Лабораторная работа №3

Дисциплина: Сетевые технологии

Ибрахим Мохсейн Алькамаль

2025-12-20

Содержание I

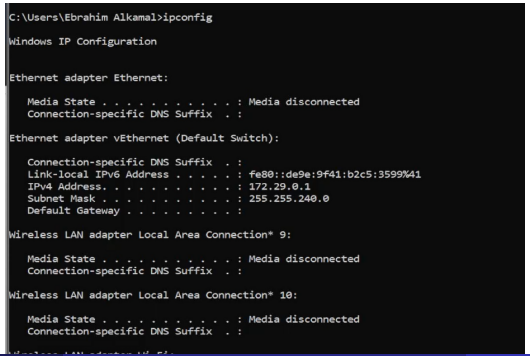
1 Цель работы

Цель работы:

- Изучение кадров Ethernet
- Анализ PDU протоколов:
  - транспортного уровня
  - прикладного уровня
- Исследование работы стека TCP/IP с помощью Wireshark

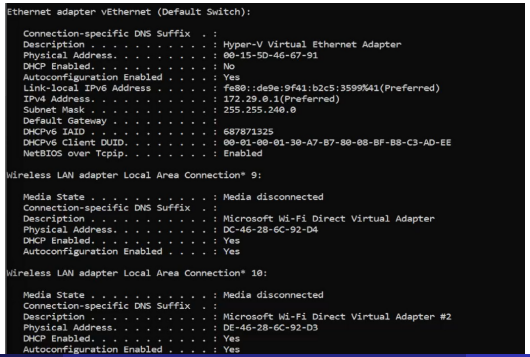
2 MAC-адресация (ipconfig)

- Использована команда `ipconfig`
- Получены параметры сетевого интерфейса:
  - IPv4-адрес
  - Маска подсети
  - Шлюз по умолчанию
- Определено активное беспроводное соединение



3 MAC-адрес устройства (ipconfig /all)

- Использована команда `ipconfig /all`
- Определён MAC-адрес сетевого адаптера:
  - **DC-46-28-6C-92-D3**
- MAC-адрес состоит из 6 октетов:
  - первые 3 — производитель
  - последние 3 — интерфейс

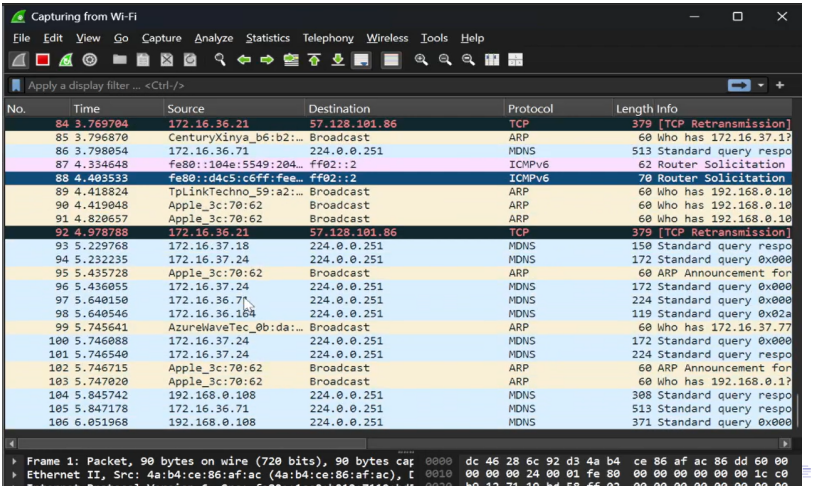


4 Анализ MAC-адреса

- Производитель по первым 3 октетам: **Intel Corporate**
- Первый байт: DC $= 11011100_2$
  - I/G bit = 0 $\longrightarrow$ индивидуальный адрес
  - L/G bit = 0 $\longrightarrow$ глобально администрируемый адрес

5 Запуск захвата в Wireshark

- Выбран беспроводной интерфейс
- Запущен захват трафика



6 ICMP: пинг шлюза

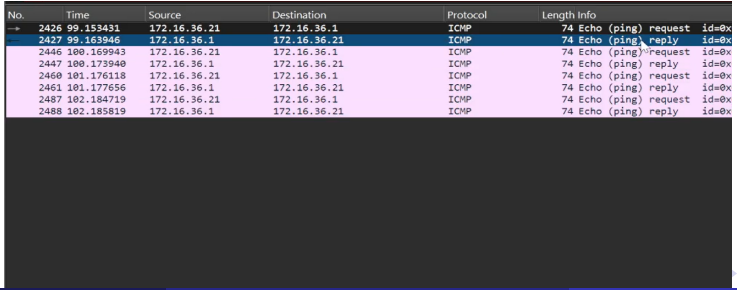
- Шлюз по умолчанию: **172.16.36.1**
- Выполнена команда:
  `ping 172.16.36.1`
- Захвачены ICMP Echo Request и Echo Reply

```
C:\Users\Ebrahim Alkamal>ping  172.16.36.1

Pinging 172.16.36.1 with 32 bytes of data:
Reply from 172.16.36.1: bytes=32 time=10ms TTL=254
Reply from 172.16.36.1: bytes=32 time=4ms TTL=254
Reply from 172.16.36.1: bytes=32 time=1ms TTL=254
Reply from 172.16.36.1: bytes=32 time=1ms TTL=254

Ping statistics for 172.16.36.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms
```

Рисунок 4: Пинг шлюза по умолчанию

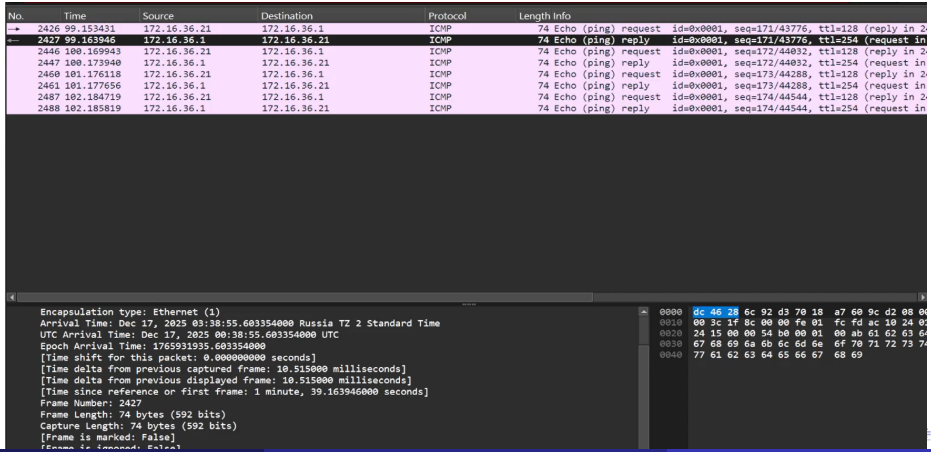
7 ICMP Echo Request

- Фильтр: `icmp`
- Проанализирован Echo Request:
  - Длина кадра: 74 байта
  - MAC источника: устройство
  - MAC назначения: шлюз
- Оба MAC-адреса:
  - индивидуальные
  - глобально администрируемые



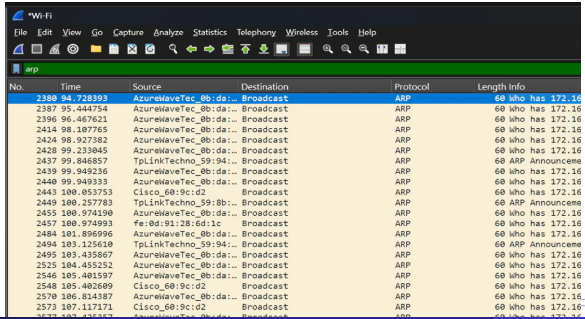
8 ICMP Echo Reply

- Echo Reply от шлюза к клиенту
- MAC-адреса источника и назначения поменялись местами
- Длина кадра также 74 байта



9 Протокол ARP

- ARP передаётся в кадре **Ethernet II**
- Общая длина кадра: **60 байт**
- Основные поля:
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4
  - Opcode: 1 (ARP Request)
- Адрес назначения: **ff:ff:ff:ff:ff:ff**



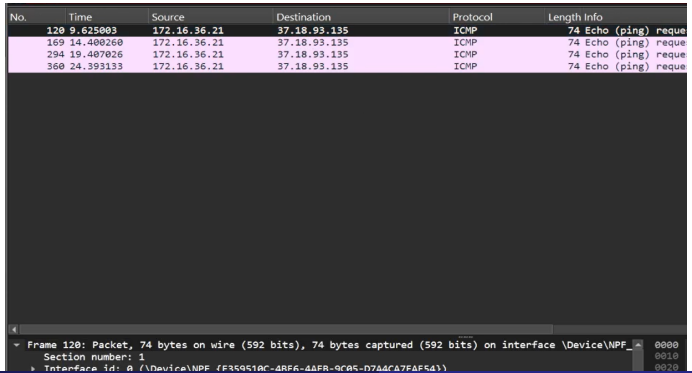
10 ICMP: ping rudn.ru

- Выполнена команда:
  `ping rudn.ru`
- Результат:
  - 4 запроса
  - 0 ответов
  - Потери: 100%
- ICMP-ответы отсутствуют

```
C:\Users\Ebrahim Alkamal>ping rudn.ru

Pinging rudn.ru [37.18.93.135] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 37.18.93.135:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

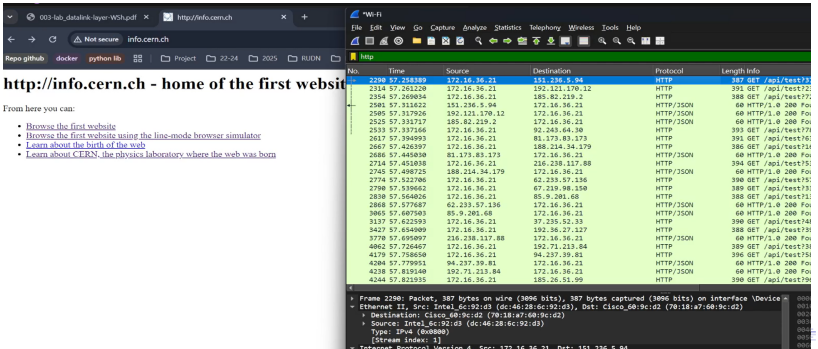
11 ICMP без ответа

- Захвачены только Echo Request
- Echo Reply отсутствуют
- Возможные причины:
  - блокировка ICMP
  - межсетевой экран
  - политики безопасности



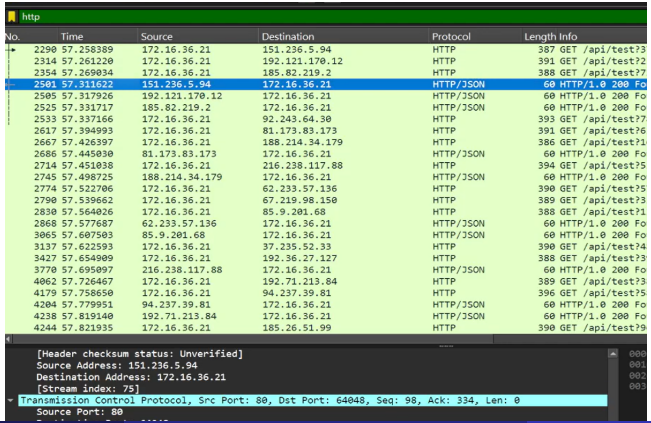
12 HTTP поверх TCP

- Открыт сайт: **http://info.cern.ch**
- Фильтр: `http`
- Анализ TCP:
  - порт источника: динамический (64048)
  - порт назначения: 80
- Используются Sequence и Acknowledgment Number



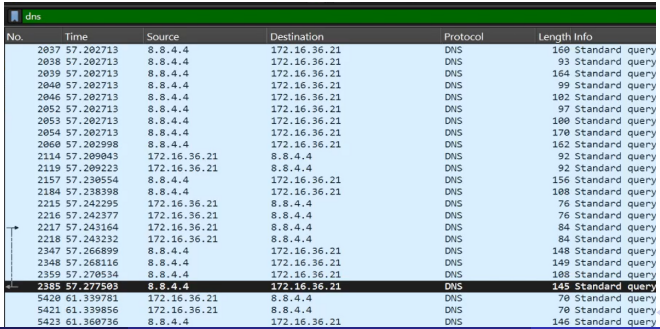
13 HTTP Response

- В ответе:
  - порт источника: 80
  - порт назначения: 64048
- Порты меняются местами



14 DNS (UDP)

- Фильтр: dns
- DNS-запрос:
  - порт источника: динамический
  - порт назначения: 53
- DNS-ответ:
  - источник: 53
  - назначение: 64317

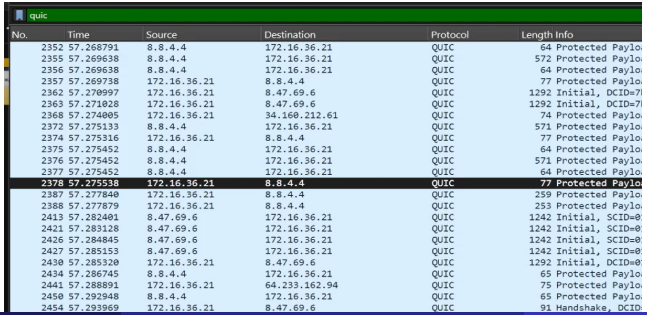


dns

No.	Time	Source	Destination	Protocol	Length	Info
2037	57.202713	8.8.4.4	172.16.36.21	DNS	160	Standard query
2038	57.202713	8.8.4.4	172.16.36.21	DNS	93	Standard query
2039	57.202713	8.8.4.4	172.16.36.21	DNS	164	Standard query
2040	57.202713	8.8.4.4	172.16.36.21	DNS	99	Standard query
2046	57.202713	8.8.4.4	172.16.36.21	DNS	102	Standard query
2052	57.202713	8.8.4.4	172.16.36.21	DNS	97	Standard query
2053	57.202713	8.8.4.4	172.16.36.21	DNS	100	Standard query
2054	57.202713	8.8.4.4	172.16.36.21	DNS	170	Standard query
2060	57.202998	8.8.4.4	172.16.36.21	DNS	162	Standard query
2114	57.209043	172.16.36.21	8.8.4.4	DNS	92	Standard query
2119	57.209223	172.16.36.21	8.8.4.4	DNS	92	Standard query
2157	57.230554	8.8.4.4	172.16.36.21	DNS	156	Standard query
2184	57.238398	8.8.4.4	172.16.36.21	DNS	108	Standard query
2215	57.242295	172.16.36.21	8.8.4.4	DNS	76	Standard query
2216	57.242377	172.16.36.21	8.8.4.4	DNS	76	Standard query
2217	57.243164	172.16.36.21	8.8.4.4	DNS	84	Standard query
2218	57.243232	172.16.36.21	8.8.4.4	DNS	84	Standard query
2347	57.266899	8.8.4.4	172.16.36.21	DNS	148	Standard query
2348	57.268116	8.8.4.4	172.16.36.21	DNS	149	Standard query
2359	57.270534	8.8.4.4	172.16.36.21	DNS	108	Standard query
2385	57.277503	8.8.4.4	172.16.36.21	DNS	145	Standard query
5420	61.339781	172.16.36.21	8.8.4.4	DNS	70	Standard query
5421	61.339856	172.16.36.21	8.8.4.4	DNS	70	Standard query
5423	61.360736	8.8.4.4	172.16.36.21	DNS	146	Standard query

15 Протокол QUIC

- Фильтр: `quic`
- Использован браузер Google Chrome
- QUIC работает поверх UDP
- Порты:
  - источник: 49768
  - назначение: 443
- Встроенное шифрование TLS 1.3

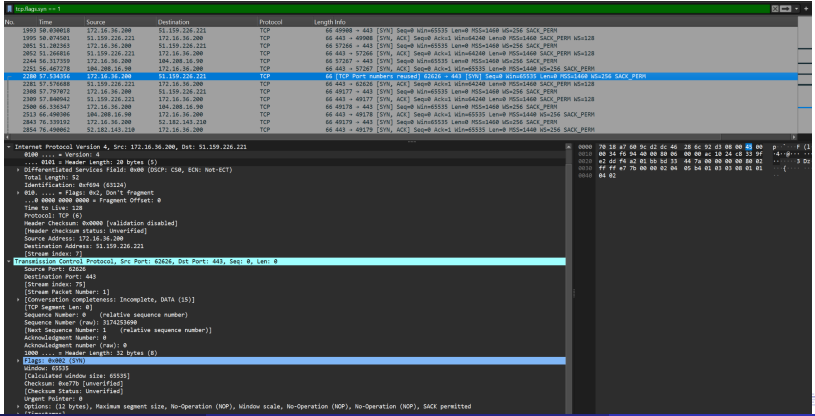


16 TCP Handshake (общее)

- TCP использует **трёхступенчатое рукопожатие**
- Этапы:
  1. SYN
  2. SYN + ACK
  3. ACK

17 Handshake: SYN

- Клиент ⟶ сервер
- Флаг: **SYN**
- Relative Sequence Number = 0
- Инициация соединения



18 Handshake: SYN + ACK

- Сервер ⟶ клиент
- Флаги: **SYN, ACK**
- Ack = 1 подтверждает SYN клиента

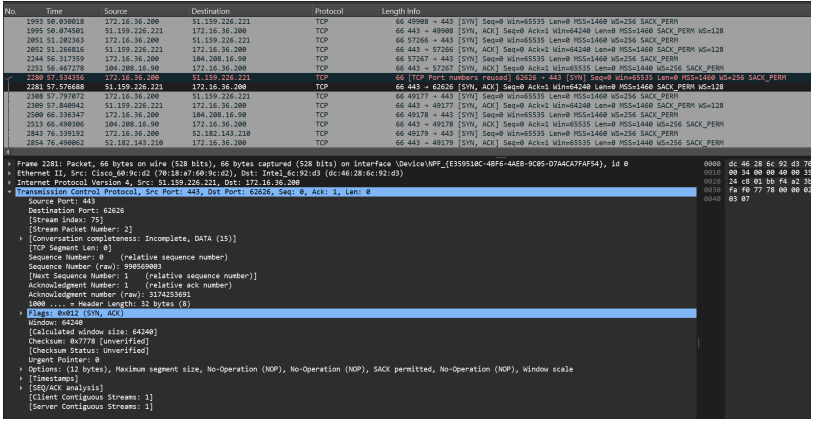
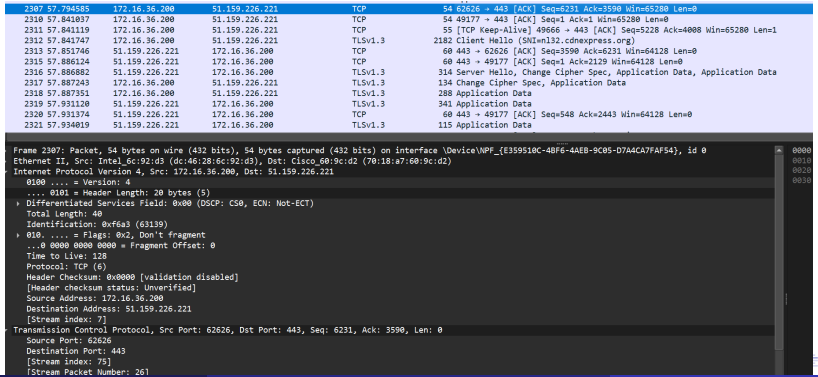


Рисунок 14. Вторая часть handshake TCP

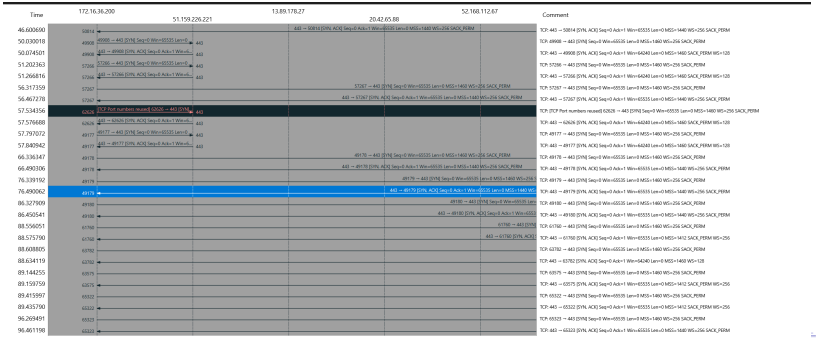
19 Handshake: ACK

- Клиент ⟶ сервер
- Флаг: **ACK**
- Sequence Number = 6231
- Acknowledgment Number = 3590
- Соединение установлено



20 Flow Graph (TCP)

- Использован инструмент **Statistics → Flow Graph**
- Наглядно показаны:
  - SYN
  - SYN, ACK
  - ACK
- Подтверждение завершения TCP-handshake



21 Завершение захвата

- Захват трафика остановлен
- Анализ завершён

22 Выводы

В ходе работы:

- Изучены кадры Ethernet
- Проанализированы протоколы:
  - ARP, ICMP
  - TCP, UDP
  - HTTP, DNS, QUIC
- Исследован TCP three-way handshake
- Получены практические навыки работы с Wireshark