Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий

Направление подготовки 11.03.02

Практическая работа №5

TCP-IP

Выполнил:

Дощенников Никита Андреевич

Группа: К3121

Проверил:

Антон Харитонов

Санкт-Петербург

2025

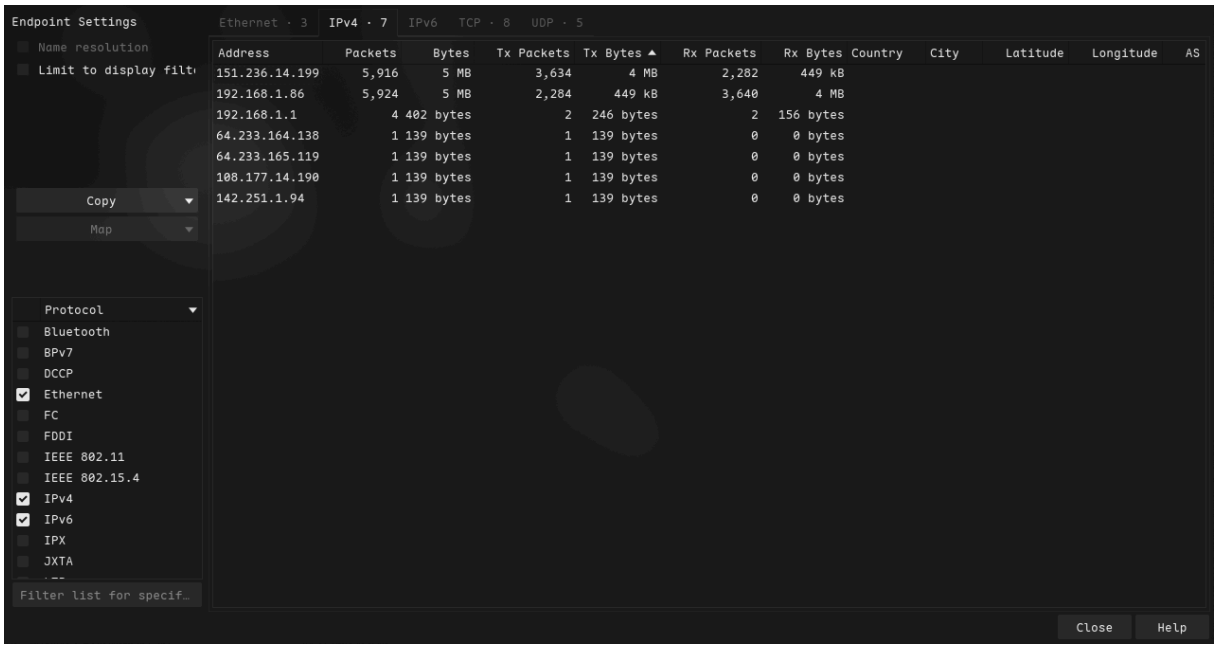
Цель.
Изучить принципы работы протоколов стека TCP/IP посредством анализа сетевого трафика в программе Wireshark, научиться собирать, фильтровать и интерпретировать пакеты различных протоколов, а также выявлять характеристики и особенности взаимодействий на разных уровнях модели TCP/IP.

Wireshark.
Чтобы остановить захват после 5 мегабайт и записать логи в файл, я выставил соответствующие настройки в разделе Capture -> Options и Capture -> Output.

Чтобы сохранять всю информацию в файл, в разделе Output я прописал соответствующий путь.

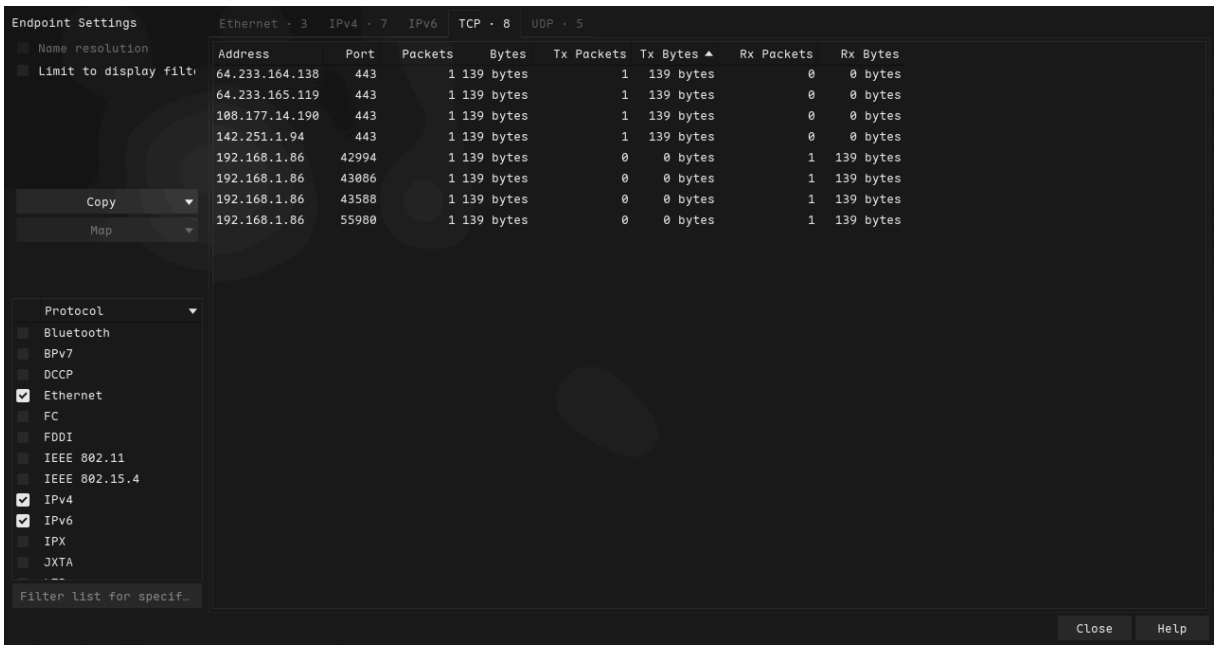
Проведем захват.

Чтобы определить узел с максимальной активностью по объему переданных данных, я в Statistics -> Endpoints отсортировал IPv4 по TxBytes.



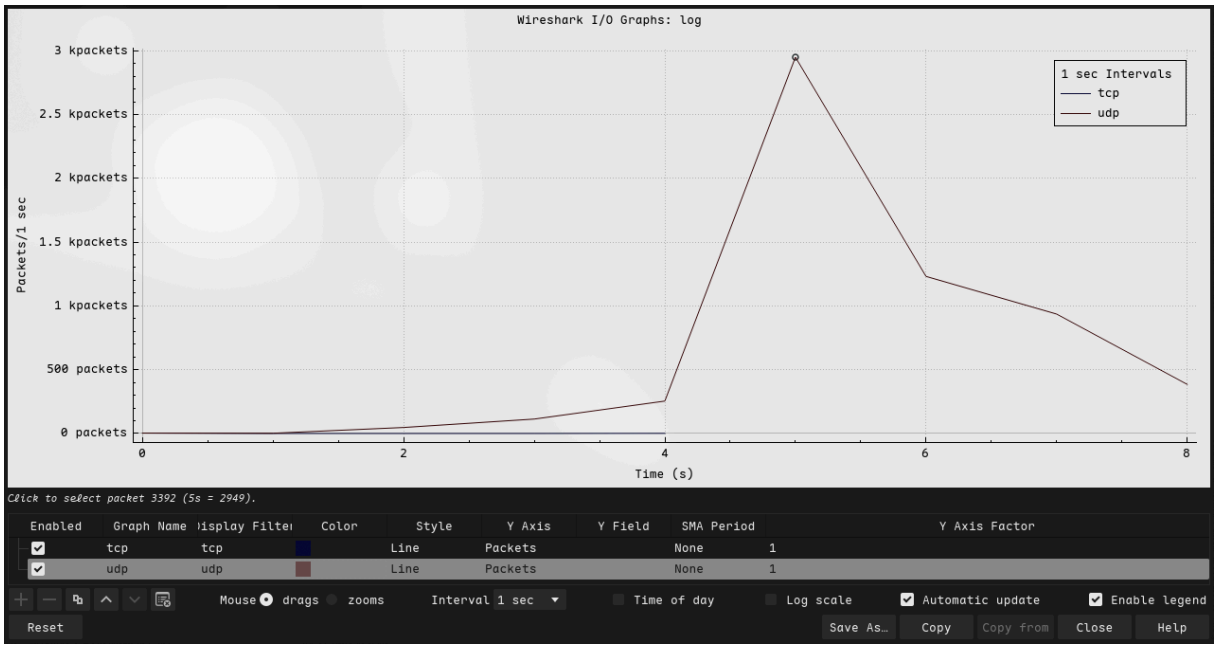
Получилось 151.236.14.199.

Теперь определим самый активный TCP хост по количеству переданных пакетов. Для этого будем смотреть на те вхождения, которые в адресе отправителя имеют 192.168.1.86. Также отсортируем по Tx Bytes.

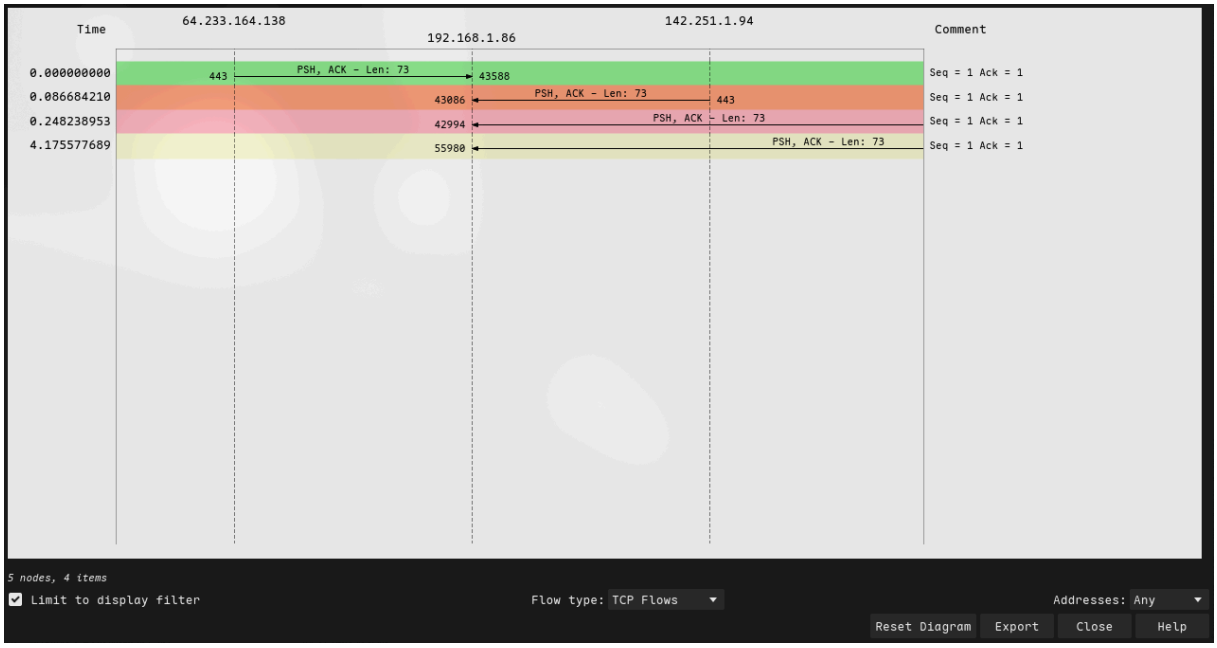


Получаем 42994.

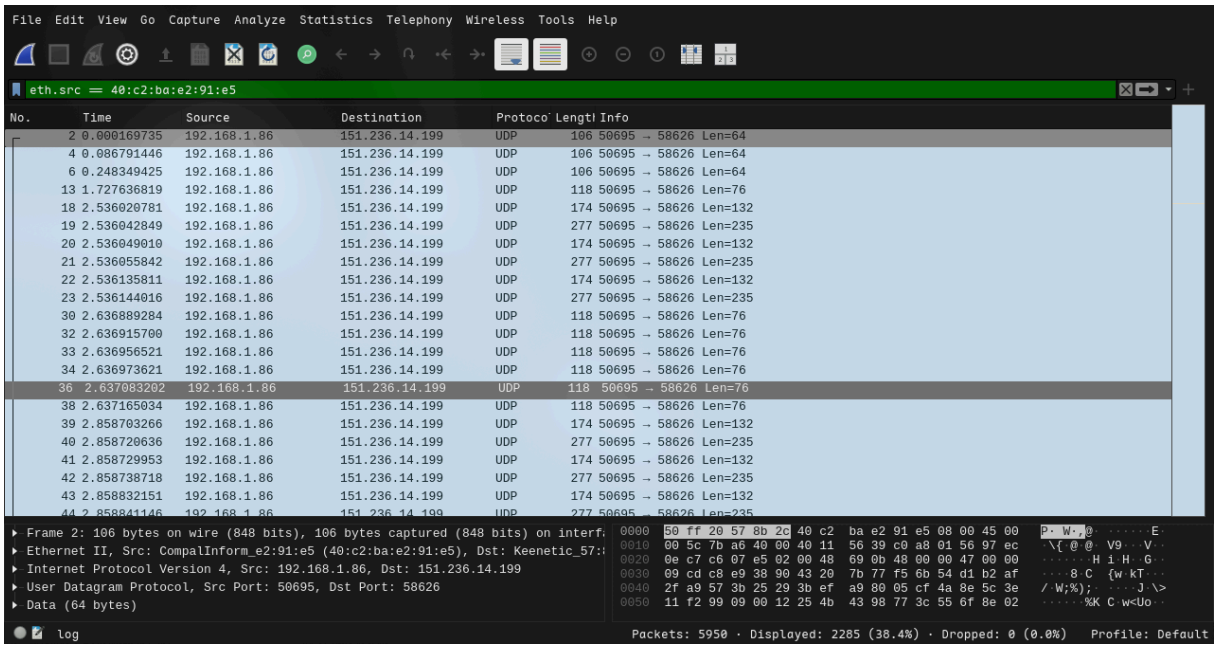
Построим граф интенсивности трафика TCP, UDP. Переходим в Statistics -> I/O Graphs.



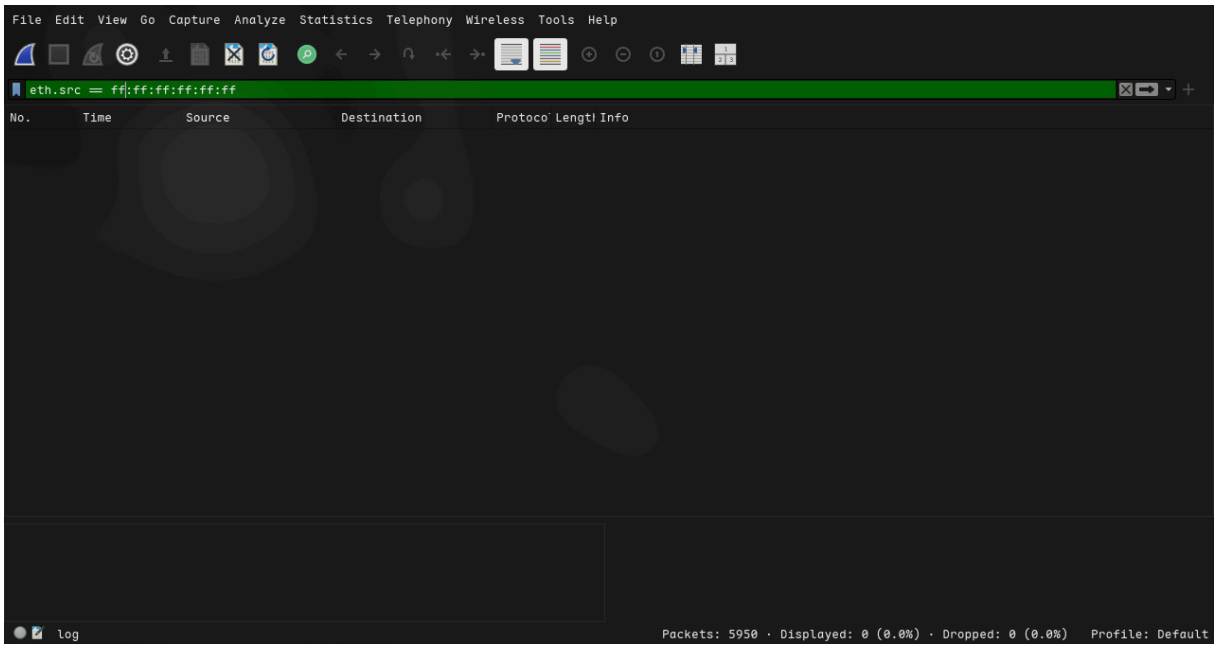
Построим диаграмму связей пакетов HTTPS. Для этого отфильтруем только порты 443 (`tcp.port == 443`). Затем Statistics -> Flow Graph ограничиваем по фильтру и в выпадающем меню выбираем TCP Flows.



Отфильтруем кадры Ethernet. Для этого применим фильтр `eth.src == 40:c2:ba:e2:91:e5`



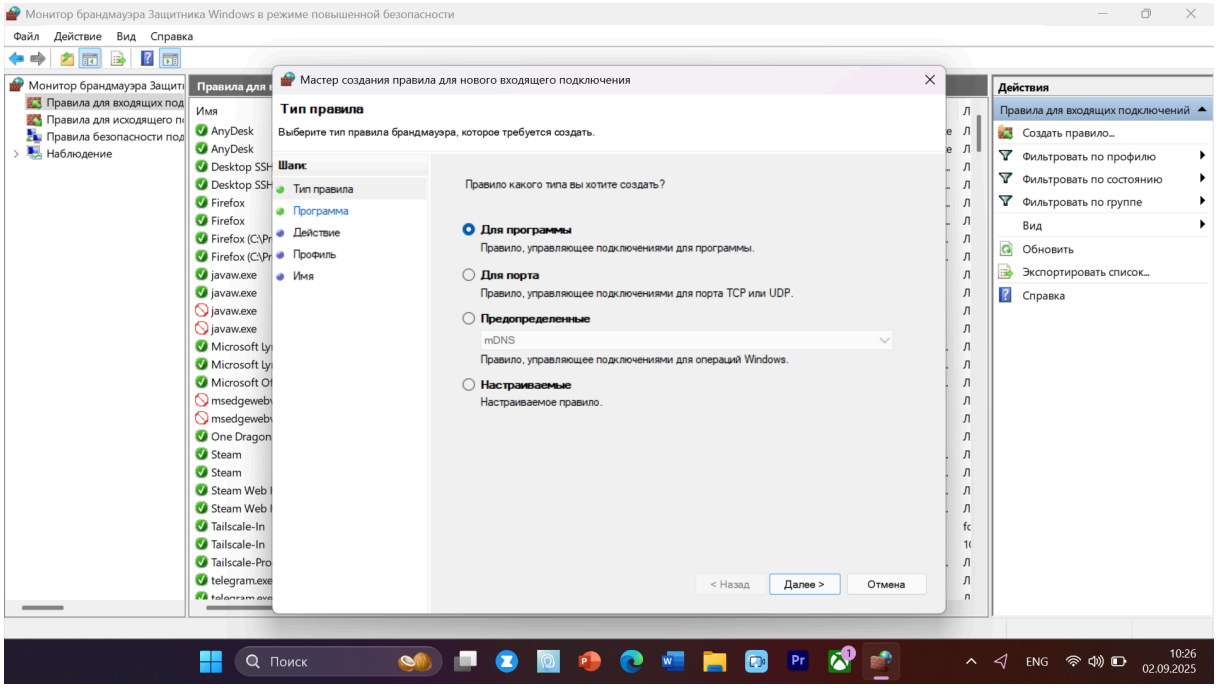
Отфильтруем только широковещательные сообщения. (`eth.src == ff:ff:ff:ff:ff:ff`)

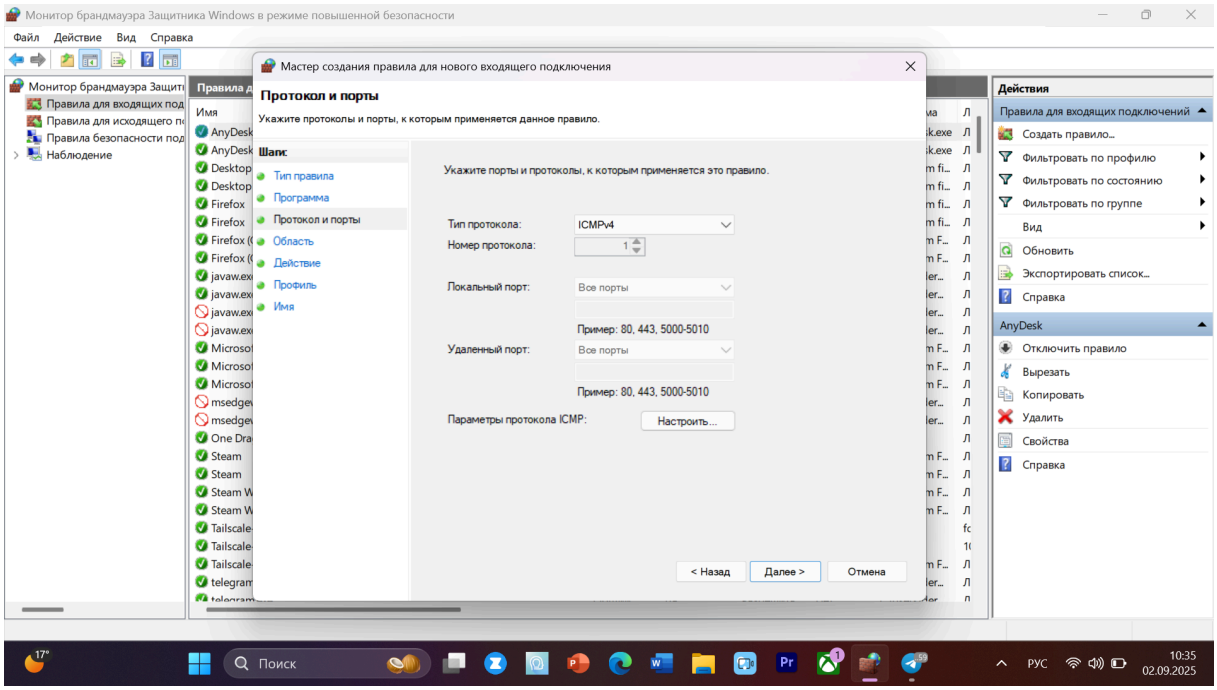


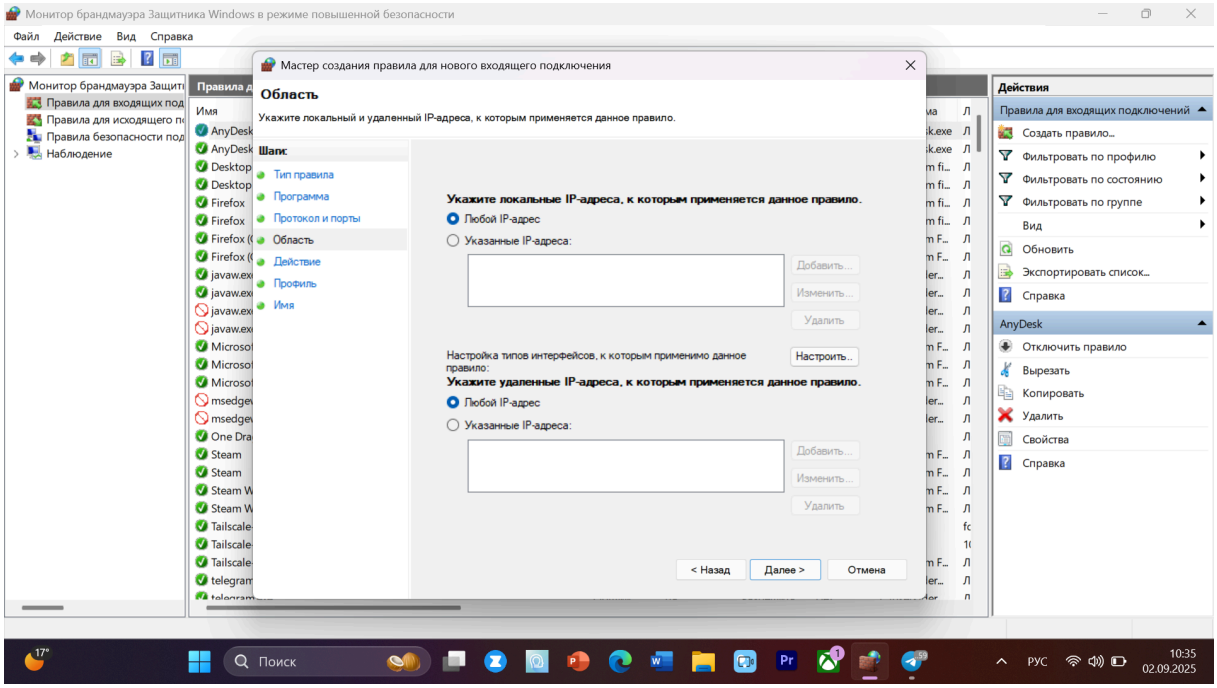
Как можно видеть, у меня не было найдено широковещательных сообщений.

ICMP.

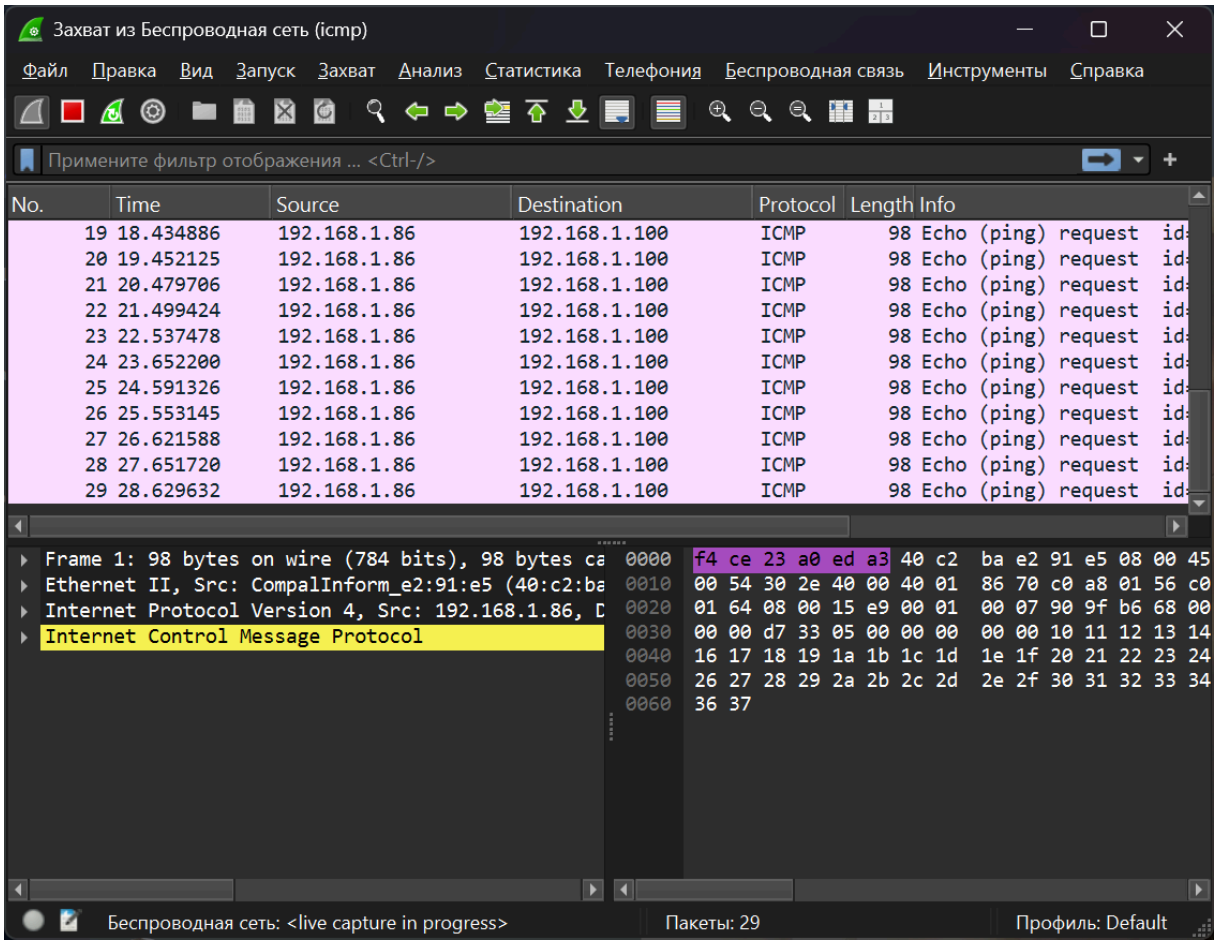
Настроим брэндмауэр чтобы разрешить icmp запросы под windows. Создадим inbound rule чтобы пропускать пакеты по icmpv4.


Монитор брандмауэра Защитника Windows в режиме повышенной безопасности
Файл Действие Вид Справка
Мастер создания правила для нового входящего подключения
Тип правила
Выберите тип правила брандмауэра, которое требуется создать.
Шаги:
Тип правила
Программа
Действие
Профиль
Имя
Правило какого типа вы хотите создать?
Для программы
Правило, управляющее подключениями для программы.
Для порта
Правило, управляющее подключениями для порта TCP или UDP.
Предопределенные
mDNS
Правило, управляющее подключениями для операций Windows.
Настраиваемые
Настраиваемое правило.
< Назад
Далее >
Отмена
Действия
Правила для входящих подключений
Создать правило...
Фильтровать по профилю
Фильтровать по состоянию
Фильтровать по группе
Вид
Обновить
Экспортировать список...
Справка
Поиск
ENG
10:26
02.09.2025


Монитор брандмауэра Защитника Windows в режиме повышенной безопасности
Файл Действие Вид Справка
Мастер создания правила для нового входящего подключения
Протокол и порты
Укажите протоколы и порты, к которым применяется данное правило.
Шаги:
Тип правила
Программа
Протокол и порты
Область
Действие
Профиль
Имя
Укажите порты и протоколы, к которым применяется это правило.
Тип протокола:
ICMPv4
Номер протокола:
Локальный порт:
Все порты
Пример: 80, 443, 5000-5010
Удаленный порт:
Все порты
Пример: 80, 443, 5000-5010
Параметры протокола ICMP:
Настроить...
< Назад
Далее >
Отмена
Действия
Правила для входящих подключений
Создать правило...
Фильтровать по профилю
Фильтровать по состоянию
Фильтровать по группе
Вид
Обновить
Экспортировать список...
Справка
AnyDesk
Отключить правило
Вырезать
Копировать
Удалить
Свойства
Справка
Поиск
РУС
10:35
02.09.2025



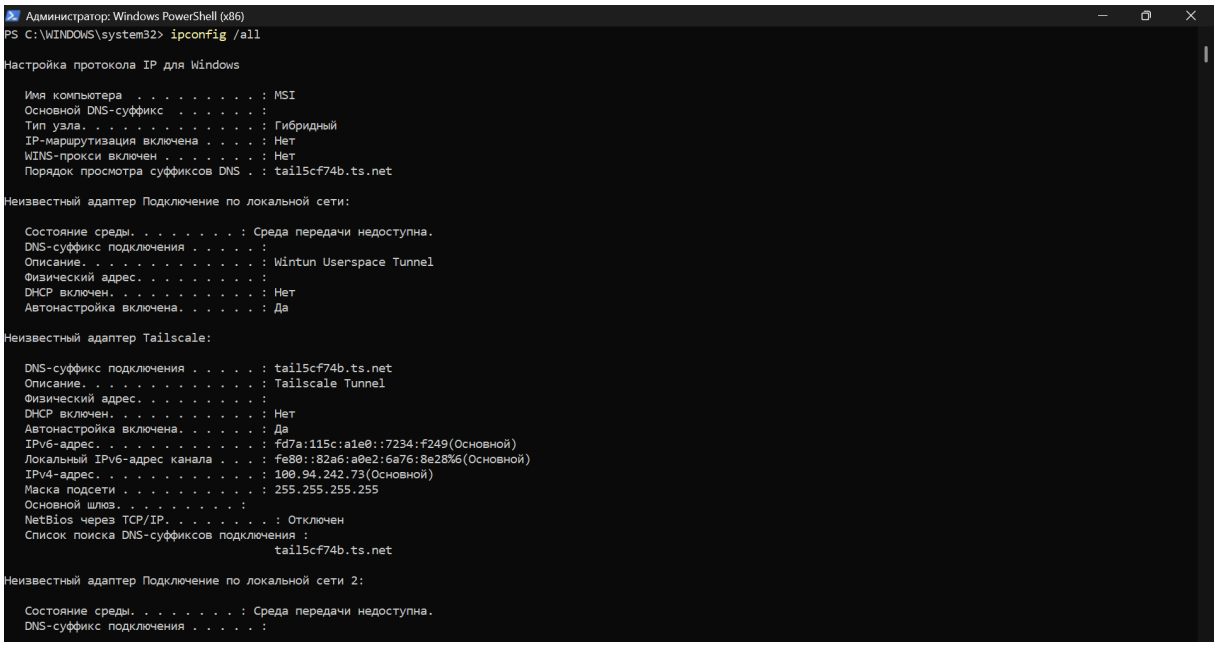
Будем отправлять icmp запросы на 192.168.1.100 с 192.168.1.86.

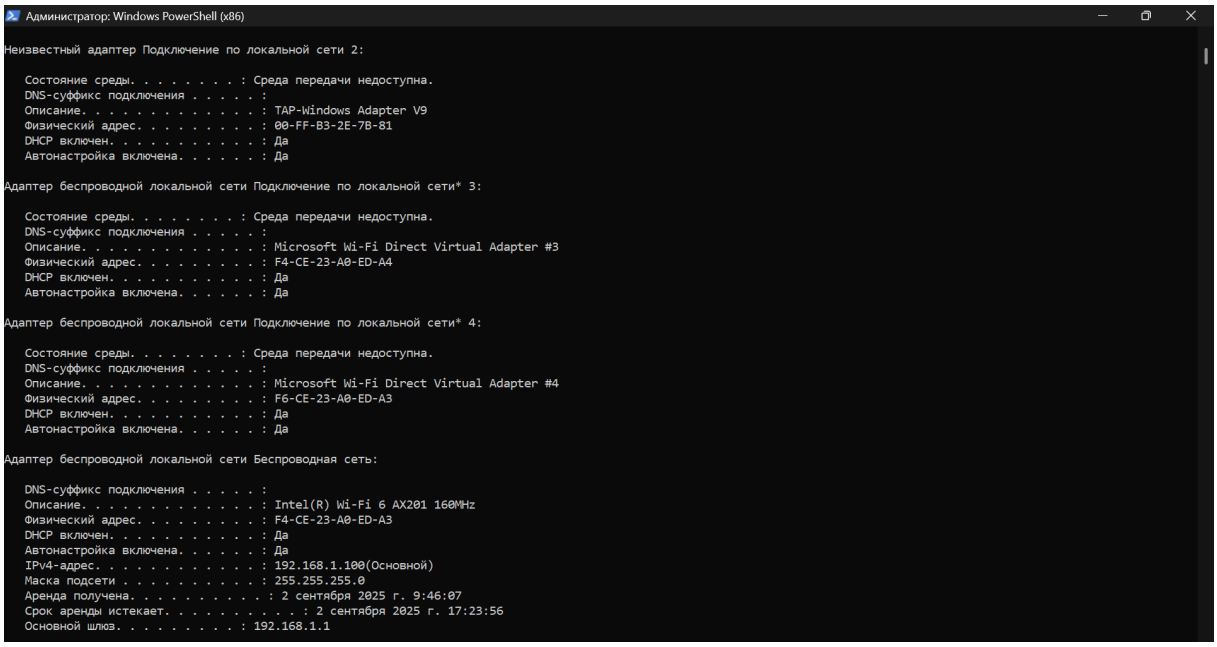


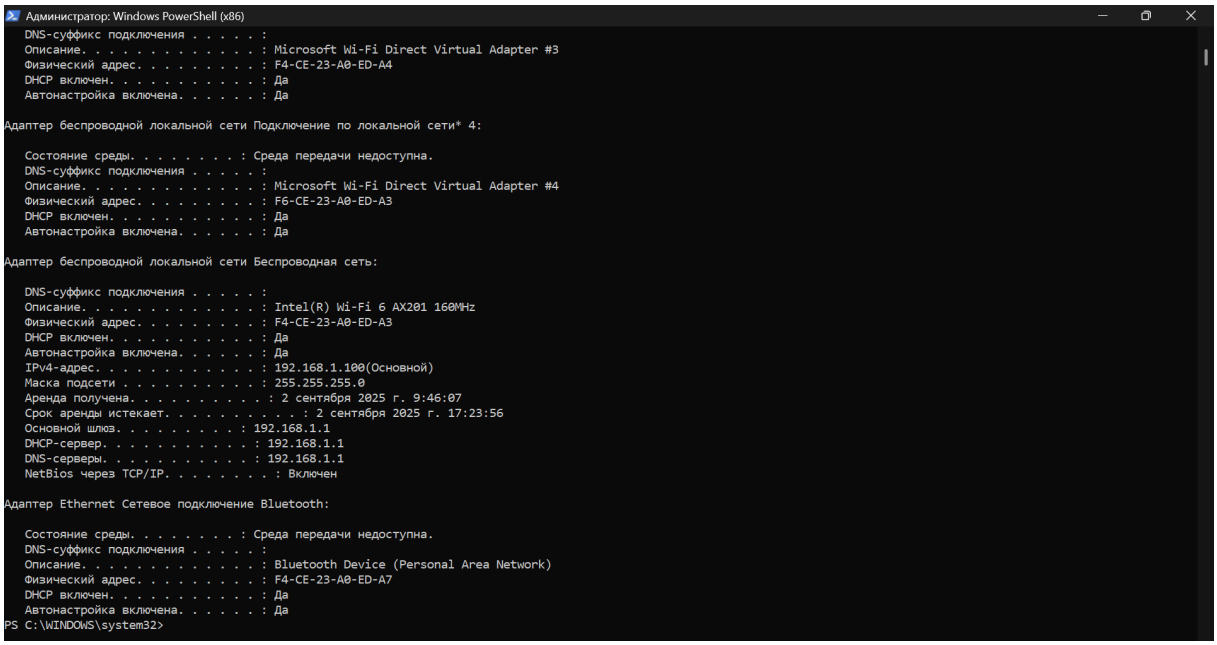
Как видно на скриншоте запросы успешно принимаются.

Проверим MAC-адреса получателя и отправителя.

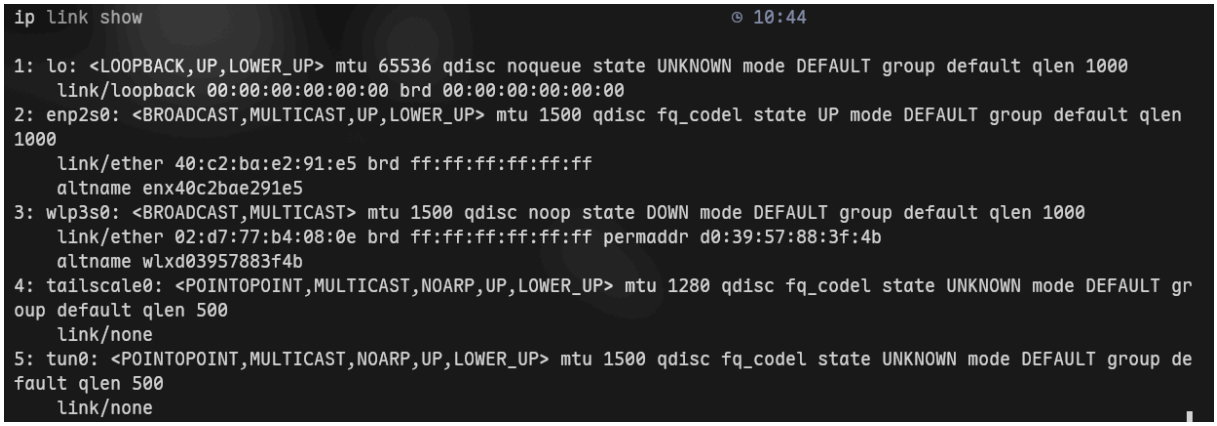
Для получателя:



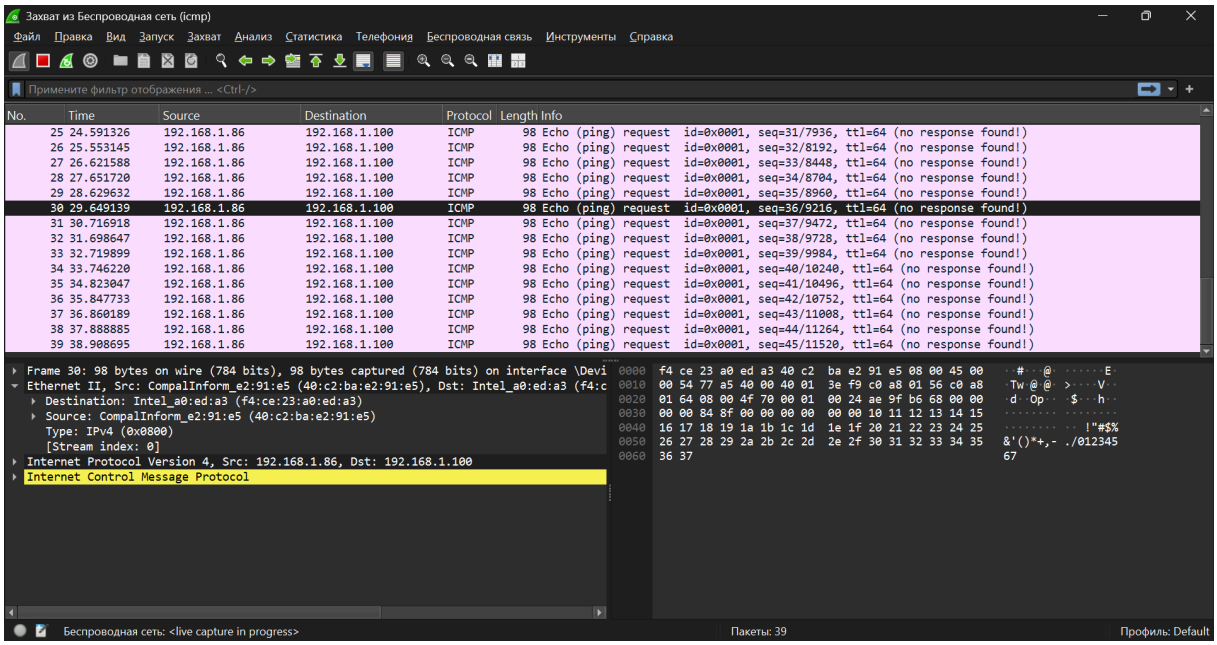




Для отправителя:

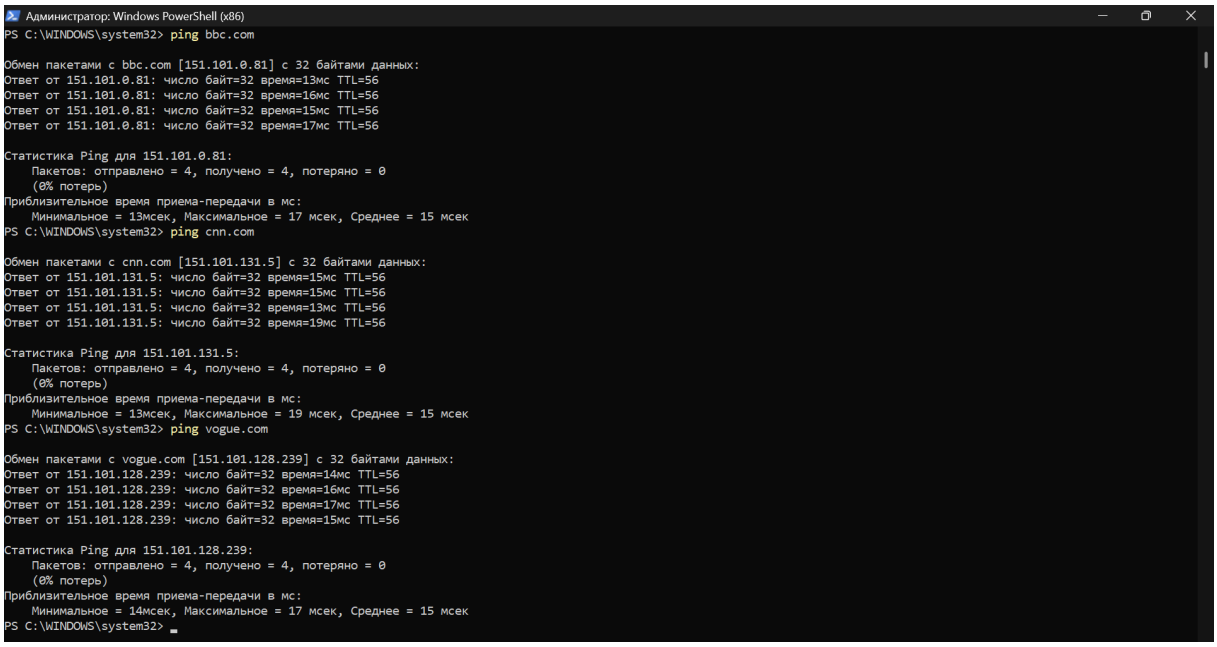


Посмотрим содержимое пакетов.



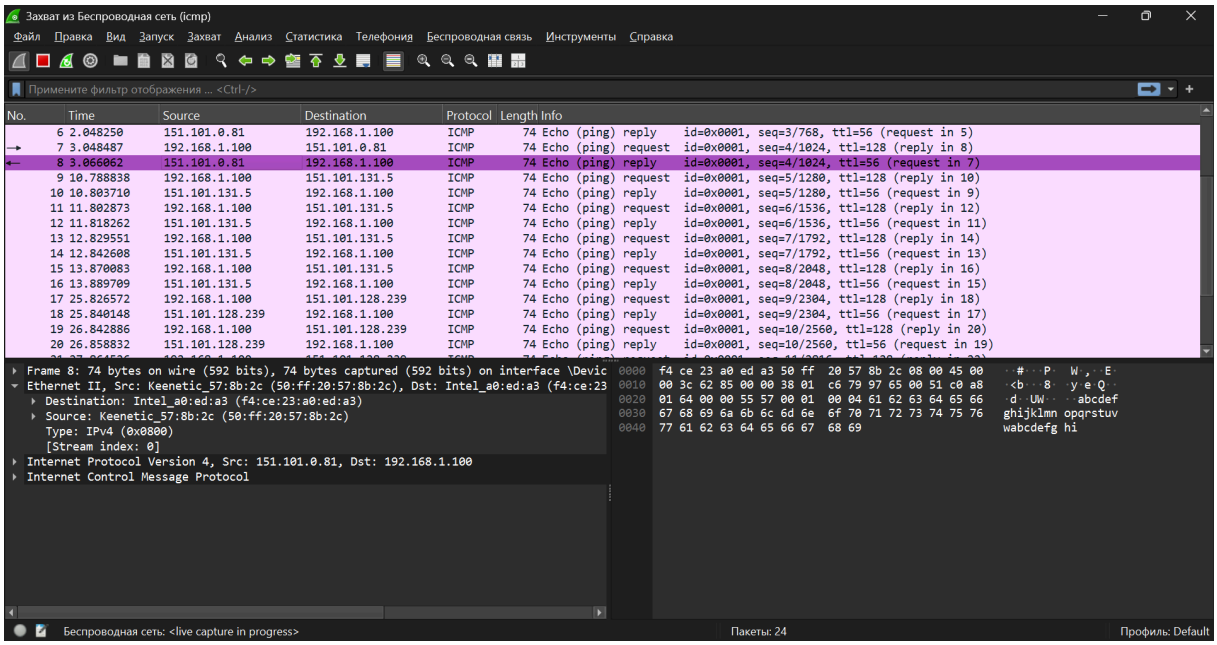
Как видно по снимку экрана адреса совпадают с полученными ранее.

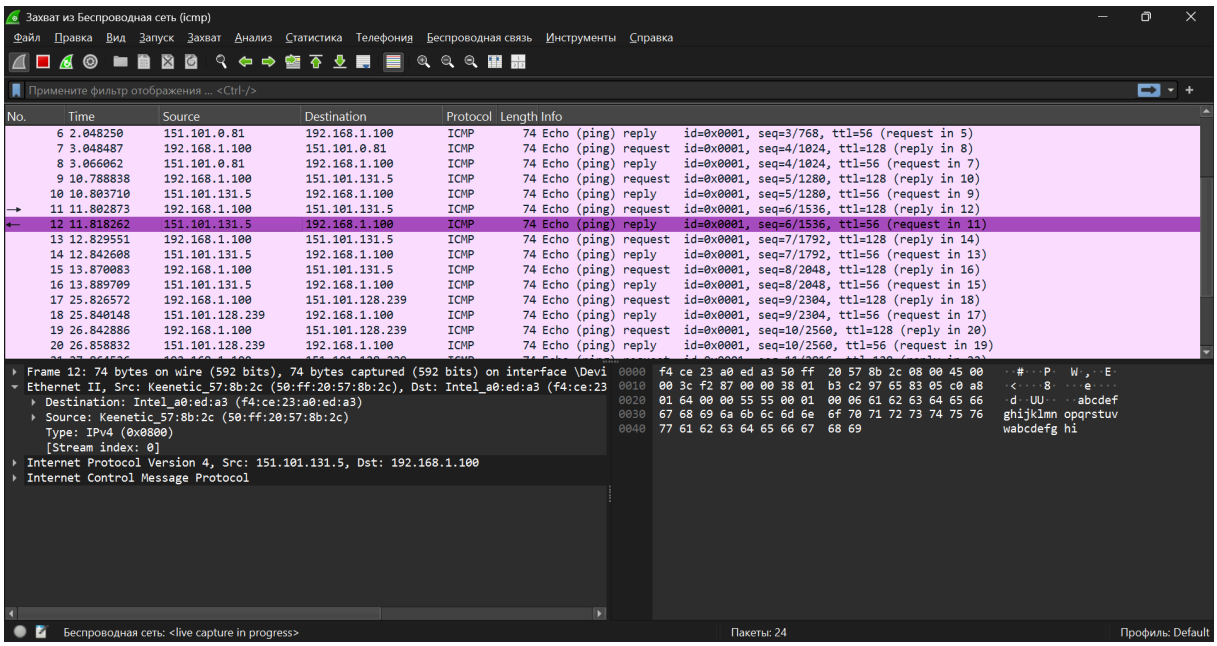
Выберем bbc.com, cnn.com, vogue.com в качестве зарубежных сми.

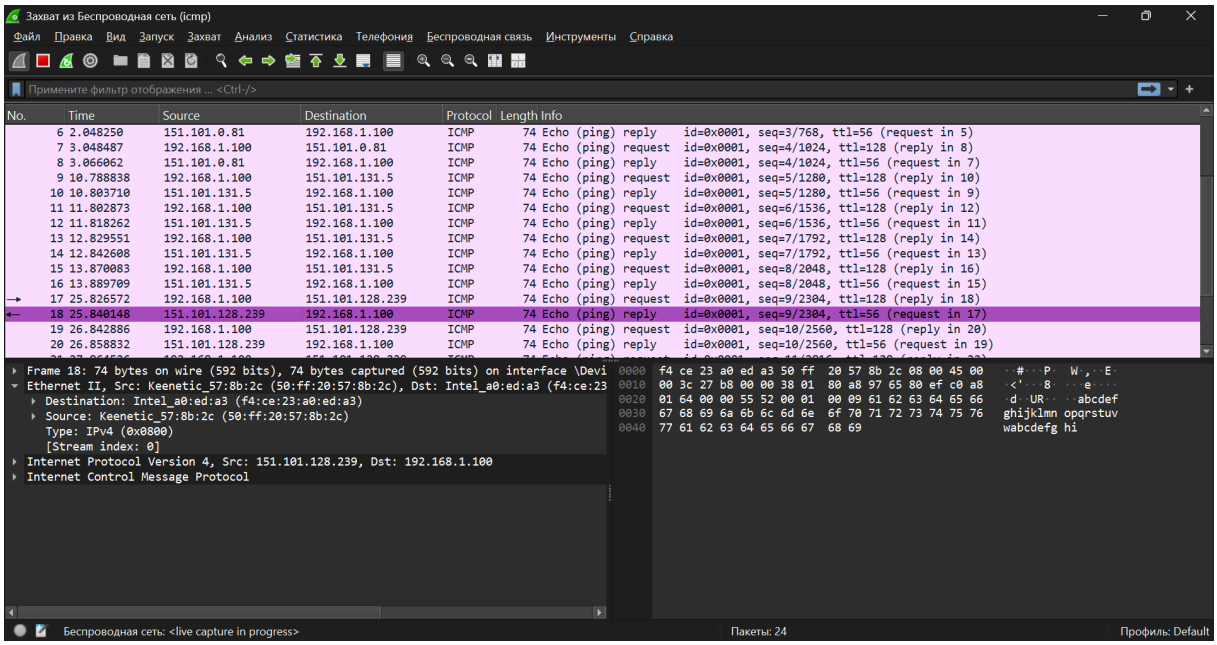


Получились следующие ip:

сми	ip
bbc.com	151.101.0.81
cnn.com	151.101.131.5
vogue.com	151.101.128.239


Захват из Беспроводная сеть (icmp)
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
Примените фильтр отображения ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
6 2.048250 151.101.0.81 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=3/768, ttl=56 (request in 5)
7 3.048487 192.168.1.100 151.101.0.81 ICMP 74 Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 8)
8 3.066062 151.101.0.81 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=4/1024, ttl=56 (request in 7)
9 10.788838 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 10)
10 10.803710 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=56 (request in 9)
11 11.802873 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 12)
12 11.818262 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=56 (request in 11)
13 12.829551 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 14)
14 12.842608 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=7/1792, ttl=56 (request in 13)
15 13.870083 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 16)
16 13.889709 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=8/2048, ttl=56 (request in 15)
17 25.826572 192.168.1.100 151.101.128.239 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 18)
18 25.840148 151.101.128.239 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=56 (request in 17)
19 26.842886 192.168.1.100 151.101.128.239 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 20)
20 26.858832 151.101.128.239 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=56 (request in 19)
Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devic
Ethernet II, Src: Keenetic_57:8b:2c (50:ff:20:57:8b:2c), Dst: Intel_a0:ed:a3 (f4:ce:23
Destination: Intel_a0:ed:a3 (f4:ce:23:a0:ed:a3)
Source: Keenetic_57:8b:2c (50:ff:20:57:8b:2c)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 151.101.0.81, Dst: 192.168.1.100
Internet Control Message Protocol
0000 f4 ce 23 a0 ed a3 50 ff 20 57 8b 2c 08 00 45 00
0010 00 3c 62 85 00 00 38 01 c6 79 97 65 00 51 c0 a8
0020 01 64 00 00 55 57 00 01 00 04 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Беспроводная сеть: <live capture in progress>
Пакеты: 24
Профиль: Default

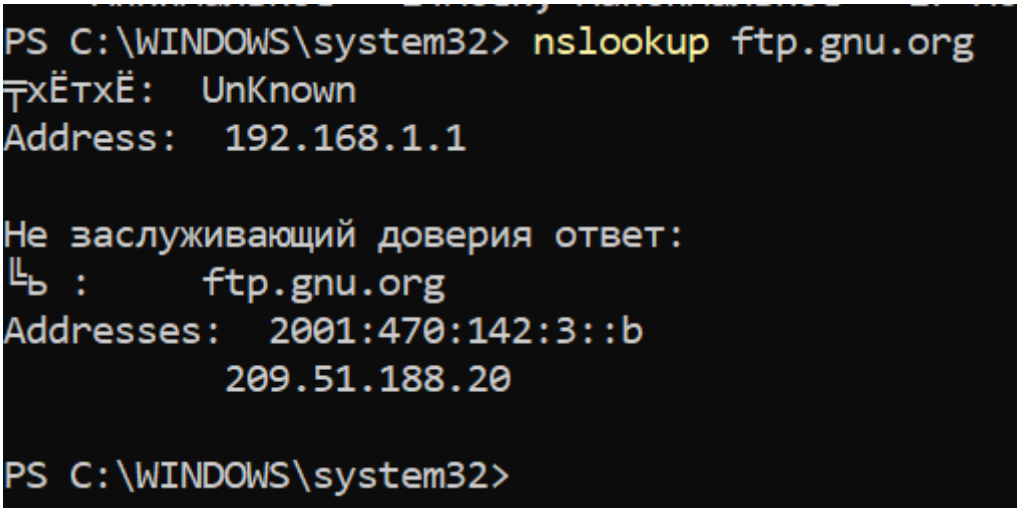

Захват из Беспроводная сеть (icmp)
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
Примените фильтр отображения ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
6 2.048250 151.101.0.81 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=3/768, ttl=56 (request in 5)
7 3.048487 192.168.1.100 151.101.0.81 ICMP 74 Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 8)
8 3.066062 151.101.0.81 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=4/1024, ttl=56 (request in 7)
9 10.788838 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 10)
10 10.803710 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=56 (request in 9)
11 11.802873 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 12)
12 11.818262 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=56 (request in 11)
13 12.829551 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 14)
14 12.842608 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=7/1792, ttl=56 (request in 13)
15 13.870083 192.168.1.100 151.101.131.5 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 16)
16 13.889709 151.101.131.5 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=8/2048, ttl=56 (request in 15)
17 25.826572 192.168.1.100 151.101.128.239 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 18)
18 25.840148 151.101.128.239 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=56 (request in 17)
19 26.842886 192.168.1.100 151.101.128.239 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 20)
20 26.858832 151.101.128.239 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=56 (request in 19)
Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devi
Ethernet II, Src: Keenetic_57:8b:2c (50:ff:20:57:8b:2c), Dst: Intel_a0:ed:a3 (f4:ce:23
Destination: Intel_a0:ed:a3 (f4:ce:23:a0:ed:a3)
Source: Keenetic_57:8b:2c (50:ff:20:57:8b:2c)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 151.101.131.5, Dst: 192.168.1.100
Internet Control Message Protocol
0000 f4 ce 23 a0 ed a3 50 ff 20 57 8b 2c 08 00 45 00
0010 00 3c f2 87 00 00 38 01 b3 c2 97 65 83 05 c0 a8
0020 01 64 00 00 55 55 00 01 00 06 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Беспроводная сеть: <live capture in progress>
Пакеты: 24
Профиль: Default



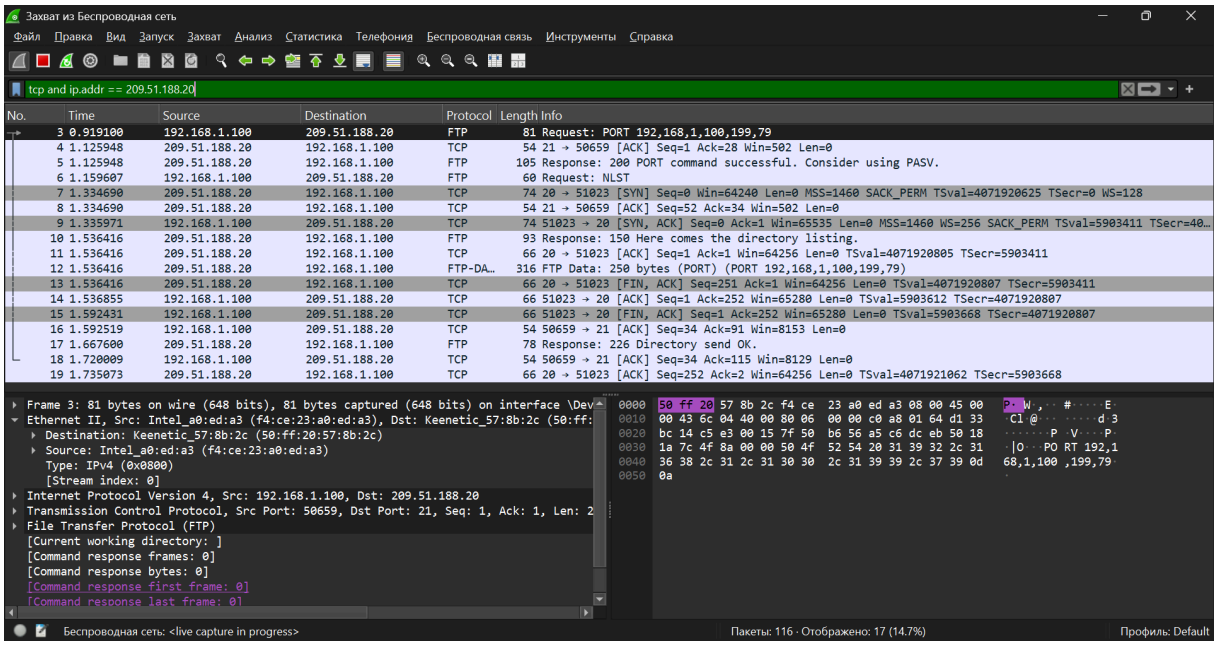
MAC адрес получателя всегда остается одним и тем же. Все отправляемые пакеты проходят через маршрутизатор, так как все узлы за пределами локальной сети.

TCP.

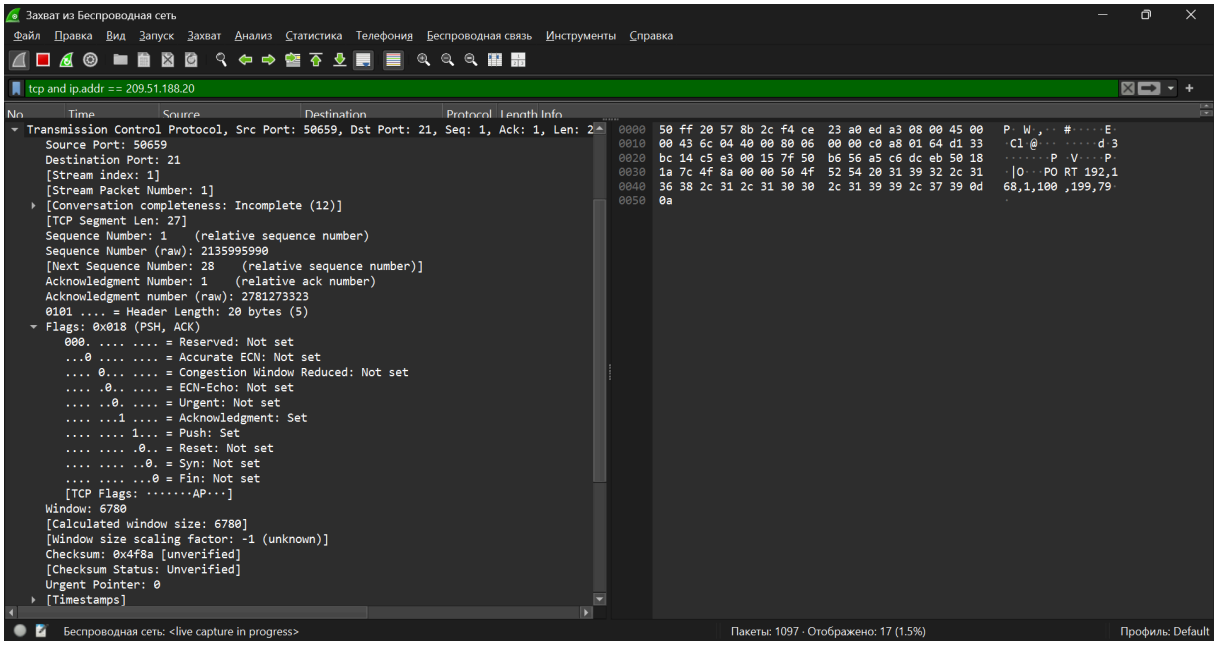
В качестве FTP сервера буду использовать ftp.gnu.org. Получим его адрес.

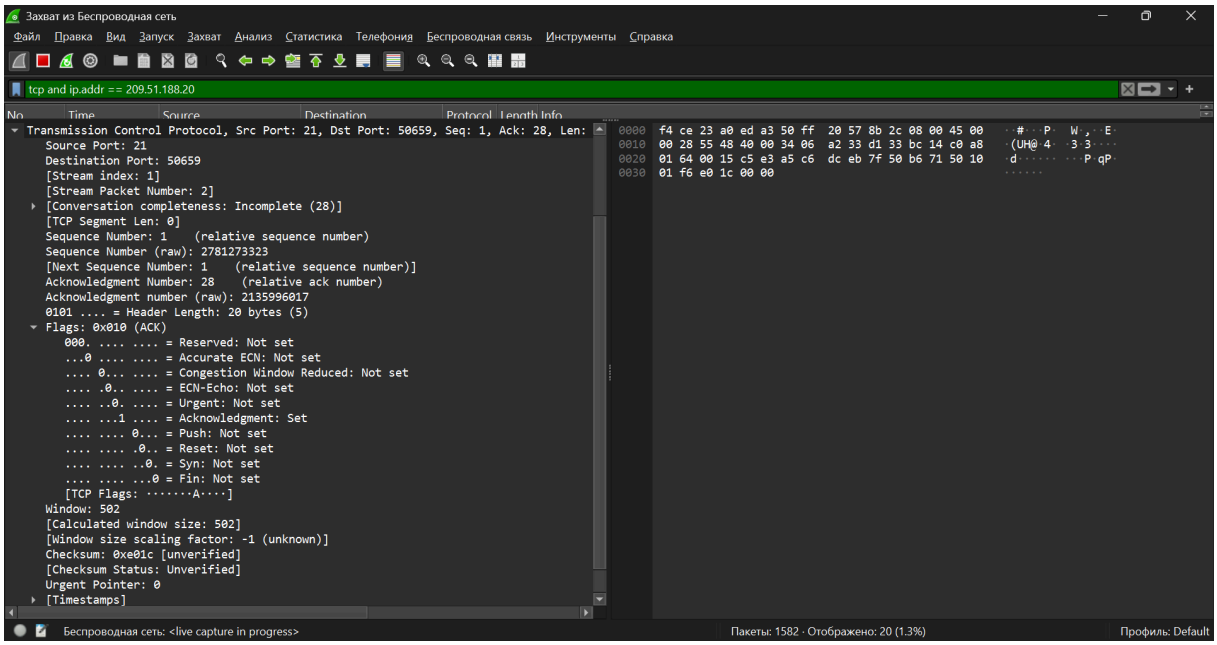


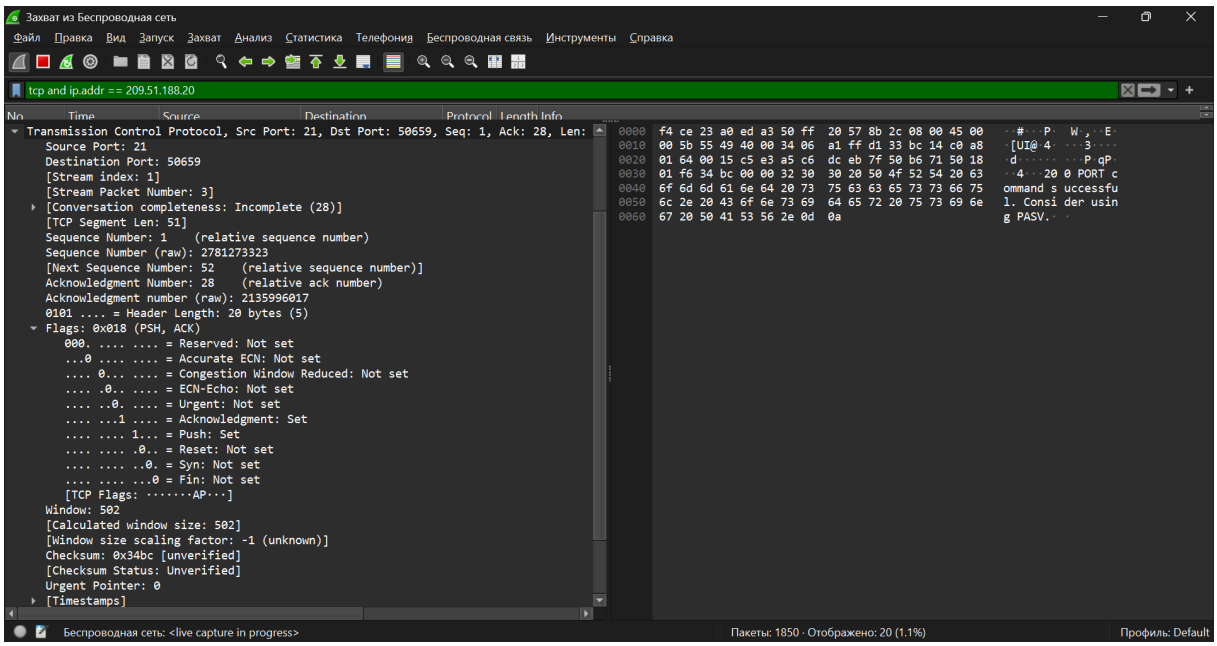
Включим перехват в Wireshark.



Рассмотрим три пакета:

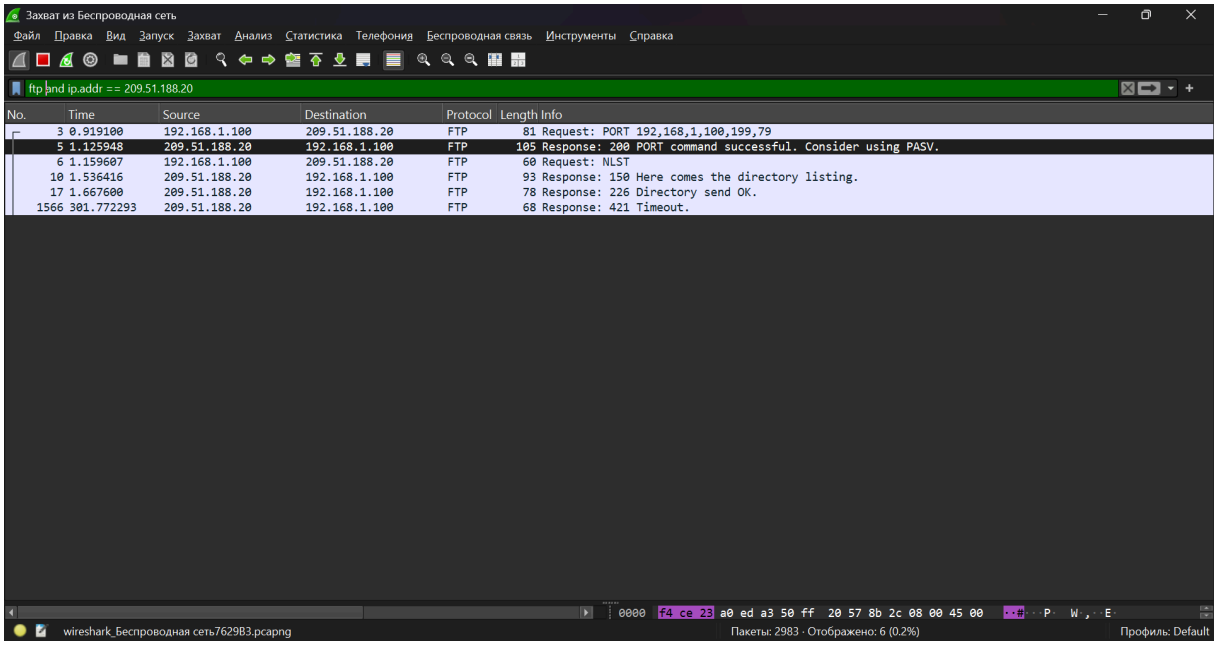






поле	1	2	3
ip src	192.168.1.100	209.51.188.20	209.51.188.20
ip dst	209.51.188.20	192.168.1.100	192.168.1.100
src port #	50659	21	21
dst port #	21	50659	50659
#	1	1	1
ackn #	1	28	28
header len	20	20	20
window size	6780	502	502

Если применить фильтр `ftp and ip.addr == 209.51.188.20`, то можно получить только ftp пакеты.



Заключение.

В ходе работы я с помощью Wireshark изучил протоколы стека TCP/IP, научился перехватывать и фильтровать трафик, анализировать ICMP- и TCP-пакеты, определять активные узлы и порты. Практика закрепила понимание принципов взаимодействия устройств в сети и работы сетевых протоколов.