

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

Факультет инфокоммуникационных технологий

Направление подготовки 11.03.02

Практическая работа №5

ТСР-IP

Выполнил:

Доценников Никита Андреевич

Группа: К3121

Проверил:

Антон Харитонов

Санкт-Петербург

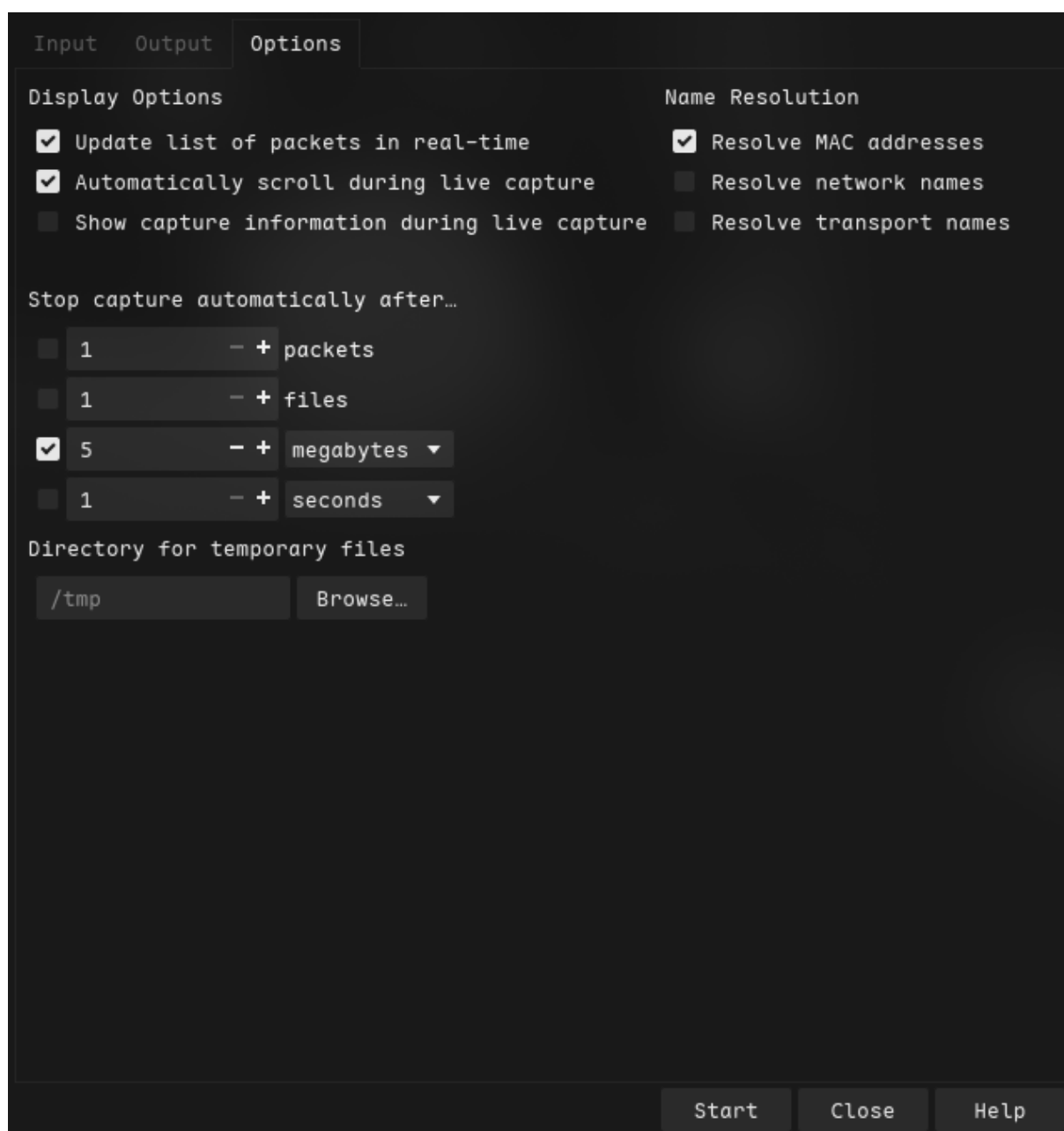
2025

Цель.

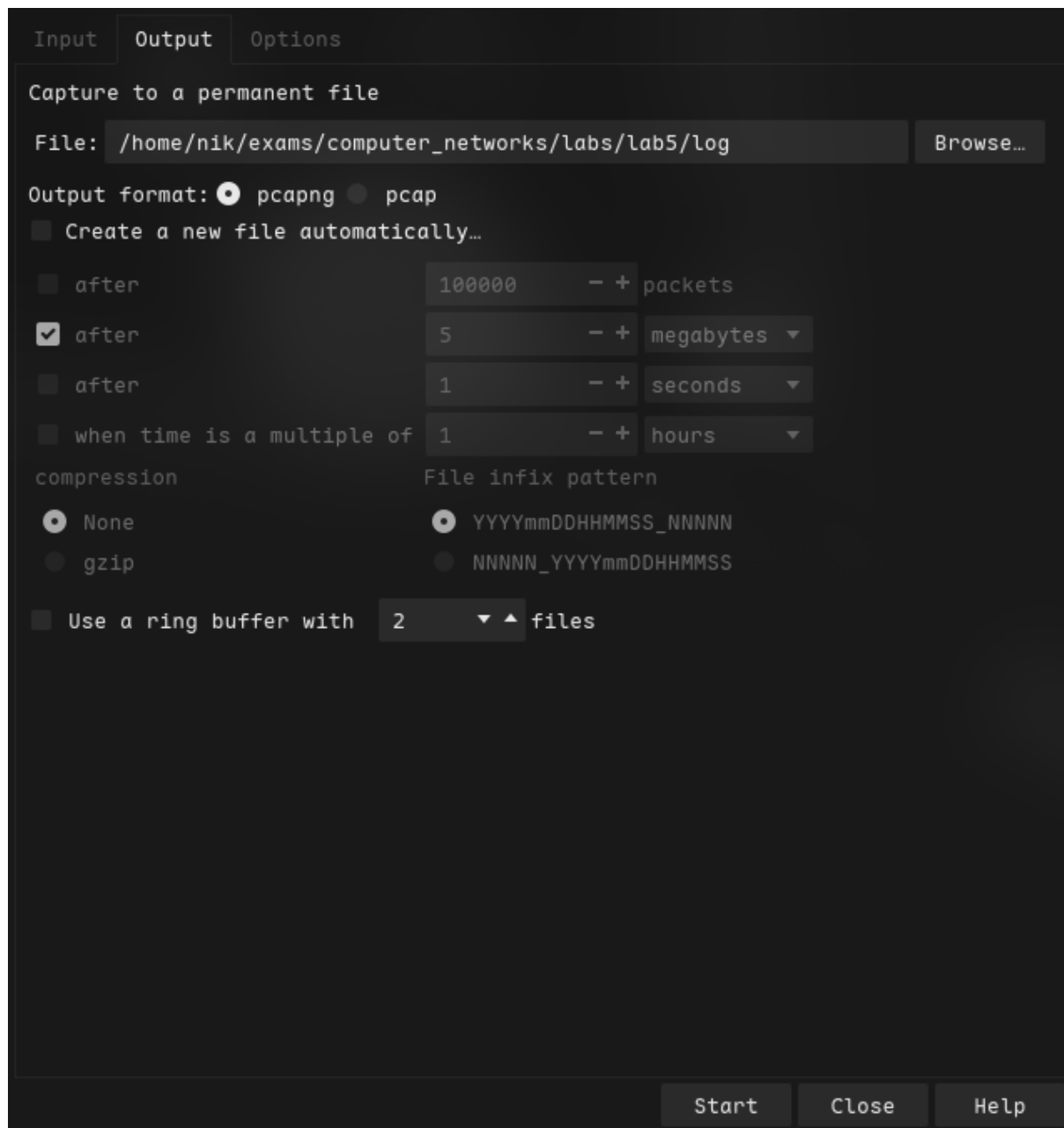
Изучить принципы работы протоколов стека TCP/IP посредством анализа сетевого трафика в программе Wireshark, научиться собирать, фильтровать и интерпретировать пакеты различных протоколов, а также выявлять характеристики и особенности взаимодействий на разных уровнях модели TCP/IP.

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.

Endpoint Settings

Name resolution

Limit to display filter

Copy

Map

Protocol

Bluetooth

BPv7

DCCP

Ethernet

FC

FDDI

IEEE 802.11

IEEE 802.15.4

IPv4

IPv6

IPX

JXTA

...

Filter list for specif...

Ethernet · 3

IPv4 · 7

IPv6

TCP · 8

UDP · 5

Address	Packets	Bytes	Tx Packets	Tx Bytes ▲	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS
151.236.14.199	5,916	5 MB	3,634	4 MB	2,282	449 kB					
192.168.1.86	5,924	5 MB	2,284	449 kB	3,640	4 MB					
192.168.1.1	4	402 bytes	2	246 bytes	2	156 bytes					
64.233.164.138	1	139 bytes	1	139 bytes	0	0 bytes					
64.233.165.119	1	139 bytes	1	139 bytes	0	0 bytes					
108.177.14.190	1	139 bytes	1	139 bytes	0	0 bytes					
142.251.1.94	1	139 bytes	1	139 bytes	0	0 bytes					

Close

Help

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.

Endpoint Settings

Name resolution

Limit to display filter

Copy

Map

Protocol

Bluetooth

BPv7

DCCP

Ethernet

FC

FDDI

IEEE 802.11

IEEE 802.15.4

IPv4

IPv6

IPX

JXTA

...

Filter list for specif...

Ethernet · 3

IPv4 · 7

IPv6

TCP · 8

UDP · 5

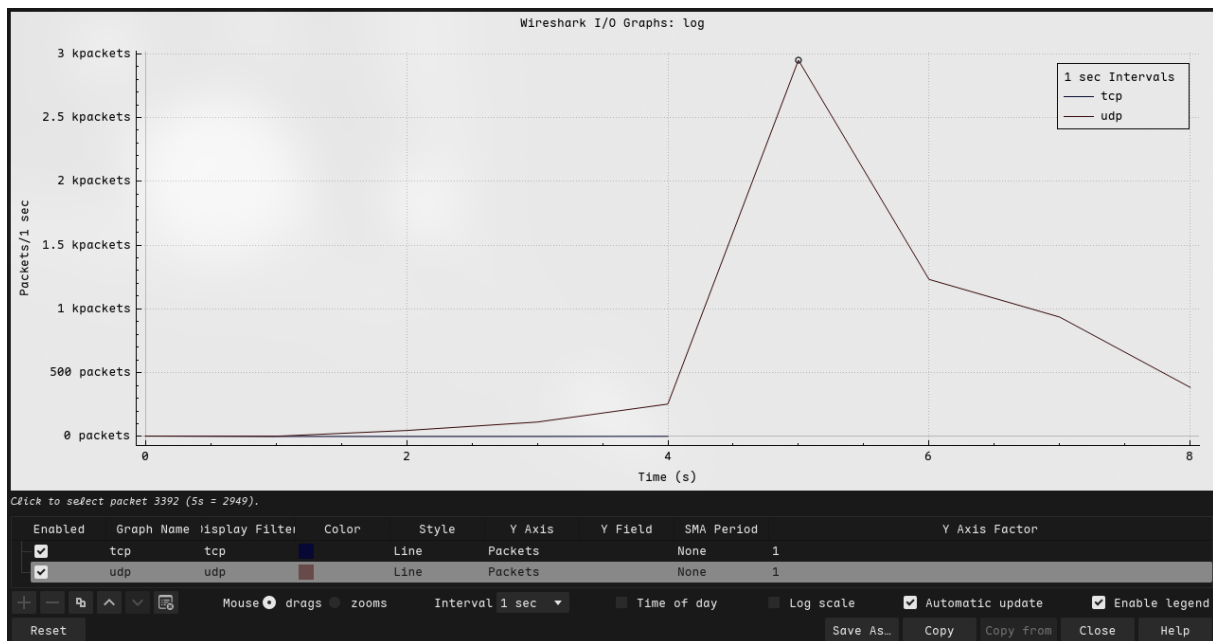
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes ▲	Rx Packets	Rx Bytes
64.233.164.138	443	1	139 bytes	1	139 bytes	0	0 bytes
64.233.165.119	443	1	139 bytes	1	139 bytes	0	0 bytes
108.177.14.190	443	1	139 bytes	1	139 bytes	0	0 bytes
142.251.1.94	443	1	139 bytes	1	139 bytes	0	0 bytes
192.168.1.86	42994	1	139 bytes	0	0 bytes	1	139 bytes
192.168.1.86	43086	1	139 bytes	0	0 bytes	1	139 bytes
192.168.1.86	43588	1	139 bytes	0	0 bytes	1	139 bytes
192.168.1.86	55900	1	139 bytes	0	0 bytes	1	139 bytes

Close

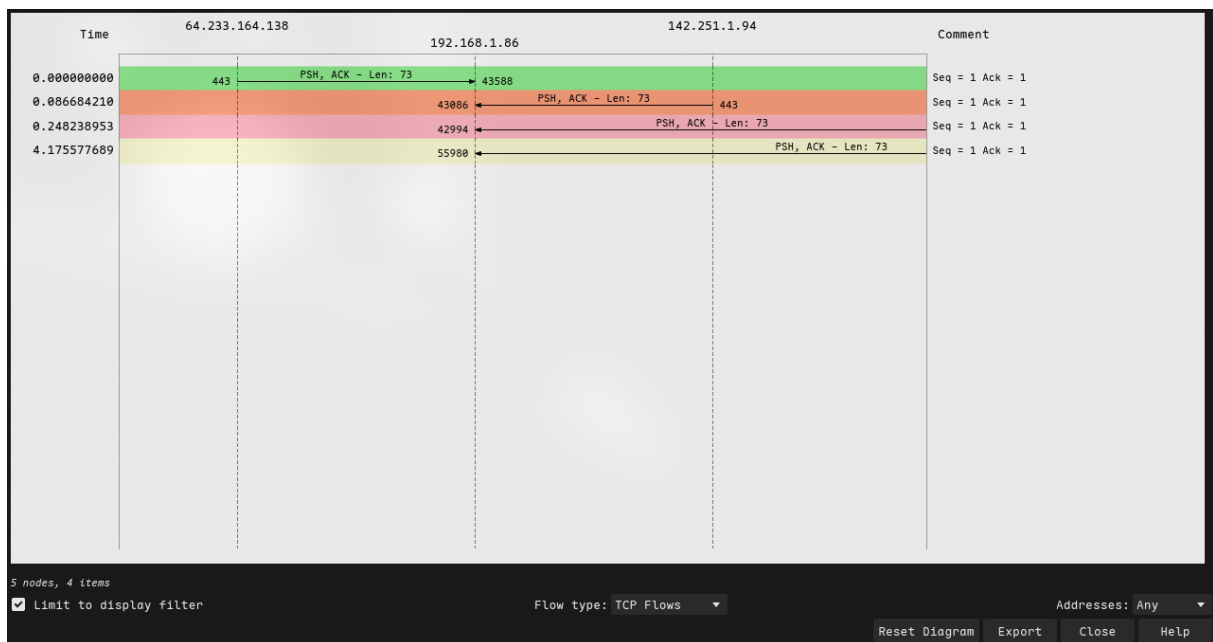
Help

Получаем 42994.

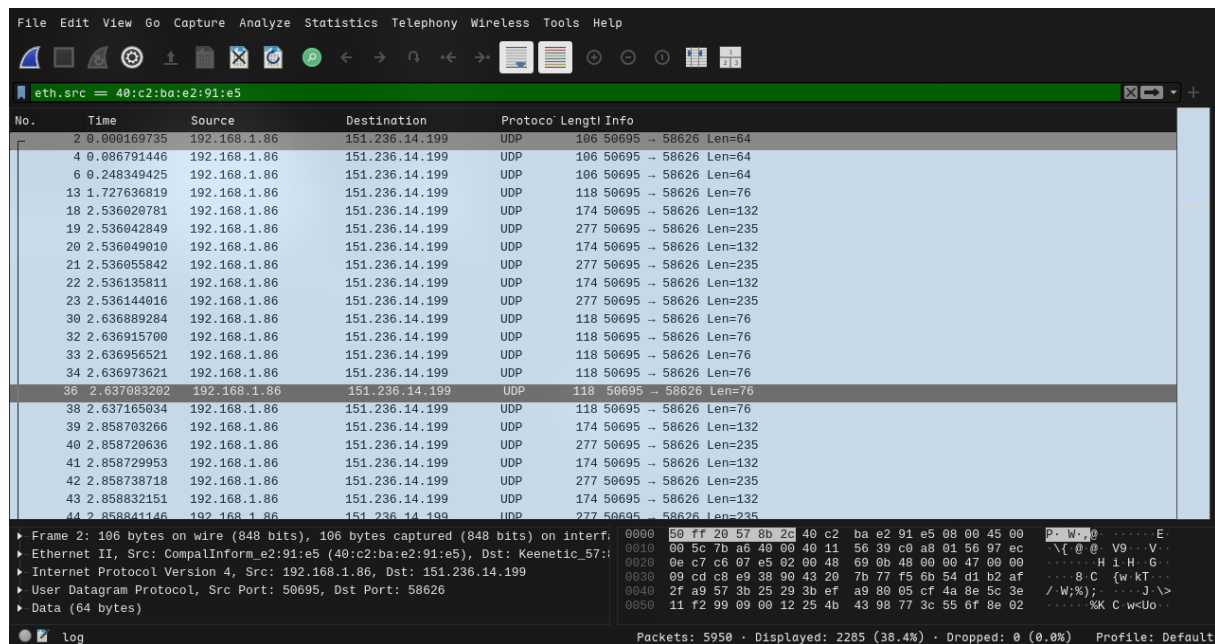
Построим граф интенсивности трафика TCP, UDP. Переходим в Statistics -> I/O Graphs.



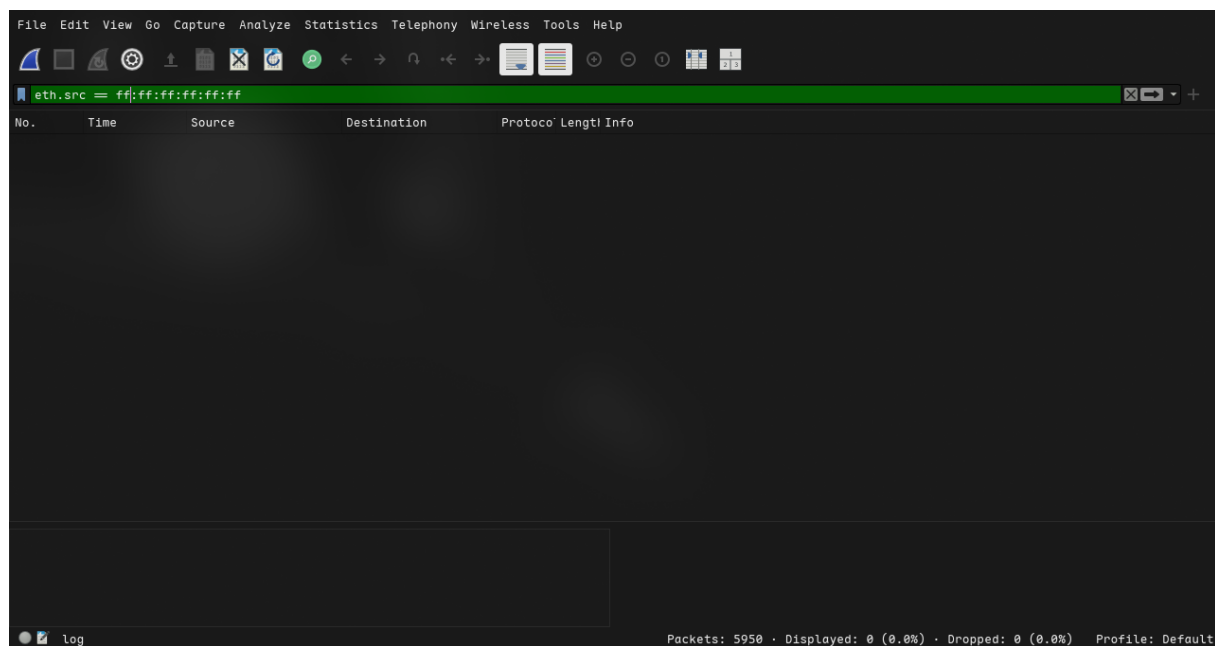
Построим диаграмму связей пакетов HTTPS. Для этого отфильтруем только порты 443 (`tcp.port == 443`). Затем Statistics -> Flow Graph ограничиваем по фильтру и в выпадающем меню выбираем TCP Flows.



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



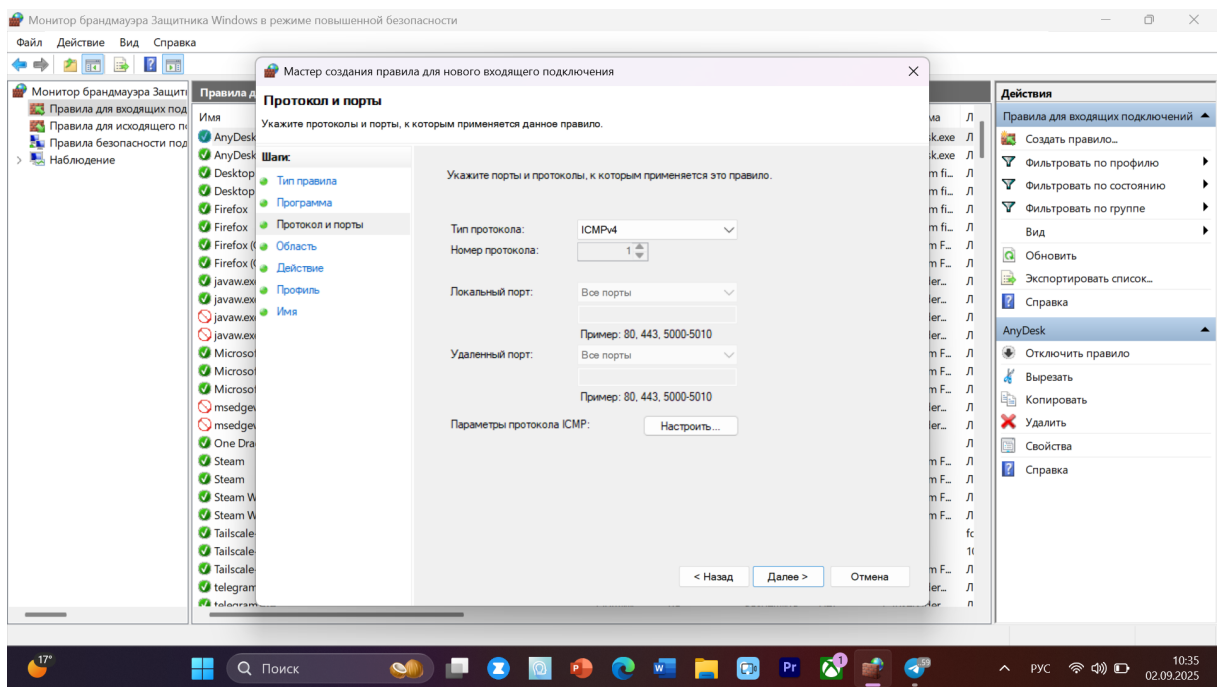
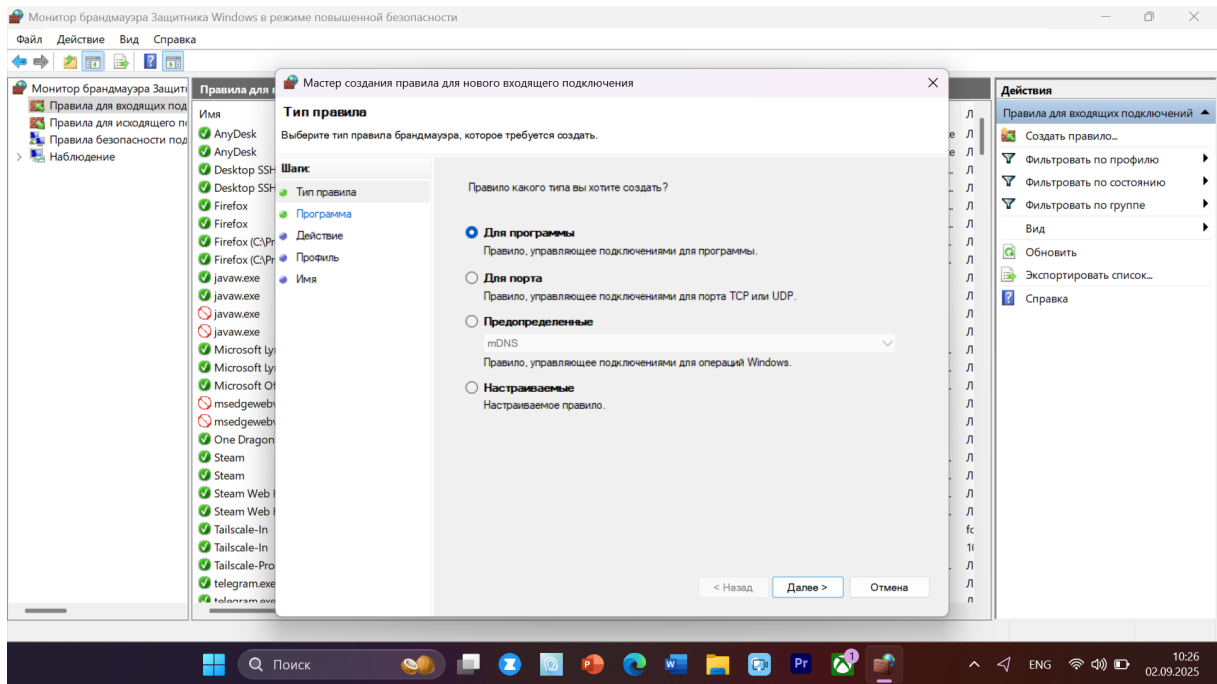
Отфильтруем только широковещательные сообщения. (`eth.src == ff:ff:ff:ff:ff:ff`)

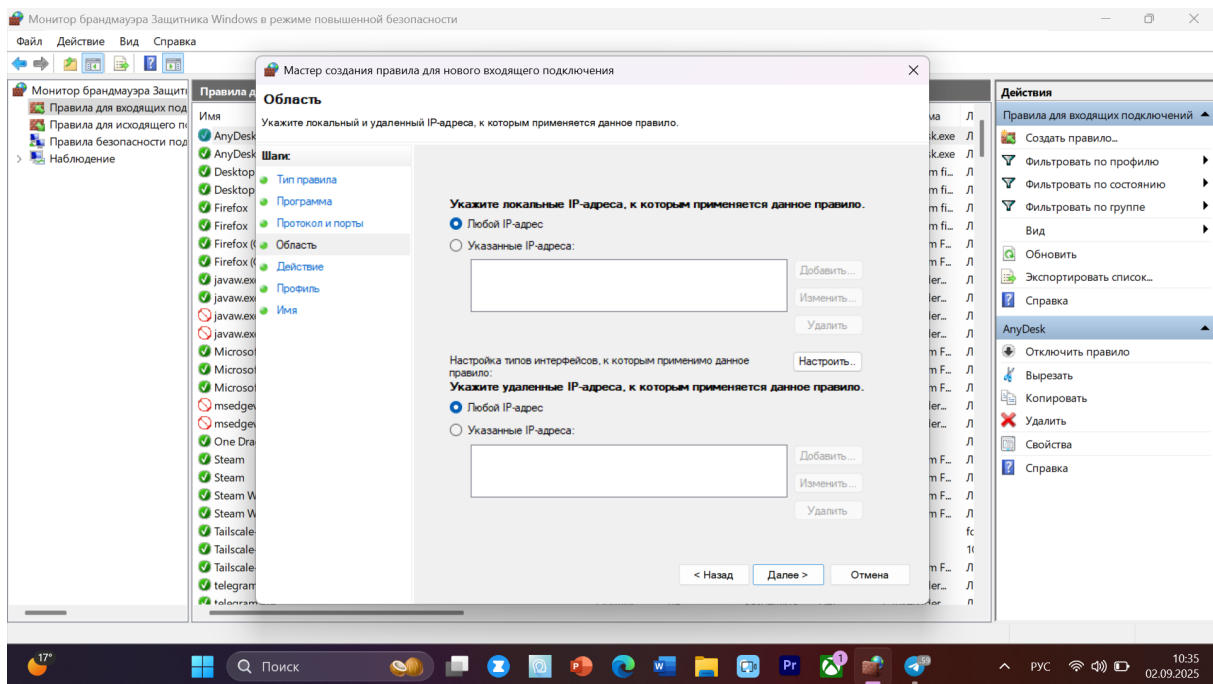


Как можно видеть, у меня не было найдено широковещательных сообщений.

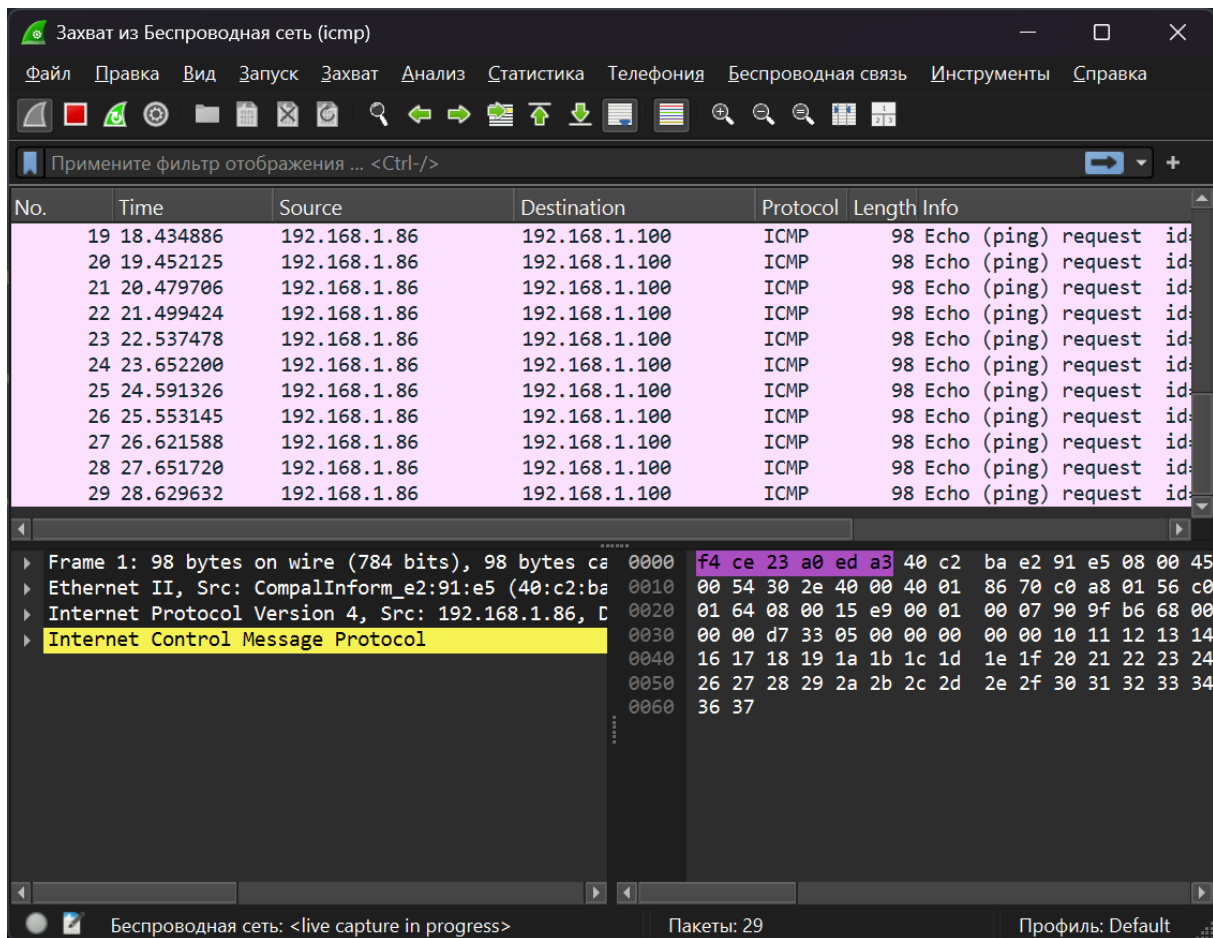
ICMP.

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





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:

```
Администратор: Windows PowerShell (x86)
PS C:\WINDOWS\system32> ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : MSI
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . . . . . : tailscf74b.ts.net

Неизвестный адаптер Подключение по локальной сети:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Wintun Userspace Tunnel
Физический адрес. . . . . :
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

Неизвестный адаптер Tailscale:

DNS-суффикс подключения . . . . . : tailscf74b.ts.net
Описание. . . . . : Tailscale Tunnel
Физический адрес. . . . . :
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
IPv6-адрес. . . . . : fd7a:115c:a1e0:7234:f249(Основной)
Локальный IPv6-адрес канала . . . . . : fe80:82a6:a0e2:6a76:8e28%(Основной)
IPv4-адрес. . . . . : 100.94.242.73(Основной)
Маска подсети . . . . . : 255.255.255.255
Основной шлюз. . . . . :
NetBios через TCP/IP. . . . . : Отключен
Список поиска DNS-суффиксов подключения :
    tailscf74b.ts.net

Неизвестный адаптер Подключение по локальной сети 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
```

```
Администратор: Windows PowerShell (x86)

Неизвестный адаптер Подключение по локальной сети 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : TAP-Windows Adapter V9
Физический адрес. . . . . : 00-FF-B3-2E-7B-81
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Физический адрес. . . . . : F4-CE-23-A0-ED-A4
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 4:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Физический адрес. . . . . : F6-CE-23-A0-ED-A3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Физический адрес. . . . . : F4-CE-23-A0-ED-A3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
IPv4-адрес. . . . . : 192.168.1.100(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 2 сентября 2025 г. 9:46:07
Срок аренды истекает. . . . . : 2 сентября 2025 г. 17:23:56
Основной шлюз. . . . . : 192.168.1.1
```

```
Администратор: Windows PowerShell (x86)
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Физический адрес. . . . . : F4-CE-23-A0-ED-A4
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 4:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Физический адрес. . . . . : F6-CE-23-A0-ED-A3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Физический адрес. . . . . : F4-CE-23-A0-ED-A3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
IPv4-адрес. . . . . : 192.168.1.100(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 2 сентября 2025 г. 9:46:07
Срок аренды истекает. . . . . : 2 сентября 2025 г. 17:23:56
Основной шлюз. . . . . : 192.168.1.1
DNS-сервер. . . . . : 192.168.1.1
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен

Адаптер Ethernet Сетевое подключение Bluetooth:

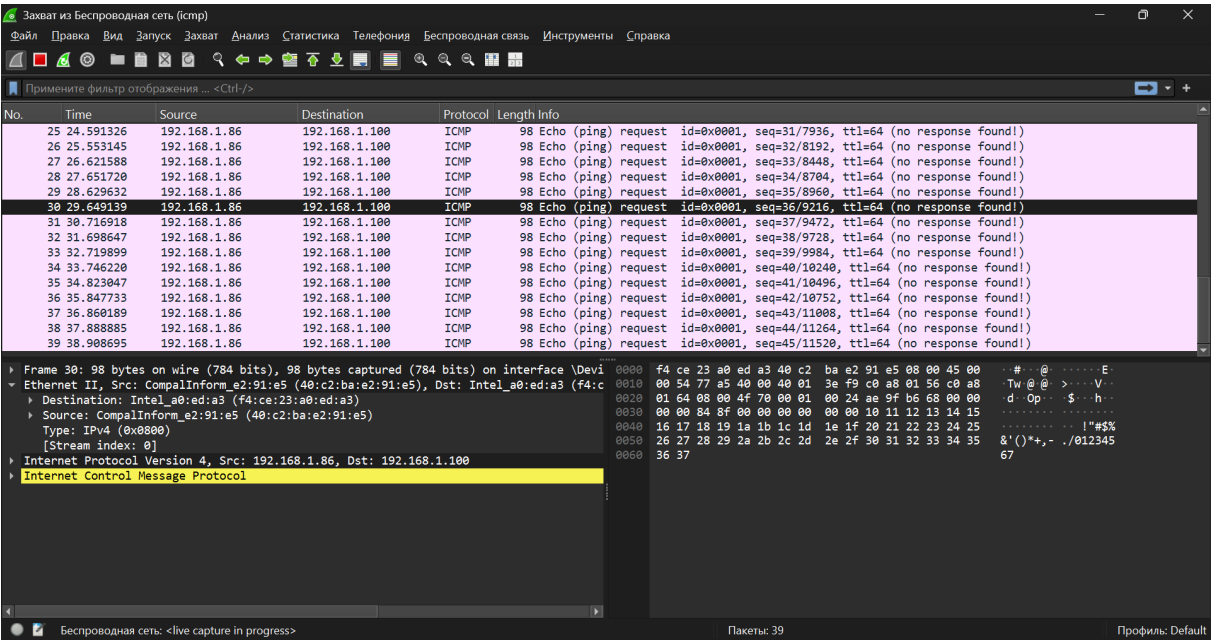
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Bluetooth Device (Personal Area Network)
Физический адрес. . . . . : F4-CE-23-A0-ED-A7
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
PS C:\WINDOWS\system32>
```

Для отправителя:

```
ip link show © 10:44

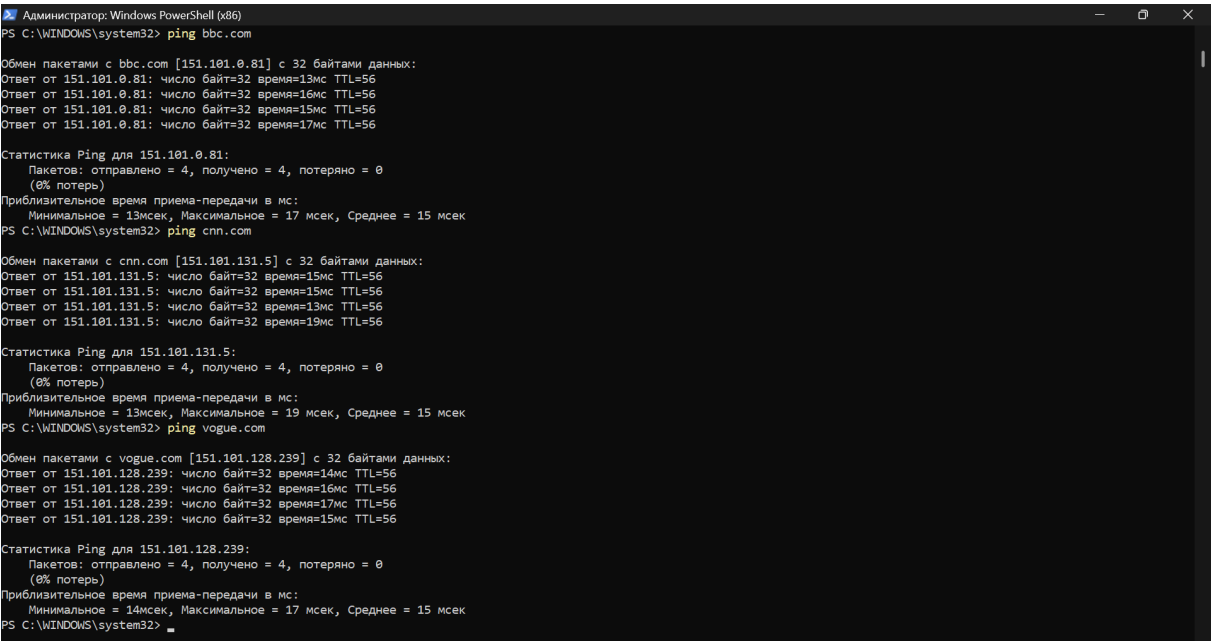
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 40:c2:ba:e2:91:e5 brd ff:ff:ff:ff:ff:ff
    altnam enx40c2bae291e5
3: wlp3s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000
    link/ether 02:d7:77:b4:08:0e brd ff:ff:ff:ff:ff:ff permaddr d0:39:57:88:3f:4b
    altnam wlx03957883f4b
4: tailscale0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1280 qdisc fq_codel state UNKNOWN mode DEFAULT group default qlen 500
    link/none
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN mode DEFAULT group default qlen 500
    link/none
```

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 (снур)

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 \Device\NPF...
Ethernet II, Src: Keenetic_57:8b:2c (50:ff:20:57:8b:2c), Dst: Intel_a0:ed:a3 (f4:ce:23:a0:ed:a3)
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

Беспроводная сеть: <live capture in progress> Пакеты: 24 Профиль: Default

Захват из Беспроводная сеть (снур)

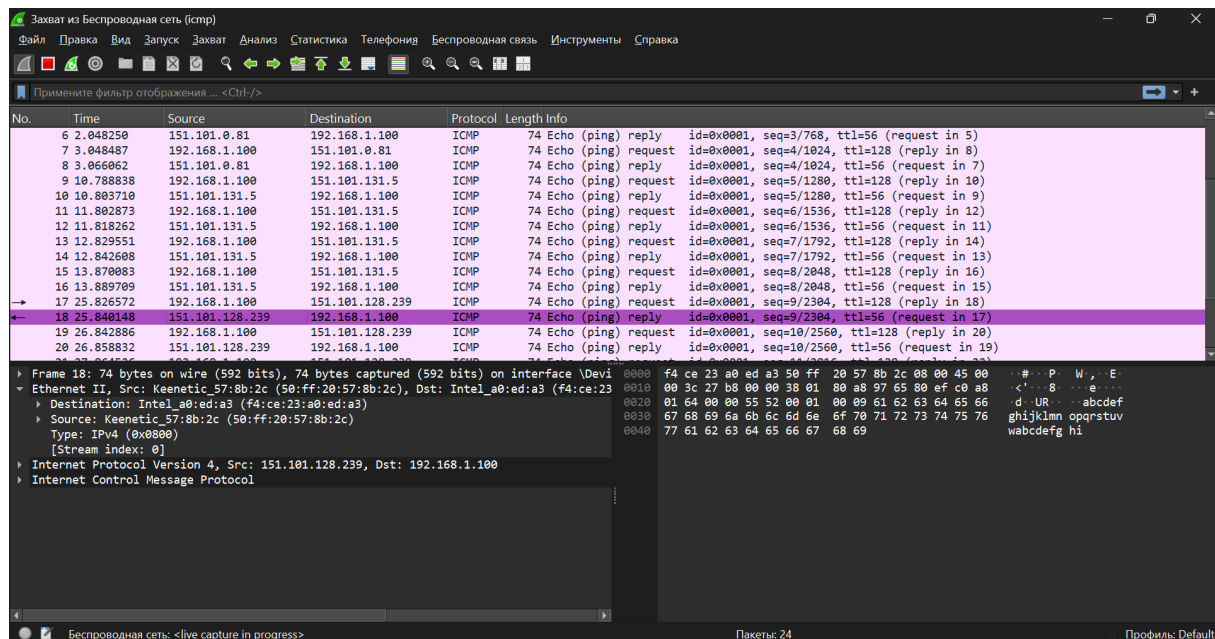
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

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 \Device\NPF...
Ethernet II, Src: Keenetic_57:8b:2c (50:ff:20:57:8b:2c), Dst: Intel_a0:ed:a3 (f4:ce:23:a0:ed:a3)
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

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.

ТСР.

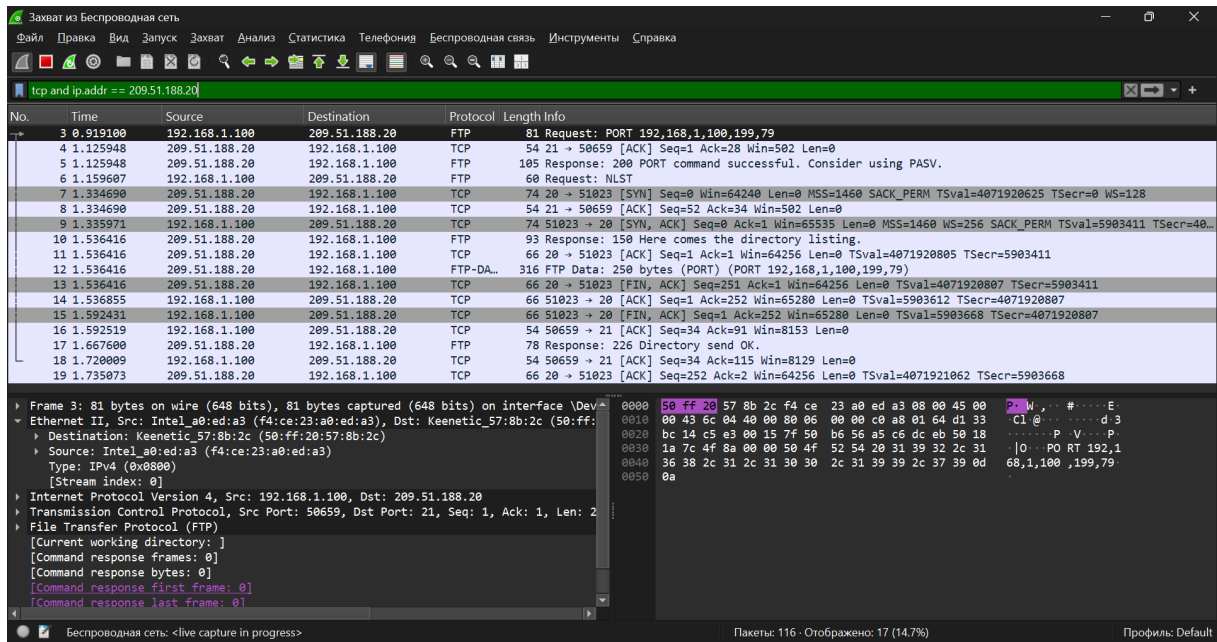
В качестве FTP сервера буду использовать ftp.gnu.org. Получим его адрес.

```
PS C:\WINDOWS\system32> nslookup ftp.gnu.org
Server: UnKnown
Address: 192.168.1.1

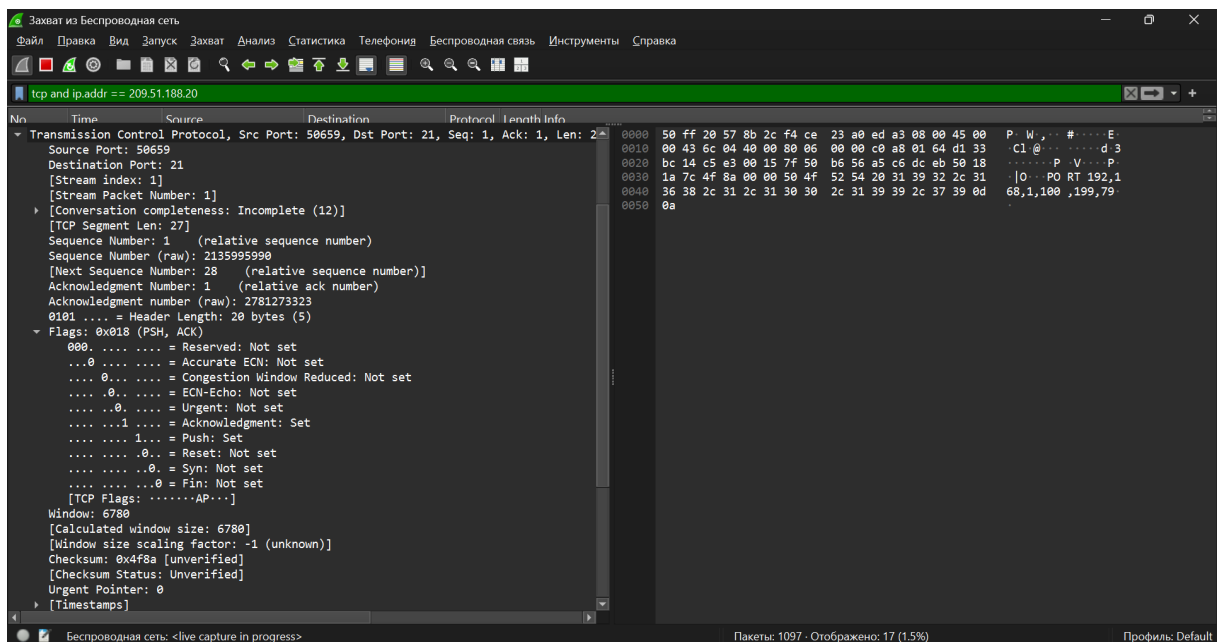
Не заслуживающий доверия ответ:
Server: ftp.gnu.org
Addresses: 2001:470:142:3::b
          209.51.188.20

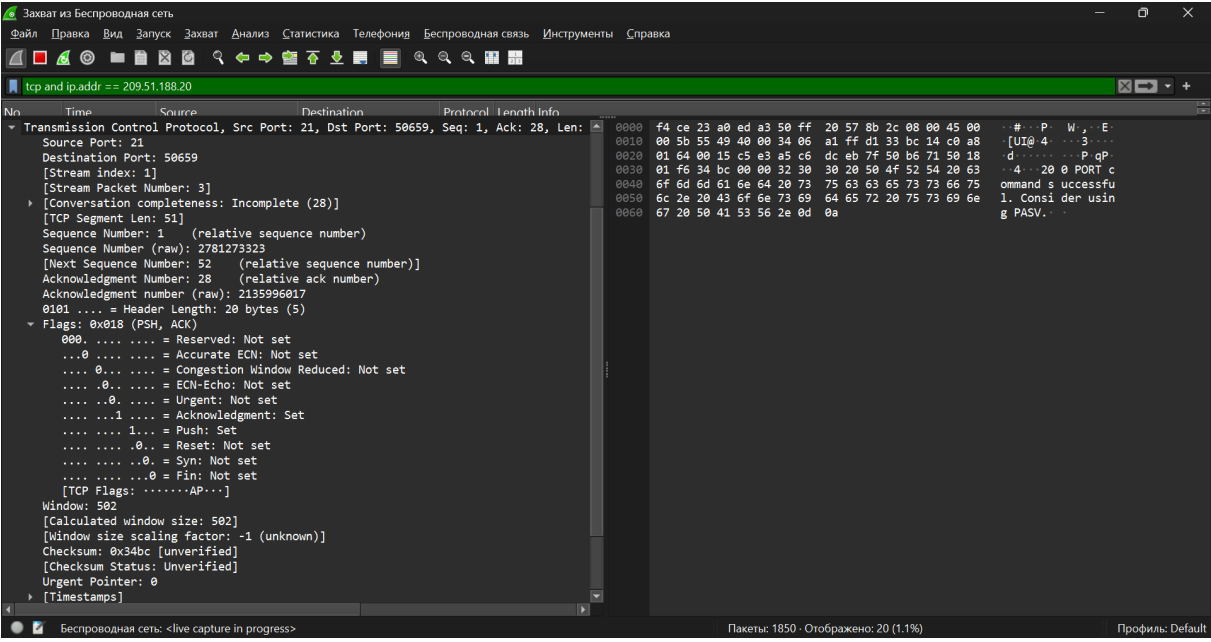
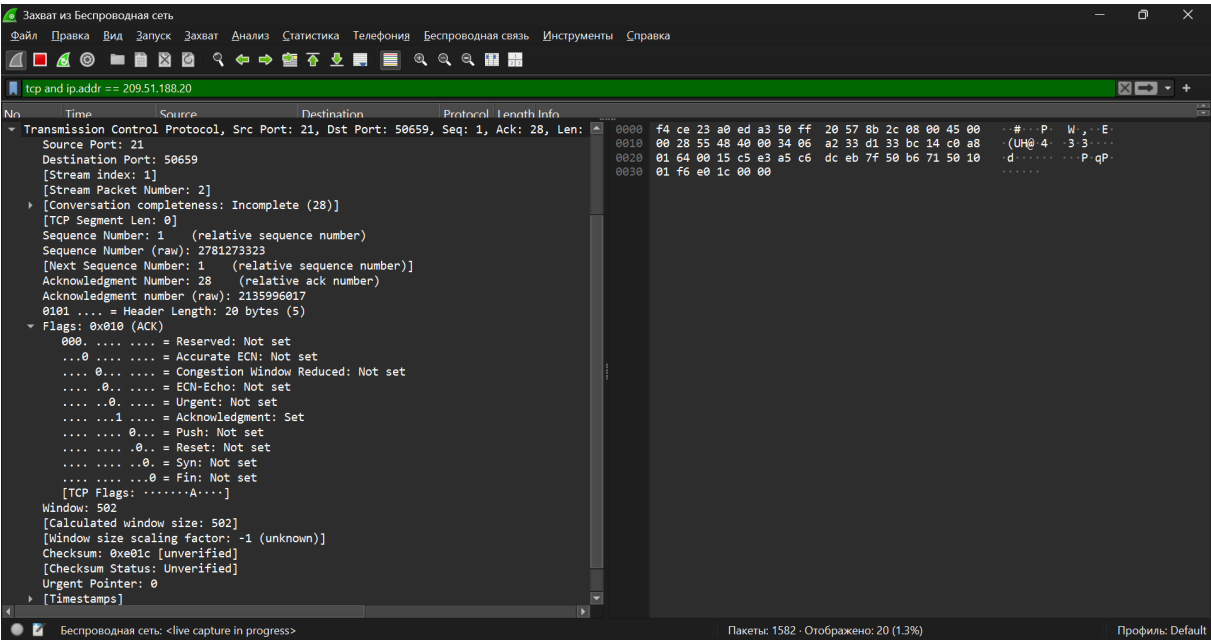
PS C:\WINDOWS\system32>
```

Включим перехват в Wireshark.



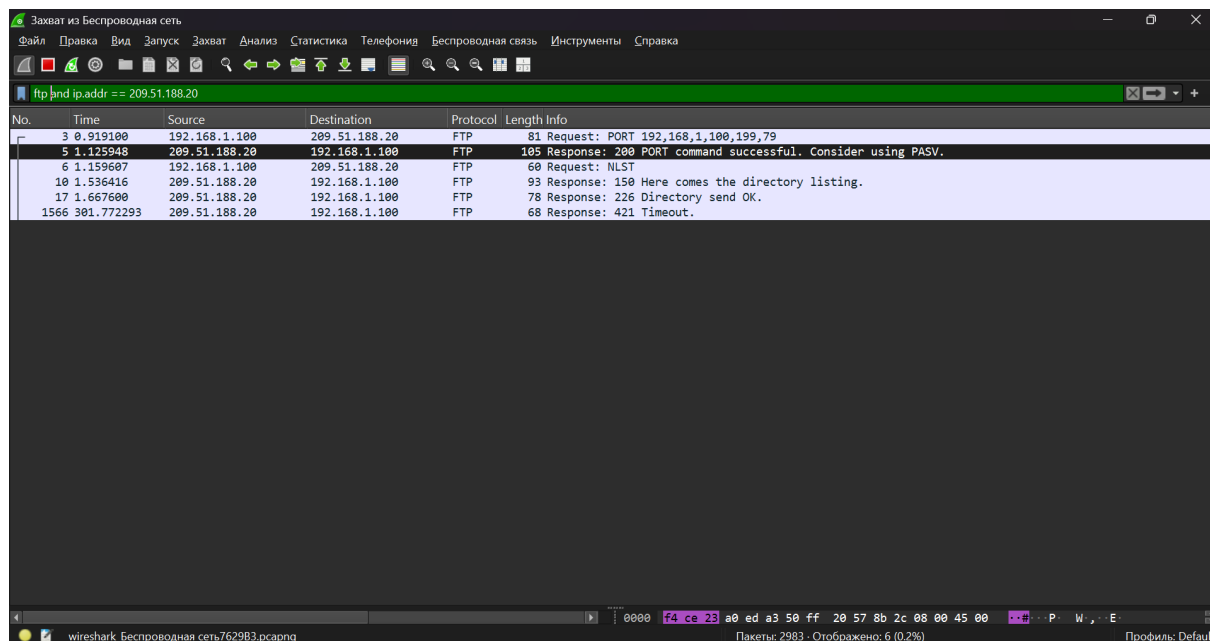
Рассмотрим три пакета:





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.