

**Министерство образования и науки Российской Федерации**  
**Федеральное государственное автономное образовательное**  
**учреждение высшего образования**  
**«Национальный исследовательский Университет ИТМО»**

**Факультет информационных технологий и программирования**  
**Кафедра компьютерных технологий**

**Практическая работа № 3**

**Выполнили студенты группы**  
**М3435, М3436:**

**Бурцева Полина Сергеевна**

**Кочетков Никита Олегович**

**Проверил:**

**Береснев Артем Дмитриевич**

**Санкт-Петербург**

**2020**

## Тексты команд и консольный вывод из Части 1, п.4-5

1.4

Имя хоста:

hostname

Ip-адрес:

hostname -i

Адрес DNS:

hostname -f

```
[root@c7 ~]# hostname
c7
[root@c7 ~]# hostname -i
fe80::a00:27ff:fed4:dcc8%enp0s3 192.168.31.102
[root@c7 ~]# hostname -f
c7
```

1.5

ping -c 5 8.8.8.8

```
[root@c7 ~]# ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=79.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=66.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=18.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=24.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=28.7 ms
```

## Скриншоты окон Wireshark с необходимыми данными заданий Части 2, п.2

2.2

Wireshark - Endpoints - Wi-Fi: en0

Ethernet · 4 IPv4 · 125 IPv6 · 2 TCP · 240 UDP · 141

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
63.35.29.156	3,150	3638 k	2,402	3581 k	748	56 k	—	—	—	—
151.236.74.70	2,505	2944 k	1,931	2905 k	574	38 k	—	—	—	—
173.194.222.18	2,083	1638 k	1,285	1502 k	798	136 k	—	—	—	—
87.240.185.199	973	933 k	611	907 k	362	25 k	—	—	—	—
87.240.190.72	1,011	862 k	591	827 k	420	35 k	—	—	—	—
192.168.31.33	16,355	14 M	5,852	810 k	10,503	13 M	—	—	—	—
87.240.185.151	541	493 k	323	476 k	218	16 k	—	—	—	—
93.186.227.134	375	339 k	223	328 k	152	11 k	—	—	—	—
173.194.221.196	345	340 k	255	327 k	90	12 k	—	—	—	—
173.194.73.99	408	287 k	282	266 k	126	20 k	—	—	—	—
87.240.185.161	221	192 k	128	185 k	93	7279	—	—	—	—
93.158.134.90	212	189 k	129	183 k	83	6828	—	—	—	—
93.186.227.146	212	183 k	123	175 k	89	8873	—	—	—	—
77.88.55.70	287	184 k	151	149 k	136	35 k	—	—	—	—
87.240.185.166	173	150 k	102	144 k	71	5827	—	—	—	—
93.186.227.148	150	128 k	86	122 k	64	5976	—	—	—	—
3.123.248.34	302	136 k	140	95 k	162	40 k	—	—	—	—
87.240.185.148	117	97 k	67	92 k	50	4441	—	—	—	—
93.186.227.140	126	94 k	70	88 k	56	6055	—	—	—	—
93.186.227.150	100	83 k	59	80 k	41	3847	—	—	—	—
93.186.227.152	108	81 k	61	74 k	47	6603	—	—	—	—
87.240.185.133	88	69 k	50	65 k	38	3648	—	—	—	—
87.240.185.134	81	63 k	46	60 k	35	3462	—	—	—	—
93.186.227.131	72	57 k	41	53 k	31	3187	—	—	—	—
87.240.185.135	81	53 k	43	48 k	38	4877	—	—	—	—
87.240.185.143	76	48 k	40	43 k	36	5369	—	—	—	—
64.233.162.101	93	47 k	54	39 k	39	8017	—	—	—	—
87.250.250.90	49	39 k	30	38 k	19	1785	—	—	—	—
87.240.185.140	55	38 k	29	35 k	26	3465	—	—	—	—
64.233.165.97	39	35 k	24	32 k	15	2724	—	—	—	—
213.180.204.239	38	31 k	22	28 k	16	3422	—	—	—	—
87.250.247.183	52	30 k	26	27 k	26	3002	—	—	—	—
64.233.162.95	58	36 k	30	27 k	28	8663	—	—	—	—
87.240.185.138	38	24 k	21	22 k	17	2351	—	—	—	—

☐ Name resolution ☐ Limit to display filter Endpoint Types ▾

Help Copy Map Close

a.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**eth.dst == ff:ff:ff:ff:ff:ff**

No.	Time	Source	Destination	Protocol	Length	Info
5449	24.279607366	XIAOMIE1_28:fe:b3	Broadcast	ARP	42	ARP Annou
5458	24.382606630	XIAOMIE1_28:fe:b3	Broadcast	ARP	42	Who has :
5459	24.382606813	XIAOMIE1_28:fe:b3	Broadcast	ARP	42	Who has :

Wireshark

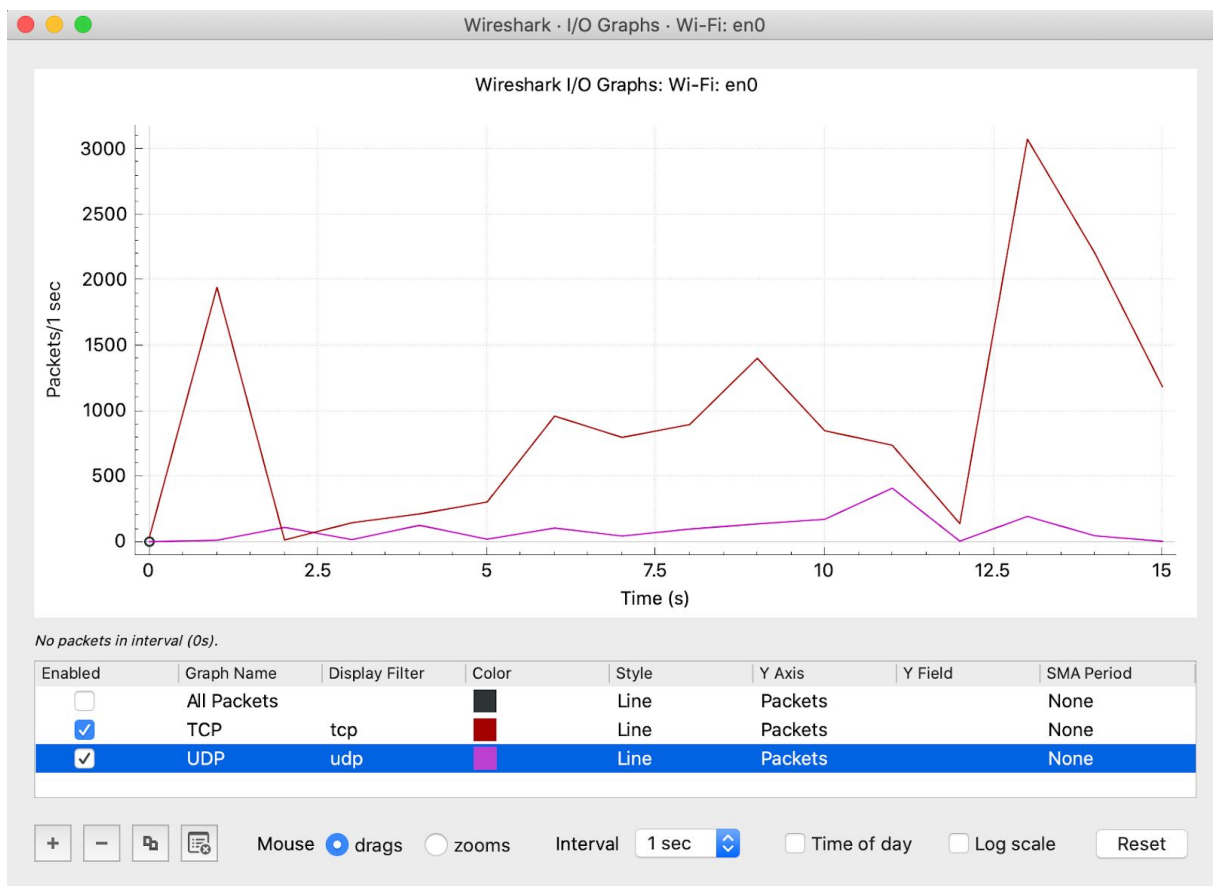
Ethernet · 2 IPv4 IPv6 TCP UDP

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
40:31:3c:28:fe:b3	248	10 k	248	10 k	0	
ff:ff:ff:ff:ff:ff	248	10 k	0	0	248	

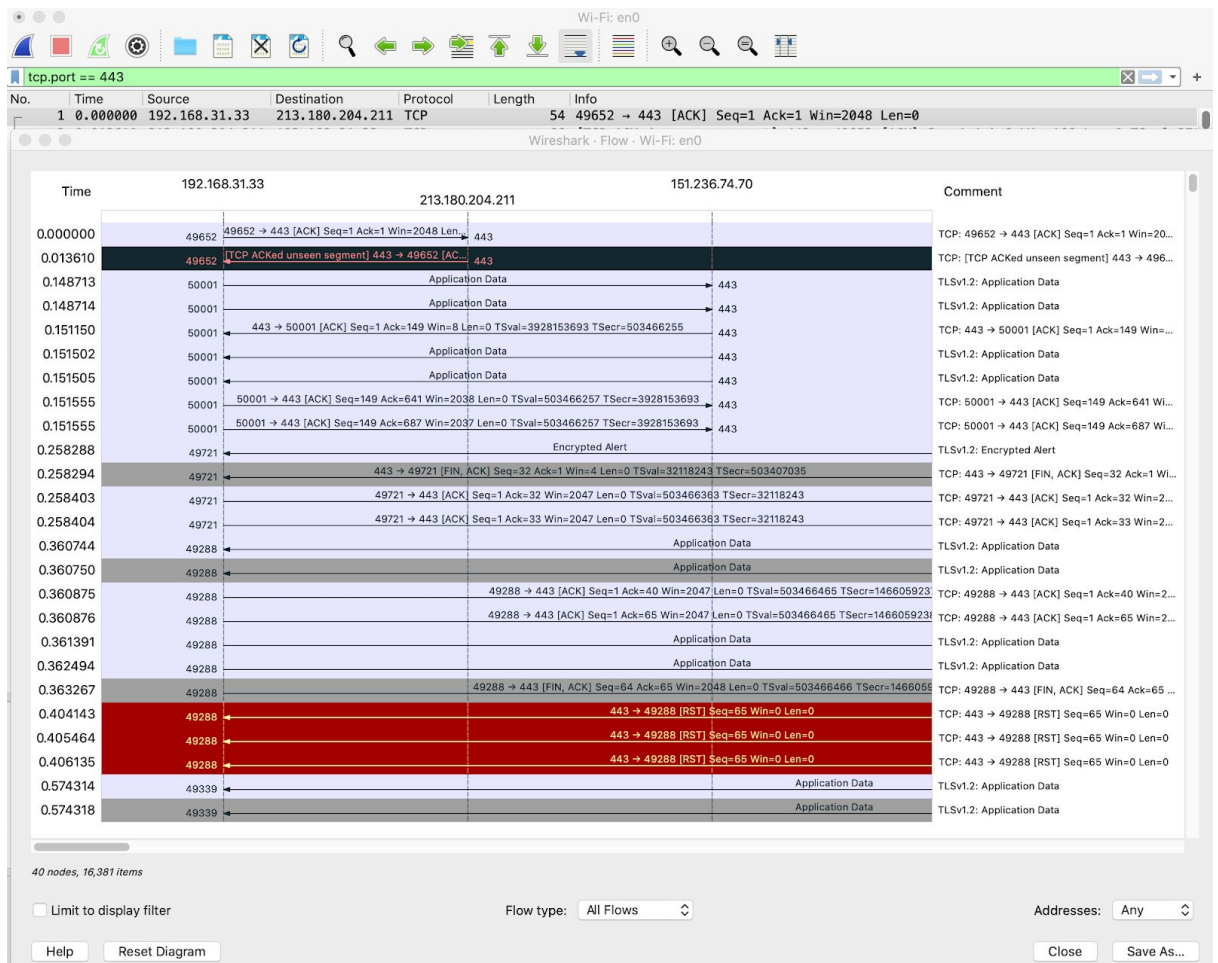
b.

Ethernet · 4    IPv4 · 125    IPv6 · 2    TCP · 240    UDP · 141							
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
63.35.29.156	443	3,150	3638 k	2,402	3581 k	748	56 k
151.236.74.70	443	2,505	2944 k	1,931	2905 k	574	38 k
173.194.222.18	443	2,083	1638 k	1,285	1502 k	798	136 k
192.168.31.33	50098	2,083	1638 k	798	136 k	1,285	1502 k
192.168.31.33	50094	2,851	3396 k	618	43 k	2,233	3353 k
87.240.185.199	443	973	933 k	611	907 k	362	25 k
87.240.190.72	443	1,011	862 k	591	827 k	420	35 k
192.168.31.33	50001	2,505	2944 k	574	38 k	1,931	2905 k
192.168.31.33	49978	1,011	862 k	420	35 k	591	827 k
192.168.31.33	50170	973	933 k	362	25 k	611	907 k
87.240.185.151	443	541	493 k	323	476 k	218	16 k
93.186.227.134	443	375	339 k	223	328 k	152	11 k
192.168.31.33	50130	541	493 k	218	16 k	323	476 k
192.168.31.33	50158	375	339 k	152	11 k	223	328 k
77.88.55.70	443	287	184 k	151	149 k	136	35 k
192.168.31.33	50107	284	130 k	151	39 k	133	91 k
3.123.248.34	443	302	136 k	140	95 k	162	40 k
192.168.31.33	49621	287	184 k	136	35 k	151	149 k
192.168.31.33	50111	299	241 k	130	13 k	169	227 k
93.158.134.90	443	212	189 k	129	183 k	83	6828
87.240.185.161	443	221	192 k	128	185 k	93	7279
93.186.227.146	443	212	183 k	123	175 k	89	8873
87.240.185.166	443	173	150 k	102	144 k	71	5827
192.168.31.33	50134	221	192 k	93	7279	128	185 k
192.168.31.33	50137	212	183 k	89	8873	123	175 k
93.186.227.148	443	150	128 k	86	122 k	64	5976
192.168.31.33	50171	212	189 k	83	6828	129	183 k
192.168.31.33	50117	173	150 k	71	5827	102	144 k
93.186.227.140	443	126	94 k	70	88 k	56	6055
87.240.185.148	443	117	97 k	67	92 k	50	4441
192.168.31.33	50122	150	128 k	64	5976	86	122 k
93.186.227.152	443	108	81 k	61	74 k	47	6603
93.186.227.150	443	100	83 k	59	80 k	41	3847
192.168.31.33	50161	117	97 k	50	4441	67	92 k

C.



d.



e.

## Текст фильтров Части 2, п.3.

### 2.3

- ((http.request or ftp.request) and !(ip.dst == 192.168.31.139)) or ((http.response or ftp.response) and !(ip.src == 192.168.31.139))
- eth.src == 60:f2:62:56:f9:73
- eth.dst == ff:ff:ff:ff:ff:ff
- eth.dst == ff:ff:ff:ff:ff:ff щелкаем на строку и смотрим на

```

Frame 9040: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: XIAOMIEI_28:fe:b3 (40:31:3c:28:fe:b3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: XIAOMIEI_28:fe:b3 (40:31:3c:28:fe:b3)
  Sender IP address: 192.168.31.1
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.31.254

```

MAC - каналный

IP - сетевой

- На которые поступают это, видимо, target
- e. eth.dst == ff:ff:ff:ff:ff:ff && arp -- других нет(((
  - f. Маршрутизатор (находит связь с роутером)

## Тексты команд и консольный вывод из Части 3, п.3-4.

### 3.3

```
nikita@UNIT-1620 ~$ netstat -an | grep -i listen
tcp4      0      0  127.0.0.1.6463      *.*          LISTEN
tcp4      0      0  *.49592             *.*          LISTEN
tcp6      0      0  *.49166             *.*          LISTEN
tcp4      0      0  *.49166             *.*          LISTEN
tcp46     0      0  *.3283              *.*          LISTEN
tcp6      0      0  fe80::aede:48ff:.49157 *.*          LISTEN
tcp6      0      0  fe80::aede:48ff:.49156 *.*          LISTEN
tcp6      0      0  fe80::aede:48ff:.49155 *.*          LISTEN
tcp6      0      0  fe80::aede:48ff:.49154 *.*          LISTEN
tcp6      0      0  fe80::aede:48ff:.49153 *.*          LISTEN
tcp4      0      0  *.88                *.*          LISTEN
tcp6      0      0  *.88                *.*          LISTEN
tcp4      0      0  *.5900              *.*          LISTEN
tcp6      0      0  *.5900              *.*          LISTEN
```



```

nikita@UNIT-1620 ~$ netstat -an | grep -i established
tcp6      0      0 fe80::14ac:1d16::56784 fe80::818:d2b0:5.62078 ESTABLISHED
tcp6      0      0 fe80::14ac:1d16::56780 fe80::818:d2b0:5.62078 ESTABLISHED
tcp6      0    444 fe80::14ac:1d16::56779 fe80::818:d2b0:5.62078 ESTABLISHED
tcp4      0      0 192.168.31.33.55825    185.165.123.185.443   ESTABLISHED
tcp4      0      0 192.168.31.33.52206    35.190.80.1.443      ESTABLISHED
tcp4      0      0 192.168.31.33.63456    162.159.138.232.443  ESTABLISHED
tcp4      0      0 192.168.31.33.60396    87.240.139.194.443   ESTABLISHED
tcp4      0      0 192.168.31.33.53442    162.159.134.234.443  ESTABLISHED
tcp4      0      0 192.168.31.33.53201    162.159.138.234.443  ESTABLISHED
tcp4      0      0 192.168.31.33.58708    213.180.204.210.443  ESTABLISHED
tcp4      0      0 192.168.31.33.57552    213.180.204.210.443  ESTABLISHED
tcp4      0      0 192.168.31.33.50333    149.154.167.51.443   ESTABLISHED
tcp4      0      0 192.168.31.33.50042    151.236.74.70.443    ESTABLISHED
tcp4      0      0 192.168.31.33.50759    192.168.31.102.22    ESTABLISHED
tcp4      0      0 192.168.31.33.49488    63.35.29.156.443     ESTABLISHED
tcp4      0      0 192.168.31.33.52156    87.240.129.186.443   ESTABLISHED
tcp6      0      0 fe80::aede:48ff::53999 fe80::aede:48ff::49410 ESTABLISHED
tcp4      0      0 192.168.31.33.62058    149.154.167.50.443   ESTABLISHED
tcp6      0      0 fe80::aede:48ff::50191 fe80::aede:48ff::49430 ESTABLISHED
tcp4      0      0 192.168.31.33.50165    93.186.225.198.443   ESTABLISHED
tcp4      0      0 192.168.31.33.50111    63.35.29.156.443     ESTABLISHED
tcp6      0      0 fe80::aede:48ff::50109 fe80::aede:48ff::49409 ESTABLISHED
tcp4      0      0 192.168.31.33.50093    213.180.204.179.443  ESTABLISHED
tcp4      0      0 192.168.31.33.49936    5.255.255.77.443     ESTABLISHED
tcp4      0      0 192.168.31.33.49807    87.250.251.15.443    ESTABLISHED
tcp4      0      0 192.168.31.33.49659    87.250.251.15.443    ESTABLISHED
tcp4      0      0 192.168.31.33.49638    213.180.204.179.443  ESTABLISHED
tcp4      0      0 192.168.31.33.49634    87.250.251.119.443   ESTABLISHED
tcp4      0      0 192.168.31.33.49621    77.88.55.70.443      ESTABLISHED
tcp4      0      0 192.168.31.33.49620    5.255.255.77.443     ESTABLISHED
tcp4      0      0 192.168.31.33.49406    64.233.163.188.5228  ESTABLISHED
tcp4      0      0 192.168.31.33.49166    192.168.31.94.57535   ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49309 fe80::aede:48ff::49428 ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49216 fe80::aede:48ff::49422 ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49180 fe80::aede:48ff::49414 ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49163 fe80::aede:48ff::49413 ESTABLISHED
tcp4      0      0 192.168.31.33.49162    17.57.146.133.5223   ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49153 fe80::aede:48ff::49434 ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49158 fe80::aede:48ff::49425 ESTABLISHED
tcp6      0      0 fe80::aede:48ff::49152 fe80::aede:48ff::59602 ESTABLISHED
nikita@UNIT-1620 ~$

```

```

[root@ec7 ~]# netstat -an | grep -i established
Active Internet connections (servers and established)
tcp      0      0 192.168.31.102:22      192.168.31.33:50759    ESTABLISHED
tcp      0      0 192.168.31.102:22      192.168.31.139:54286   ESTABLISHED
Active UNIX domain sockets (servers and established)

```

```

[root@ec7 ~]# netstat -tulpn | grep -i listen
tcp      0      0 0.0.0.0:22             0.0.0.0:*              LISTEN    831/sshd
tcp      0      0 127.0.0.1:25            0.0.0.0:*              LISTEN    1036/master
tcp6     0      0 :::22                  :::*                    LISTEN    831/sshd
tcp6     0      0 :::1:25                 :::*                    LISTEN    1036/master
[root@ec7 ~]#

```

```

[root@c7 ~]# tcpdump -A -i enp0s3 host 192.168.31.36 and port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:23:20.049697 IP 192.168.31.36.58039 > c7.ssh: Flags [P.], seq 4056707355, ack 38848502
59, win 2048, options [nop,nop,TS val 593420090 ecr 673056], length 36
EH.X..@.0.z}...$.f.....q....S.....
#^.:.
E.....z...'.%<...Zj.....+Kp.....7
16:23:20.049839 IP c7.ssh > 192.168.31.36.58039: Flags [P.], seq 1:37, ack 36, win 315, options [nop
,nop,TS val 819956 ecr 593420090], length 36
E..X.00.0.g....f...$......S..q?...;.%....
...#^.:.17*U.....llg.H....}e...9.Q...K.;1.
16:23:20.049960 IP 192.168.31.36.58039 > c7.ssh: Flags [P.], ack 37, win 2047, options [nop,nop,TS va
l 593420090 ecr 819956], length 0
EH.4..@.0.z}...$.f.....q?...w.....i....
#^.:.
16:23:20.732556 IP 192.168.31.36.58039 > c7.ssh: Flags [P.], seq 36:72, ack 37, win 2048, options [n
op,nop,TS val 593420765 ecr 819956], length 36
EH.X..@.0.z}...$.f.....q?...w.....
#^.....kK.r.%.....}..N..C...n.P...<D.
C
16:23:20.732725 IP c7.ssh > 192.168.31.36.58039: Flags [P.], seq 37:73, ack 72, win 315, options [no
p,nop,TS val 820638 ecr 593420765], length 36
E..X.10.0.g....f...$......w..qc...;%....
...#^..aU2..@..D..BwD...l..w.R...l./}...j..
16:23:20.732897 IP 192.168.31.36.58039 > c7.ssh: Flags [P.], ack 73, win 2047, options [nop,nop,TS va
l 593420765 ecr 820638], length 0
EH.4..@.0.z}...$.f.....qc.....
#^.....

```

## Вопросы и задания:

1. MTR работает по умолчанию по протоколу ICMP(Internet Control Message Protocol), однако с помощью флагов --tcp --udp можно переходить на использование TCP SYN-пакетов или UDP-датаграмм. Для того, чтобы определить можно запустить mtr, зайти в Wireshark и посмотреть протокол общения.
2. HOST — имя хоста;  
Loss% — процент потерь пакетов;  
Snt — количество отправленных пакетов;  
Last — время задержки последнего отправленного пакета в миллисекундах;  
Avg — среднее время задержки;  
Best — минимальное время задержки;  
Wrst — максимальное время задержки;  
StDev — среднееквадратичное отклонение времени задержки;
3. Кадры Ethernet:
  - Ethernet II
  - Ethernet 802.3
  - Ethernet 802.2
  - Ethernet SNAP

Из этих 4х кадров Ethernet II и 802.3 - являются базовыми и отличаются лишь назначением одного поля ("Длина/тип"):

В Ethernet II в поле "Длина/тип" всегда указывается тип протокола.



Ethernet 802.3 Данный тип кадра не содержит никакой информации о протоколе. Поле "Длина/тип" всегда указывает длину кадра.

Что касается 2х других:

Ethernet 802.2 В данном типе кадра сразу за адресом отправителя следует поле длины, имеющее такое же назначение. Кроме того, этот тип кадра содержит несколько дополнительных полей, рекомендованных подкомитетом IEEE 802.3: "DSAP", "SSAP", "Контроль".

Кадр Ethernet SNAP, являющийся дальнейшим развитием Ethernet 802.2, содержит следующие дополнительные поля: "Код организации", "Идентификатор протокола".

4. В анализируемой сети используется протокол Ethernet II. Это можно посмотреть в Wireshark.

```
▶ Frame 9039: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp0s20f3, id 0
▶ Ethernet II, Src: XIAOMI_E1_28:fe:b3 (40:31:3c:28:fe:b3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Address Resolution Protocol (request)
```

5. Используя описание источников и адреса назначения, а также используемые при передаче протоколы.
6. Используются широковещательные адреса, вид которых зависит от протокола. Так, в IP-сетях широковещательные адреса формируются следующим образом: к адресу подсети прибавляется побитовая инверсия маски подсети (то есть все биты адреса подсети, соответствующие нулям в маске, устанавливаются в «1»).
7. Используется широковещательный MAC-адрес FF:FF:FF:FF:FF:FF для передачи служебных датаграмм (например, ARP-запросов). Датаграммы, отправленные на такой адрес, принимаются всеми сетевыми устройствами локальной сети.
8. Для взлома сети.
9. `ip neigh show` - показать все записи ARP

`ip neigh flush` - удалить все записи ARP

Если вы заметили, что в работе сети появились такие проблемы, как например, ошибки при загрузке определенных сайтов или отсутствие пинга некоторых IP-адресов, то стоит попробовать очистить ARP-кэш, так как для устройства в сети мог измениться IP адрес.

10. `tcpdump host 192.168.0.254 and udp or port 80`