

Лабораторная работа № 3.

Анализ трафика в Wireshark

Диана Алексеевна Садова

Содержание

1	Цель работы	5
2	MAC-адресация	6
2.1	Постановка задачи	6
2.2	Порядок выполнения работы	6
3	Анализ кадров канального уровня в Wireshark	11
3.1	Постановка задачи	11
3.2	Порядок выполнения работы	11
4	Анализ протоколов транспортного уровня в Wireshark	19
4.1	Постановка задачи	19
4.2	Порядок выполнения работы	19
5	Анализ handshake протокола TCP в Wireshark	24
5.1	Постановка задачи	24
5.2	Порядок выполнения работы	24
6	Выводы	27
	Список литературы	28

Список иллюстраций

2.1	Обычная команда <code>ipconfig</code>	7
2.2	Команда <code>ipconfig /all</code>	8
2.3	Команда <code>ipconfig /all</code>	8
2.4	Команда <code>ipconfig /renew</code>	9
2.5	MAC-адрес локальной сети *3	9
2.6	MAC-адрес беспроводной сети	10
3.1	Wireshark	12
3.2	IP-адрес и шлюз	12
3.3	пропингуем шлюз	13
3.4	Фильтр <code>arp or icmp</code>	13
3.5	пакеты что сгенерированы с помощью команды <code>ping</code>	13
3.6	ICMP — эхо-запрос	14
3.7	ICMP — эхо-ответ	15
3.8	Ethernet II	15
3.9	Пропингуем <code>rudn.ru</code>	16
3.10	Запросы и ответы	16
3.11	эхо-запрос	17
3.12	эхо-ответ	17
4.1	Сайт <code>http://info.cern.ch/</code>	20
4.2	Наш фильтр	20
4.3	Информация	20
4.4	эхо-запрос и эхо-ответ	21
4.5	Информация	21
4.6	эхо-запрос	22
4.7	эхо-ответ	23
5.1	Запускаем фильтр с протоколом TCP	25
5.2	График порта 80	25

Список таблиц

1 Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

2 МАС-адресация

2.1 Постановка задачи

1. Изучение возможностей команды `ipconfig` для ОС типа Windows (`ifconfig` для систем типа Linux).
2. Определение МАС-адреса устройства и его типа.

2.2 Порядок выполнения работы

1. С помощью команды `ipconfig` для ОС типа Windows или `ifconfig` для систем типа Linux выведите информацию о текущем сетевом соединении. Используйте разные опции команды. В отчёте поясните детально полученную в каждом случае при выводе информацию. Подтвердите свой ответ скриншотами.(рис. 2.1),(рис. 2.2),(рис. 2.3),(рис. 2.4)

```
C:\Users\sadov>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . : fe80::e359:e4be:f94b:c9be%16
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 4:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : IGD_MGTS
    Локальный IPv6-адрес канала . . . : fe80::235a:977:fac4:d579%7
    IPv4-адрес. . . . . : 192.168.1.23
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.1.1

C:\Users\sadov>
```

Рис. 2.1: Обычная команда ipconfig

Обычная команда ipconfig - выдает базовую информацию о текущем сетевом соединении

```

C:\Users\sadov>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 . : IGD_MGTS

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес. . . . . : 0A-00-27-00-00-10
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e359:e4be:f94b:c9be%16(Основной)
IPv4-адрес. . . . . : 192.168.56.1(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 705298471
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2D-61-87-85-70-A8-D3-DB-DB-16
NetBios через TCP/IP. . . . . : Включен

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. . . . . : 70-A8-D3-DB-DB-17
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. . . . . : 72-A8-D3-DB-DB-16
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

```

Рис. 2.2: Команда ipconfig /all

```

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : IGD_MGTS
Описание. . . . . : Killer(R) Wi-Fi 6E AX1675s 160MHz Wireless Network Adapter (211D2W)
Физический адрес. . . . . : 70-A8-D3-DB-DB-16
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::235a:977:fac4:d579%7(Основной)
IPv4-адрес. . . . . : 192.168.1.23(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 5 октября 2025 г. 9:47:25
Срок аренды истекает. . . . . : 6 октября 2025 г. 18:08:48
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 108046547
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2D-61-87-85-70-A8-D3-DB-DB-16
DNS-серверы. . . . . : fe80::5af8:5cff:fe6a:c2b1%7
                       192.168.1.1
NetBios через TCP/IP. . . . . : Включен

C:\Users\sadov>

```

Рис. 2.3: Команда ipconfig /all

Команда ipconfig /all - выдает более полную (расширенную) информацию о те-

кущем сетевом соединении

```
C:\Users\sadov>ipconfig /renew

Настройка протокола IP для Windows

Невозможно выполнять операции над Подключение по локальной сети* 3, пока отключена сеть.
Невозможно выполнять операции над Подключение по локальной сети* 4, пока отключена сеть.

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . : fe80::e359:e4be:f94b:c9be%16
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 4:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : IGD_MGTS
    Локальный IPv6-адрес канала . . . : fe80::235a:977:fac4:d579%7
    IPv4-адрес. . . . . : 192.168.1.23
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.1.1

C:\Users\sadov>
```

Рис. 2.4: Команда ipconfig /renew

Команда ipconfig /renew - обновляет IP текущего сетевого соединении

2. Определите MAC-адреса сетевых интерфейсов на вашем компьютере. Подтвердите свой ответ скриншотом.(рис. 2.5),(рис. 2.6)

```
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. . . . . : 70-A8-D3-DB-DB-17
    DHCP включен. . . . . : Да
    Автонастройка включена. . . . . : Да
```

Рис. 2.5: MAC-адрес локальной сети *3

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : IGD_MGTS
Описание. . . . . : Killer(R) Wi-Fi 6E AX1675s 160MHz Wireless Network Adapter (211D2W)
Физический адрес. . . . . : 70-A8-D3-DB-DB-16
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::235a:977:fac4:d579%7(Основной)
IPv4-адрес. . . . . : 192.168.1.23(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 5 октября 2025 г. 9:47:25
Срок аренды истекает. . . . . : 6 октября 2025 г. 18:08:48
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 108046547
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2D-61-87-85-70-A8-D3-DB-DB-16
DNS-серверы. . . . . : fe80::5af8:5cff:fe6a:c2b1%7
                        192.168.1.1
NetBios через TCP/IP. . . . . : Включен
```

Рис. 2.6: MAC-адрес беспроводной сети

3. Опишите структуру MAC-адресов вашего устройства. Какая часть адреса идентифицирует производителя? Какая часть адреса идентифицирует сетевой интерфейс? Определите, каким является адрес — индивидуальным или групповым, глобально администрируемым или локально администрируемым. Поясните свой ответ. Используйте шестнадцатеричную запись MAC-адреса для пояснения.

Адрес 70:A8:D3:DB:DB:17 является индивидуальным (Unicast) и глобально администрируемым (UAA)

3 Анализ кадров канального уровня в Wireshark

3.1 Постановка задачи

1. Установить на домашнем устройстве Wireshark.
2. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня.

3.2 Порядок выполнения работы

1. Установите на вашем устройстве Wireshark.
2. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.(рис. 3.1)

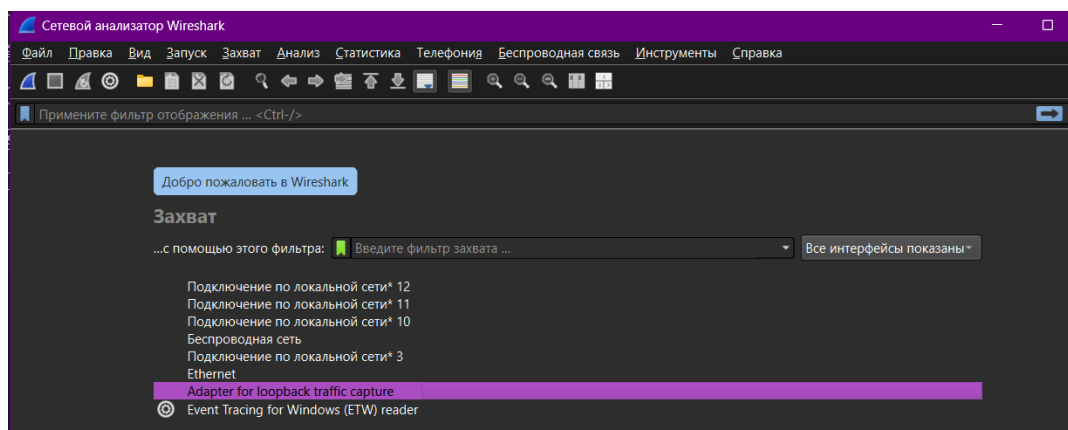


Рис. 3.1: Wireshark

3. На вашем устройстве в консоли определите с помощью команды `ipconfig` для ОС типа Windows или `ifconfig` для систем типа Linux IP-адрес вашего устройства и шлюз по умолчанию (default gateway).(рис. 3.2)

```
IPv4-адрес. . . . . : 192.168.1.23(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 5 октября 2025 г. 9:47:25
Срок аренды истекает. . . . . : 6 октября 2025 г. 18:08:48
Основной шлюз. . . . . : 192.168.1.1
```

Рис. 3.2: IP-адрес и шлюз

4. На вашем устройстве в консоли с помощью команды `ping` адрес_шлюза пропингуйте шлюз по умолчанию. Для остановки процесса используйте комбинацию клавиш `Ctrl + c` или изначально при помощи параметров команды `ping` задайте число сообщений эхо-запроса.(рис. 3.3)

```

C:\Users\sadov>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек

C:\Users\sadov>

```

Рис. 3.3: пропингуем шлюз

- В Wireshark остановите захват трафика. В строке фильтра пропишите фильтр `arp or icmp`. Убедитесь, что в списке пакетов отобразятся только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды `ping`, отправленной с вашего устройства на шлюз по умолчанию. (рис. 3.4), (рис. 3.5)

arp or icmp					
No.	Time	Source	Destination	Protocol	Length Info
73	10.588234	LLCProizvods_6a:c2:...	Broadcast	ARP	60 Who has 192.168.1.10? Tell 192.168.1.1
74	10.588234	LLCProizvods_6a:c2:...	Broadcast	ARP	60 Who has 192.168.1.17? Tell 192.168.1.1
75	10.588234	LLCProizvods_6a:c2:...	Broadcast	ARP	60 Who has 192.168.1.11? Tell 192.168.1.1
76	10.588234	LLCProizvods_6a:c2:...	Broadcast	ARP	60 Who has 192.168.1.23? Tell 192.168.1.1
77	10.588294	Intel_db:db:16	LLCProizvods_6a:c2:...	ARP	42 192.168.1.23 is at 70:a8:d3:db:db:16

Рис. 3.4: Фильтр `arp or icmp`

870	163.069390	192.168.1.23	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=21/5376, ttl=128 (reply in 871)
871	163.071051	192.168.1.1	192.168.1.23	ICMP	78 Echo (ping) reply	id=0x0001, seq=21/5376, ttl=64 (request in 870)
873	164.085605	192.168.1.23	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=22/5632, ttl=128 (reply in 874)
874	164.087340	192.168.1.1	192.168.1.23	ICMP	78 Echo (ping) reply	id=0x0001, seq=22/5632, ttl=64 (request in 873)
875	165.099545	192.168.1.23	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=23/5888, ttl=128 (reply in 876)
876	165.101291	192.168.1.1	192.168.1.23	ICMP	78 Echo (ping) reply	id=0x0001, seq=23/5888, ttl=64 (request in 875)

Рис. 3.5: пакеты что сгенерированы с помощью команды `ping`

- Изучите эхо-запрос и эхо-ответ ICMP в программе Wireshark:
 - На панели списка пакетов (верхний раздел) выберите первый указанный кадр ICMP — эхо-запрос. Изучите информацию на панели сведений о па-

кете в средней части экрана. В отчёте укажите длину кадра, к какому типу Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.(рис. 3.6)

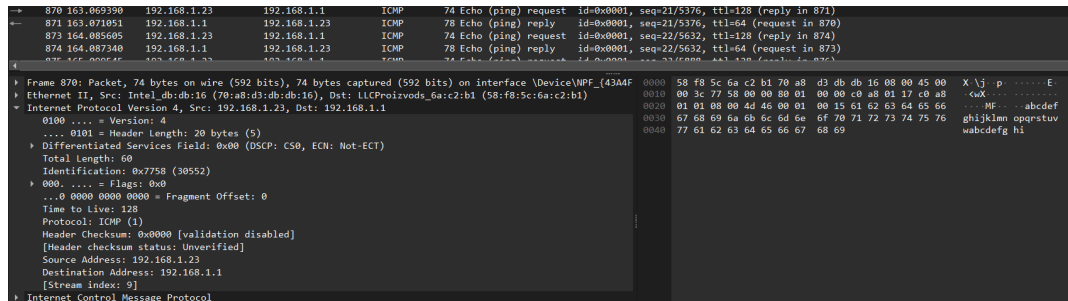


Рис. 3.6: ICMP — эхо-запрос

Длина кадра (Frame Length) - 74 байта

Типу Ethernet - Ethernet II

MAC-адреса источника - 70:a8:d3:db:db:16

Шлюз (Destination): MAC-адрес маршрутизатора (шлюза) с IP 192.168.1.1. Фактический MAC-адрес шлюза нужно посмотреть в захвате трафика Wireshark в поле “Destination” раздела “Ethernet II”. Например, это может быть адрес вида a4:b3:c2:d1:e0:f9.

Тип MAC-адресов:

- MAC-адрес источника (70:a8:d3:db:db:16): Индивидуальный (Unicast): Младший бит первого байта (70 = 01110000) равен 0. Глобально администрируемый (UAA): Второй младший бит первого байта равен 0.
- MAC-адрес назначения (шлюза a4:b3:c2:d1:e0:f9): Индивидуальный (Unicast): Младший бит первого байта (a4 = 10100100) равен 0. Глобально администрируемый (UAA): Второй младший бит первого байта равен 0.
- На панели списка пакетов (верхний раздел) выберите второй указанный кадр ICMP — эхо-ответ. Изучите информацию на панели сведений о пакете в средней части экрана. В отчёте укажите длину кадра, к какому ти-

пу Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.(рис. 3.7)

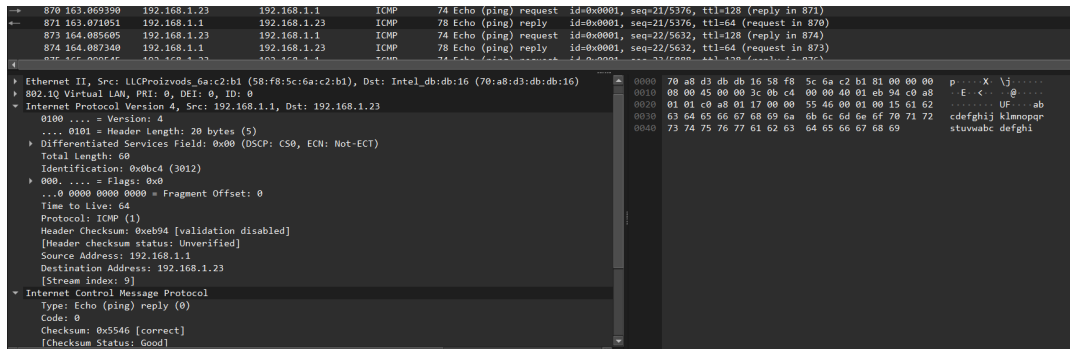


Рис. 3.7: ICMP — эхо-ответ

Длина кадра - 78 байт

Тип Ethernet - Ethernet II

MAC источника - 58:48:5c:6a:c2:b1

MAC назначения - 70:a8:d3:db:db:16

Тип адресов - Оба индивидуальные (Unicast) и глобальные (UAA)

7. Изучите кадры данных протокола ARP. Изучите данные в полях заголовка Ethernet II.(рис. 3.8)

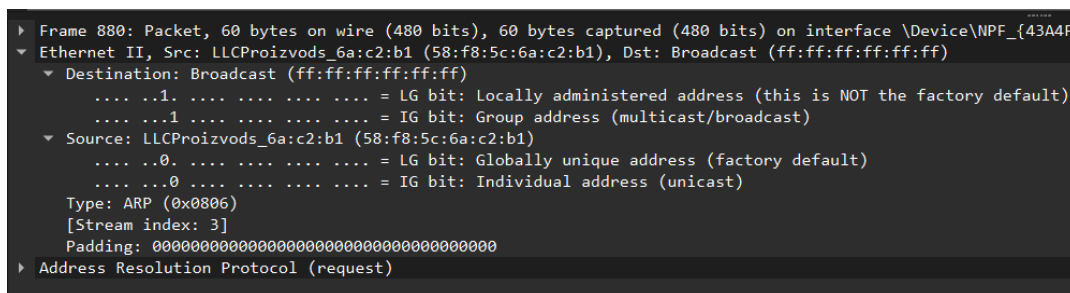


Рис. 3.8: Ethernet II

Длина кадра (Frame Length) - 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Типу Ethernet - Ethernet II

Broadcast ff:ff:ff:ff:ff:ff - Широковещательный адрес - кадр предназначен ВСЕМ устройствам в локальной сети

Source: LICProizvods_6a:c2:b1 (58:f8:5c:6a:c2:b1)

MAC-адрес источника: 58:f8:5c:6a:c2:b1

Производитель: OUI 58:f8:5c соответствует производителю LICProizvods

Type: ARP (0x0806)

Stream index: 3 - Индекс потока для отслеживания связанных пакетов

8. Начните новый процесс захвата трафика в Wireshark. На вашем устройстве в консоли пропингуйте по имени какой-нибудь известный вам адрес, например ping rudn.ru.(рис. 3.9)

```
C:\Users\sadov>ping rudn.ru

Обмен пакетами с rudn.ru [185.178.208.57] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 185.178.208.57:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\sadov>
```

Рис. 3.9: Пропингуем rudn.ru

9. В Wireshark остановите захват трафика. Изучите запросы и ответы протоколов ARP и ICMP. Определите MAC-адреса источника и получателя, определите тип MAC-адресов.(рис. 3.10),(рис. 3.11),(рис. 3.12)

1721	418.970537	192.168.1.23	185.178.208.57	ICMP	74 Echo (ping) request	id=0x0001, seq=26/6656, ttl=128 (no response found!)
1733	423.958308	192.168.1.23	185.178.208.57	ICMP	74 Echo (ping) request	id=0x0001, seq=27/6912, ttl=128 (no response found!)
1744	428.960716	192.168.1.23	185.178.208.57	ICMP	74 Echo (ping) request	id=0x0001, seq=28/7168, ttl=128 (no response found!)

Рис. 3.10: Запросы и ответы


```
Frame 1744: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{43...}
Ethernet II, Src: Intel_db:db:16 (70:a8:d3:db:db:16), Dst: LLCProizvods_6a:c2:b1 (58:f8:5c:6a:c2:b1)
  Destination: LLCProizvods_6a:c2:b1 (58:f8:5c:6a:c2:b1)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: Intel_db:db:16 (70:a8:d3:db:db:16)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.23, Dst: 185.178.208.57
Internet Control Message Protocol
```

Рис. 3.11: эхо-запрос

```
Frame 2017: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{43A4...}
Ethernet II, Src: Intel_db:db:16 (70:a8:d3:db:db:16), Dst: LLCProizvods_6a:c2:b1 (58:f8:5c:6a:c2:b1)
  Destination: LLCProizvods_6a:c2:b1 (58:f8:5c:6a:c2:b1)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: Intel_db:db:16 (70:a8:d3:db:db:16)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  [Stream index: 0]
Address Resolution Protocol (reply)
```

Рис. 3.12: эхо-ответ

ARP Request (запрос)

MAC-адреса:

Источник (Source): 58:f8:5c:6a:c2:b1

- Тип: Индивидуальный (Unicast)
- Администрирование: Глобальное (UAA)

Получатель (Destination): ff:ff:ff:ff:ff:ff

- Тип: Групповой (Broadcast)
- Администрирование: Широковещательный адрес

ARP Reply (ответ)

MAC-адреса:

Источник (Source): 70:a8:d3:db:db:16

- Тип: Индивидуальный (Unicast)

- Администрирование: Глобальное (UAA)

Получатель (Destination): 58:f8:5c:6a:c2:b1

- Тип: Индивидуальный (Unicast)
- Администрирование: Глобальное (UAA)

4 Анализ протоколов транспортного уровня в Wireshark

4.1 Постановка задачи

С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.

4.2 Порядок выполнения работы

1. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.
2. На вашем устройстве в браузере перейдите на сайт, работающий по протоколу HTTP (например, на сайт CERN <http://info.cern.ch/>). При необходимости получения большей информации для Wireshark поперемещайтесь по ссылкам или разделам сайта в браузере.(рис. 4.1)

WWW Daemon user guide

The http daemon, [httpd](http://info.cern.ch/), is a general server program which runs a w3 protocol, "[HTTP](http://info.cern.ch/)".

More Information

[Distribution](#)

How to get the code.

[Compilation](#)

How to compile the daemon for your system.

[Installation](#)

How to install a server under unix internet daemon

[Options](#)

Command line options at run time

Рис. 4.1: Сайт <http://info.cern.ch/>

3. В Wireshark в строке фильтра укажите http и проанализируйте информацию по протоколу TCP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.(рис. 4.2),(рис. 4.3),



Рис. 4.2: Наш фильтр

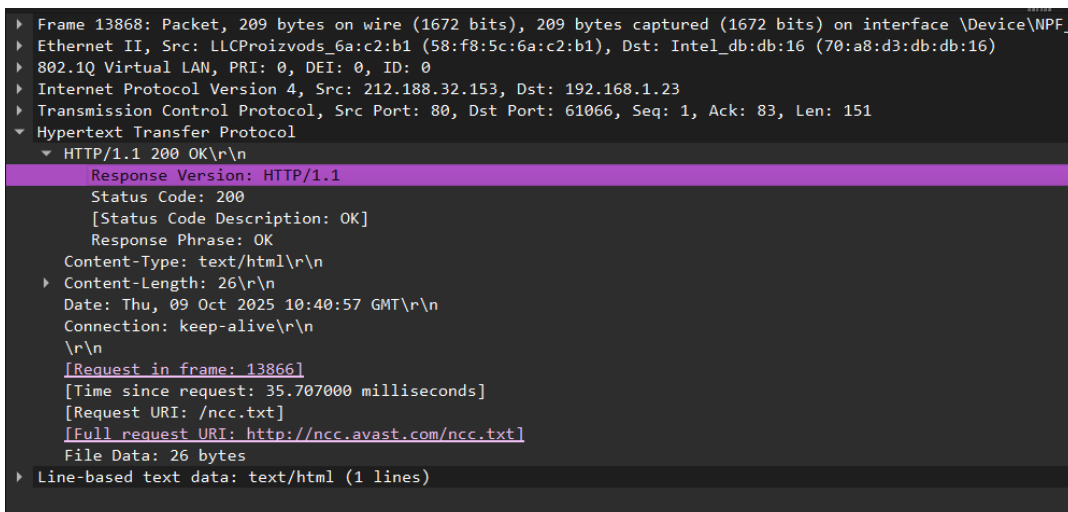


Рис. 4.3: Информация

Анализ уровня приложений (HTTP):

Статус: 200 OK - успешное выполнение запроса

Версия протокола: HTTP/1.1

Тип содержимого: text/html

Размер содержимого: 26 bytes

Соединение: keep-alive (повторное использование TCP-соединения)

Контекст запроса:

Запрос был в кадре: 13866

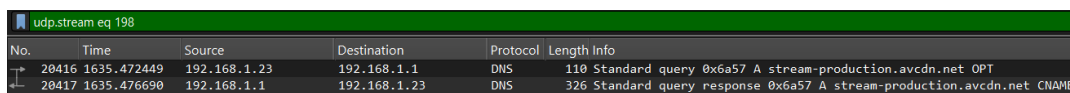
Время обработки: 35.707 ms - быстрый ответ сервера

Запрашиваемый ресурс: /ncc.txt

Полный URL: http://ncc.avast.com/ncc.txt

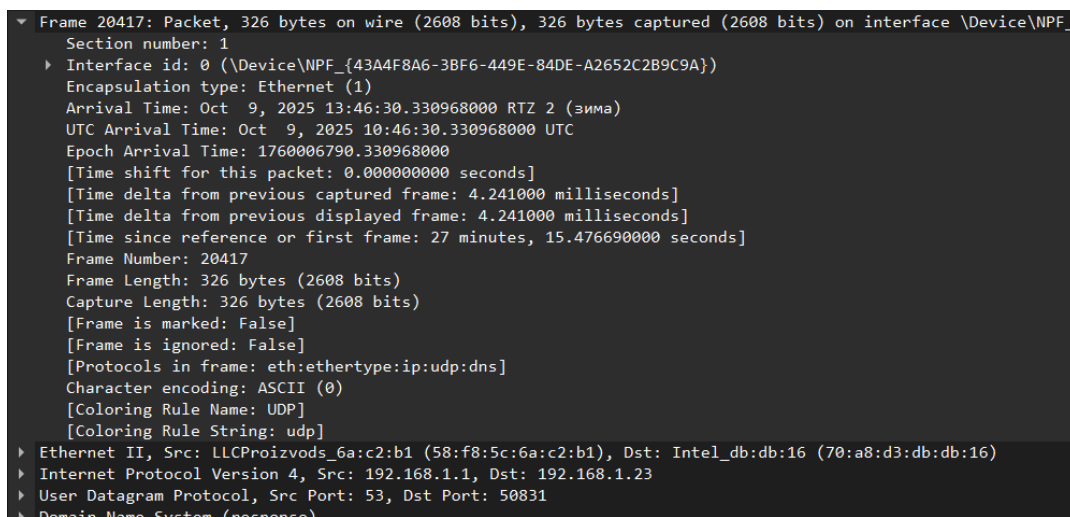
Сервер: Сервер компании Avast (антивирусное ПО)

4. Wireshark в строке фильтра укажите dns и проанализируйте информацию по протоколу UDP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.(рис. 4.4),(рис. 4.5)



No.	Time	Source	Destination	Protocol	Length	Info
20416	1635.472449	192.168.1.23	192.168.1.1	DNS	110	Standard query 0x6a57 A stream-production.avcdn.net OPT
20417	1635.476690	192.168.1.1	192.168.1.23	DNS	326	Standard query response 0x6a57 A stream-production.avcdn.net CNAME

Рис. 4.4: эхо-запрос и эхо-ответ



```
▼ Frame 20417: Packet, 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface \Device\NPF_{43A4F8A6-3BF6-449E-84DE-A2652C2B9C9A}
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{43A4F8A6-3BF6-449E-84DE-A2652C2B9C9A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 9, 2025 13:46:30.330968000 RTZ 2 (зима)
    UTC Arrival Time: Oct 9, 2025 10:46:30.330968000 UTC
    Epoch Arrival Time: 176006790.330968000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 4.241000 milliseconds]
    [Time delta from previous displayed frame: 4.241000 milliseconds]
    [Time since reference or first frame: 27 minutes, 15.476690000 seconds]
    Frame Number: 20417
    Frame Length: 326 bytes (2608 bits)
    Capture Length: 326 bytes (2608 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    Character encoding: ASCII (0)
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  ▶ Ethernet II, Src: LLCProizvods_6a:c2:b1 (58:f8:5c:6a:c2:b1), Dst: Intel_db:db:16 (70:a8:d3:db:db:16)
  ▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.23
  ▶ User Datagram Protocol, Src Port: 53, Dst Port: 50831
  ▶ Domain Name System (response)
```

Рис. 4.5: Информация

Анализ пакета

Номер кадра: 20417

Длина кадра: 326 байт

Протоколы в кадре: eth:ethertype:ip:udp:dns

Источник: 192.168.1.1 (вероятно, локальный DNS-сервер или маршрутизатор)

Назначение: 192.168.1.23 (клиентское устройство)

Порты:

- Src Port: 53 (стандартный порт DNS-сервера)
- Dst Port: 50831 (порт клиента, с которого был отправлен запрос)

5. Wireshark в строке фильтра укажите quic и проанализируйте информацию по протоколу quic в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.(рис. 4.6),(рис. 4.7)

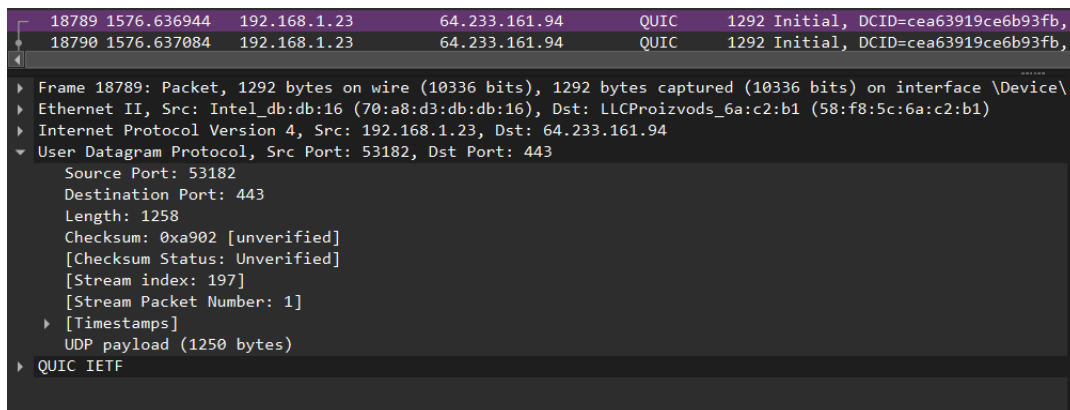


Рис. 4.6: эхо-запрос

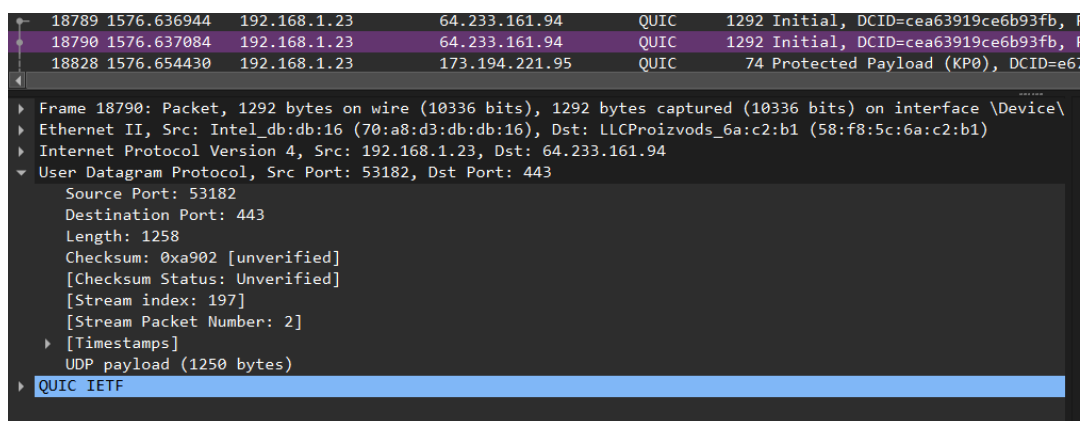


Рис. 4.7: эхо-ответ

Анализ пакета

Номер кадра: 18790

Время: 1576.637084 секунд от начала захвата

Источник: 192.168.1.23 (клиент)

Назначение: 64.233.161.94 (сервер, принадлежит Google)

Порты:

- Src Port: 53182 (клиентский)
- Dst Port: 443 (HTTPS/QUIC)

Длина UDP-датаграммы: 1258 байт

Протоколы в кадре: eth:ip:udp:quic

6. Остановите захват трафика в Wireshark.

5 Анализ handshake протокола TCP в Wireshark

5.1 Постановка задачи

С помощью Wireshark проанализировать handshake протокола TCP.

5.2 Порядок выполнения работы

1. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.
2. На вашем устройстве или используйте подсоединение по telnet или ssh к вашему маршрутизатору (например с помощью PUTTY или соответствующих команд в консоли), или соединение по HTTP с каким-то сайтом для захвата в Wireshark пакетов TCP.

Для работы с telnet нужно в консоле ее отдельно подключить. На версиях Windows 10/11 эта команда отключена. Ее можно обратно включить зайдя в настройки устройства в раздел с подключением дополнительных параметров. После подключения, мне не потребовалось обновлять коомпьютер и я продолжила работу в терменале.

3. В Wireshark проанализируйте handshake протокола TCP, в отчёте приведи-

те пример с пояснениями изменения значений соответствующих сообщений при установлении соединения по ТСР.(рис. 5.1)

No.	Time	Source	Destination	Protocol	Length	Info
146	25.729262	192.168.1.23	149.154.167.99	TCP	54	63097 → 443 [ACK] Seq=2078 Ack=4727 Win=65015 Len=0
148	27.211389	192.168.1.23	34.104.35.123	TCP	66	[TCP Retransmission] 53415 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
150	28.229827	18.97.36.64	192.168.1.23	TLSv1.2	82	Application Data
151	28.229827	18.97.36.64	192.168.1.23	TCP	58	443 → 61270 [FIN, ACK] Seq=49 Ack=29 Win=404 Len=0
152	28.230635	192.168.1.23	18.97.36.64	TCP	54	61270 → 443 [ACK] Seq=29 Ack=50 Win=255 Len=0
153	28.231188	192.168.1.23	18.97.36.64	TCP	54	[TCP Previous segment not captured] 61270 → 443 [FIN, ACK] Seq=53 Ack=50 Win=255 Len=0
154	28.231231	192.168.1.23	18.97.36.64	TLSv1.2	70	[TCP Out-Of-Order] , Application Data
155	29.231268	192.168.1.23	18.97.36.64	TCP	54	61270 → 443 [RST, ACK] Seq=54 Ack=50 Win=0 Len=0
156	28.357338	18.97.36.64	192.168.1.23	TCP	58	443 → 61270 [RST] Seq=50 Win=0 Len=0
157	28.357338	18.97.36.64	192.168.1.23	TCP	58	443 → 61270 [RST] Seq=50 Win=0 Len=0
158	28.698205	192.168.1.23	149.154.167.99	TLSv1.2	237	Application Data
159	28.754715	149.154.167.99	192.168.1.23	TLSv1.2	171	Application Data
160	28.806294	192.168.1.23	149.154.167.99	TCP	54	63097 → 443 [ACK] Seq=2261 Ack=4840 Win=64902 Len=0
161	29.853500	192.168.1.23	173.194.221.113	TCP	66	[TCP Retransmission] 53416 → 23 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

Рис. 5.1: Запускаем фильтр с протоколом ТСР

4. В Wireshark в меню «Статистика» выберете «График Потока». В отчёте приведите пояснения по изменениям значений соответствующих сообщений при установлении соединения по ТСР.(рис. 5.2)

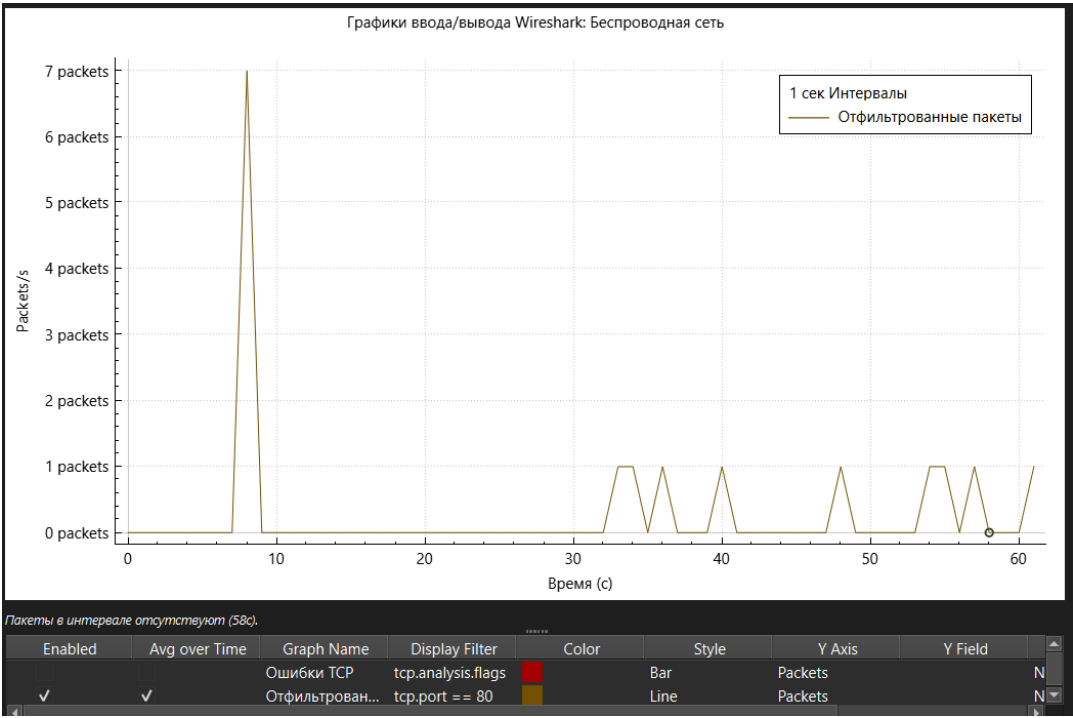


Рис. 5.2: График порта 80

На участке “Пакеты в интервале отсутствуют (58с)” оба графика падают до нуля, что означает полное отсутствие ТСР-трафика (включая ошибки) на порту 80 в течение 58 секунд.

После третьего пакета соединение установлено.

Анализируя Graph Flow, вы можете четко видеть всю жизненную цепочку TCP-сессии: от установления соединения (рукопожатие), через передачу данных с постоянно растущими номерами подтверждений (Ack), до корректного завершения соединения (обмен пакетами FIN/ACK).

5. Остановите захват трафика в Wireshark.

6 Выводы

Изучили с помощью Wireshark кадры Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP. Поработали с простейшими командами и фильтрами. Разобрались в выводимой информации Wireshark.

Список литературы