САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Практическая работа №5. Изучение работы протоколов стека TCP/IP с помощью Wireshark.

Выполнил: Титов Г.К. (409687)

Проверил: Харитонов А.Ю.

Санкт-Петербург

2025 год.

Содержание

Цель работы

Разобраться со стеком TCP/IP, анализируя пакеты, которые отправляются и принимаются с помощью данного стека.

Научиться собирать сетевой трафик с помощью программы Wireshark. Научиться фильтровать собранный трафик, находить и просматривать соединения.

Выполнение работы

1. Начало работы с Wireshark.

Перехватили 5 МБ трафика.

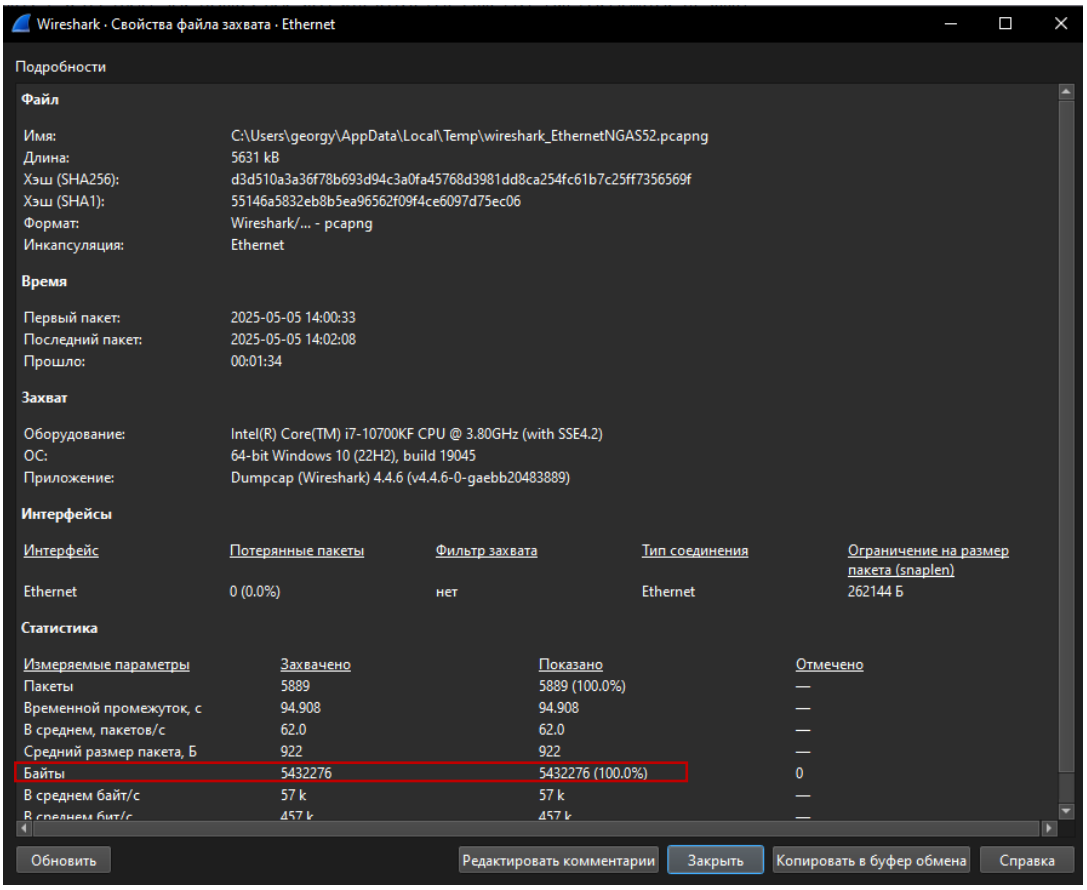


Рисунок 1 - Перехват 5 МБ трафика.

Далее ,используя инструменты статистики, определяем:

a) Узел с максимальной активностью (по объему переданных данных) – 192.168.0.106 (мой ПК)

b) Узел, осуществивший наибольшее кол-во широковещательных рассылок - TPLink_a6:b9:55 (мой роутер)

c) Самый активный TCP-порт на хосте (по кол-ву переданных пакетов) - 52306

d)

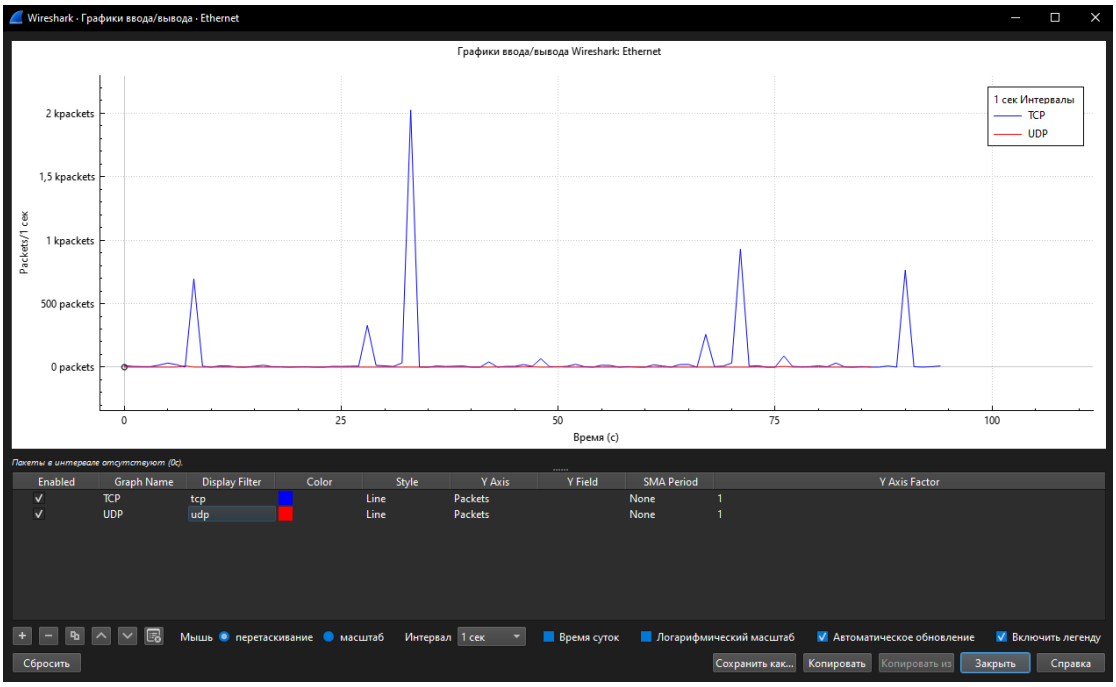


Рисунок 2 - Интенсивность TCP и UDP трафика

e)

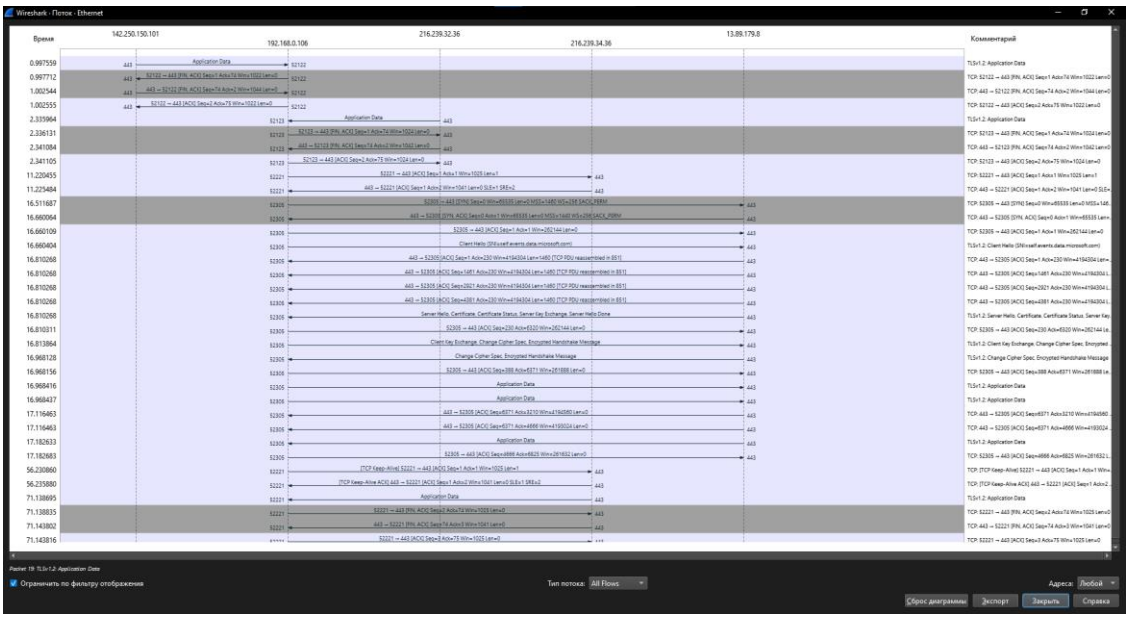


Рисунок 3 - Диаграмма связей, протокол HTTPS

Далее напишем фильтры для выделения пакетов из всего трафика:

a) HTTP между локальными клиентами и внешними серверами:

```
Tcp.dstport == 80 && !(ip.src == 127.0.0.1 || ip.dst == 127.0.0.1)
```

b) Все Ethernet-кадры, отправленные с интерфейса хоста:

```
eth.src == <ваш_MAC>
```

c) Только широковещательные сообщения:

eth.dst == ff:ff:ff:ff:ff:ff || ip.dst == 255.255.255.255

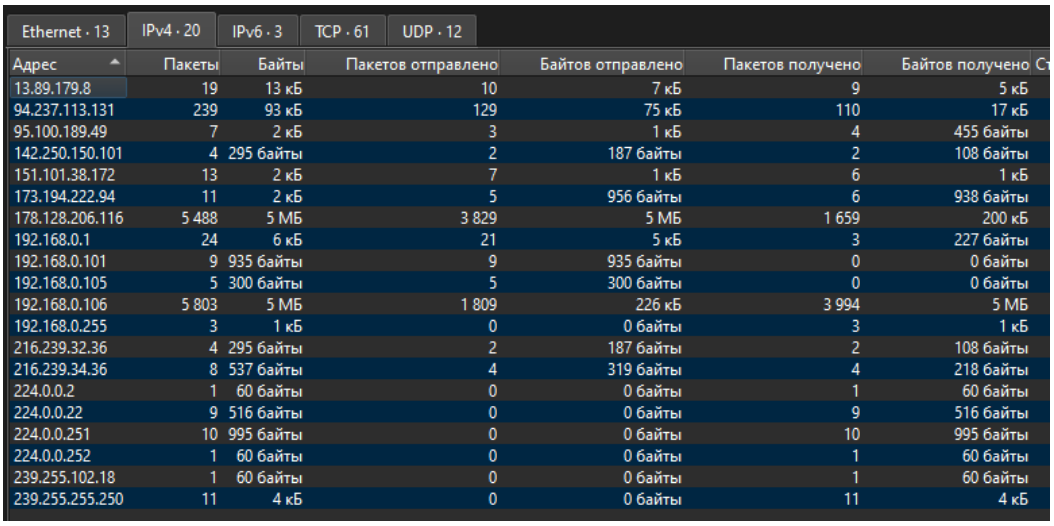
ARP (Address Resolution Protocol) – определение MAC-адреса по IP.

d)

Ethernet · 13 | IPv4 · 20 | IPv6 · 3 | TCP · 61 | UDP · 12

Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено
01:00:5e:00:00:02	1	60 байты	0	0 байты	1	60 байты
01:00:5e:00:00:16	9	516 байты	0	0 байты	9	516 байты
01:00:5e:00:00:fb	10	995 байты	0	0 байты	10	995 байты
01:00:5e:00:00:fc	1	60 байты	0	0 байты	1	60 байты
01:00:5e:7f:66:12	1	60 байты	0	0 байты	1	60 байты
01:00:5e:7f:ff:fa	11	4 кБ	0	0 байты	11	4 кБ
2c:f0:5d:85:93:d2	5 803	5 МБ	1 809	226 кБ	3 994	5 МБ
33:33:00:00:00:16	2	180 байты	0	0 байты	2	180 байты
33:33:00:00:00:fb	5	795 байты	0	0 байты	5	795 байты
38:d5:7a:f0:23:e1	5	300 байты	5	300 байты	0	0 байты
9c:a2:f4:a6:b9:55	5 864	5 МБ	4 059	5 МБ	1 805	226 кБ
a6:a5:b9:bc:61:76	16	2 кБ	16	2 кБ	0	0 байты
ff:ff:ff:ff:ff:ff	50	4 кБ	0	0 байты	50	4 кБ

Рисунок 4- MAC-адреса назначения

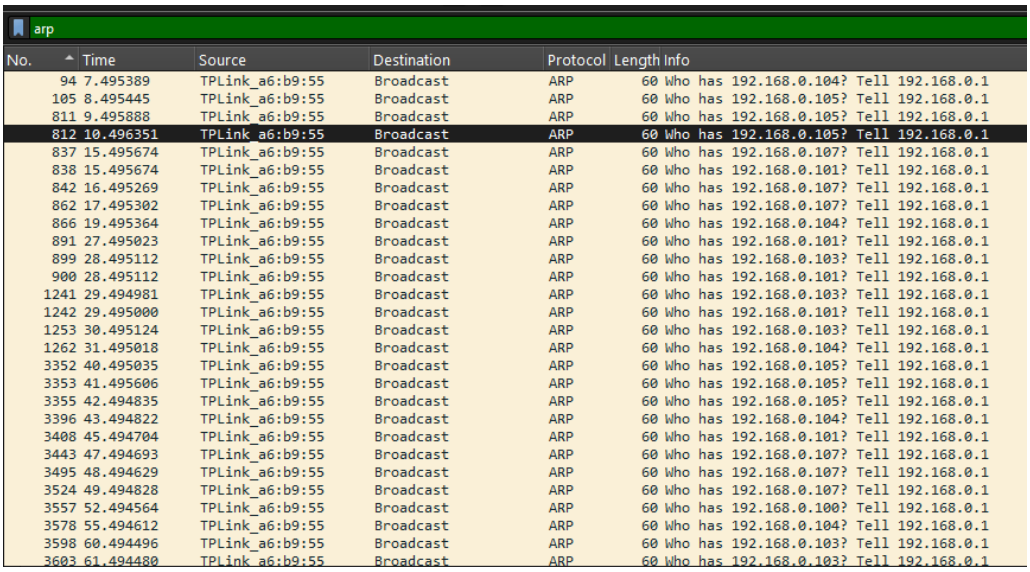


Ethernet · 13 | IPv4 · 20 | IPv6 · 3 | TCP · 61 | UDP · 12

Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено
13.89.179.8	19	13 кБ	10	7 кБ	9	5 кБ
94.237.113.131	239	93 кБ	129	75 кБ	110	17 кБ
95.100.189.49	7	2 кБ	3	1 кБ	4	455 байты
142.250.150.101	4	295 байты	2	187 байты	2	108 байты
151.101.38.172	13	2 кБ	7	1 кБ	6	1 кБ
173.194.222.94	11	2 кБ	5	956 байты	6	938 байты
178.128.206.116	5 488	5 МБ	3 829	5 МБ	1 659	200 кБ
192.168.0.1	24	6 кБ	21	5 кБ	3	227 байты
192.168.0.101	9	935 байты	9	935 байты	0	0 байты
192.168.0.105	5	300 байты	5	300 байты	0	0 байты
192.168.0.106	5 803	5 МБ	1 809	226 кБ	3 994	5 МБ
192.168.0.255	3	1 кБ	0	0 байты	3	1 кБ
216.239.32.36	4	295 байты	2	187 байты	2	108 байты
216.239.34.36	8	537 байты	4	319 байты	4	218 байты
224.0.0.2	1	60 байты	0	0 байты	1	60 байты
224.0.0.22	9	516 байты	0	0 байты	9	516 байты
224.0.0.251	10	995 байты	0	0 байты	10	995 байты
224.0.0.252	1	60 байты	0	0 байты	1	60 байты
239.255.102.18	1	60 байты	0	0 байты	1	60 байты
239.255.255.250	11	4 кБ	0	0 байты	11	4 кБ

Рисунок 5 - IP-адреса назначения

e) Фильтр для ARP (Resolution Protocol) – arp.



arp

No.	Time	Source	Destination	Protocol	Length	Info
94	7.495389	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.1
105	8.495445	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.105? Tell 192.168.0.1
811	9.495888	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.105? Tell 192.168.0.1
812	10.496351	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.105? Tell 192.168.0.1
837	15.495674	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
838	15.495674	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
842	16.495269	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
862	17.495302	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
866	19.495364	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.1
891	27.495023	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
899	28.495112	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
900	28.495112	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
1241	29.494981	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
1242	29.495000	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
1253	30.495124	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
1262	31.495018	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.1
3352	40.495035	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.105? Tell 192.168.0.1
3353	41.495606	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.105? Tell 192.168.0.1
3355	42.494835	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.105? Tell 192.168.0.1
3396	43.494822	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.1
3408	45.494704	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.101? Tell 192.168.0.1
3443	47.494693	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
3495	48.494629	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
3524	49.494828	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
3557	52.494564	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.100? Tell 192.168.0.1
3578	55.494612	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.1
3598	60.494496	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
3603	61.494480	TPLink_a6:b9:55	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1

Рисунок 6- Фильтр ARP

f) Используемый компьютер подключен к маршрутизатору. На это указывает несколько факторов. Например вся ARP-активность наблюдалась только с одного устройства (MAC-адреса) – маршрутизатора. Если посмотреть заголовки канального уровня, то видно, что получателем всех исходящих от хоста запросов в интернет. является роутер (маршрутизатор).

2. Сбор и анализ данных ICMP.

Для разрешения ICMP – запросов в Windows необходимо настроить брандмауэр. Для этого нужно создать новое правило для входящего подключения, которое будет пропускать все входящие пакеты по протоколу ICMPv4.

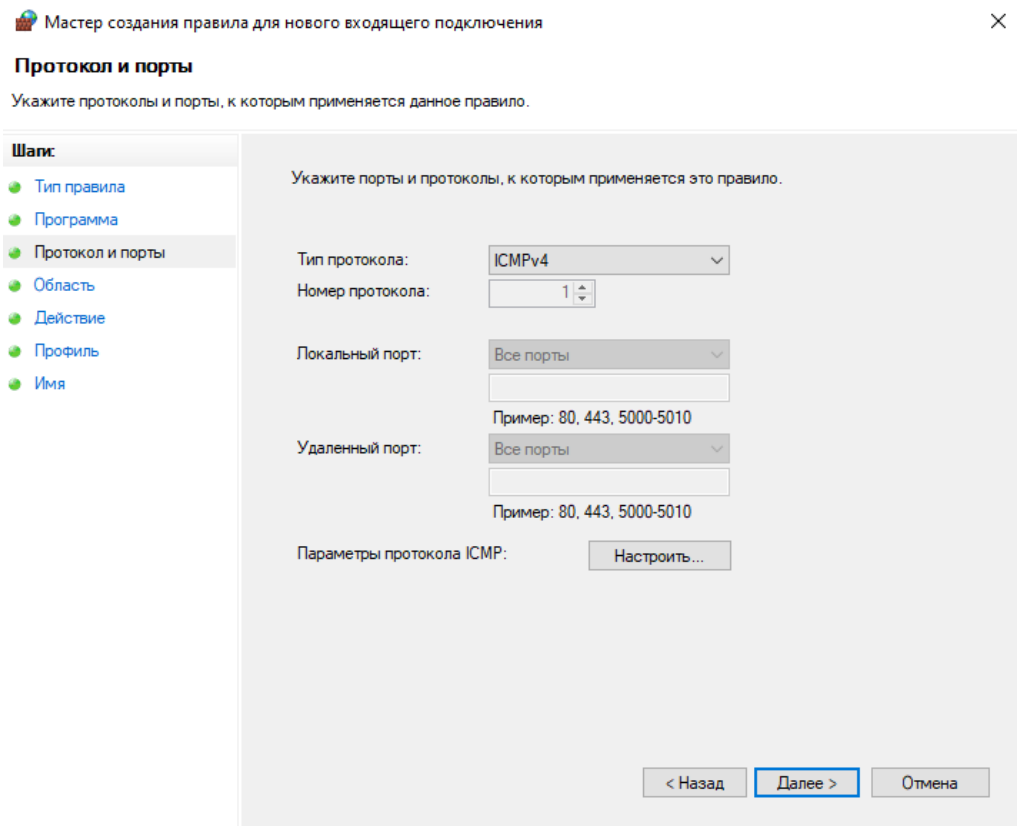


Рисунок 7 - Создание правила

Узнаем IP и MAC адреса двух устройств в нашей сети (в моем случае ПК и ноутбук).

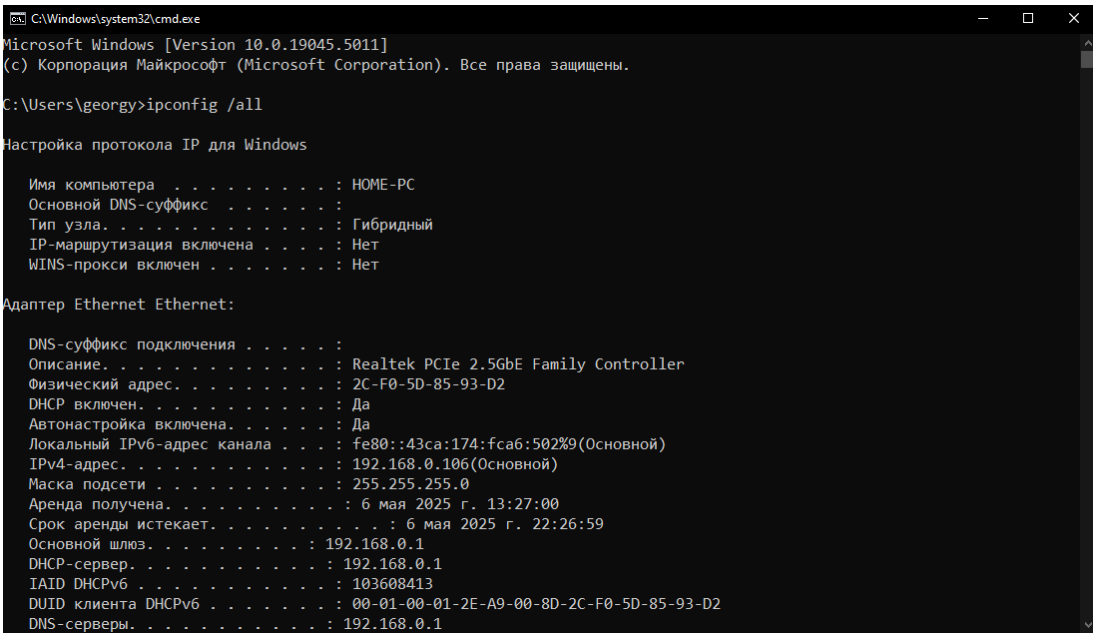


Рисунок 8 - Сетевые параметры ПК

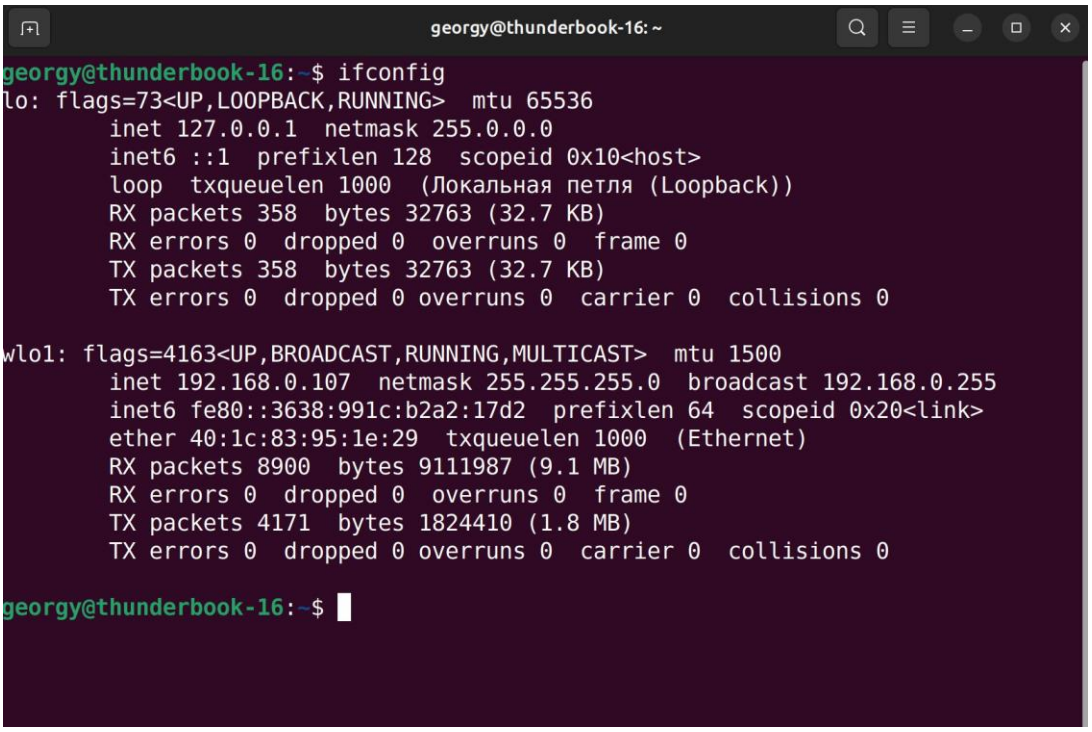


Рисунок 9 - Сетевые параметры ноутбука

Пропингуем ПК с ноутбука (на ПК работает Wireshark и захватывает сетевой трафик)

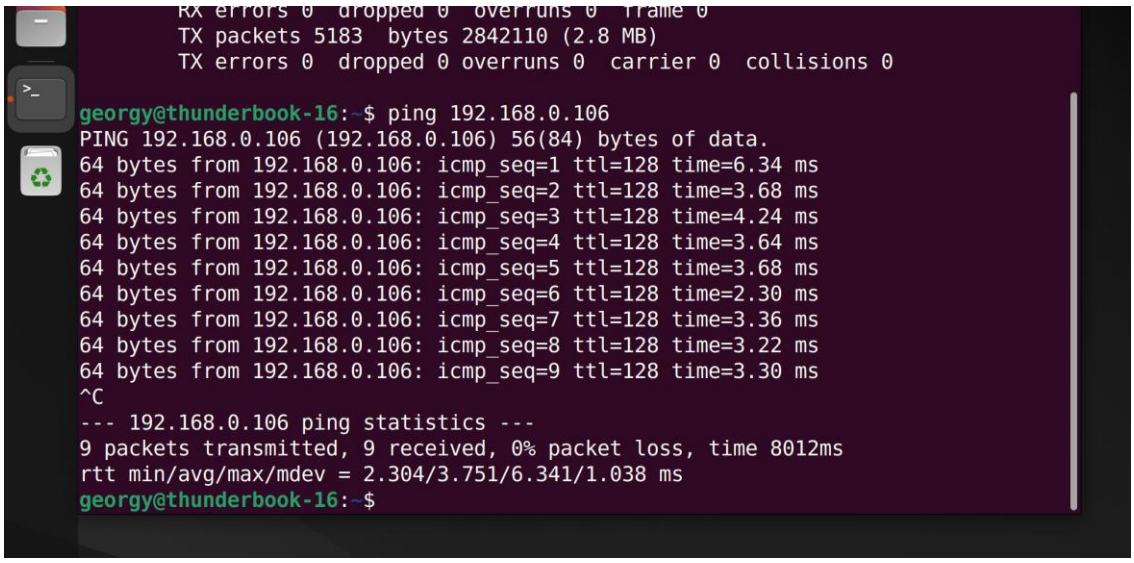


Рисунок 10 - Пинг ПК с ноутбука

Пинг прошел успешно. Смотрим какие данные перехватил Wireshark.

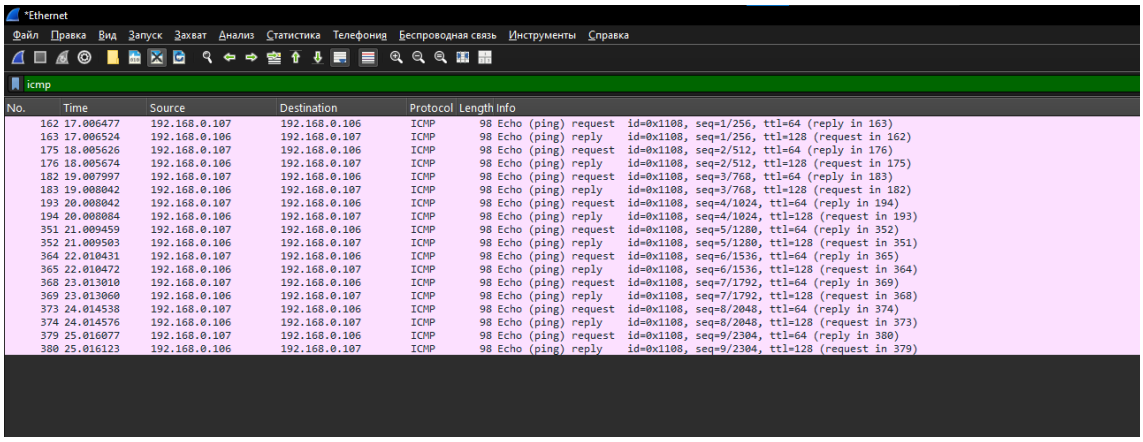


Рисунок 11 - Захват Wireshark

Видим чтоWireshark отследил все 9 пакетов.

Выберем первый ICMP запрос и посмотрим совпадают ли MAC-адреса источника и получателя с MAC-адресами наших устройств.

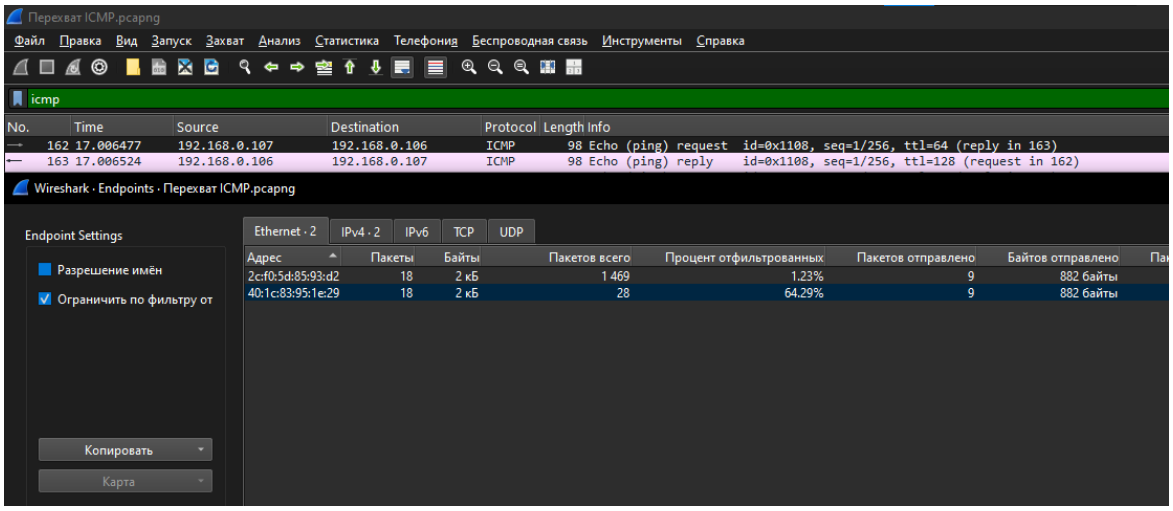


Рисунок 12 - Сравнение MAC-адресов

При сравнении с конфигурациями устройств выше можно заметить, что MAC-адреса совпали, что означает, что устройства успешно обменялись пакетами данных и нигде не произошло ошибки.

Как ПК определил MAC-адрес другого устройства при отправке ping?

ОС проверяет, есть ли MAC-адрес для IP 192.168.0.5 в **ARP-кэше**:

- Если **да** → сразу отправляется ICMP Echo Request.

- Если **нет** → ПК отправляет **ARP-запрос**: "Кто владелец IP-адреса 192.168.0.5? Ответьте мне, пожалуйста." Это широковещательный запрос на MAC-адрес ff:ff:ff:ff:ff:ff.
- Компьютер с IP 192.168.0.5 получает запрос и отправляет **ARP-ответ**: "Это я, мой MAC-адрес — XX:XX:XX:XX:XX:XX".
- После этого твой ноутбук записывает MAC-адрес в **ARP-кэш** и отправляет ICMP Echo Request напрямую на MAC-адрес целевого ПК.

Сбор и анализ данных ICMP.

Отправим эхо-запросы с помощью команды ping на 3 удаленных узла (расположенные за пределами локальной сети): сайты зарубежных СМИ.

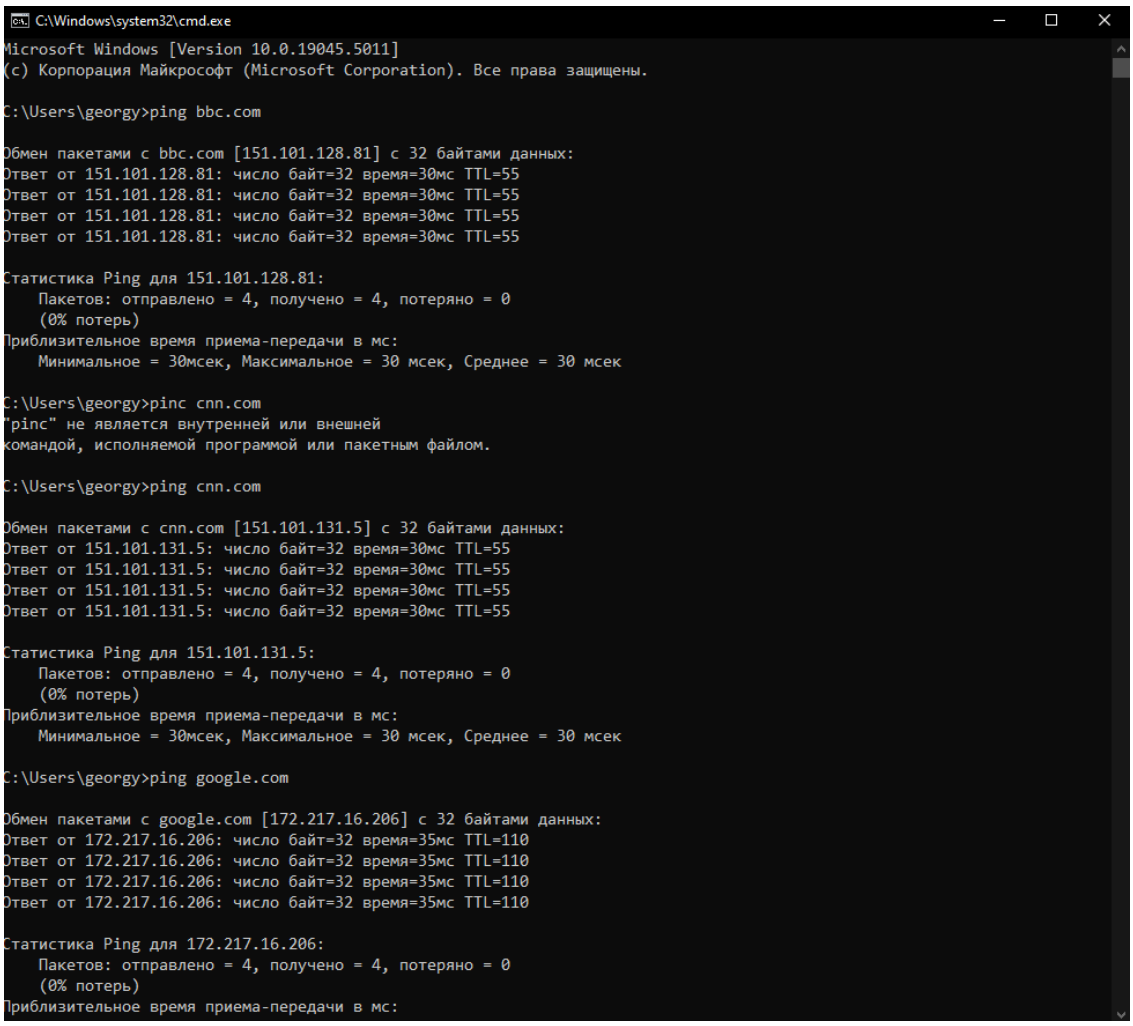


Рисунок 13- PING зарубежных СМИ

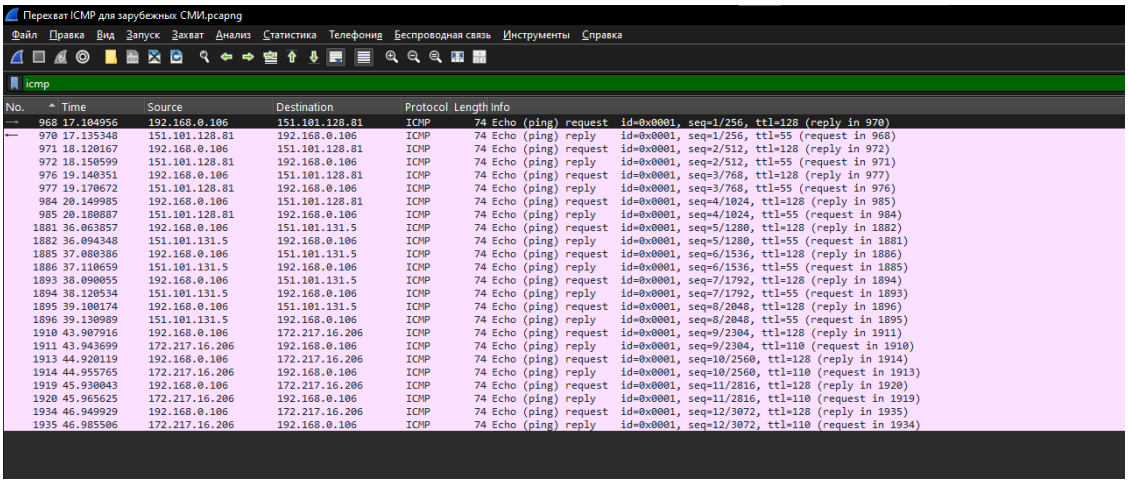


Рисунок 14 - Захват ICMP при помощи Wireshark

BBC.com – IP (151.101.128.81) MAC (Destination: TPLink_a6:b9:55 (9c:a2:f4:a6:b9:55))

CNN.com – IP (151.101.131.5) MAC (Destination: TPLink_a6:b9:55 (9c:a2:f4:a6:b9:55)

Google.com – IP (172.217.16.206) MAC (Destination: TPLink_a6:b9:55 (9c:a2:f4:a6:b9:55))

Почему Wireshark не показывает MAC удалённых узлов**?** Пакеты ICMP проходят через шлюз (роутер), который подменяет MAC-адрес назначения на свой. Реальный MAC сервера (например, BBC) недоступен в локальной сети.

3. Анализ полей TCP.

В качестве FTP-сервера, к которому будет произведено подключение, был выбран FTP – сервер CDC здравоохранения США. С адресом ftp.cdc.gov. Для того, чтобы узнать ip-адрес сервера, использовалась утилита nslookup.

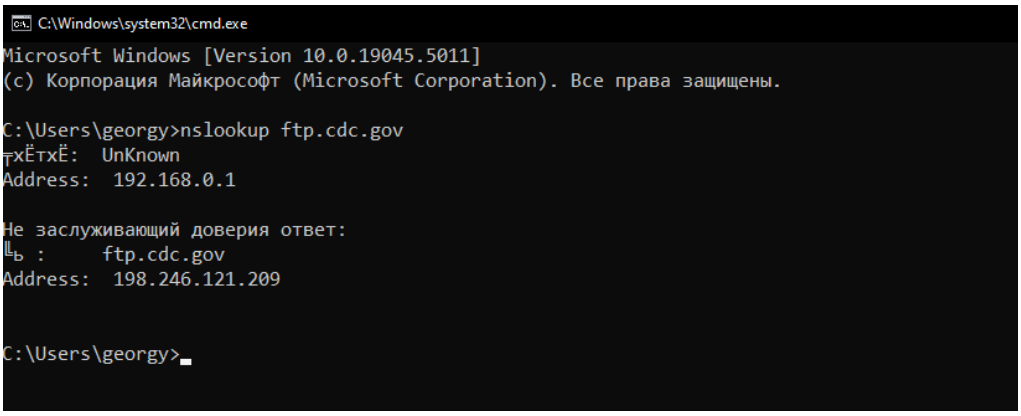


Рисунок 15 - Определение IP-адреса FTP-сервера

После того, как был получен IP-адрес FTP сайта – был запущен захват трафика в Wireshark, в течении этого захвата был совершён вход на сайт ftp.cdc.gov.

Фильтр: tcp and ip.addr == 198.246.121.209

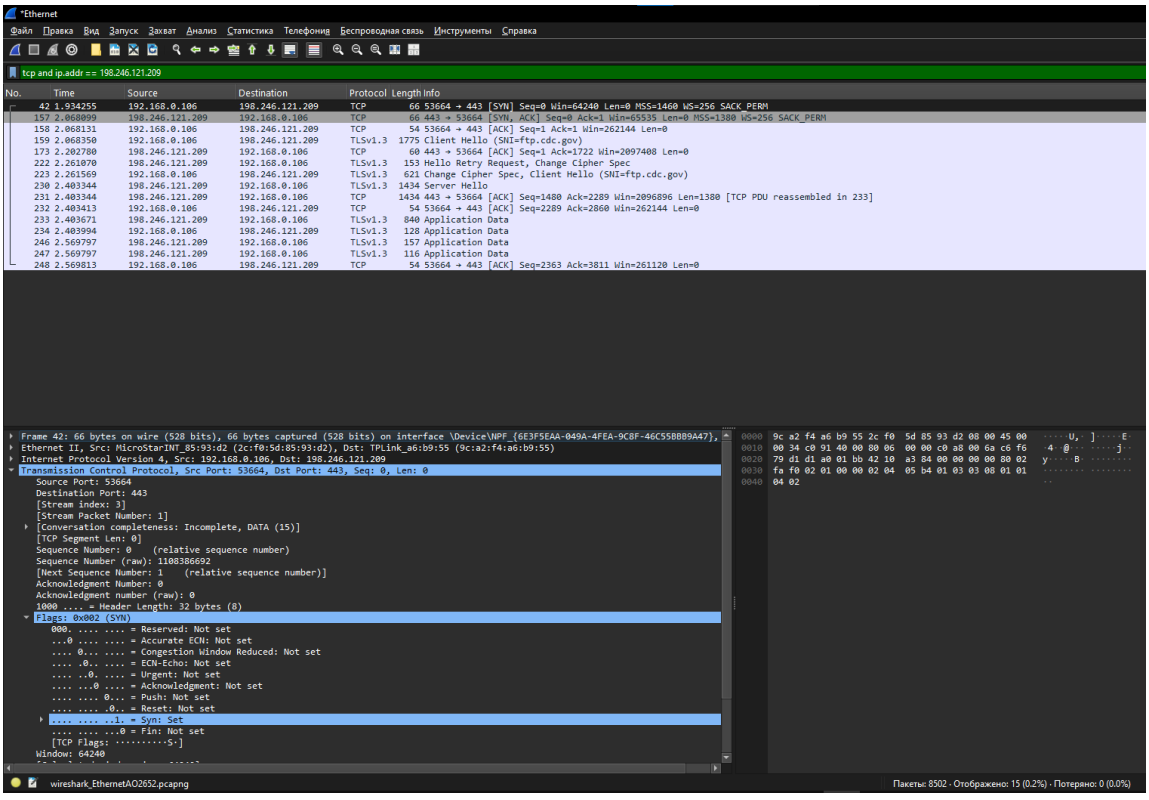


Рисунок 16 - Первый перехваченный TCP пакет

Название поля	Значение поля
IP-адрес источника	192.168.0.106
IP-адрес назначения	198.246.121.209

Номер порта источника	53664
Номер порта назначения	443
Порядковый номер	0
Номер подтверждения	0
Длина заголовка	32
Размер окна	64240

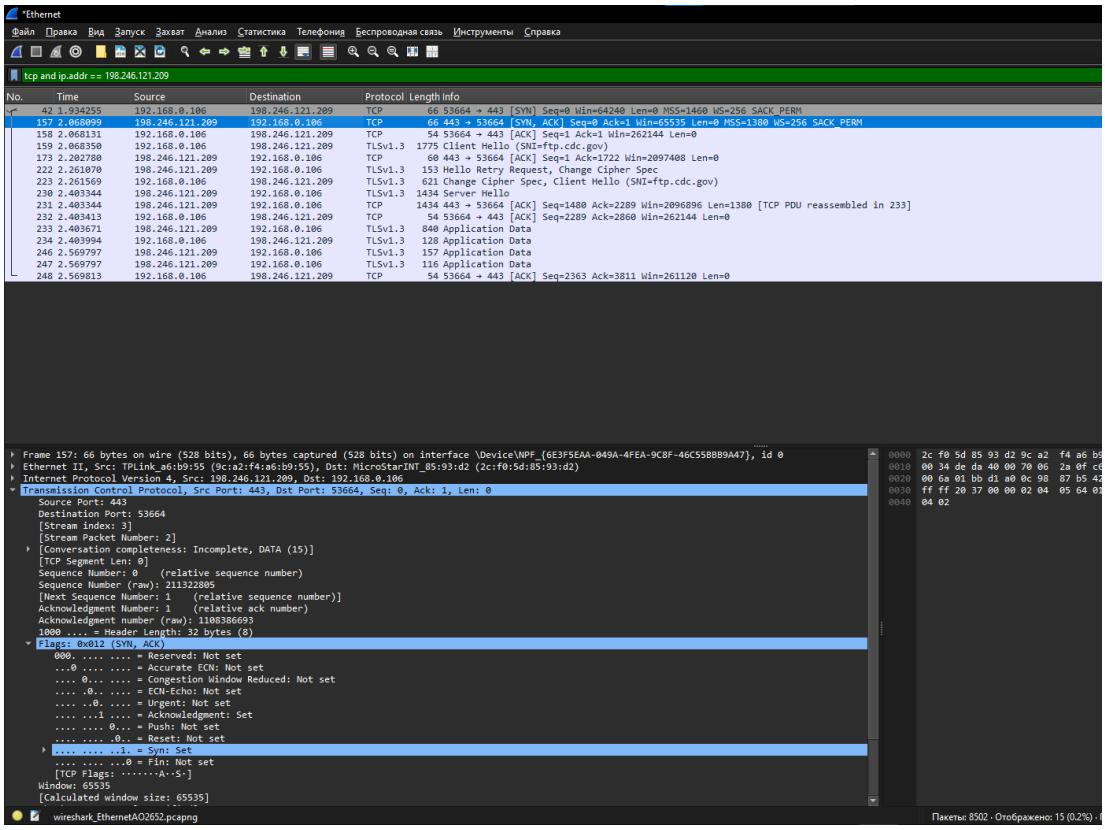


Рисунок 17 - Второй перехваченный TCP пакет

Название поля	Значение поля
IP-адрес источника	198.246.121.209
IP-адрес назначения	192.168.0.106
Номер порта источника	443
Номер порта назначения	53664
Порядковый номер	0
Номер подтверждения	1
Длина заголовка	32
Размер окна	65535

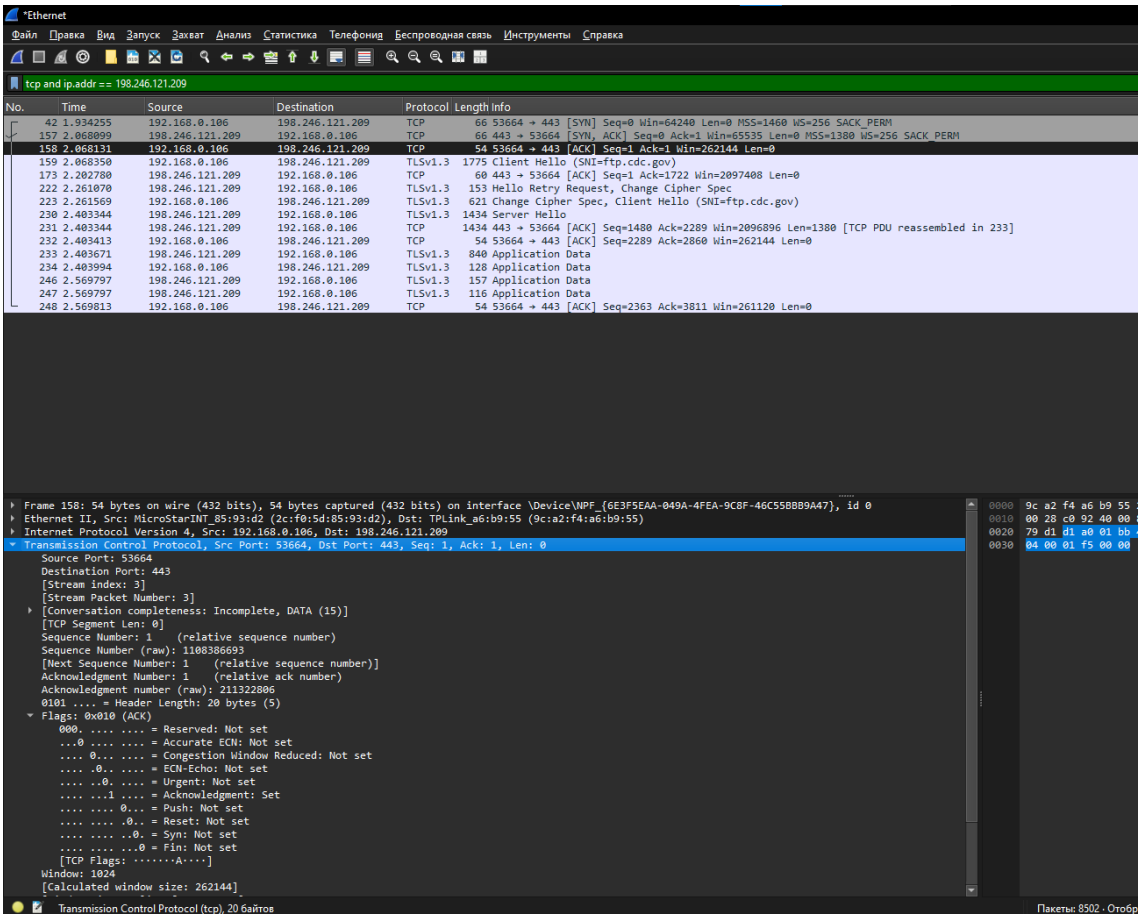


Рисунок 18 – Третий перехваченный TCP пакет

Название поля	Значение поля
IP-адрес источника	192.168.0.106
IP-адрес назначения	198.246.121.209
Номер порта источника	533664
Номер порта назначения	443
Порядковый номер	1
Номер подтверждения	1
Длина заголовка	20
Размер окна	1024

При помощи данного фильтра (**ftp and ip.addr == 198.246.121.209**) можем подробнее отследить и проанализировать FTP трафик.

Заключение

В ходе выполнения данной лабораторной работы были получены практические навыки работы с программой **Wireshark** — одним из самых мощных инструментов для анализа сетевого трафика. Особое внимание было уделено сбору, фильтрации и интерпретации данных, передаваемых по протоколам стека **TCP/IP**.

В процессе захвата трафика были изучены различные типы пакетов, включая TCP, UDP, ICMP, ARP и HTTPS. На практике был произведён анализ структуры пакетов, определены адреса источника и назначения на канальном и сетевом уровнях, а также были построены графики интенсивности сетевого взаимодействия. Кроме того, была отработана **навыковая часть фильтрации трафика**: написаны и протестированы фильтры для выделения широковещательных сообщений, протоколов HTTP, ICMP и других.