

Курбатов Ярослав, РПО МКН

1. Wireshark: DHCP

1) DHCP работает поверх UDP:

No.

Time

Source

Destination

Protocol

Length

Info

58

12.199333517

0.0.0.0

255.255.255.255

DHCP

342

DHCP Discover - Transaction ID 0x58311952

59

12.205127175

192.168.0.1

192.168.0.141

DHCP

590

DHCP Offer - Transaction ID 0x58311952

60

12.205808731

0.0.0.0

255.255.255.255

DHCP

342

DHCP Request - Transaction ID 0x58311952

61

12.211808568

192.168.0.1

192.168.0.141

DHCP

590

DHCP ACK - Transaction ID 0x58311952

Frame 58: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlx7062b8b3c121, id 0

Ethernet II, Src: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x58311952

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)

0020

ff

ff

00

40

00

40

01

34

21

b0

01

01

00

00

58

31

0-C-4 !

X1

0030

19

52

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

R

9

0040

00

00

00

00

00

70

62

b8

b3

c1

21

00

00

00

00

00

00

00

00

pb

!

0050

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

0060

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

0070

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

0080

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

0090

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00a0

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00b0

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00c0

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

00

2) чтобы узнать мой mac address, посмотрим вкладку ethernet:

bootp

No.	Time	Source	Destination	Protocol	Length	Info
58	12.190333517	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x58311952
59	12.205127175	192.168.0.1	192.168.0.141	DHCP	590	DHCP Offer - Transaction ID 0x58311952
60	12.205808731	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x58311952
61	12.211808568	192.168.0.1	192.168.0.141	DHCP	590	DHCP ACK - Transaction ID 0x58311952

Frame 58: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlx7062b8b3c121, id 0

Ethernet II, Src: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Source Port: 68

Destination Port: 67

Length: 308

Checksum: 0x21b6 [unverified]

[Checksum Status: Unverified]

[Stream Index: 1]

[Timestamps]

UDP payload (300 bytes)

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x58311952

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

0000	ff	ff	ff	ff	ff	70	62	b8	b3	c1	21	00	00	45	10pb.....E	
0010	01	48	00	00	00	00	11	39	06	00	00	00	00	ff	ffH.....9	
0020	ff	ff	00	40	00	40	01	34	21	b0	01	01	00	00	58	31D-C-4 !.....X1
0030	19	52	00	00	00	00	00	00	00	00	00	00	00	00	00	00R.....9
0040	00	00	00	00	00	00	70	62	b8	b3	c1	21	00	00	00	00pb.....!
0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

адрес 70:62:b8:b3:c1:21.

3) значение Transaction-ID – 0x58311952:

No.	Time	Source	Destination	Protocol	Length	Info
58	12.198333517	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x58311952
59	12.205127175	192.168.0.1	192.168.0.141	DHCP	590	DHCP Offer - Transaction ID 0x58311952
60	12.205808731	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x58311952
61	12.211808568	192.168.0.1	192.168.0.141	DHCP	590	DHCP ACK - Transaction ID 0x58311952

Dynamic Host Configuration Protocol (ACK)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x58311952
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.0.141
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: D-LinkIn b3:c1:21 (70:62:b8:b3:c1:21)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Option: (54) DHCP Server Identifier (192.168.0.1)
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask (255.255.255.0)
Option: (3) Router
Option: (6) Domain Name Server

0020 00 0d 00 43 00 44 02 2c c6 09 02 01 00 00 50 31 - C.D. .1....X
0030 ff ff 00 00 00 00 00 00 00 00 c0 a8 0d 00 00 12 -
0040 00 00 00 00 00 00 70 62 b8 b3 c1 21 00 00 00 00 -pb
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -

Поле используется чтобы клиенты могли отличать свои запросы от чужих, так как в локальной сети одновременно может протекать несколько DHCP запросов/ответов.

4) Хост использует адрес отправки 0.0.0.0 и адрес назначения 255.255.255.255 (бродкаст):

No.	Time	Source	Destination	Protocol	Length	Info
58	12.198333517	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x58311952
59	12.205127175	192.168.0.1	192.168.0.141	DHCP	590	DHCP Offer - Transaction ID 0x58311952
60	12.205808731	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x58311952
61	12.211808568	192.168.0.1	192.168.0.141	DHCP	590	DHCP ACK - Transaction ID 0x58311952

Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
Total Length: 328
Identification: 0x0000 (0)
Flags: 0x00
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x3996 [validation disabled]
[Header checksum status: Unverified]
Source Address: 0.0.0.0
Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x58311952
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0

0010 01 48 00 00 00 00 11 39 96 50 00 00 00 ff ff - H.....9.....
0020 ff ff 00 44 00 43 01 34 21 b6 01 01 00 00 58 31 - D.C.4.1.....X1
0030 19 52 00 00 00 00 00 00 00 00 00 00 00 00 00 - R.....
0040 00 00 00 00 00 70 62 b8 b3 c1 21 00 00 00 00 -pb
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -

5) IP-адрес DHCP-севера – 192.168.0.1 (роутер):

No.	Time	Source	Destination	Protocol	Length	Info
58	12.190333517	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x58311952
59	12.205127175	192.168.0.1	192.168.0.141	DHCP	590	DHCP Offer - Transaction ID 0x58311952
60	12.20500731	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x58311952
61	12.211808568	192.168.0.1	192.168.0.141	DHCP	590	DHCP ACK - Transaction ID 0x58311952


```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
+ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total length: 576
Identification: 0x0000 (0)
+ Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xf0ce [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.141
Destination Address: 192.168.0.141
+ User Datagram Protocol, Src Port: 67, Dst Port: 68
- Dynamic Host Configuration Protocol (ACK)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x58311952
Seconds elapsed: 0
+ Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
0010 02 40 00 00 00 00 40 11 f6 ce 00 00 00 01 c0 a8 .....0.....X1
0020 00 00 00 43 00 44 02 2c c0 09 02 01 00 00 51 ...C.D.....X1
0030 19 52 00 00 00 00 00 00 00 00 c0 a8 00 0d 00 ..R.....
0040 00 00 00 00 00 00 70 62 bb b3 c1 21 00 00 00 .....pb.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

б) Lease time – это способ не допустить ситуации, когда один хост навсегда забирает из пула IP-адрес. Хост должен либо запросить продление своего адреса до окончания lease time, либо запросить новый после окончания lease. В моем случае этот период составляет 7 дней:

```

L  61 12.211808568  192.168.0.1          192.168.0.141      DHCP      590 DHCP ACK      - Transaction ID 0x58311952

Hardware address length: 6
Hops: 0
Transaction ID: 0x58311952
Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.141
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (ACK)
  ▶ Option: (54) DHCP Server Identifier (192.168.0.1)
  ▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (604800s) 7 days
  ▶ Option: (1) Subnet Mask (255.255.255.0)
  ▶ Option: (3) Router
  ▶ Option: (6) Domain Name Server
  ▶ Option: (255) End

0120 a8 00 01 33 04 00 09 3a 80 01 04 ff ff ff 00 03  --3...:  .....
0130 04 c0 a8 00 01 06 04 c0 a8 00 01 ff 00 00 00 00  .....
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

2. Программирование

1. Проверка целостности пакетов

Ruby MRI ~>3.0.0

Вычисление CRC8: 01-crc/crc8.rb

Запуск: ruby 01-crc/main.rb (ввод текстом, ctrl-d для сабмита)

Пример:

```
viralpraxis@primary:~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/13$ ruby 01-crc/main.rb
aiosdmjaqwrwiejmrflwiesjrflwiesjwerf
dpqwejkfrmwolkfrwejwfnwerjfg
9q34ier9230rfpsmfslk dfoiwmejiporjfmweiojpfewfs
wesfkdownsefjweoifj
[info]: changed byte at chunk 10
[info]: changed byte at chunk 11
[info]: changed byte at chunk 19
[info]: changed byte at chunk 22
[info]: changed byte at chunk 26
chunk: 1 payload: [97, 105, 111, 115, 100] crc8: 25 correct: true
chunk: 2 payload: [109, 106, 97, 113, 119] crc8: 202 correct: true
chunk: 3 payload: [114, 119, 105, 101, 106] crc8: 80 correct: true
chunk: 4 payload: [109, 114, 102, 105, 111] crc8: 188 correct: true
chunk: 5 payload: [119, 101, 115, 106, 114] crc8: 88 correct: true
chunk: 6 payload: [102, 105, 111, 119, 101] crc8: 99 correct: true
chunk: 7 payload: [115, 106, 119, 101, 114] crc8: 109 correct: true
chunk: 8 payload: [102, 10, 100, 112, 113] crc8: 231 correct: true
chunk: 9 payload: [119, 101, 106, 107, 102] crc8: 185 correct: true
chunk: 10 payload: [114, 109, 119, 111, 109] crc8: 181 correct: false ( actual: 178 )
chunk: 11 payload: [107, 102, 114, 120, 101] crc8: 118 correct: false ( actual: 181 )
chunk: 12 payload: [106, 119, 102, 110, 119] crc8: 248 correct: true
chunk: 13 payload: [101, 114, 106, 102, 103] crc8: 164 correct: true
chunk: 14 payload: [10, 57, 113, 51, 52] crc8: 148 correct: true
chunk: 15 payload: [105, 101, 114, 57, 50] crc8: 167 correct: true
chunk: 16 payload: [51, 48, 114, 102, 112] crc8: 52 correct: true
chunk: 17 payload: [115, 109, 102, 115, 108] crc8: 181 correct: true
chunk: 18 payload: [107, 32, 100, 102, 111] crc8: 50 correct: true
chunk: 19 payload: [105, 120, 109, 101, 106] crc8: 118 correct: false ( actual: 164 )
chunk: 20 payload: [105, 112, 111, 114, 106] crc8: 254 correct: true
chunk: 21 payload: [102, 109, 119, 101, 105] crc8: 145 correct: true
chunk: 22 payload: [111, 112, 107, 102, 101] crc8: 91 correct: false ( actual: 48 )
chunk: 23 payload: [119, 102, 115, 10, 119] crc8: 140 correct: true
chunk: 24 payload: [101, 115, 102, 107, 100] crc8: 168 correct: true
chunk: 25 payload: [111, 119, 115, 101, 102] crc8: 151 correct: true
chunk: 26 payload: [106, 119, 102, 111, 105] crc8: 10 correct: false ( actual: 183 )
chunk: 27 payload: [102, 106, 10] crc8: 249 correct: true
viralpraxis@primary:~/Documents/spbu/2023-spring/networks/spbu-masters-compnet/homeworks/13$
```

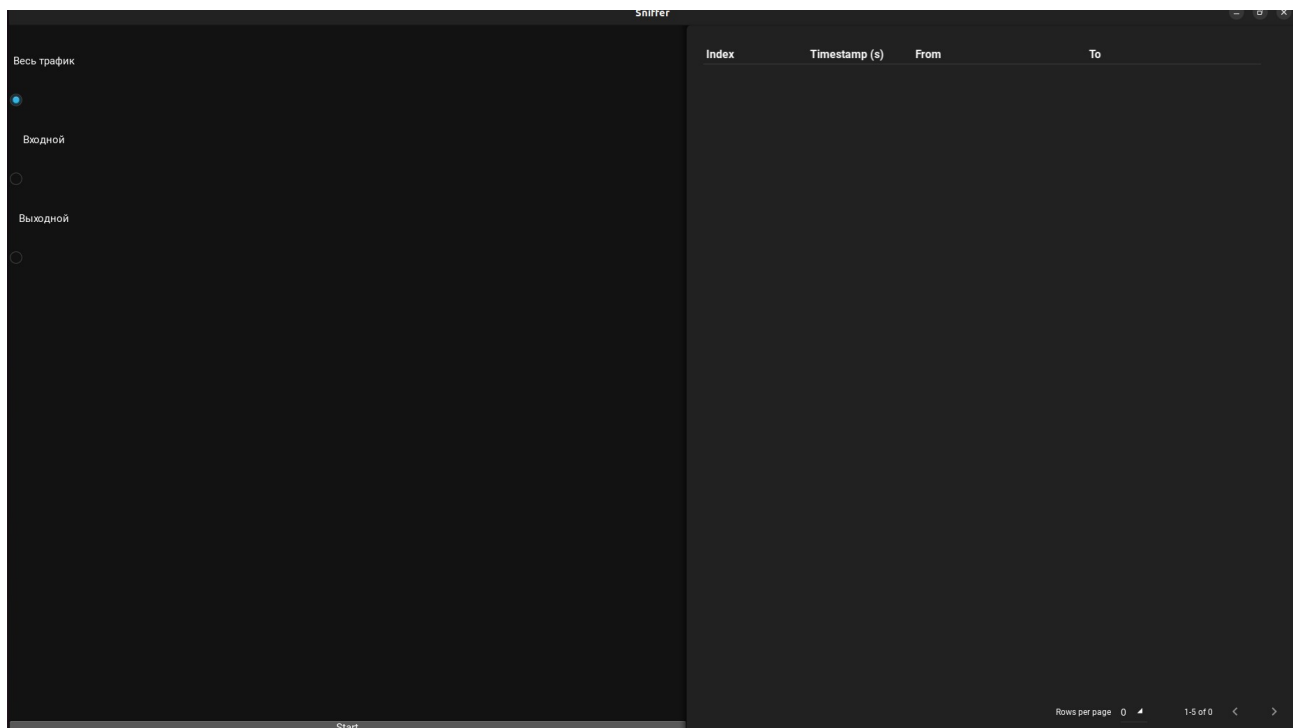
2. Подсчет сетевого трафика

Python ~> 3.10

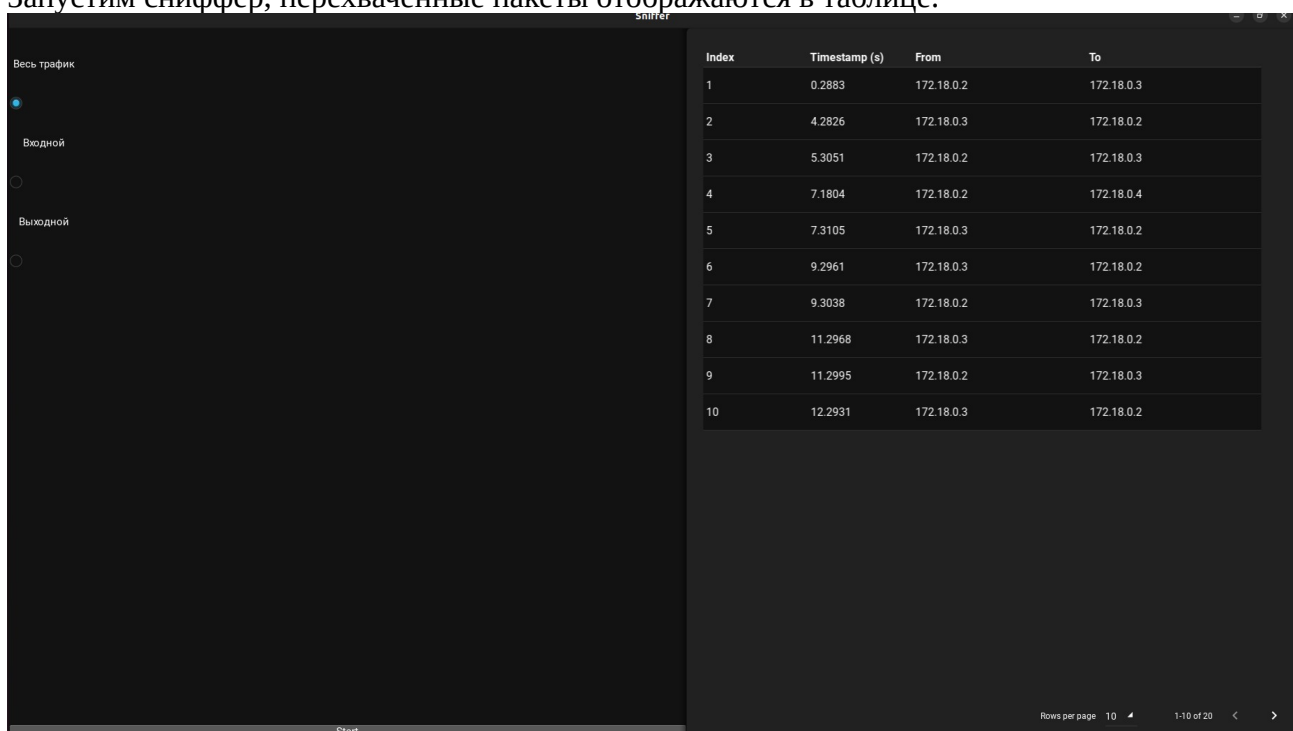
Зависимости указаны в 02-sniffer/requirements.txt

Запуск: [sudo] python main.py (нужны права su)

Начальное состояние UI:



Запустим сниффер, перехваченные пакеты отображаются в таблице:



При клике на пакет в таблице отображается информация о пакетах протоколов, которые инкапсулированы в этот пакет:

Весь трафик

Входной

Выходной

PROTOCOL: ethernet
src: 02:42:ac:12:00:02
dest: 02:42:ac:12:00:03
len: 66
epoch: 1685181455.5873976
—
PROTOCOL: ipv4
src: 172.18.0.2
dest: 172.18.0.3
len: 52
ttl: 64
checksum: 0xc0ca1
—
PROTOCOL: TCP
src port: 33904
dest port: 8123
seqnum: 347377433
window: 546

Start

Index	Timestamp (s)	From	To
1	0.2883	172.18.0.2	172.18.0.3
2	4.2826	172.18.0.3	172.18.0.2
3	5.3051	172.18.0.2	172.18.0.3
4	7.1804	172.18.0.2	172.18.0.4
5	7.3105	172.18.0.3	172.18.0.2
6	9.2961	172.18.0.3	172.18.0.2
7	9.3038	172.18.0.2	172.18.0.3
8	11.2968	172.18.0.3	172.18.0.2
9	11.2995	172.18.0.2	172.18.0.3
10	12.2931	172.18.0.3	172.18.0.2

Rows per page 10 1-10 of 25

Переключимся на режим “Входной трафик”:

Весь трафик

Входной

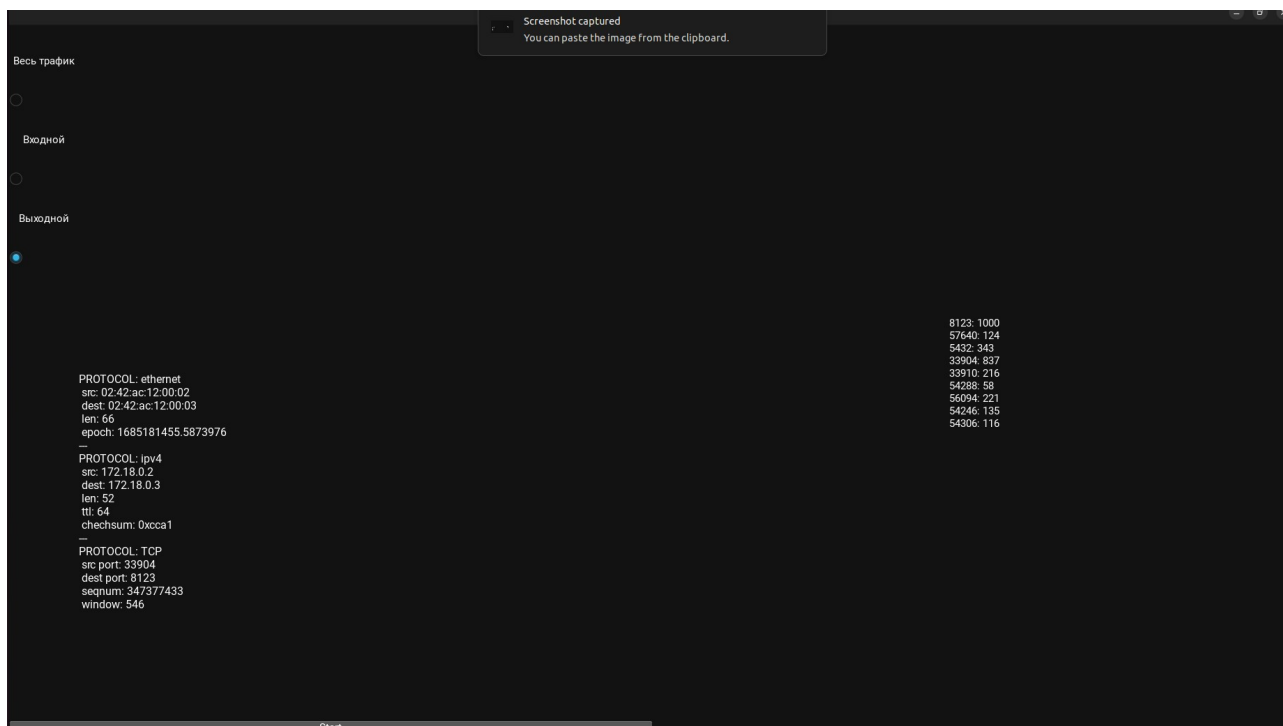
Выходной

PROTOCOL: ethernet
src: 02:42:ac:12:00:02
dest: 02:42:ac:12:00:03
len: 66
epoch: 1685181455.5873976
—
PROTOCOL: ipv4
src: 172.18.0.2
dest: 172.18.0.3
len: 52
ttl: 64
checksum: 0xc0ca1
—
PROTOCOL: TCP
src port: 33904
dest port: 8123
seqnum: 347377433
window: 546

Start

56028: 156
8123: 1266
54238: 52
33910: 104
57640: 52
56094: 344
5432: 251
33904: 344
54308: 57
54266: 63
54246: 57
54288: 57

И на режим “выходной трафик”:



NB: для удобства тестирования в таблице отображается только каждый 200-ый пакет (чтобы за ними можно уследить)

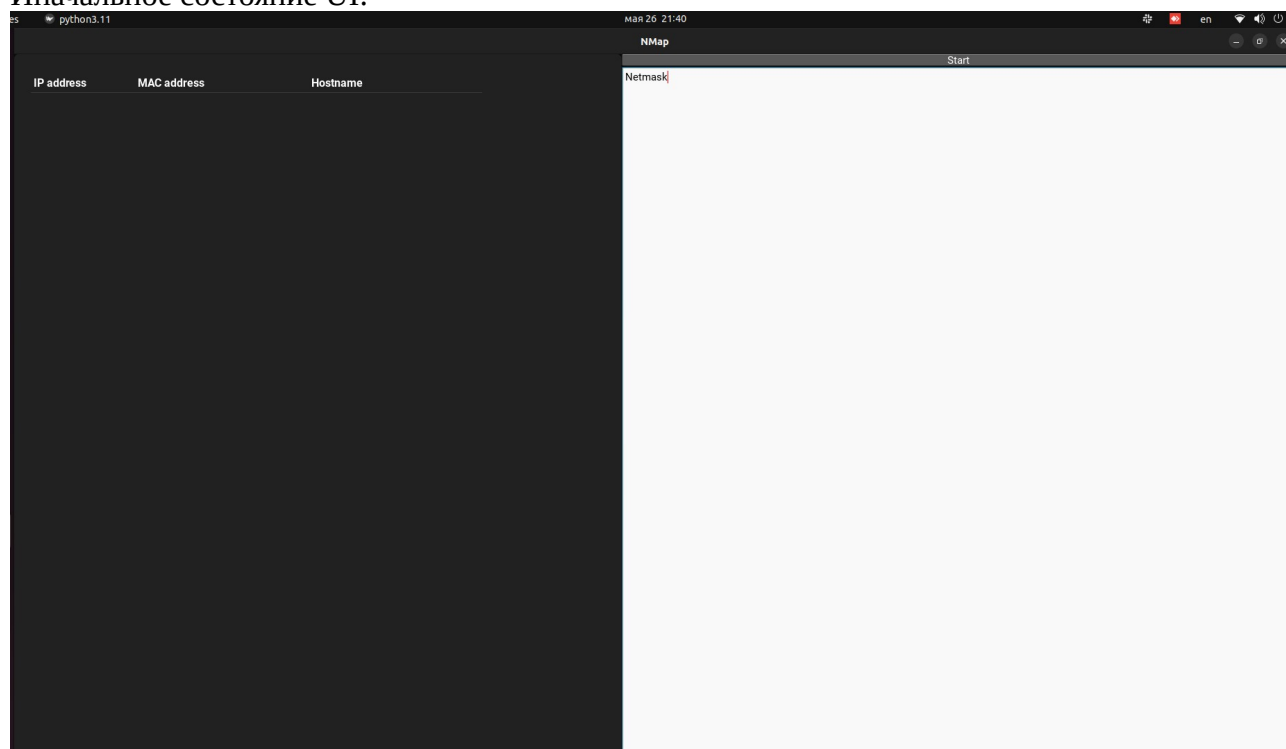
3. Определение всех компьютеров в сети

python ~> 3.11

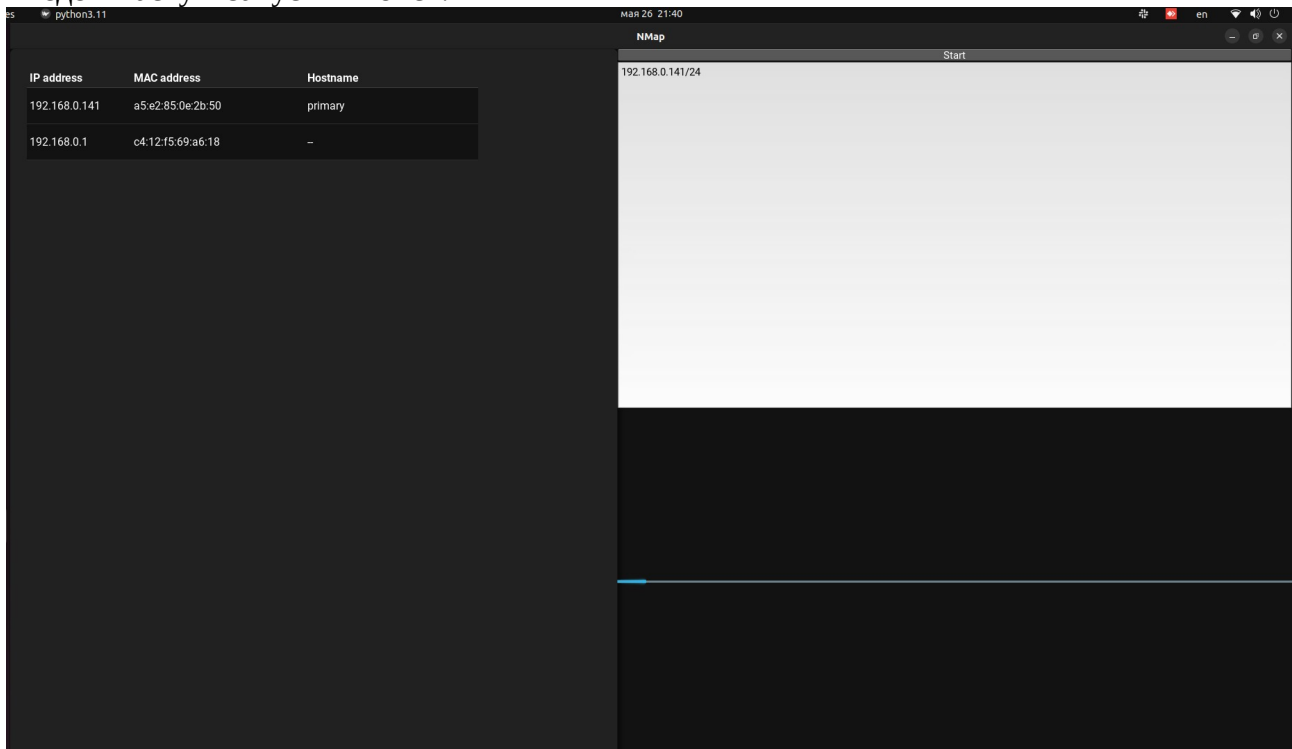
Зависимости указаны в 03-nmap/requirements.txt

Запуск: python 03-nmap/nmap/main.py

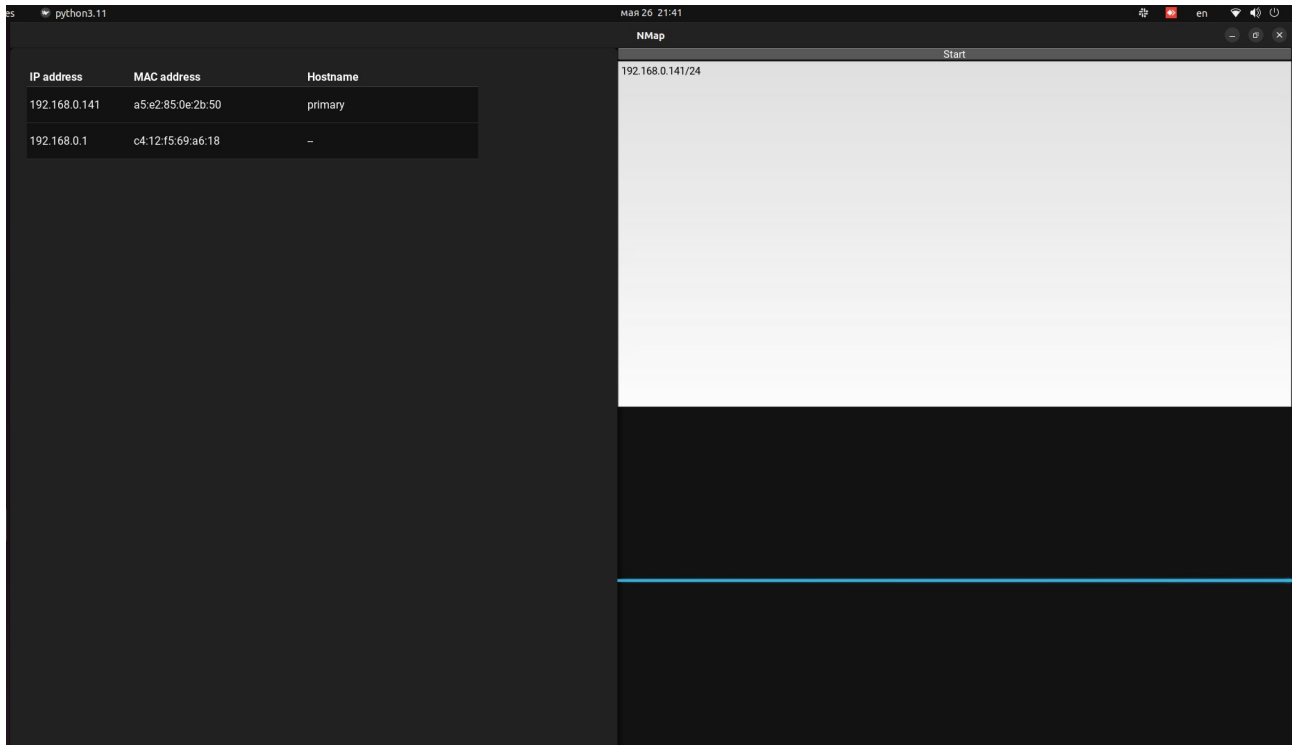
Иначальное состояние UI:



Введем маску и запустим поиск:



В результате программа обнаружила в локальной сети только мой роутер (в данный момент только он в сети и есть):



NB: отмечу, что первый IP адрес (адрес хоста) находится следующим образом: берется список всех адресов всех сетевых интерфейсов, из них находится тот, что удовлетворяет маске (см. `self_resolver.py`).

Задачи

Задача 1

а)

$$f(p) = Np(1-p)^{(N-1)}$$

найдем производную $f(p)$, считая N константой:

$$z(p) = dp/df f(p) = n(1-np)(1-p)^{(n-2)}$$

т.к. p лежит в $(0, 1)$, очевидно, $z(p) = 0$ при $p = 1/N$

Ответ: $N^{(-1)}$.

б)

Найдем $\lim Np(1-p)^{(N-1)}$ при $N \rightarrow \infty$

подставим $p = 1/N$

$$\lim (1 - 1/n)^{(n-1)} \text{ при } n \rightarrow \infty$$

$$\text{пусть } y = \lim_{n \rightarrow \infty} (1 - 1/n)^{(n-1)}$$

$$\ln y = \lim_{n \rightarrow \infty} \ln(1 - 1/n)^{(n-1)} = \lim_{n \rightarrow \infty} \ln(1 - 1/n) / (n-1)^{(-1)}$$

очевидно, можем применить правило Лопиталя:

$$\ln y = \lim_{n \rightarrow \infty} \ln(1 - 1/n) / (n-1)^{(-1)} = \lim_{n \rightarrow \infty} -1 * (n-1)^2 / (n-1) n = -1 * (n-1) n$$

$$\ln y = -1$$

$$y = e^{-1} \sim 0.367$$

Ответ: $1/e$