

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 ..... 3**

**Выполнение работы ..... 4**

**Заключение..... 16**

## **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.

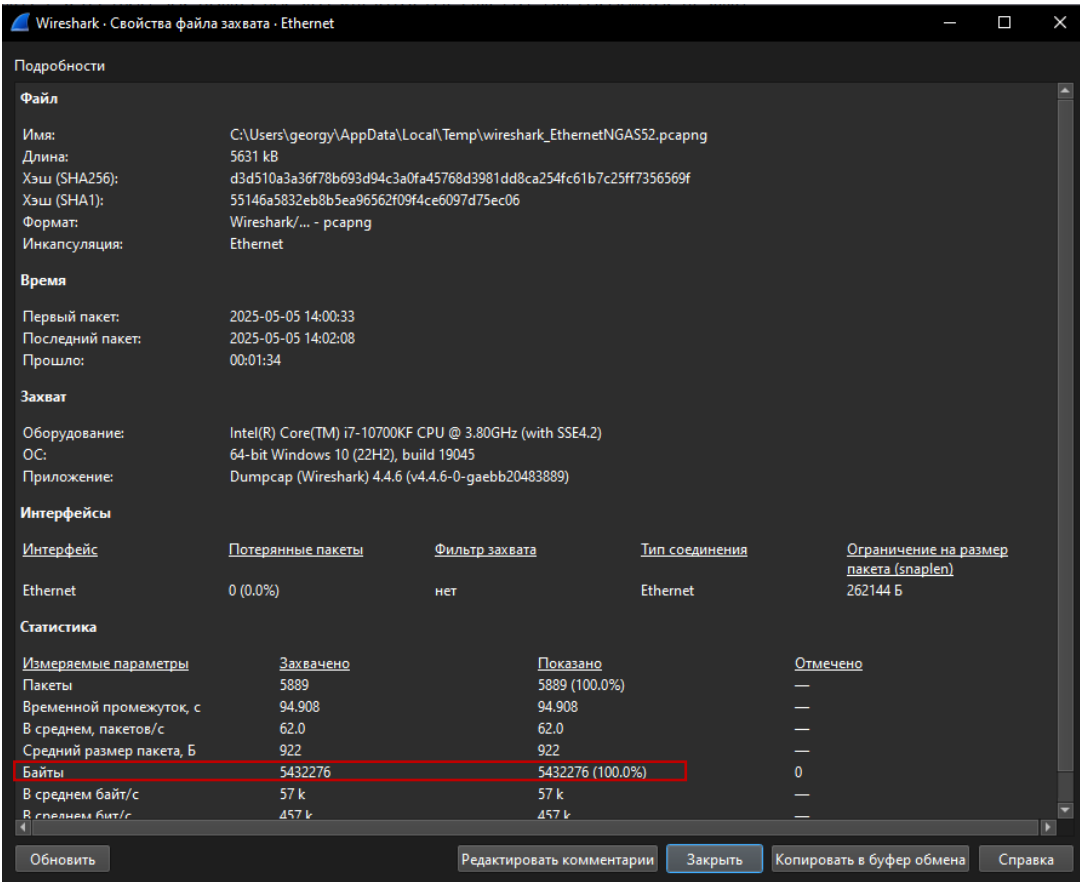
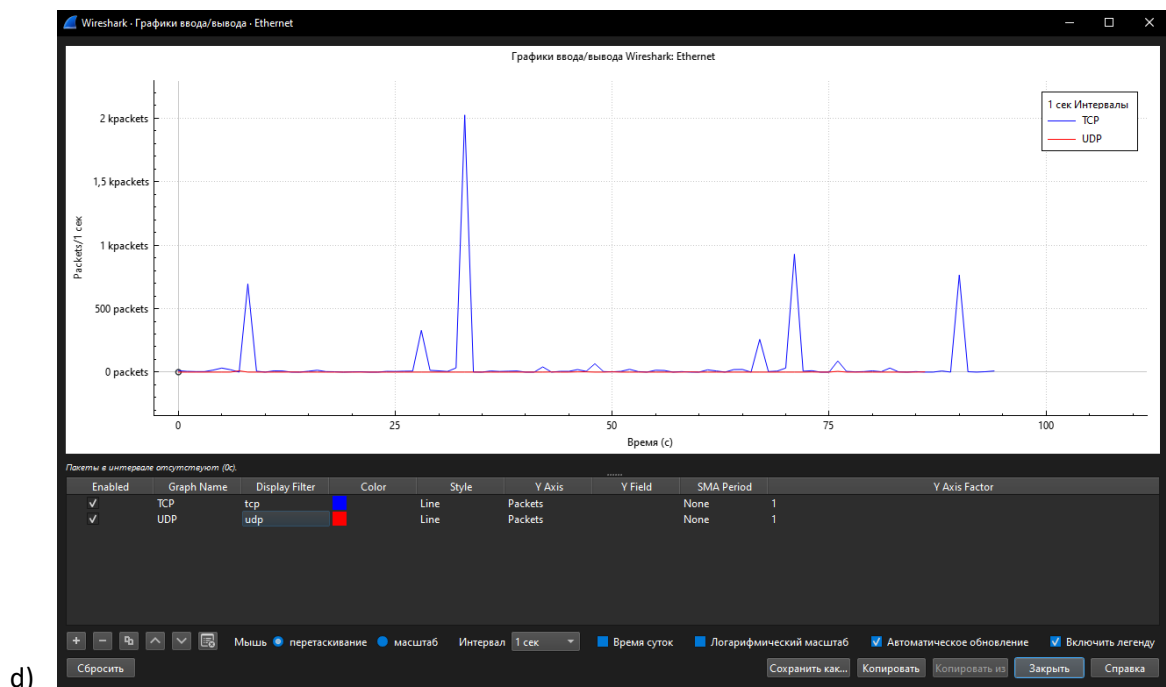


Рисунок 1 - Перехват 5 МБ трафика.

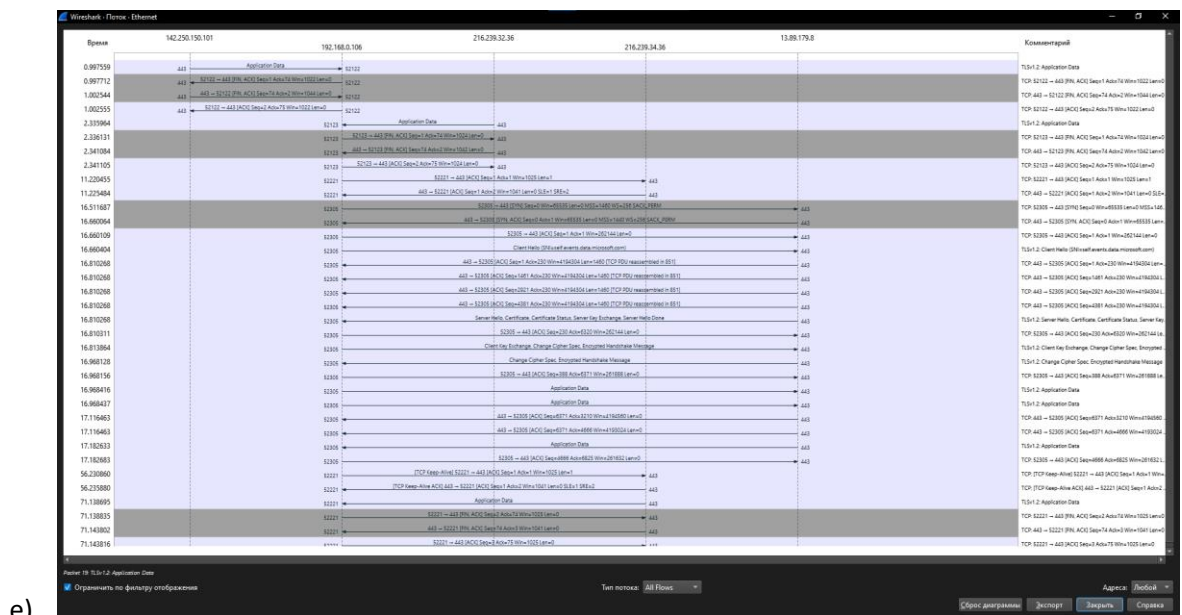
Далее ,используя инструменты статистики, определяем:

- а) Узел с максимальной активностью (по объему переданных данных) – 192.168.0.106 (мой ПК)
- б) Узел, осуществивший наибольшее кол-во широковещательных рассылок - TPLink\_a6:b9:55 (мой роутер)
- с) 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	
а6: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

е) 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.

## 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: 1

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

Рисунок 7 - Создание правила

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

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.5011]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\georgy>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : HOME-PC
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek PCIe 2.5GbE Family Controller
Физический адрес. . . . . : 2C-F0-5D-85-93-D2
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::43ca:174:fca6:502%9(Основной)
IPv4-адрес. . . . . : 192.168.0.106(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 6 мая 2025 г. 13:27:00
Срок аренды истекает. . . . . : 6 мая 2025 г. 22:26:59
Основной шлюз. . . . . : 192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 103608413
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2E-A9-00-8D-2C-F0-5D-85-93-D2
DNS-серверы. . . . . : 192.168.0.1
```

Рисунок 8 - Сетевые параметры ПК



```
georgy@thunderbook-16:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Локальная петля (Loopback))
    RX packets 358 bytes 32763 (32.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 358 bytes 32763 (32.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.107 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::3638:991c:b2a2:17d2 prefixlen 64 scopeid 0x20<link>
    ether 40:1c:83:95:1e:29 txqueuelen 1000 (Ethernet)
    RX packets 8900 bytes 9111987 (9.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4171 bytes 1824410 (1.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

georgy@thunderbook-16:~$
```

Рисунок 9 - Сетевые параметры ноутбука

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

```
georgy@thunderbook-16:~$ ping 192.168.0.106
PING 192.168.0.106 (192.168.0.106) 56(84) bytes of data.
64 bytes from 192.168.0.106: icmp_seq=1 ttl=128 time=6.34 ms
64 bytes from 192.168.0.106: icmp_seq=2 ttl=128 time=3.68 ms
64 bytes from 192.168.0.106: icmp_seq=3 ttl=128 time=4.24 ms
64 bytes from 192.168.0.106: icmp_seq=4 ttl=128 time=3.64 ms
64 bytes from 192.168.0.106: icmp_seq=5 ttl=128 time=3.68 ms
64 bytes from 192.168.0.106: icmp_seq=6 ttl=128 time=2.30 ms
64 bytes from 192.168.0.106: icmp_seq=7 ttl=128 time=3.36 ms
64 bytes from 192.168.0.106: icmp_seq=8 ttl=128 time=3.22 ms
64 bytes from 192.168.0.106: icmp_seq=9 ttl=128 time=3.30 ms
^C
--- 192.168.0.106 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 2.304/3.751/6.341/1.038 ms
georgy@thunderbook-16:~$
```

Рисунок 10 - Пинг ПК с ноутбука

Пинг прошел успешно. Смотрим какие данные перехватил Wireshark.

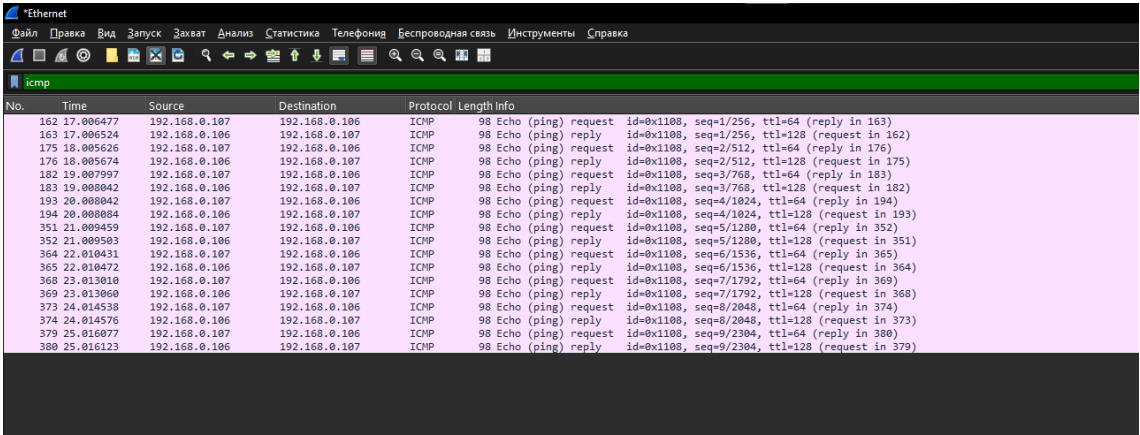


Рисунок 11 - Захват Wireshark

Видим чтоWireshark отследил все 9 пакетов.

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

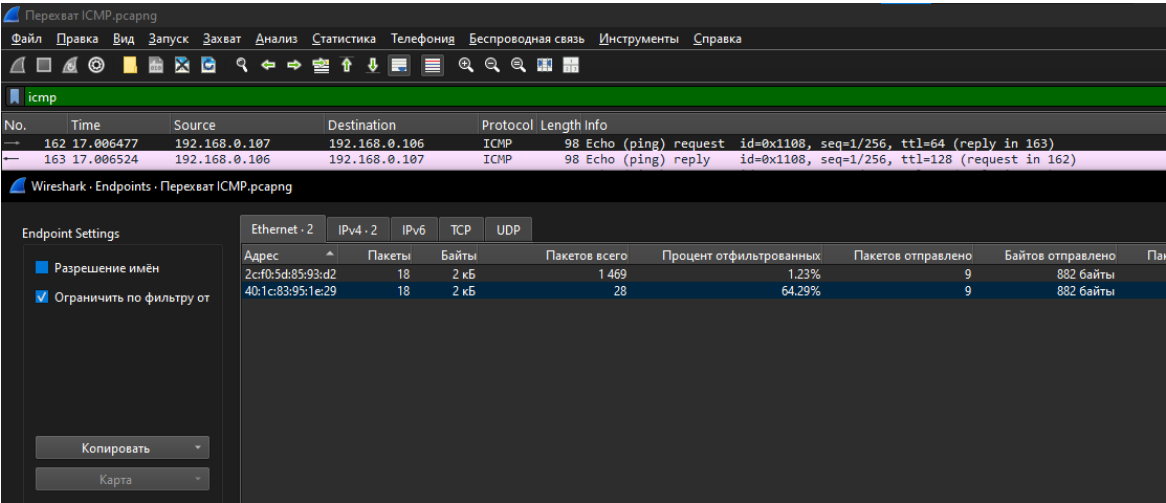


Рисунок 12 - Сравнение MAC-адресов

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.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.5011]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\georgy>ping bbc.com

Обмен пакетами с bbc.com [151.101.128.81] с 32 байтами данных:
Ответ от 151.101.128.81: число байт=32 время=30мс TTL=55
Ответ от 151.101.128.81: число байт=32 время=30мс TTL=55
Ответ от 151.101.128.81: число байт=32 время=30мс TTL=55
Ответ от 151.101.128.81: число байт=32 время=30мс TTL=55

Статистика Ping для 151.101.128.81:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 30мсек, Максимальное = 30 мсек, Среднее = 30 мсек

C:\Users\georgy>ping cnn.com
"ping" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\Users\georgy>ping cnn.com

Обмен пакетами с cnn.com [151.101.131.5] с 32 байтами данных:
Ответ от 151.101.131.5: число байт=32 время=30мс TTL=55
Ответ от 151.101.131.5: число байт=32 время=30мс TTL=55
Ответ от 151.101.131.5: число байт=32 время=30мс TTL=55
Ответ от 151.101.131.5: число байт=32 время=30мс TTL=55

Статистика Ping для 151.101.131.5:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 30мсек, Максимальное = 30 мсек, Среднее = 30 мсек

C:\Users\georgy>ping google.com

Обмен пакетами с google.com [172.217.16.206] с 32 байтами данных:
Ответ от 172.217.16.206: число байт=32 время=35мс TTL=110
Ответ от 172.217.16.206: число байт=32 время=35мс TTL=110
Ответ от 172.217.16.206: число байт=32 время=35мс TTL=110
Ответ от 172.217.16.206: число байт=32 время=35мс TTL=110

Статистика Ping для 172.217.16.206:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:

```

Рисунок 13- PING зарубежных СМИ

No.	Time	Source	Destination	Protocol	Length	Info
968	17.104956	192.168.0.106	151.101.128.81	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 970)
970	17.135348	151.101.128.81	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=55 (request in 968)
971	18.120167	192.168.0.106	151.101.128.81	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 972)
972	18.150599	151.101.128.81	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=55 (request in 971)
976	19.140351	192.168.0.106	151.101.128.81	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 977)
977	19.170672	151.101.128.81	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=55 (request in 976)
984	20.149985	192.168.0.106	151.101.128.81	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 985)
985	20.180887	151.101.128.81	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=55 (request in 984)
1881	36.063057	192.168.0.106	151.101.131.5	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1882)
1882	36.094348	151.101.131.5	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=55 (request in 1881)
1885	37.080386	192.168.0.106	151.101.131.5	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1886)
1886	37.110659	151.101.131.5	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=55 (request in 1885)
1893	38.090055	192.168.0.106	151.101.131.5	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 1894)
1894	38.120534	151.101.131.5	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=55 (request in 1893)
1895	39.100174	192.168.0.106	151.101.131.5	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1896)
1896	39.130989	151.101.131.5	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=55 (request in 1895)
1910	43.907916	192.168.0.106	172.217.16.206	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 1911)
1911	43.943699	172.217.16.206	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=110 (request in 1910)
1913	44.920119	192.168.0.106	172.217.16.206	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 1914)
1914	44.955765	172.217.16.206	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=110 (request in 1913)
1919	45.930043	192.168.0.106	172.217.16.206	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 1920)
1920	45.965625	172.217.16.206	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=110 (request in 1919)
1934	46.949929	192.168.0.106	172.217.16.206	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 1935)
1935	46.985506	172.217.16.206	192.168.0.106	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=110 (request in 1934)

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](http://ftp.cdc.gov). Для того, чтобы узнать ip-адрес сервера, использовалась утилита nslookup.

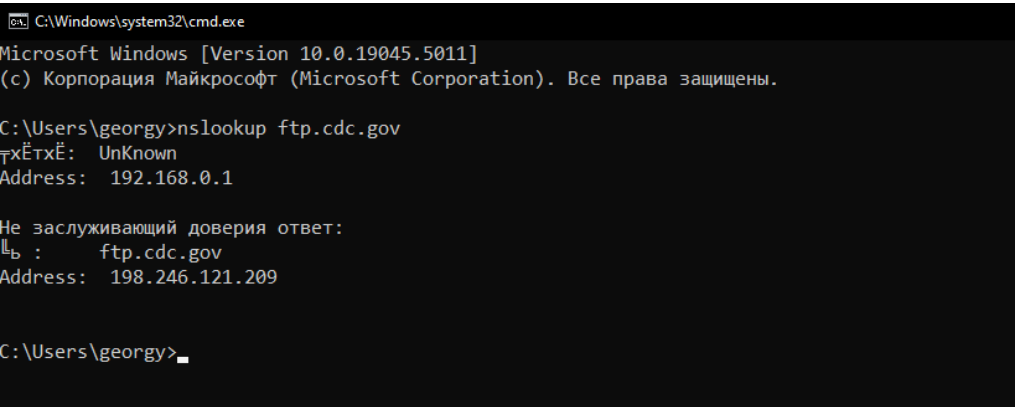


Рисунок 15 - Определение IP-адреса FTP-сервера

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](http://ftp.cdc.gov).

**Фильтр: tcp and ip.addr == 198.246.121.209**

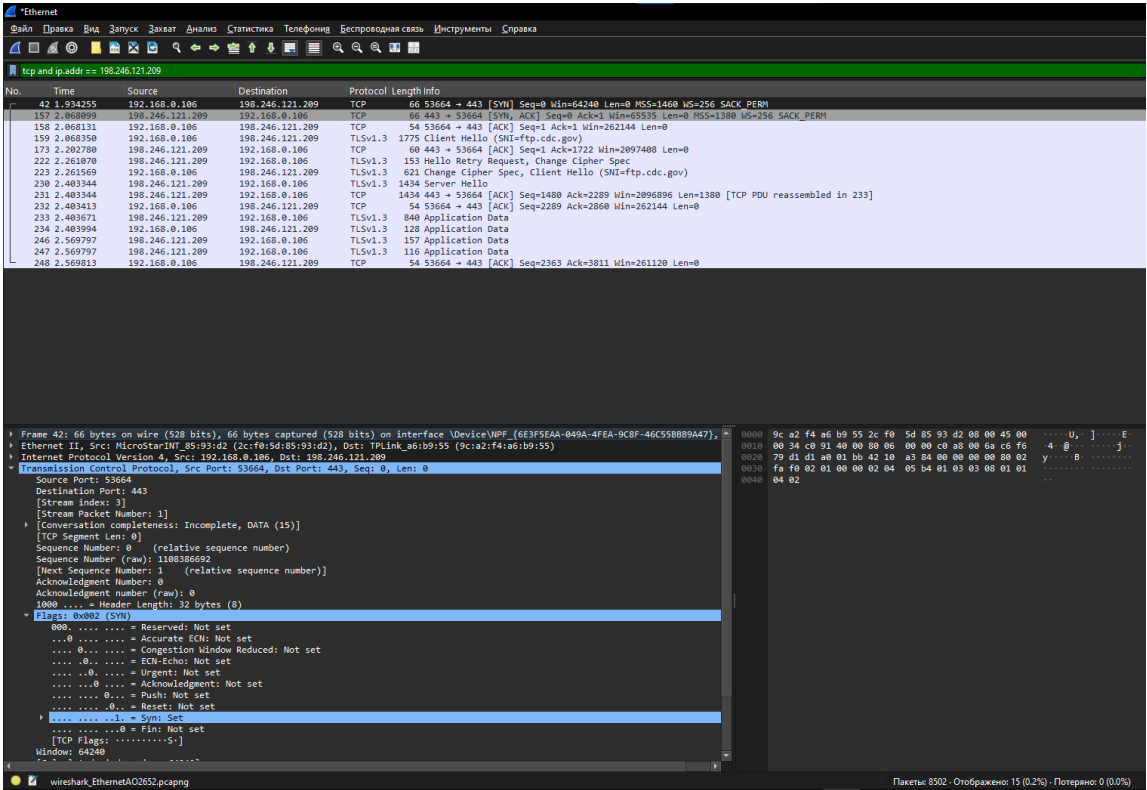


Рисунок 16 - Первый перехваченный TCP пакет

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

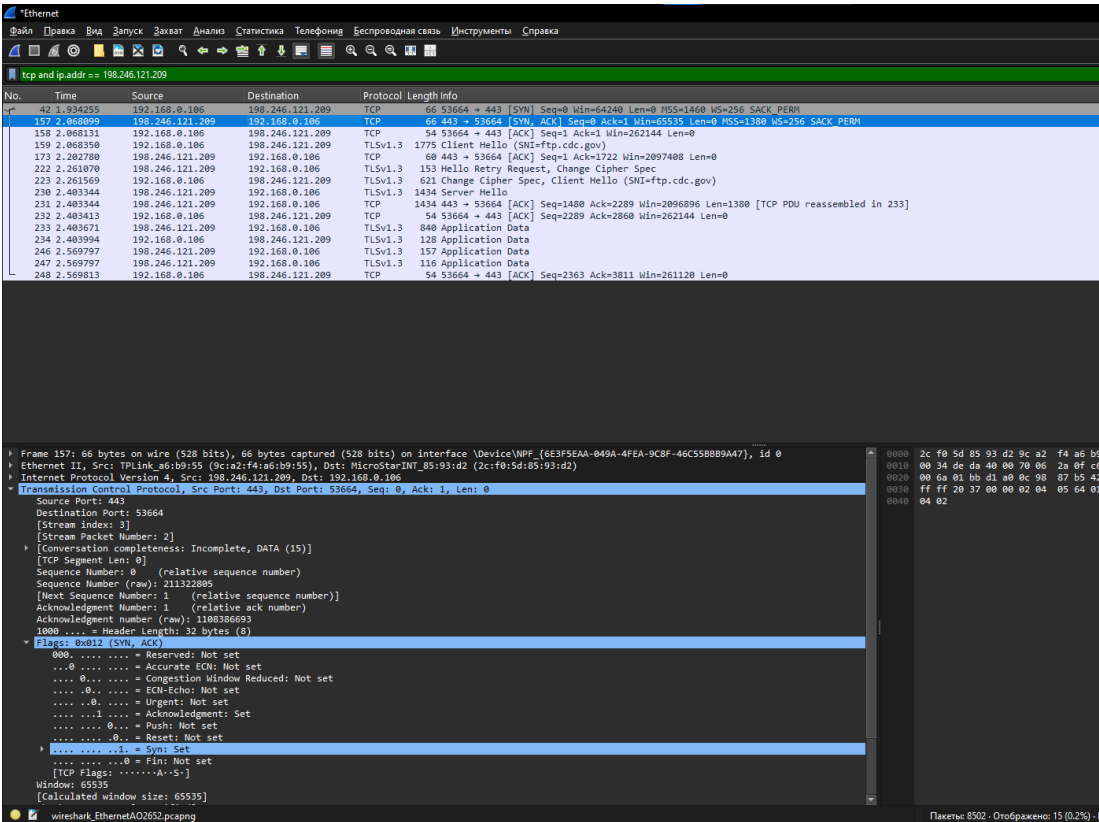


Рисунок 17 - Второй перехваченный TCP пакет

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



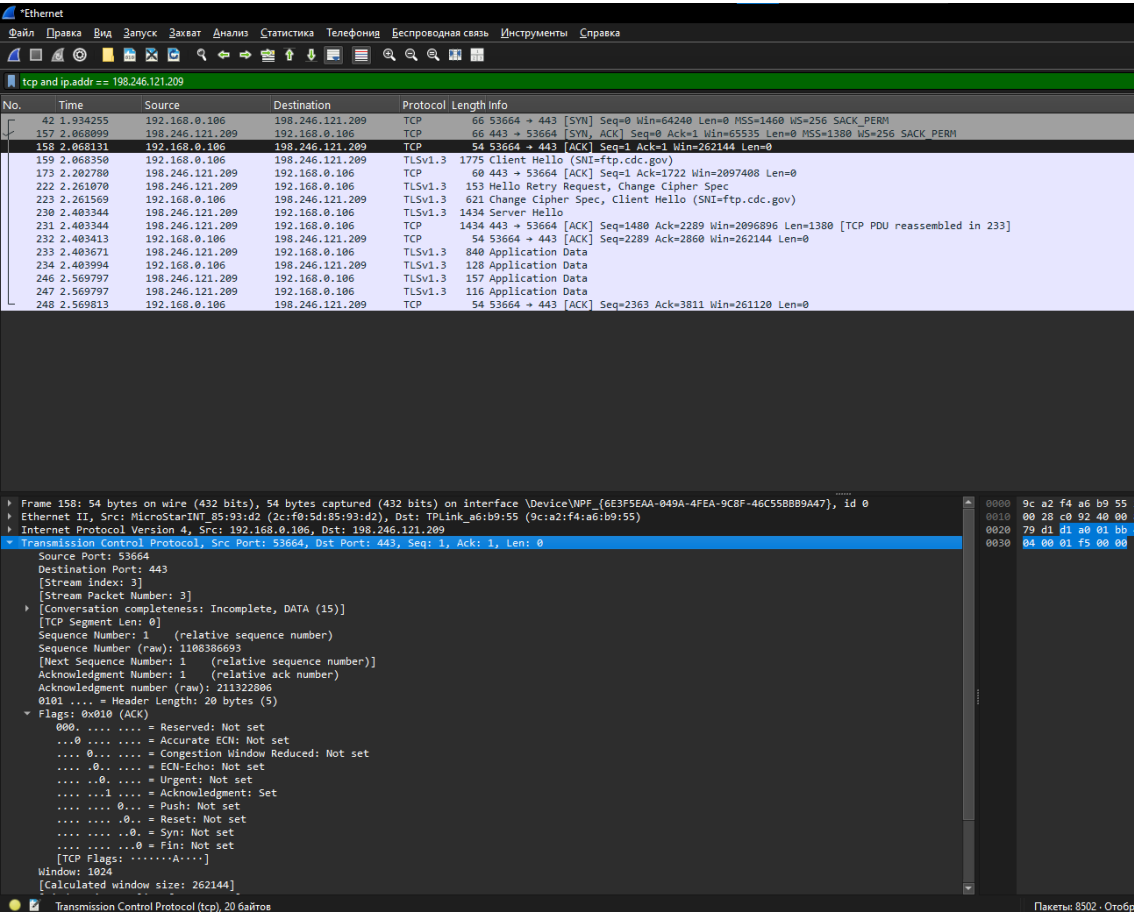


Рисунок 18 – Третий перехваченный TCP пакет

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.