

# 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

```
C:\Users\Ebrahim Alkamal>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter vEthernet (Default Switch):

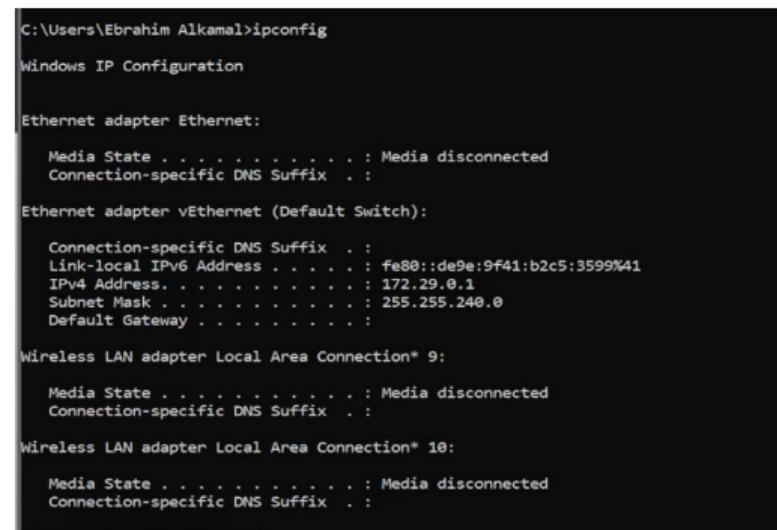
    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::de9e:9f41:b2c5:3599%41
    IPv4 Address. . . . . : 172.29.0.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
```



# 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

```
Ethernet adapter vEthernet (Default Switch):
  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Hyper-V Virtual Ethernet Adapter
  Physical Address . . . . . : 00-15-5D-46-67-91
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::de9e:9f41:b2c5:3599%41(Preferred)
    IPv4 Address . . . . . : 172.29.0.1(PREFERRED)
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 
    DHCPv6 IAID . . . . . : 687871325
    DHCPv6 Client DUID . . . . . : 00-01-00-01-30-A7-B7-80-88-BF-B8-C3-AD-EE
    NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection® 9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
  Physical Address . . . . . : DC-46-28-6C-92-D4
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection® 10:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
  Physical Address . . . . . : DE-46-28-6C-92-D3
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
```



## 4 Анализ MAC-адреса

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

# 5 Запуск захвата в Wireshark

- Выбран беспроводной интерфейс
- Запущен захват трафика

The screenshot shows the Wireshark interface capturing traffic from a wireless interface. The main window displays a list of network frames, each with columns for number, time, source, destination, protocol, and length/info. The frames are color-coded by protocol: TCP (black), ARP (yellow), MDNS (light blue), ICMPv6 (pink), and Broadcast (orange). The list includes several frames from the local host (172.16.36.21) and other devices on the network (e.g., CenturyXinya, Apple\_3c:70:62, AzureWaveTec\_0b:da:...). The bottom pane shows the raw hex and ASCII representations of frame 1.

No.	Time	Source	Destination	Protocol	Length Info
84	3.769704	172.16.36.21	57.128.101.86	TCP	379 [TCP Retransmission]
85	3.796870	CenturyXinya_b6:b2:...	Broadcast	ARP	60 Who has 172.16.37.1?
86	3.798054	172.16.36.71	224.0.0.251	MDNS	513 Standard query respo
87	4.334648	fe80::104e:5549:204...	ff02::2	ICMPv6	62 Router Solicitation
88	4.403533	fe80::d4c5:c6ff:fee...	ff02::2	ICMPv6	70 Router Solicitation
89	4.418824	TpLinkTechno_59:a2:...	Broadcast	ARP	60 Who has 192.168.0.10
90	4.419048	Apple_3c:70:62	Broadcast	ARP	60 Who has 192.168.0.10
91	4.820657	Apple_3c:70:62	Broadcast	ARP	60 Who has 192.168.0.10
92	4.978788	172.16.36.21	57.128.101.86	TCP	379 [TCP Retransmission]
93	5.229768	172.16.37.18	224.0.0.251	MDNS	150 Standard query respo
94	5.232235	172.16.37.24	224.0.0.251	MDNS	172 Standard query 0x000
95	5.435728	Apple_3c:70:62	Broadcast	ARP	60 ARP Announcement for
96	5.436055	172.16.37.24	224.0.0.251	MDNS	172 Standard query 0x000
97	5.640150	172.16.36.71	224.0.0.251	MDNS	224 Standard query 0x000
98	5.640546	172.16.36.164	224.0.0.251	MDNS	119 Standard query 0x02a
99	5.745641	AzureWaveTec_0b:da:...	Broadcast	ARP	60 Who has 172.16.37.77
100	5.746088	172.16.37.24	224.0.0.251	MDNS	172 Standard query 0x000
101	5.746540	172.16.37.24	224.0.0.251	MDNS	224 Standard query respo
102	5.746715	Apple_3c:70:62	Broadcast	ARP	60 ARP Announcement for
103	5.747020	Apple_3c:70:62	Broadcast	ARP	60 Who has 192.168.0.1?
104	5.845742	192.168.0.108	224.0.0.251	MDNS	308 Standard query respo
105	5.847178	172.16.36.71	224.0.0.251	MDNS	513 Standard query respo
106	6.051968	192.168.0.108	224.0.0.251	MDNS	371 Standard query 0x000

## 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

No.	Time	Source	Destination	Protocol	Length Info
→ 2426	99.153431	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x
← 2427	99.163946	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x
2446	100.169943	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x
2447	100.173940	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x
2468	101.176118	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x
2461	101.177656	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x
2487	102.184719	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x
2488	102.185819	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x

# 8 ICMP Echo Reply

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

No.	Time	Source	Destination	Protocol	Length Info
→	2426 99.153431	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x0001, seq=171/43776, ttl=128 (reply in 2)
←	2427 99.163946	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x0001, seq=171/43776, ttl=254 (request in)
	2446 100.169943	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x0001, seq=172/44032, ttl=128 (reply in 2)
	2447 100.173948	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x0001, seq=172/44032, ttl=254 (request in)
	2460 101.176118	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x0001, seq=173/44288, ttl=128 (reply in 2)
	2461 101.177656	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x0001, seq=173/44288, ttl=254 (request in)
	2487 102.184719	172.16.36.21	172.16.36.1	ICMP	74 Echo (ping) request id=0x0001, seq=174/44544, ttl=128 (reply in 2)
	2488 102.185819	172.16.36.1	172.16.36.21	ICMP	74 Echo (ping) reply id=0x0001, seq=174/44544, ttl=254 (request in)

Encapsulation type: Ethernet (1)  
Arrival Time: Dec 17, 2025 03:38:55.603354000 Russia TZ 2 Standard Time  
UTC Arrival Time: Dec 17, 2025 00:38:55.603354000 UTC  
Epoch Arrival Time: 1765931935.603354000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 10.515000 milliseconds]  
[Time delta from previous displayed frame: 10.515000 milliseconds]  
[Time since reference or first frame: 1 minute, 39.163946000 seconds]  
Frame Number: 2427  
Frame Length: 74 bytes (592 bits)  
Capture Length: 74 bytes (592 bits)  
[Frame is marked: False]  
[Frame is broadcast: False]

0000 dc 46 28 6c 92 d3 70 18 a7 60 9c d2 08 00  
0010 00 3c 1f 8c 00 00 fe 01 fc fd ac 10 24 00  
0020 24 15 00 00 54 b0 00 01 00 ab 61 62 63 64  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74  
0040 77 61 62 63 64 65 66 67 68 69

# 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**

No.	Time	Source	Destination	Protocol	Length	Info
2380	94.728393	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2387	95.444754	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2396	96.467621	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2414	98.107765	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2424	98.927382	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2428	99.233045	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2437	99.846857	TpLinkTechno_59:94:..	Broadcast	ARP	60	ARP Announce
2439	99.949236	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2440	99.949333	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2443	100.053753	Cisco_60:9c:d2	Broadcast	ARP	60	Who has 172.16
2449	100.257783	TpLinkTechno_59:8b:..	Broadcast	ARP	60	ARP Announce
2455	100.974190	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2457	100.974993	fe:0d:91:28:6d:1c	Broadcast	ARP	60	Who has 172.16
2484	101.896996	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2494	103.125610	TpLinkTechno_59:94:..	Broadcast	ARP	60	ARP Announce
2495	103.435867	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2525	104.455252	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2546	105.401597	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2548	105.402609	Cisco_60:9c:d2	Broadcast	ARP	60	Who has 172.16
2570	106.814387	AzureWaveTec_0b:da:..	Broadcast	ARP	60	Who has 172.16
2573	107.117171	Cisco_60:9c:d2	Broadcast	ARP	60	Who has 172.16

## 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

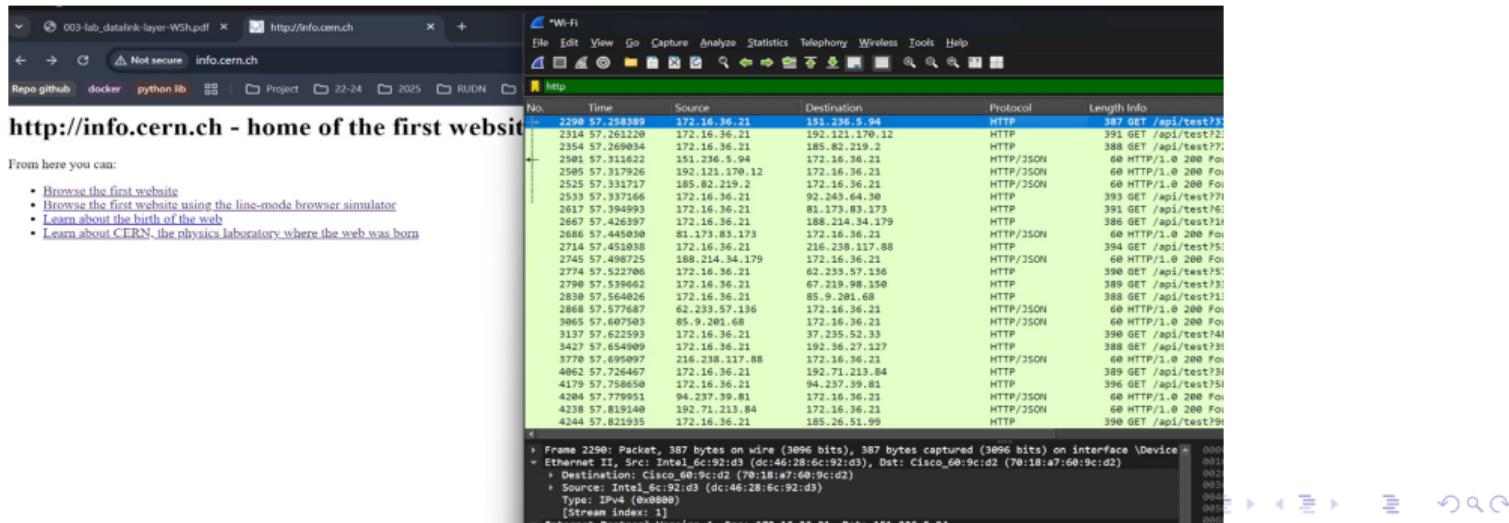
- Захвачены только Echo Request
- Echo Reply отсутствуют
- Возможные причины:
  - блокировка ICMP
  - межсетевой экран
  - политики безопасности

No.	Time	Source	Destination	Protocol	Length Info
120	9.625003	172.16.36.21	37.18.93.135	ICMP	74 Echo (ping) request
169	14.400260	172.16.36.21	37.18.93.135	ICMP	74 Echo (ping) request
294	19.407026	172.16.36.21	37.18.93.135	ICMP	74 Echo (ping) request
360	24.393133	172.16.36.21	37.18.93.135	ICMP	74 Echo (ping) request



## 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



# 13 HTTP Response

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

No.	Time	Source	Destination	Protocol	Length Info
2290	57.258389	172.16.36.21	151.236.5.94	HTTP	387 GET /api/test?3
2314	57.261220	172.16.36.21	192.121.170.12	HTTP	391 GET /api/test?2
2354	57.269034	172.16.36.21	185.82.219.2	HTTP	388 GET /api/test?7
2501	57.311622	151.236.5.94	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
2505	57.317926	192.121.170.12	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
2525	57.331717	185.82.219.2	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
2533	57.337166	172.16.36.21	92.243.64.30	HTTP	393 GET /api/test?7
2617	57.394993	172.16.36.21	81.173.83.173	HTTP	391 GET /api/test?6
2667	57.426397	172.16.36.21	188.214.34.179	HTTP	386 GET /api/test?1
2686	57.445030	81.173.83.173	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
2714	57.451038	172.16.36.21	216.238.117.88	HTTP	394 GET /api/test?5
2745	57.498725	188.214.34.179	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
2774	57.522706	172.16.36.21	62.233.57.136	HTTP	390 GET /api/test?5
2798	57.539662	172.16.36.21	67.219.98.150	HTTP	389 GET /api/test?3
2830	57.564026	172.16.36.21	85.9.201.68	HTTP	388 GET /api/test?1
2868	57.577687	62.233.57.136	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
3065	57.607503	85.9.201.68	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
3137	57.622593	172.16.36.21	37.235.52.33	HTTP	399 GET /api/test?4
3427	57.654909	172.16.36.21	192.36.27.127	HTTP	388 GET /api/test?3
3770	57.695097	216.238.117.88	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
4062	57.726467	172.16.36.21	192.71.213.84	HTTP	389 GET /api/test?3
4179	57.758650	172.16.36.21	94.237.39.81	HTTP	396 GET /api/test?5
4204	57.779951	94.237.39.81	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
4238	57.819140	192.71.213.84	172.16.36.21	HTTP/JSON	60 HTTP/1.0 200 Fo
4244	57.821935	172.16.36.21	185.26.51.99	HTTP	390 GET /api/test?9

# 14 DNS (UDP)

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

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	57.2777503	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

No.	Time	Source	Destination	Protocol	Length Info
2352	57.268791	8.8.4.4	172.16.36.21	QUIC	64 Protected Payload
2355	57.269638	8.8.4.4	172.16.36.21	QUIC	572 Protected Payload
2356	57.269638	8.8.4.4	172.16.36.21	QUIC	64 Protected Payload
2357	57.269738	172.16.36.21	8.8.4.4	QUIC	77 Protected Payload
2362	57.270997	172.16.36.21	8.47.69.6	QUIC	1292 Initial, DCID=71
2363	57.271028	172.16.36.21	8.47.69.6	QUIC	1292 Initial, DCID=71
2368	57.274005	172.16.36.21	34.160.212.61	QUIC	74 Protected Payload
2372	57.275133	8.8.4.4	172.16.36.21	QUIC	571 Protected Payload
2374	57.275316	172.16.36.21	8.8.4.4	QUIC	77 Protected Payload
2375	57.275452	8.8.4.4	172.16.36.21	QUIC	64 Protected Payload
2376	57.275452	8.8.4.4	172.16.36.21	QUIC	571 Protected Payload
2377	57.275452	8.8.4.4	172.16.36.21	QUIC	64 Protected Payload
2378	57.275538	172.16.36.21	8.8.4.4	QUIC	77 Protected Payload
2387	57.277840	172.16.36.21	8.8.4.4	QUIC	259 Protected Payload
2388	57.277879	172.16.36.21	8.8.4.4	QUIC	253 Protected Payload
2413	57.282401	8.47.69.6	172.16.36.21	QUIC	1242 Initial, SCID=0
2421	57.283128	8.47.69.6	172.16.36.21	QUIC	1242 Initial, SCID=0
2426	57.284845	8.47.69.6	172.16.36.21	QUIC	1242 Initial, SCID=0
2427	57.285153	8.47.69.6	172.16.36.21	QUIC	1242 Initial, SCID=0
2430	57.285320	172.16.36.21	8.47.69.6	QUIC	1292 Initial, DCID=0
2434	57.286745	8.8.4.4	172.16.36.21	QUIC	65 Protected Payload
2441	57.288891	172.16.36.21	64.233.162.94	QUIC	75 Protected Payload
2458	57.292948	8.8.4.4	172.16.36.21	QUIC	65 Protected Payload
2454	57.293969	172.16.36.21	8.47.69.6	QUIC	91 Handshake, DCID=0

# 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

No.	Time	Source	Destination	Protocol	Length Info	Content
1993	00:00:00.018	172.16.36.200	51.159.226.221	TCP	66 49908 + 443	[SYN] Seq# 0 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
1995	00:00:00.045	51.159.226.221	172.16.36.200	TCP	66 443 + 49177	[SYN ACK] Seq# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM NS=128
2000	00:00:00.053	172.16.36.200	51.159.226.221	TCP	66 443 + 49177	[SYN ACK] Seq# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2052	01:56:46.016	51.159.226.221	172.16.36.200	TCP	66 443 + 57266	[SYN ACK] Seq# 0 Win=64240 Len=0 MSS=1460 Wo=256 SACK_PERM
2244	01:57:31.759	172.16.36.200	104.208.16.90	TCP	66 57267 + 443	[SYN] Seq# 0 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2251	01:56:46.728	104.208.16.90	172.16.36.200	TCP	66 443 + 57267	[SYN, ACK] Seq# 0 Ack# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2260	01:56:57.534	172.16.36.200	51.159.226.221	TCP	66 [TCP Port numbers reused] 63626 + 443 [SYN] Seq# 0 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM	
2308	01:56:57.535	51.159.226.221	172.16.36.200	TCP	66 443 + 49177	[SYN ACK] Seq# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2308	01:57:57.958	172.16.36.200	51.159.226.221	TCP	66 49177 + 443	[SYN ACK] Seq# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2309	01:57:57.959	51.159.226.221	172.16.36.200	TCP	66 443 + 49177	[SYN ACK] Seq# 0 Ack# 1 Win=64240 Len=0 MSS=1460 SACK_PERM NS=128
2500	06:55:35.847	172.16.36.200	104.208.16.90	TCP	66 49178 + 443	[SYN] Seq# 0 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2513	06:56:49.902	104.208.16.90	172.16.36.200	TCP	66 443 + 49178	[SYN, ACK] Seq# 0 Ack# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2843	06:39:31.912	172.16.36.200	52.187.143.210	TCP	66 49179 + 443	[SYN] Seq# 0 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
2843	06:39:49.002	52.187.143.210	172.16.36.200	TCP	66 443 + 49179	[SYN, ACK] Seq# 0 Ack# 1 Win=65535 Len=0 MSS=1460 Wo=256 SACK_PERM
- Internal Protocol Version 4, Src: 172.16.36.200, Dst: 51.159.226.221						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (\$)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not ECN)						
Time to Live: 128						
Identification: 0x0004 (8192)						
0100 .... = Flags: 0x2, Don't fragment						
.... 0000 0000 0000 = Fragment Offset: 0						
Time to Live: 128						
Protocol: 6 (TCP)						
Header Checksum: 0x0000 [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.36.200						
Destination Address: 51.159.226.221						
[String length: 0]						
+ Transmission Control Protocol, Src Port: 62626, Dst Port: 443, Seq: 0, Len: 0						
Source Port: 62626						
Destination Port: 443						
[Stream index: 75]						
[Stream Packet Number: 1]						
Flow Label: 0x00000000 [Incomplete, DATA (15)]						
[TCP Segment Len: 0]						
Sequence Number: 0 (relative sequence number)						
Sequence Number (raw): 3174251690						
[Next Sequence Number: 1 (relative sequence number)]						
Acknowledgment Number: 0						
Acknowledgment number (raw): 0						
1000 .... = Header Length: 32 bytes (\$)						
+ Flags: 0x0002 (SYN)						
Window: 0x0035						
[Window scale: 0, Window size: 65535]						
Checksum: 0x7770 [Unverified]						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
+ Options: (32 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted						

# 18 Handshake: SYN + ACK

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

No.	Time	Source	Destination	Protocol	Length Info	Content
1993	50.038018	172.16.36.200	51.159.226.221	TCP	66 49988 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
1995	50.074501	51.159.226.221	172.16.36.200	TCP	66 443 - 49988 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
2051	51.202363	172.16.36.200	51.159.226.221	TCP	66 57266 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2052	51.206816	51.159.226.221	172.16.36.200	TCP	66 443 - 57266 [SYN, ACK] Seq=0 Ack=2 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
2244	56.317359	172.16.36.200	184.208.16.98	TCP	66 57267 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2251	56.467278	104.208.16.98	172.16.36.200	TCP	66 443 - 57267 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2288	57.534356	172.16.36.200	51.159.226.221	TCP	66 [TCP Port numbers reused] 62626 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2281	57.576688	51.159.226.221	172.16.36.200	TCP	66 443 - 62626 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
2308	57.797072	172.16.36.200	51.159.226.221	TCP	66 49177 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2309	57.848942	51.159.226.221	172.16.36.200	TCP	66 443 - 49177 [SYN, ACK] Seq=0 Ack=2 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
2500	66.336347	172.16.36.200	184.208.16.98	TCP	66 49178 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2513	66.499306	104.208.16.98	172.16.36.200	TCP	66 443 - 49178 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM	
2843	76.339192	172.16.36.200	52.182.143.210	TCP	66 49179 - 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2854	76.498662	52.182.143.210	172.16.36.200	TCP	66 443 - 49179 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM	

> Frame 2281: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{E359510C-48F6-4AEB-9C05-07AA4CA7FAF54}, id 0  
  > Ethernet II, Src: Cisco\_60:9c:d2 (7e:08:a7:60:9c:d2), Dst: Intel\_6c:92:d3 (dc:46:28:6c:92:d3)

> Internet Protocol Version 4, Src: 51.159.226.221, Dst: 172.16.36.200

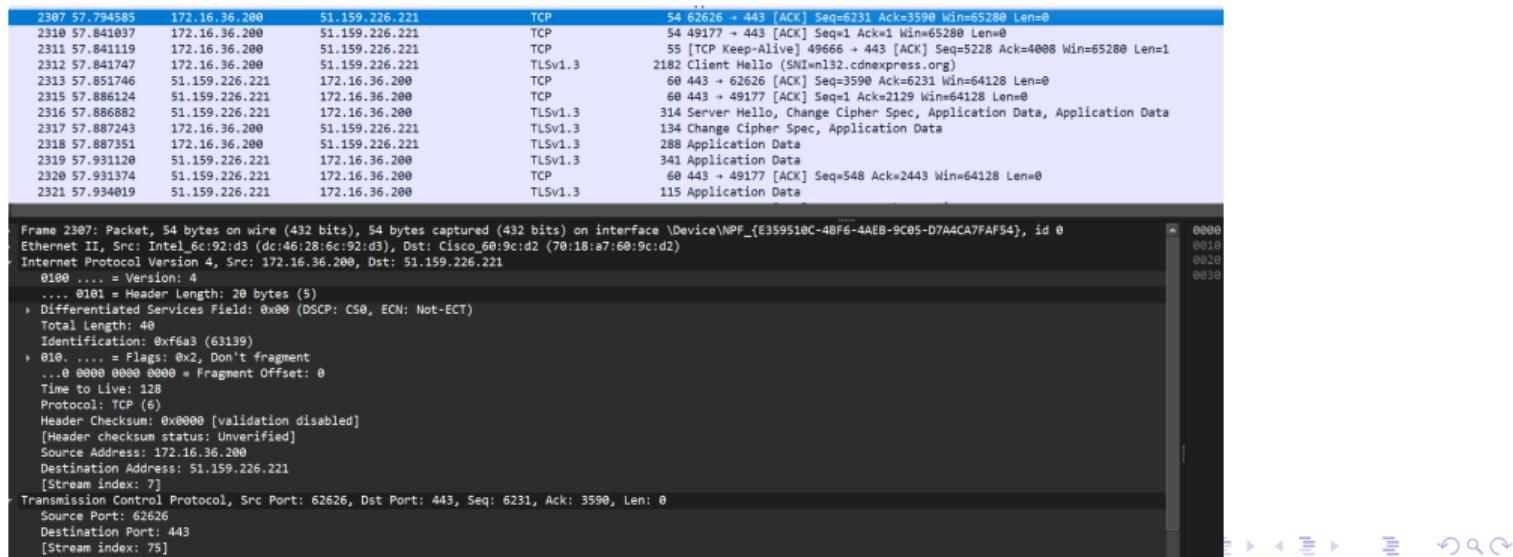
> Transmission Control Protocol, Src Port: 443, Dst Port: 62626, Seq: 0, Ack: 1, Len: 0

    Source Port: 443  
    Destination Port: 62626  
    [Stream index: 75]  
    [Stream Packet Number: 2]  
    [Conversation completeness: Incomplete, DATA (15)]  
    [TCP Segment Len: 0]  
    Sequence Number: 0 (relative sequence number)  
    Sequence Number (raw): 998569983  
    [Next Sequence Number: 1 (relative sequence number)]  
    Acknowledgment Number: 1 (relative ack number)  
    Acknowledgment number (raw): 3174253691  
    1000 ... z Header Length: 32 bytes (8)  
    Flags: 0x012 (SYN, ACK)  
    Window: 64240  
    [Calculated window size: 64240]  
    Checksum: 0x7778 [unverified]  
    [Checksum Status: Unverified]  
    Urgent Pointer: 0  
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale  
    [Timestamps]  
    [SEQ/ACK analysis]  
    [Client Contiguous Streams: 1]  
    [Server Contiguous Streams: 1]

# 19 Handshake: ACK

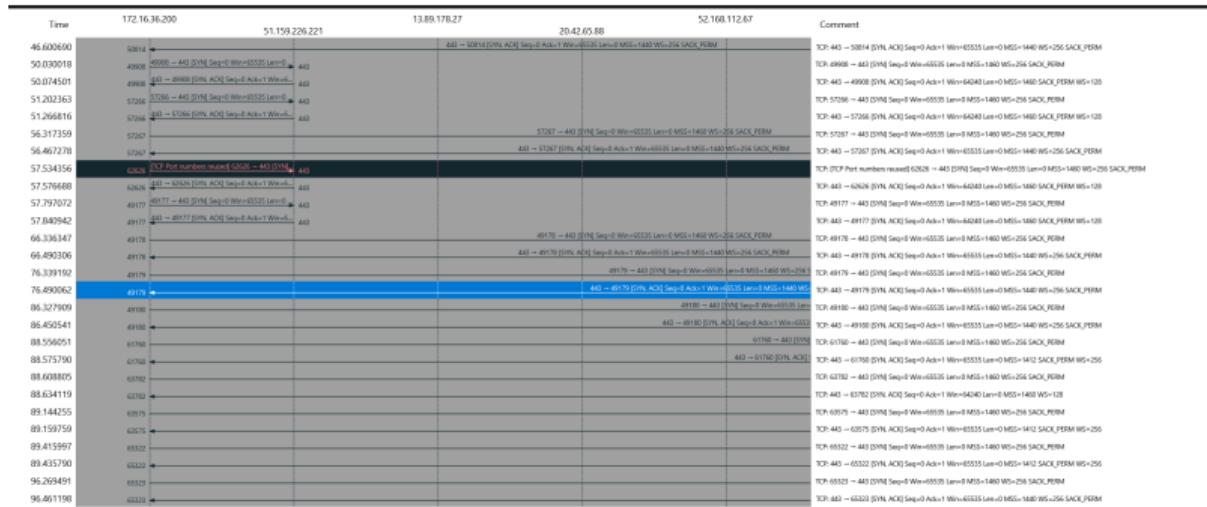
- Клиент → сервер
- Флаг: **ACK**
- Sequence Number = 6231
- Acknowledgment Number = 3590
- Соединение установлено

Frame	Source IP	Destination IP	Protocol	Sequence Number	Acknowledgment Number	Flags	Length
2307	57.794585	172.16.36.200	TCP	51.159.226.221	54 62626	→ 443 [ACK] Seq=6231 Ack=3590 Win=65280 Len=0	
2310	57.841037	172.16.36.200	TCP	51.159.226.221	54 49177	→ 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0	
2311	57.841119	172.16.36.200	TCP	51.159.226.221	55	[TCP Keep-Alive] 49666 → 443 [ACK] Seq=5228 Ack=4008 Win=65280 Len=1	
2312	57.841747	172.16.36.200	TLSv1.3	51.159.226.221	2182	Client Hello (SNI=m132.cdneexpress.org)	
2313	57.851746	51.159.226.221	TCP	172.16.36.200	60 443	→ 62626 [ACK] Seq=3590 Ack=6231 Win=64128 Len=0	
2315	57.886124	51.159.226.221	TCP	172.16.36.200	60 443	→ 49177 [ACK] Seq=1 Ack=129 Win=64128 Len=0	
2316	57.886882	51.159.226.221	TLSv1.3	172.16.36.200	314	Server Hello, Change Cipher Spec, Application Data, Application Data	
2317	57.887243	172.16.36.200	TLSv1.3	51.159.226.221	134	Change Cipher Spec, Application Data	
2318	57.887351	172.16.36.200	TLSv1.3	51.159.226.221	288	Application Data	
2319	57.931120	51.159.226.221	TLSv1.3	172.16.36.200	341	Application Data	
2320	57.931374	51.159.226.221	TCP	172.16.36.200	60 443	→ 49177 [ACK] Seq=548 Ack=2443 Win=64128 Len=0	
2321	57.934019	51.159.226.221	TLSv1.3	172.16.36.200	115	Application Data	

# 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

### 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