Анализ трафика в Wireshark

Лабораторная работа №3

Суннатилло Махмудов

02 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Изучение и анализ сетевых протоколов на разных уровнях модели OSI с помощью анализатора трафика **Wireshark**.

Задачи лабораторной работы

1. Определить параметры сетевых интерфейсов и изучить структуру MAC-адреса.
2. Проанализировать кадры канального уровня (ARP, ICMP).
3. Исследовать транспортные протоколы (**TCP, UDP, QUIC**) и их особенности.
4. Рассмотреть механизм установления соединения TCP (*three-way handshake*).

Теоретическая часть

Основные протоколы

- **MAC-адресация** — уникальная идентификация сетевого интерфейса.
- **ARP** — сопоставление IP и MAC-адресов.
- **ICMP** — служебные сообщения, диагностика (ping).
- **TCP** — надёжная передача данных, трёхстороннее рукопожатие.
- **UDP** — простой протокол без установления соединения.
- **QUIC** — работает поверх UDP, обеспечивает шифрование и ускорение.
- **Wireshark** — анализатор пакетов для исследования уровней модели OSI.

Выполнение работы

MAC-адресация

- Получение параметров интерфейса с помощью `ipconfig`.
- Определение MAC-адреса устройства.
- Разбор структуры адреса: OUI (производитель), уникальный идентификатор, тип (unicast/global).

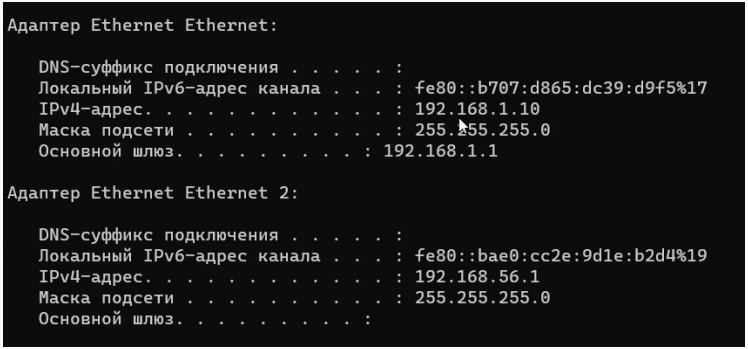
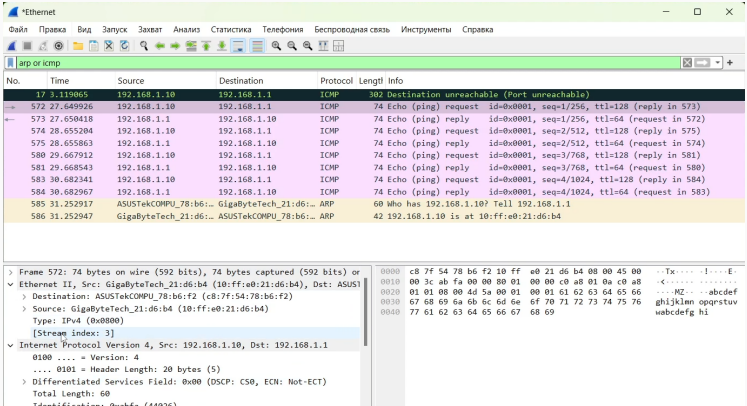


Рис. 1: Вывод команды ipconfig

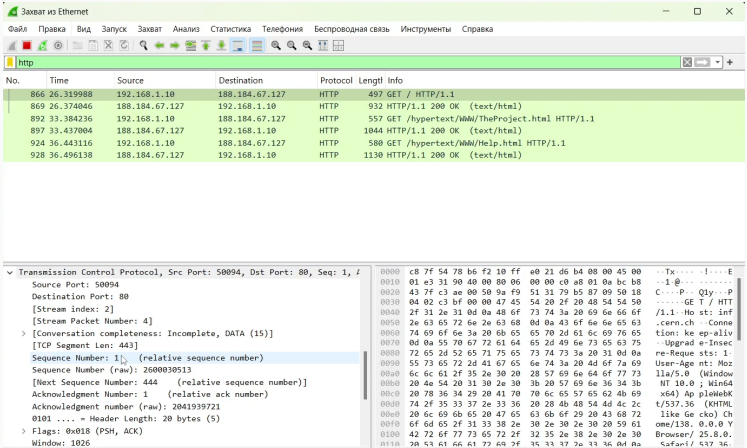
Анализ ARP и ICMP

- Ping шлюза по умолчанию.
- Фильтрация трафика в Wireshark: **arp or icmp**.
- Анализ эхо-запросов и эхо-ответов.
- Изучение ARP-запросов и ответов.



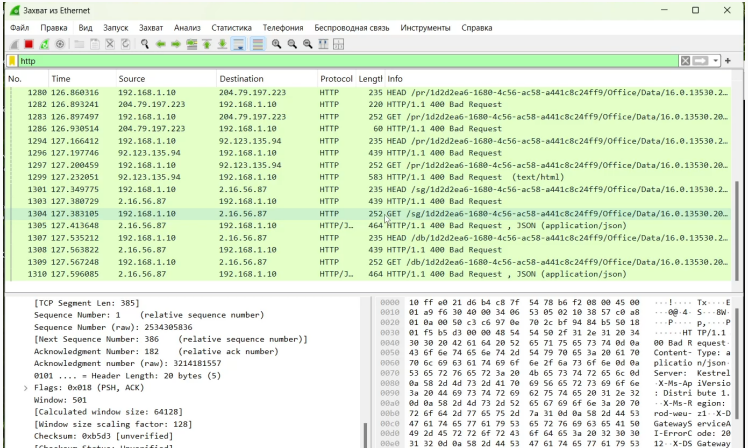
Анализ транспортных протоколов

- HTTP-трафик (TCP): запросы GET, ответы 200 OK.
- DNS-трафик (UDP): запросы A/HTTPS-записей.
- QUIC-трафик (UDP+TLS 1.3): зашифрованные сегменты и Handshake.



Анализ handshake TCP

- Установление соединения: SYN → SYN+ACK → ACK.
- Визуализация в Wireshark через «График потока».
- Наблюдение последовательности, подтверждений и завершения сеанса.



Вывод

Вывод

В ходе работы:

* Изучены MAC-адреса и протоколы ARP/ICMP.
* Проанализированы транспортные протоколы TCP, UDP, QUIC.
* Подробно рассмотрен процесс установления TCP-соединения.
* Использование **Wireshark** позволило наглядно изучить работу сетевых протоколов на разных уровнях модели OSI.