Сетевые технологии

Лабораторная работа №3

Элсаиед Адел

19 января 2026

Российский университет дружбы народов, Москва, Россия

Цель и задачи работы

Цель лабораторной работы

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

Ход выполнения работы

Вывод параметров подключения (ipconfig /all)

- Определены параметры интерфейса Wi-Fi
- Зафиксированы DHCP/DNS и срок аренды
- Получены IPv4/IPv6 адреса, маска, шлюз по умолчанию

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
   Физический адрес. . . . . . . . . : F8-FE-5E-6F-7B-EC
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
   Локальный IPv6-адрес канала . . . : fe80::da3b:4057:9ef4:1e28%7(Основной)
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.69(Основной)
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Аренда получена. . . . . . . . . . : 19 января 2026 г. 11:23:48
   Срок аренды истекает. . . . . . . . . . : 20 января 2026 г. 11:23:46
   Основной шлюз. . . . . . . . . : 192.168.1.1
   DHCP-сервер. . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . : 133758558
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-30-47-94-1A-10-FF-E0-21-D6-B4
   DNS-серверы. . . . . . . . . . . : 192.168.1.1
   NetBios через TCP/IP. . . . . . . . : Включен
```

Основные параметры сети

- IPv4-адрес: `192.168.1.69`
- Маска: `255.255.255.0`
- Шлюз по умолчанию: `192.168.1.1`
- DNS/DHCP: `192.168.1.1`
- MAC (Wi-Fi): `F8-FE-5E-6F-7B-EC`

Проверка доступности шлюза (ping)

- Выполнен `ping 192.168.1.1`
- Потерь пакетов нет, задержка < 1 мс
- Связность в локальном сегменте подтверждена

```
PS C:\Users\Adel\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 = 1 мсек, Среднее = 0 мсек
```

Рис. 2: ping 192.168.1.1

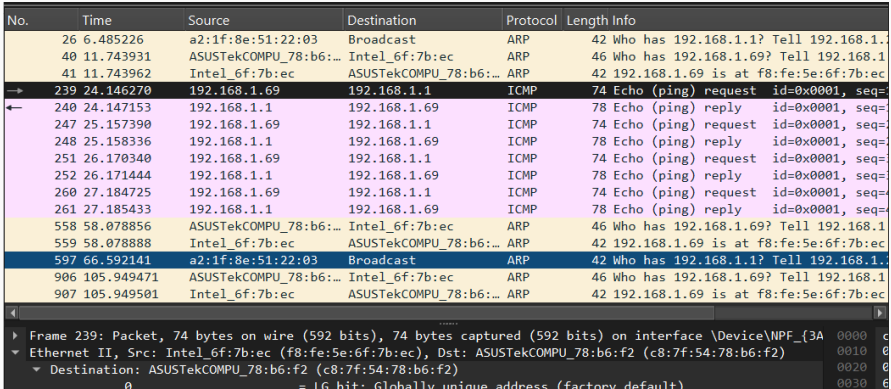
Структура MAC-адреса

Пример: `F8-FE-5E-6F-7B-EC` - OUI (производитель): `F8-FE-5E` (первые 24 бита) - NIC (интерфейс): `6F-7B-EC` (последние 24 бита)

Определение типа по первому октету `F8` = `11111000`: - I/G (bit0) = 0 → **unicast** - U/L (bit1) = 0 → **globally administered**

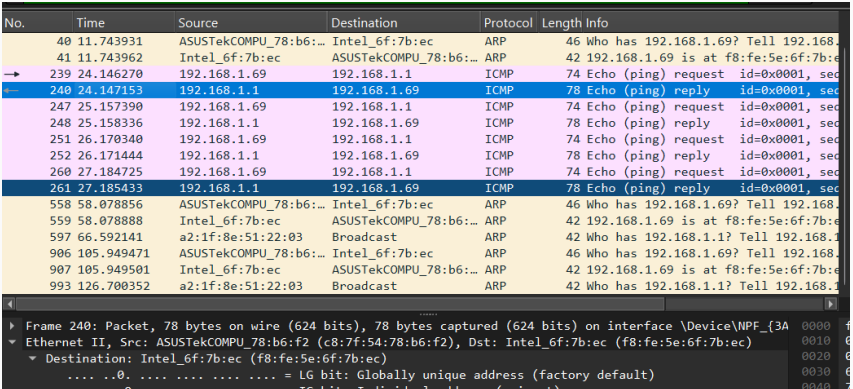
Фильтрация трафика и ICMP Echo Request

- ICMP Echo Request к шлюзу:
  - Ethernet II
  - Длина кадра: 74 bytes
  - Src MAC: `f8:fe:5e:6f:7b:ec`
  - Dst MAC: `c8:7f:54:78:b6:f2`



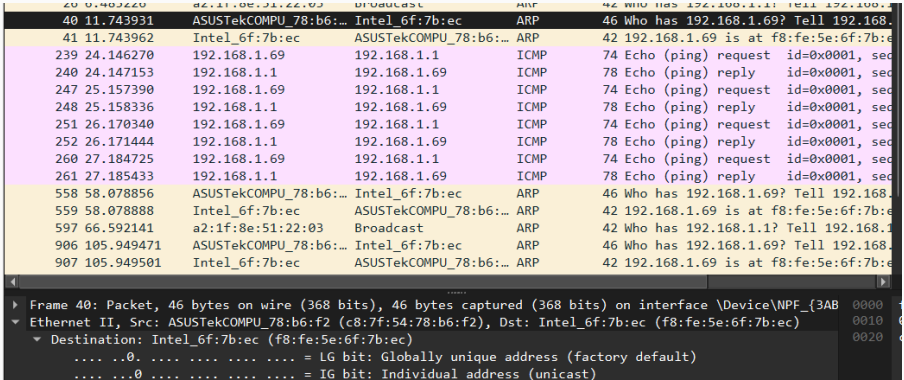
ICMP Echo Reply

- ICMP Echo Reply от шлюза:
  - Длина кадра: 78 bytes
  - Ethernet II (фиксируется 802.1Q VLAN в деталях)
  - Src MAC: `c8:7f:54:78:b6:f2`
  - Dst MAC: `f8:fe:5e:6f:7b:ec`



ARP request

- ARP используется для сопоставления IP↔MAC в сегменте L2
- Рассмотрен ARP request:
  - Ethernet II + ARP (0x0806)
  - Длина кадра: 46 bytes
  - Отображается 802.1Q VLAN (0x8100)



Ping по доменному имени и ARP reply

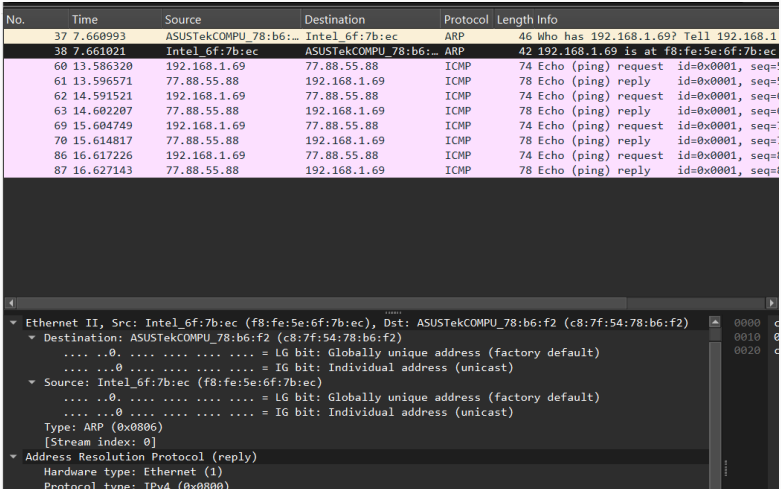
- Выполнен `ping www.yandex.ru`

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

Обмен пакетами с www.yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=53

Статистика Ping для 77.88.55.88:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 9мсек, Максимальное = 10 мсек, Среднее = 9 мсек
```

Рис. 6: ping www.yandex.ru

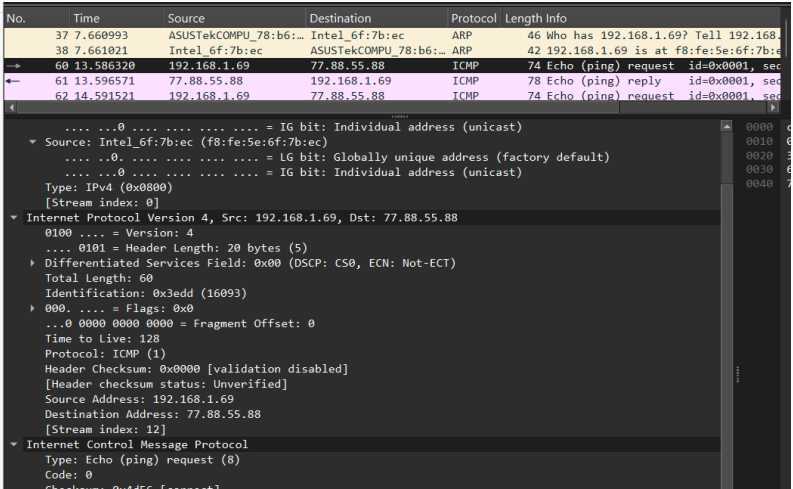
Ping по доменному имени и ARP reply

- Имя разрешено в `77.88.55.88`
- ARP reply подтверждает сопоставление IP устройства и его MAC



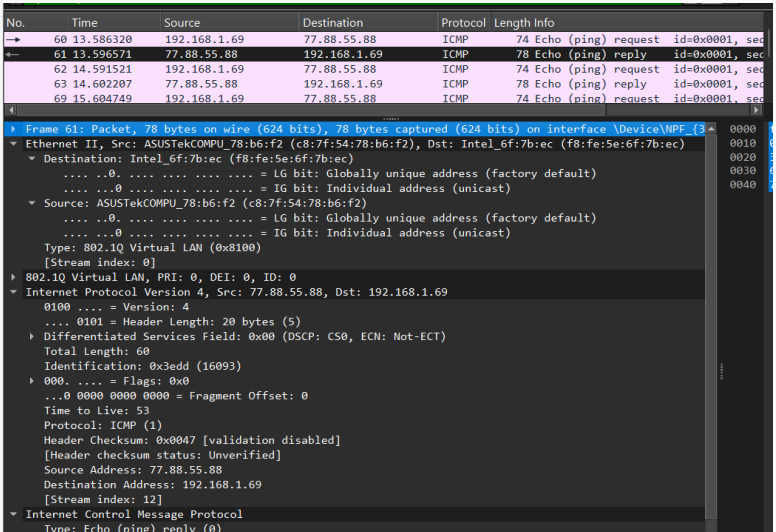
ICMP к внешнему узлу: роль шлюза

- ICMP Echo Request на `77.88.55.88`
- На канальном уровне кадр адресован **MAC шлюза**, т.к. цель вне подсети



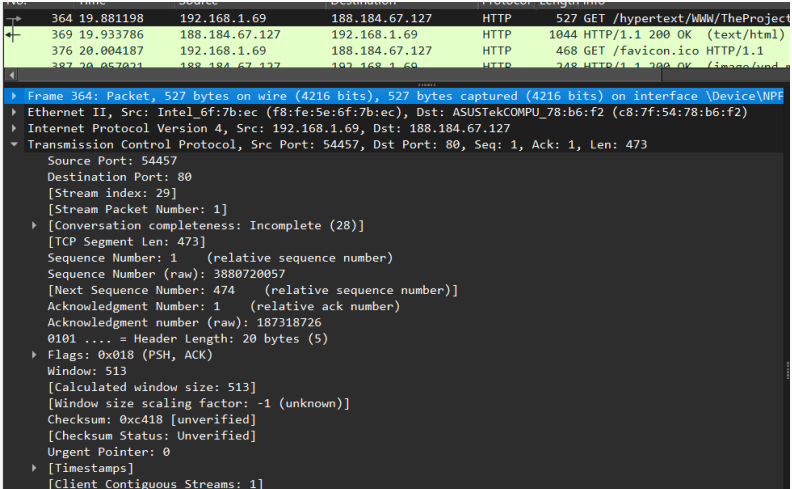
ICMP к внешнему узлу: роль шлюза

- Echo Reply приходит в локальную сеть от MAC шлюза



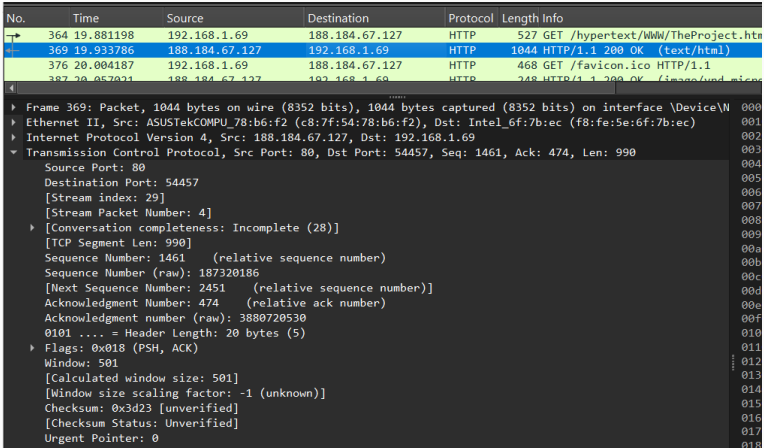
HTTP поверх TCP: GET-запрос

Фильтр: `http` - TCP: Src Port `54457` → Dst Port `80` - Флаги: `PSH, ACK` - HTTP: `GET /hypertext/WWW/TheProject.html`



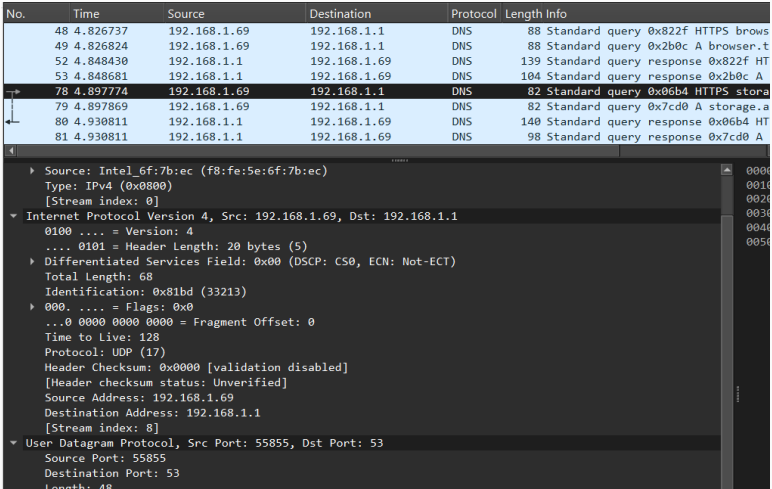
HTTP ответ сервера

- HTTP/1.1 `200 OK`
- Content-Type: `text/html`
- Данные передаются несколькими сегментами (reassembly)



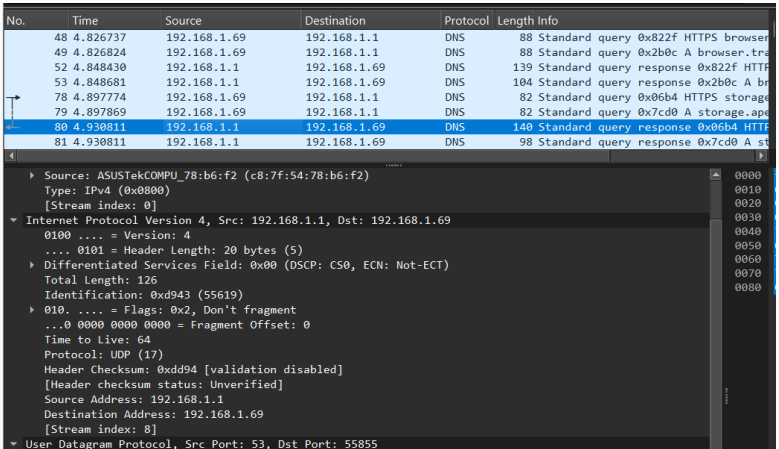
DNS поверх UDP: запрос

Фильтр: `dns` - UDP: Src Port `55855` → Dst Port `53` - Src IP: `192.168.1.69` → Dst IP: `192.168.1.1` - Standard query (запрос A/HTTPS)



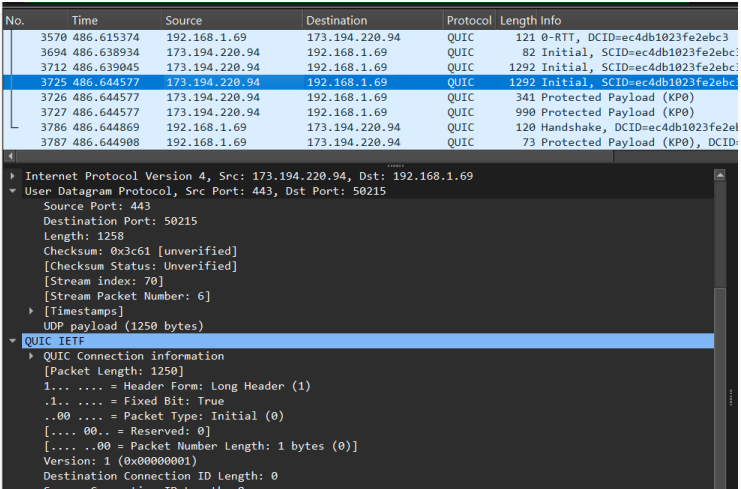
DNS поверх UDP: ответ

- Ответ от DNS-сервера `192.168.1.1`
- Возвращается сопоставление имени с IP
- Фиксируется TTL и служебные признаки IP



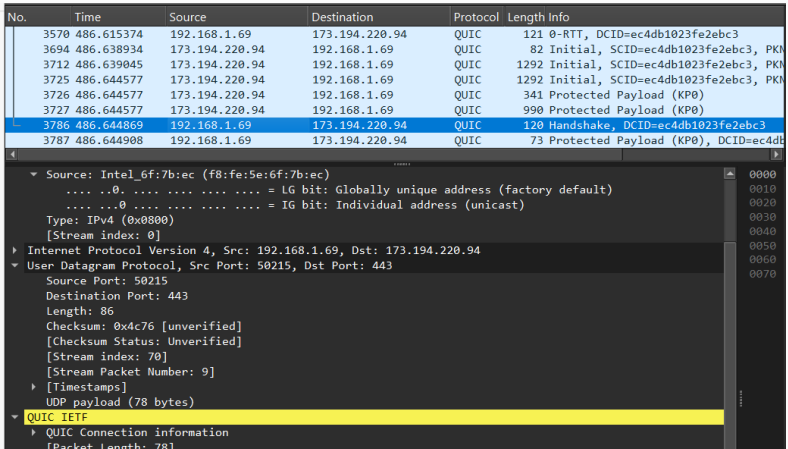
QUIC поверх UDP: Initial

Фильтр: `quic` - UDP: Src Port `443` → Dst Port `50215` - QUIC: Long Header, Packet Type: Initial - Используются Connection ID, передаётся криптографическая информация



QUIC: Handshake

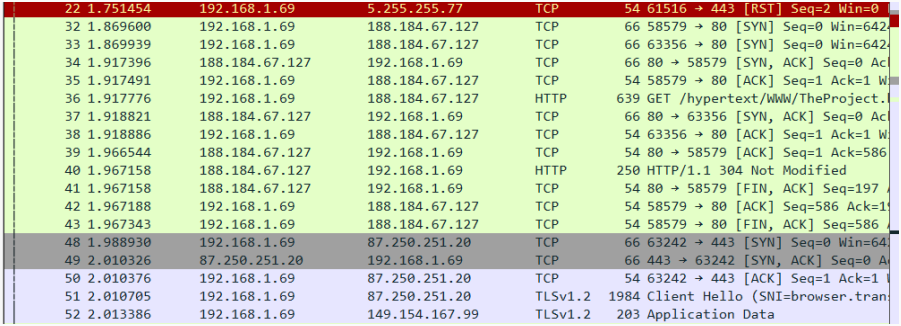
- QUIC Handshake фиксируется как отдельный тип пакета
- Часть нагрузки зашифрована (без ключей расшифровка невозможна)
- QUIC объединяет транспортные механизмы и защиту соединения



Установление TCP-соединения (3-way handshake)

Пример соединения к `188.184.67.127:80` - 1) **SYN** (клиент → сервер), Seq = 0 - 2) **SYN, ACK** (сервер → клиент), Ack = 1 - 3) **ACK** (клиент → сервер), Seq = 1, Ack = 1

Далее передаются данные (PSH, ACK) и соединение закрывается (FIN, ACK). RST фиксирует принудительное завершение отдельных попыток.

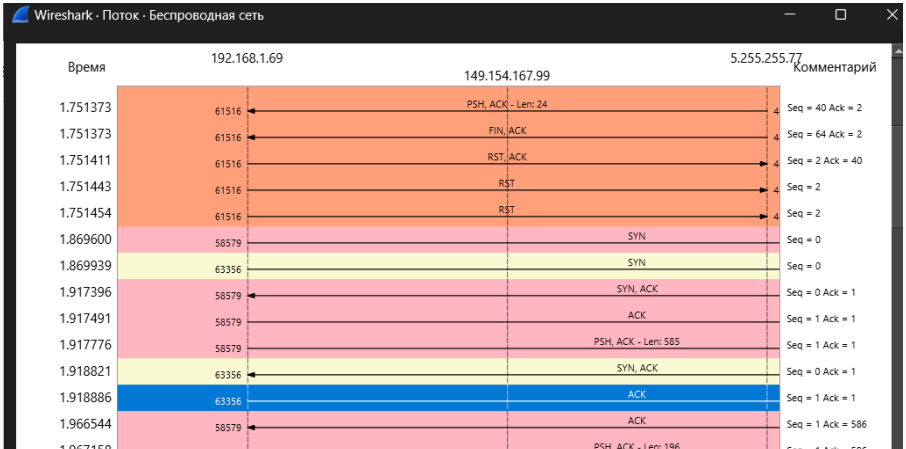


22	1.751454	192.168.1.69	5.255.255.77	TCP	54	61516 → 443 [RST] Seq=2 Win=0
32	1.869600	192.168.1.69	188.184.67.127	TCP	66	58579 → 80 [SYN] Seq=0 Win=642
33	1.869939	192.168.1.69	188.184.67.127	TCP	66	63356 → 80 [SYN] Seq=0 Win=642
34	1.917396	188.184.67.127	192.168.1.69	TCP	66	80 → 58579 [SYN, ACK] Seq=0 Ac
35	1.917491	192.168.1.69	188.184.67.127	TCP	54	58579 → 80 [ACK] Seq=1 Ack=1 W
36	1.917776	192.168.1.69	188.184.67.127	HTTP	639	GET /hypertext/WWW/TheProject.
37	1.918821	188.184.67.127	192.168.1.69	TCP	66	80 → 63356 [SYN, ACK] Seq=0 Ac
38	1.918886	192.168.1.69	188.184.67.127	TCP	54	63356 → 80 [ACK] Seq=1 Ack=1 W
39	1.966544	188.184.67.127	192.168.1.69	TCP	54	80 → 58579 [ACK] Seq=1 Ack=586
40	1.967158	188.184.67.127	192.168.1.69	HTTP	250	HTTP/1.1 304 Not Modified
41	1.967158	188.184.67.127	192.168.1.69	TCP	54	80 → 58579 [FIN, ACK] Seq=197
42	1.967188	192.168.1.69	188.184.67.127	TCP	54	58579 → 80 [ACK] Seq=586 Ack=1
43	1.967343	192.168.1.69	188.184.67.127	TCP	54	58579 → 80 [FIN, ACK] Seq=586
48	1.988930	192.168.1.69	87.250.251.20	TCP	66	63242 → 443 [SYN] Seq=0 Win=64
49	2.010326	87.250.251.20	192.168.1.69	TCP	66	443 → 63242 [SYN, ACK] Seq=0 A
50	2.010376	192.168.1.69	87.250.251.20	TCP	54	63242 → 443 [ACK] Seq=1 Ack=1
51	2.010705	192.168.1.69	87.250.251.20	TLSv1.2	1984	Client Hello (SNI=browser.tran
52	2.013386	192.168.1.69	149.154.167.99	TLSv1.2	203	Application Data

Рис. 16: TCP handshake в списке пакетов

График потока (Flow Graph)

- Наглядно отображены этапы `SYN → SYN,ACK → ACK`
- Видны направления обмена, рост Seq/Ack
- Отражены PSH/ACK при передаче данных и FIN/ACK при закрытии



Итоговые выводы

Заключение

- Определены параметры сетевого подключения (IP/шлюз/DNS/MAC) и подтверждена связность с шлюзом.
- Проанализированы ARP и ICMP: показаны IP↔MAC соответствия и отличие L2-доставки в локальной сети и при выходе во внешние сети.
- Рассмотрены HTTP (TCP), DNS (UDP), QUIC (UDP): выявлены различия в доставке данных и служебных механизмах.
- На практике подтверждён механизм TCP handshake и интерпретация Seq/Ack по графику потока Wireshark.