пакет с флагом FIN.
- RST (Reset): Используется для сброса соединения. Это может произойти, если ожидается, что соединение было потеряно или если одно из устройств не может обработать запрос.

- PSH (Push): Указывает на то, что данные, содержащиеся в данном пакете, должны быть немедленно переданы выше по стеку. Это может быть полезно для интерактивных приложений, где задержка недопустима.
- URG (Urgent): Указывает на то, что данные в пакете являются срочными. Это позволяет передать приоритетные данные первым, даже если другие пакеты в очереди имеют более низкий приоритет.
- ECE (ECN-Echo): Используется для сигнализации о сетевой перегрузке, в рамках механизма контроля перегрузки.
- CWR (Congestion Window Reduced): Используется для подтверждения получения уведомления о перегрузке (ECE) и уведомляет об уменьшении размера окна передачи.
- NS (Nonce Sum): Используется для защиты от атак на последовательность номеров в TCP.

Заключение

В ходе лабораторной работы №2 были изучены команды для определения параметров сети, проверки подключения (ping), трассировки маршрутов (traceroute), так же получены навыки работы с программой сбора и анализа трафика с помощью встроенной (UNIX) утилиты tcpdump.

Для решения задач был использован терминал zsh, утилита tcpdump, команды сохраняющие в файл lab прочитанный дамп формата .pcap, и отфильтрованный командами tcpdump -г.