Анализ трафика в Wireshark

Лабораторная работа №3

Гафоров Нурмухаммад

9 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Изучить принципы работы сетевых протоколов ARP, ICMP, TCP, UDP и QUIC посредством анализа трафика в программе **Wireshark**.

Ход выполнения

Определение сетевых параметров

На локальном компьютере с помощью команды `ipconfig` были определены IP-адрес, маска подсети и шлюз по умолчанию.

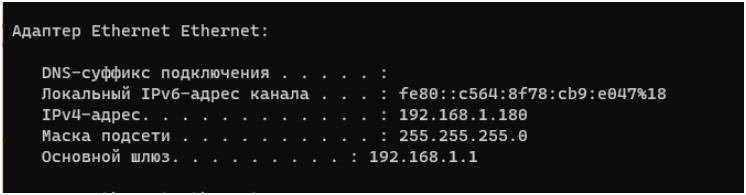


Рис. 1: Определение IP-адреса и шлюза по умолчанию

Проверка доступности шлюза

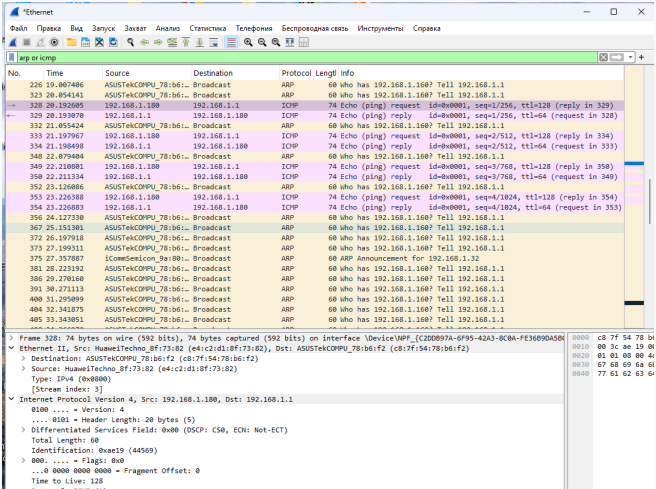
Был выполнен тест связи командой `ping 192.168.1.1`. Пакеты получены без потерь, что подтвердило корректную работу сети.

```
PS C:\Users\gaforov\Documents> 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 = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\Users\gaforov\Documents>
```

Рис. 2: Проверка доступности шлюза

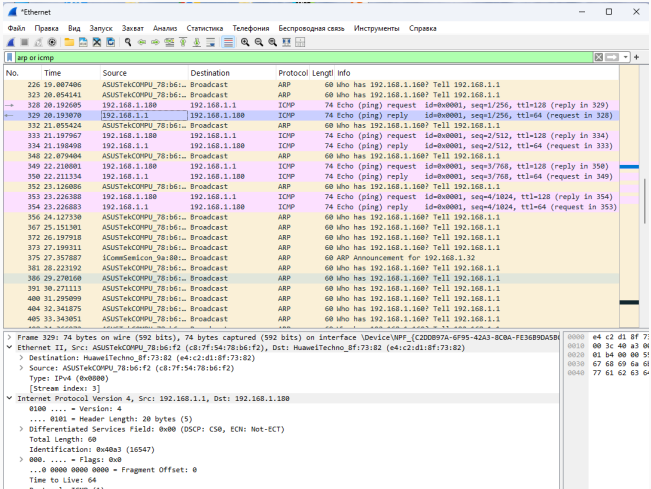
Анализ ICMP-трафика

В Wireshark применён фильтр `arp or icmp`. Зафиксированы пакеты ICMP Echo Request и Echo Reply между устройством и шлюзом.



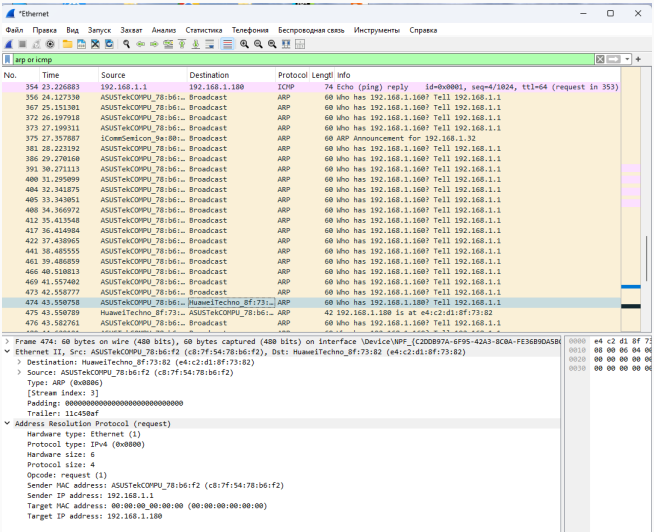
Анализ ICMP-трафика

В Wireshark применён фильтр `arp or icmp`. Зафиксированы пакеты ICMP Echo Request и Echo Reply между устройством и шлюзом.



Анализ ARP-протокола

Перед ICMP-обменом выполняется разрешение MAC-адреса шлюза через ARP-запрос и ответ.



Проверка связи с внешним ресурсом

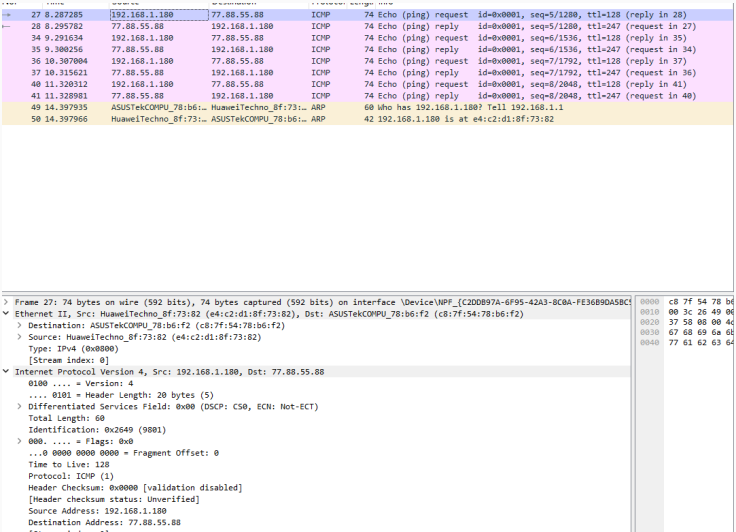
Командой `ping yandex.ru` выполнен тест соединения с удалённым узлом. Среднее время отклика составило 8 мс.

```
PS C:\Users\gaforov\Documents>
PS C:\Users\gaforov\Documents> ping yandex.ru

Обмен пакетами с yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247

Статистика Ping для 77.88.55.88:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 8мсек, Максимальное = 8 мсек, Среднее = 8 мсек
PS C:\Users\gaforov\Documents>
```

Рис. 6: Проверка доступности внешнего ресурса

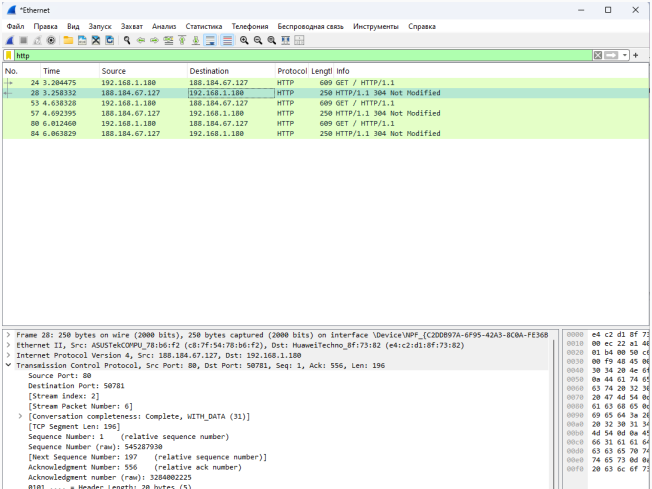
Анализ ICMP при обращении к внешнему серверу

Фильтр `arp or icmp` показал обмен ICMP-запросами с адресом 77.88.55.88 (yandex.ru).



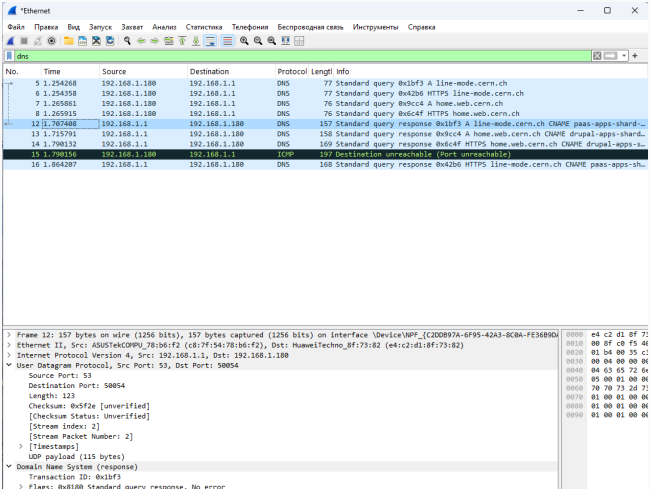
При фильтрации по `http` зафиксированы запросы **GET** и ответы **HTTP/1.1 304 Not Modified**.

Данные передаются через TCP с портом 80.



Анализ DNS и UDP

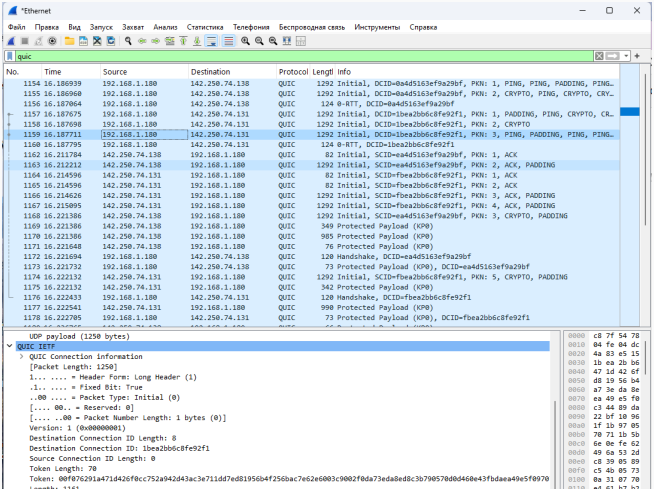
С помощью фильтра **dns** зафиксированы DNS-запросы и ответы, использующие порты 53 (сервер) и 50854 (клиент).



Анализ протокола QUIC

Фильтр `quic` выявил пакеты **Initial**, **Handshake**, **PING** и **CRYPTO**, передаваемые по UDP.

Протокол обеспечивает быструю и защищённую передачу данных.



Анализ handshake TCP

Исследован процесс установления TCP-соединения (**Three-Way Handshake**):

1. SYN — инициация соединения клиентом.
2. SYN/ACK — подтверждение сервером.
3. ACK — завершение установления.

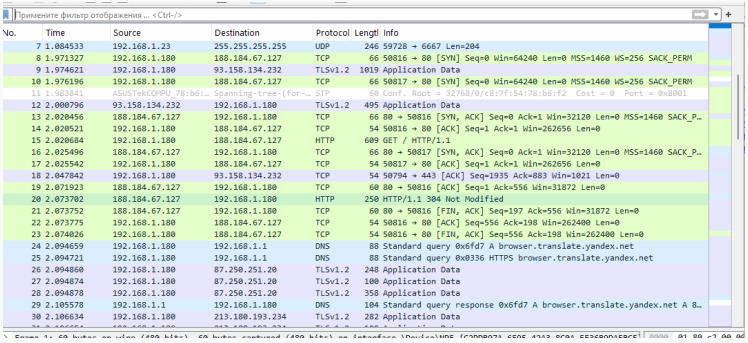
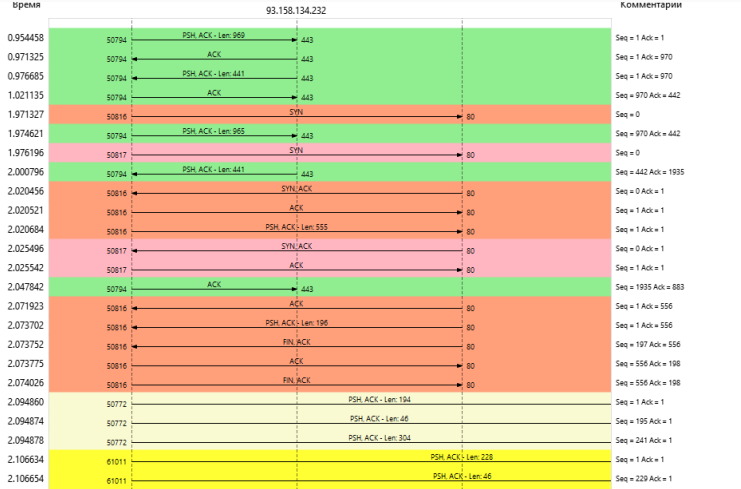


Рис. 11: Захват TCP handshake в Wireshark

График потока TCP

На графике потока отображается последовательность обмена сегментами SYN → SYN/ACK → ACK, подтверждающая корректное установление соединения.



Выводы

Итог лабораторной работы

В результате работы были исследованы протоколы **ARP**, **ICMP**, **TCP**, **UDP** и **QUIC** с помощью анализатора **Wireshark**.
Получены практические навыки по анализу сетевого трафика и пониманию принципов работы транспортного уровня стека TCP/IP.

Процесс трёхэтапного установления соединения (**TCP Handshake**) был подробно изучен, что подтвердило надёжность и согласованность протокола TCP.