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 M3435, M3436:

Бурцева Полина Сергеевна

Кочетков Никита Олегович

Проверил:

Береснев Артем Дмитриевич

Санкт-Петербург

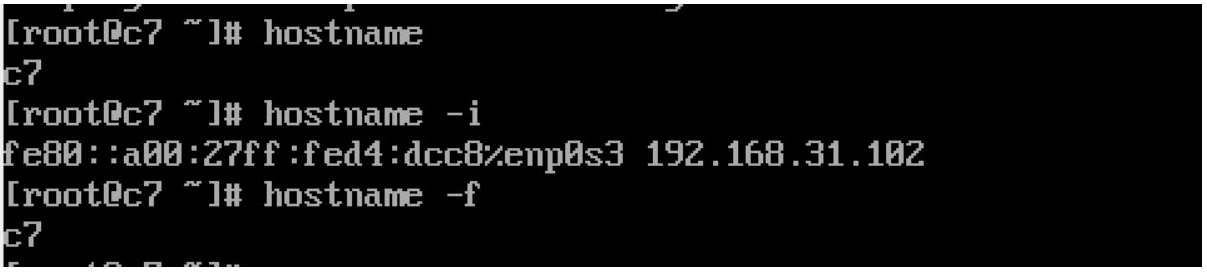
2020

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

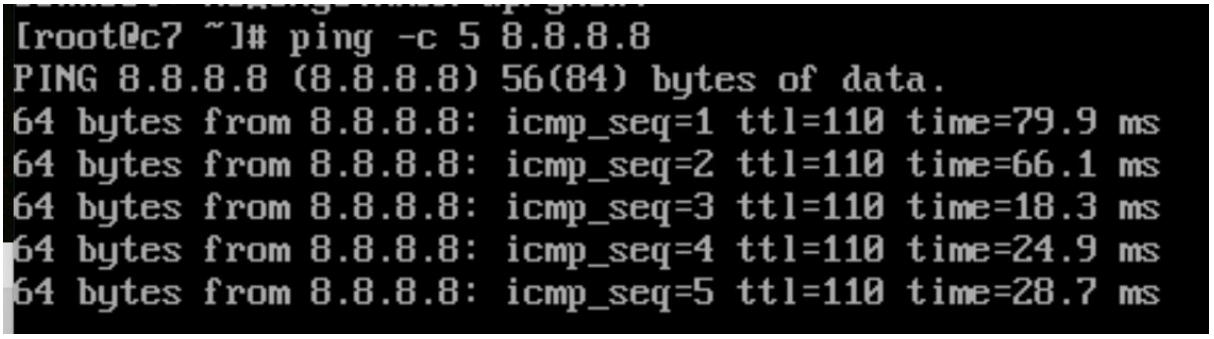
1.4
Имя хоста:
hostname

Ip-адрес:
hostname -i

Адрес DNS:
hostname -f



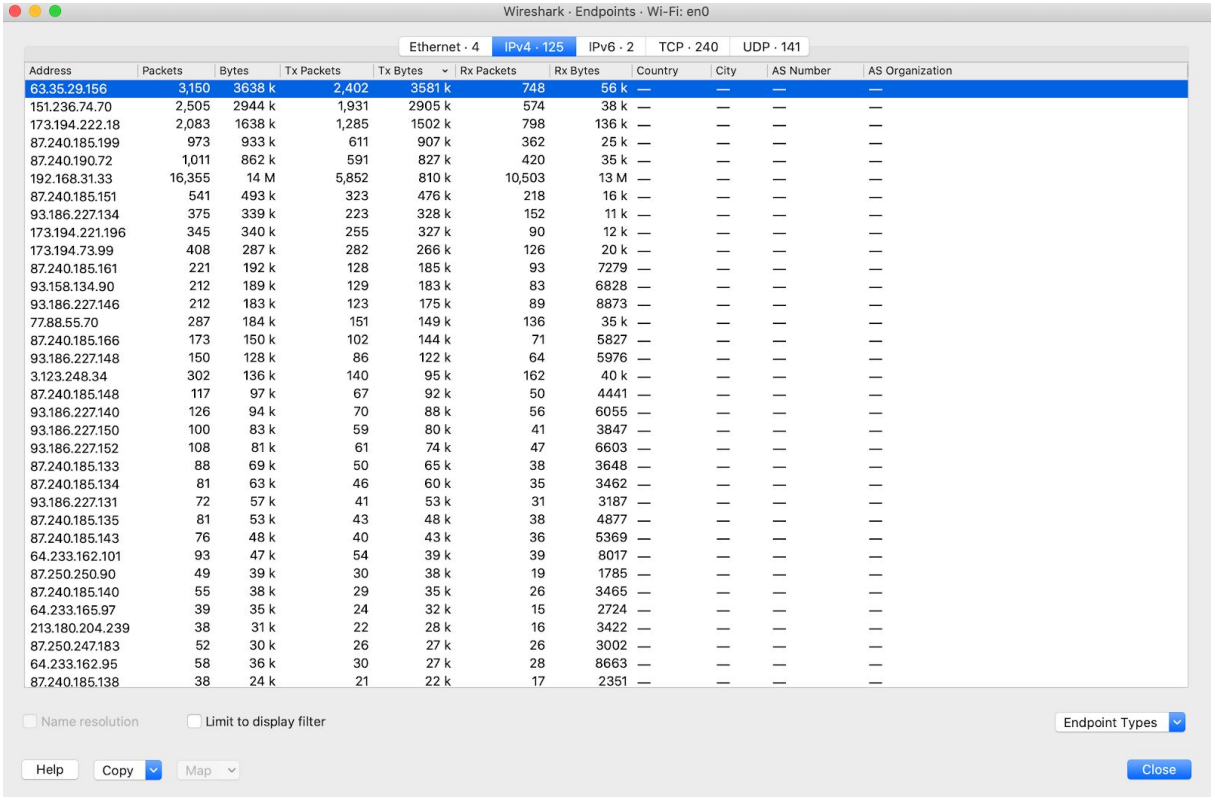
1.5
ping -c 5 8.8.8.8



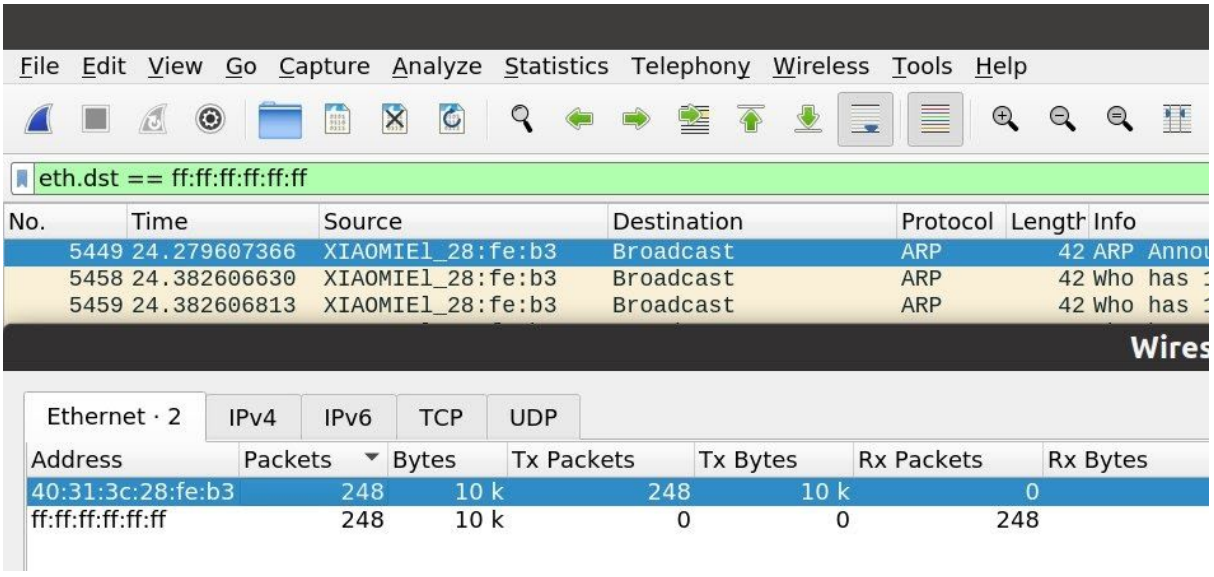
Скриншоты окон Wireshark с необходимыми данными заданий Части 2, п.2

2.2

a.



b.



c.

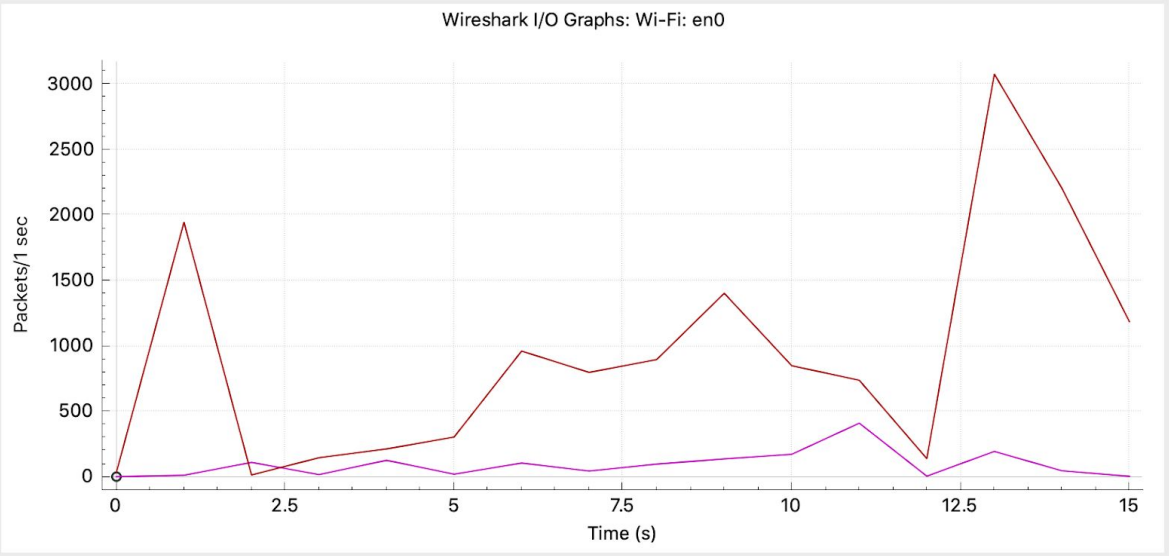
Ethernet · 4 | IPv4 · 125 | IPv6 · 2 | TCP · 240 | UDP · 141

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

Name resolution | Limit to display filter | Endpoint Types

d.

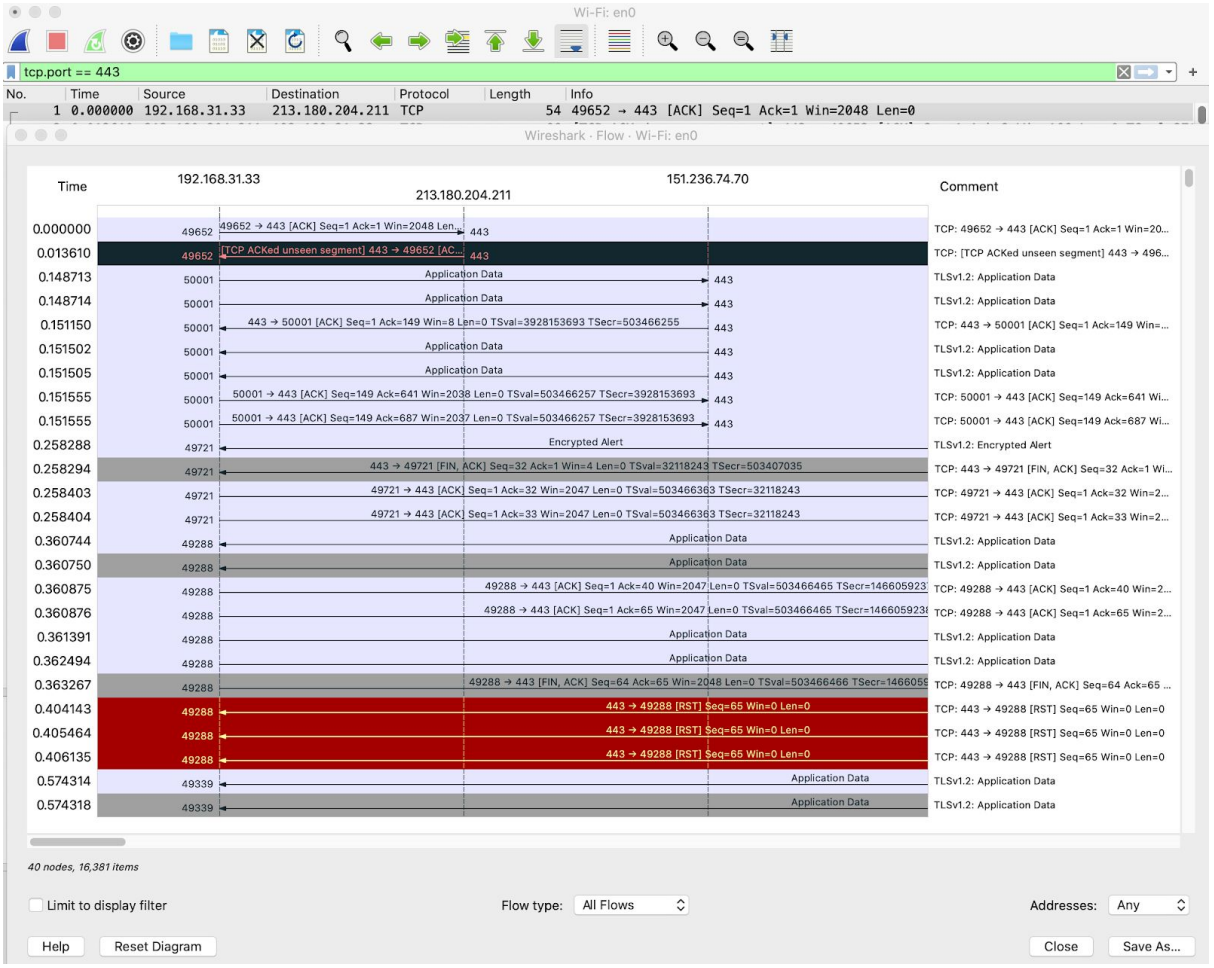
Wireshark · I/O Graphs · Wi-Fi: en0



No packets in interval (0s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☐	All Packets			Line	Packets		None
☑	TCP	tcp		Line	Packets		None
☑	UDP	udp		Line	Packets		None

Mouse ◉ drags ○ zooms | Interval 1 sec | ☐ Time of day | ☐ Log scale | Reset

e. 

Текст фильтров Части 2, п.3.

2.3

a. ((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))
b. eth.src == 60:f2:62:56:f9:73
c. eth.dst == ff:ff:ff:ff:ff:ff
d. 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: XIAOMIEl_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: XIAOMIEl_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 - канальный
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

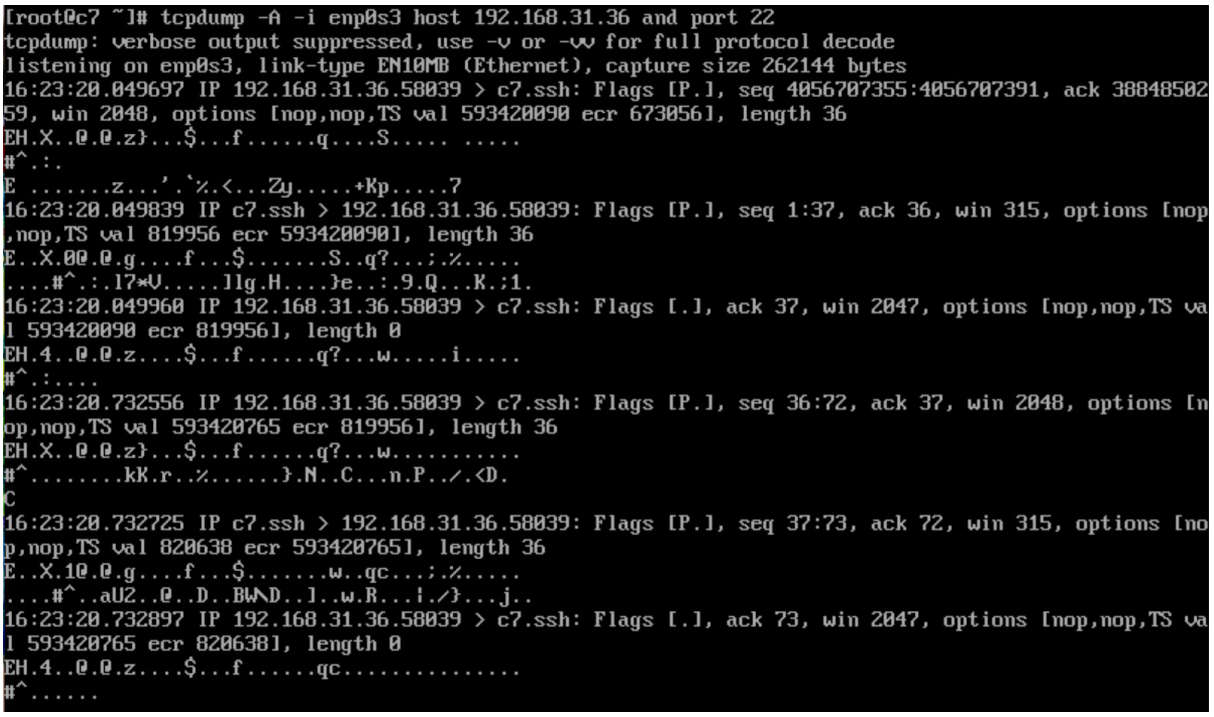
```
 nikita@UNIT-1620 ~ netstat -an | grep -i listen
tcp4       0      0  127.0.0.1.6463         *.*                    LISTEN
tcp4       0      0  *.49592                *.*                    LISTEN
tcp6       0      0  *.49166                *.*                    LISTEN
tcp4       0      0  *.49166                *.*                    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@c7 ~]# 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@c7 ~]# 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@c7 ~]#
```

3.4



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 — среднеквадратичное 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: XIAOMIEl_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