

# Лабораторная работа №3

Анализ трафика в Wireshark

---

Авдадаев Джамал Геланиевич

09 февраля 2026

## Цель работы

---

Изучение кадров Ethernet и анализ протоколов различных уровней стека TCP/IP с использованием Wireshark:

- канального уровня (ARP, Ethernet)
- сетевого уровня (ICMP)
- транспортного уровня (TCP, UDP, QUIC)
- прикладного уровня (HTTP, DNS)

## Ход выполнения

---

# Захват ARP и ICMP

- Выбран активный сетевой интерфейс
- Запущен захват трафика
- Использован фильтр:  
`arp or icmp`
- Выполнен `ping` шлюза по умолчанию

```
C:\Users\avdad>ping 172.20.10.1

Обмен пакетами с 172.20.10.1 по с 32 байтами данных:
Ответ от 172.20.10.1: число байт=32 время=2мс TTL=64
Ответ от 172.20.10.1: число байт=32 время=2мс TTL=64
Ответ от 172.20.10.1: число байт=32 время=2мс TTL=64
Ответ от 172.20.10.1: число байт=32 время=2мс TTL=64

Статистика Ping для 172.20.10.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек

C:\Users\avdad>ping www.rudn.ru

Обмен пакетами с www.rudn.ru [37.18.93.135] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 37.18.93.135:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)
```

# ICMP: эхо-запрос

- Длина кадра: 74 байта
- Тип: Ethernet II
- MAC источника — локальный компьютер
- MAC назначения — шлюз
- Тип адресации: unicast

The screenshot displays the Wireshark interface with a packet capture on the 'Беспроводная сеть' (Wireless network) interface. The packet list shows several ICMP Echo (ping) requests and replies between the local machine (172.20.10.1) and a remote host (172.20.10.2). The selected packet is a ping request (Frame 1337).

No.	Time	Source	Destination	Protocol	Length	Info
339	91.373618	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	Who has 172.20.10.2? Tell 172.20.10.1
341	91.373657	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	172.20.10.2 is at b4:8c:9d:83:b6:67
372	98.788325	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2
373	98.790910	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	172.20.10.1 is at 82:96:98:0a:49:64
730	177.403586	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	Who has 172.20.10.2? Tell 172.20.10.1
172	177.403623	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	172.20.10.2 is at b4:8c:9d:83:b6:67
1286	255.826082	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	Who has 172.20.10.2? Tell 172.20.10.1
1288	255.826088	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	172.20.10.2 is at b4:8c:9d:83:b6:67
1337	269.790786	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=64 (reply in 1338)
1338	269.793184	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=64 (request in 1337)
1339	270.799162	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=64 (reply in 1340)
1340	270.801615	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=64 (request in 1339)
1345	271.809238	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 1346)
1346	271.811630	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 1345)
1349	272.813759	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 1350)
1350	272.816056	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 1349)

Detailed view of Frame 1337 (Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...):

- Ethernet II, Src: AzureWaveTec\_83:b6:67 (b4:8c:9d:83:b6:67), Dst: 82:96:98:0a:49:64 (82:96:98:0a:49:64)
- Destination: 82:96:98:0a:49:64 (82:96:98:0a:49:64)
- Source: AzureWaveTec\_83:b6:67 (b4:8c:9d:83:b6:67)
- Type: IPv4 (0x0800)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 60
  - Identification: 0x05a3 (1443)
  - 000. .... = Flags: 0x0
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 64
  - Protocol: ICMP (1)
  - Header [Checksum: 0] (Checksum validation disabled)

# ICMP: эхо-ответ

- Источник — шлюз
- Получатель — локальный ПК
- Передача по Ethernet II
- Подтверждение работоспособности сети

The screenshot displays the Wireshark network traffic analysis tool. The top pane shows a list of captured packets, with packet 1338 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
339	91.373618	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	Who has 172.20.10.2? Tell 172.20.10.1
341	91.373657	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	172.20.10.2 is at b4:8c:9d:83:b6:67
372	98.798325	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2
373	98.798939	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	172.20.10.1 is at 82:96:98:0a:49:64
730	177.403586	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	Who has 172.20.10.2? Tell 172.20.10.1
732	177.403623	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	172.20.10.2 is at b4:8c:9d:83:b6:67
1280	255.826842	82:96:98:0a:49:64	AzureWaveTec_83:b6:67	ARP	42	Who has 172.20.10.2? Tell 172.20.10.1
1288	255.826868	AzureWaveTec_83:b6:67	82:96:98:0a:49:64	ARP	42	172.20.10.2 is at b4:8c:9d:83:b6:67
1337	269.750746	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=64 (reply in 1338)
1338	269.751284	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=64 (request in 1337)
1339	270.799102	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=64 (reply in 1340)
1340	270.801615	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=64 (request in 1339)
1345	271.809238	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 1346)
1346	271.811630	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 1345)
1349	272.823759	172.20.10.2	172.20.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 1350)
1350	272.826896	172.20.10.1	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 1349)

**Packet 1338 Details:**

- Frame 1338: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{...}
- Ethernet II, Src: 82:96:98:0a:49:64 (82:96:98:0a:49:64), Dst: AzureWaveTec\_83:b6:67 (b4:8c:9d:83:b6:67)
- Destination: AzureWaveTec\_83:b6:67 (b4:8c:9d:83:b6:67)
- Source: 82:96:98:0a:49:64 (82:96:98:0a:49:64)
- Type: IPv4 (0x0000)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2
- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0x214c (8524)
- 000. .... = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: ICMP (1)
- Header checksum: 0xad49 [validation disabled]
- [Header checksum status: Unverified]

**Raw Data:**

```
0000  b4 8c 9d 83 b6 67 32 96 98 0a 49 64 00 00 45 00  ....g...Id:E-
0010  00 3c 21 4c 00 00 40 01 ed 49 ac 14 8a 01 ac 14  <Id:g...I....
0020  0a 82 00 00 55 4a 00 01 00 04 63 62 63 64 65 66  ..U...abcde
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmnopqr
0040  77 61 62 63 64 65 66 67 68 69                      uvwdefghi
```

# Анализ ARP

- ARP-запрос отправляется широковещательно
- ARP-ответ передаётся на конкретный MAC
- Выполняется сопоставление IP ↔ MAC

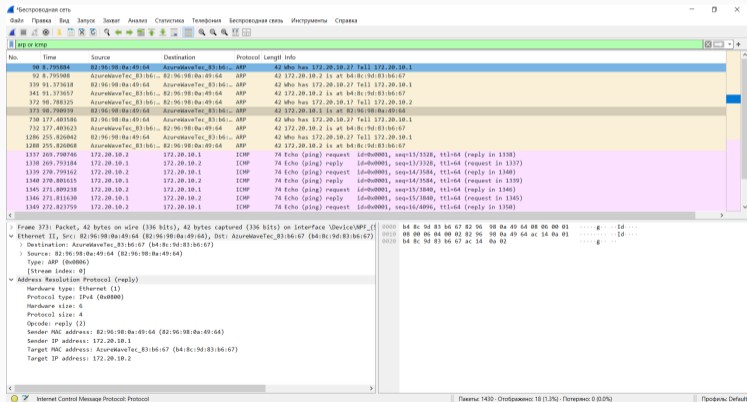
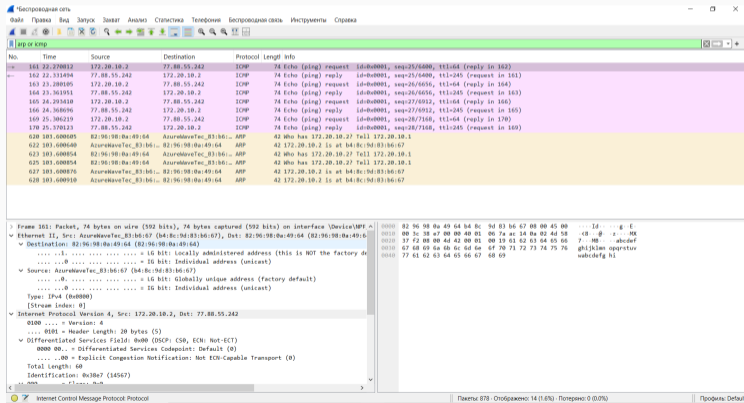


Рис. 4: ARP-трафик

## Работа с удалёнными узлами

- ICMP-пакеты направляются на MAC шлюза
- Далее маршрутизация выполняется на сетевом уровне
- Адресация остаётся unicast



# HTTP и TCP

- HTTP работает поверх TCP
- Клиент отправляет GET-запрос
- Используется порт 80
- Передача данных после установки соединения

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of captured packets, with packet 444 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
444	53.8261392	172.20.10.2	146.75.122.172	HTTP	336	GET /msdownload/update/v5/static/trustedr/en/pinruless1.cab?1738688828c5eb1 HTTP/1.1
446	53.109983	146.75.122.172	172.20.10.2	HTTP	257	HTTP/1.1 304 Not Modified
455	53.343700	172.20.10.2	204.79.197.203	GET	472	GET /ocsp/PFQwJlDQMEduTDARgigOgCgJABRQJL132132F-a6ADKBRwY2GKxVaYvHG4QUB645282v52EXQJ1s02d33c7H7YHhQJCTjPAAAGhC3PMv6sAAAAAAAY..
458	53.452929	204.79.197.203	172.20.10.2	OCSP	197	Response

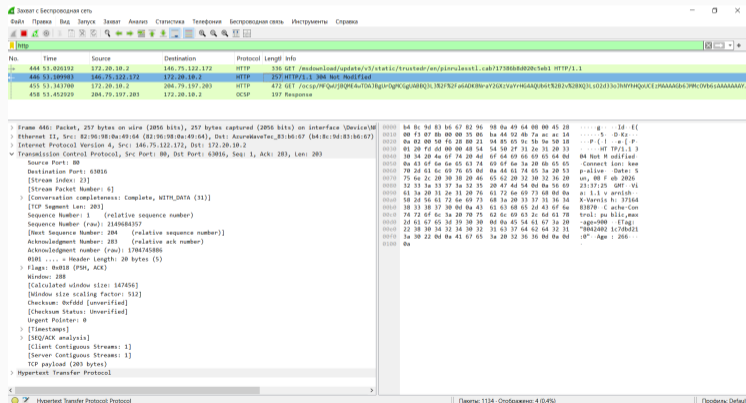
**Packet 444 Details:**

- Ethernet II, Src: AzureWaveTc\_83:b6:67 (b4:8c:94:83:b6:67), Dst: 82:96:98:0a:49:64 (82:96:98:0a:49:64)
- Internet Protocol Version 4, Src: 172.20.10.2, Dst: 146.75.122.172
- Transmission Control Protocol, Src Port: 63916, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
- Source Port: 63916
- Destination Port: 80
- [Stream index: 23]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 282]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1704745604
- [Next Sequence Number: 283 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 2149084597
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 512
- [Calculated window size: 131872]
- [Window size scaling factor: 256]
- Checksum: 0ad053 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- [Client Contiguous Streams: 1]
- [Server Contiguous Streams: 1]
- TCP payload (282 bytes)
- Hypertext Transfer Protocol

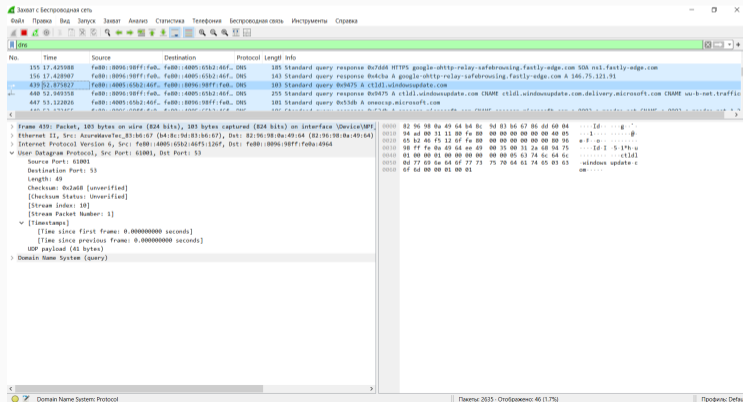
**Raw Data:**

```
0000 82 96 98 0a 49 64 b4 8c 9d 83 b6 67 08 00 45 00 ...Id...g:E-
0010 01 42 f5 df 40 00 40 06 80 c8 ac 14 0a 02 52 4b 8-@-...K
0020 7a ac fc 28 00 50 65 9c 5a 84 80 21 94 85 50 18 z:(Pe 2:1:P
0030 02 00 d0 35 00 00 47 45 54 20 2f 6d 73 64 6f 77 --3-GE T/msdown
0040 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 76 33 2f nload/up data/v3/
0050 73 74 61 74 69 65 2f 74 72 75 75 74 65 64 72 2f static/t trusted/
0060 65 6e 2f 70 69 6e 72 75 6c 65 73 73 74 6c 2e 63 en/pinru less1.c
0070 61 62 3f 31 37 33 38 36 62 38 64 30 31 30 63 35 ab?17386 88828c5
0080 65 62 31 20 48 54 54 50 2f 31 2e 31 04 0a 43 6f ebl HTTP/1.1 (Co
0090 6e 65 63 74 69 6f 6a 3a 20 4b 65 65 70 2d 41 nnection : Keep-A
00a0 6c 69 76 65 8d 0a 41 63 63 65 70 74 3a 20 2a 2f live Ac cept: /*
00b0 2a 8d 0a 49 66 2d 4d 6f 6a 69 6e 69 05 64 2d 53 *. ;f-No diff=5
00c0 69 66 63 65 3a 20 46 72 69 2c 20 30 32 20 4a 75 Ince: Fr i, 02 Ju
00d0 6e 20 32 30 31 37 20 31 37 3a 33 39 3a 30 35 20 n 2017 1 7:39:05
00e0 47 4d 54 0d 0a 49 66 2d 4e 6f 6e 65 2d 4e 61 74 GUT: 1f:None-Put
00f0 63 68 3a 20 22 38 30 34 32 34 30 32 31 63 37 64 ch: "804 24031c7d
0100 62 64 32 31 3a 30 22 0d 0a 55 73 65 72 2d 41 67 b0210". User-Ag
0110 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 43 ent: Mikrosoft-C
0120 72 79 70 74 6f 41 50 49 2f 31 30 2a 30 0d 0a 48 cryptAPI/10.0. H
0130 6f 73 74 3a 20 63 74 6c 64 6c 2e 7f 69 6e 64 6f est: cti di.windo
0140 7f 73 75 70 64 61 74 65 2e 63 6f 6d 0d 0a 0a usupdate .com...
```

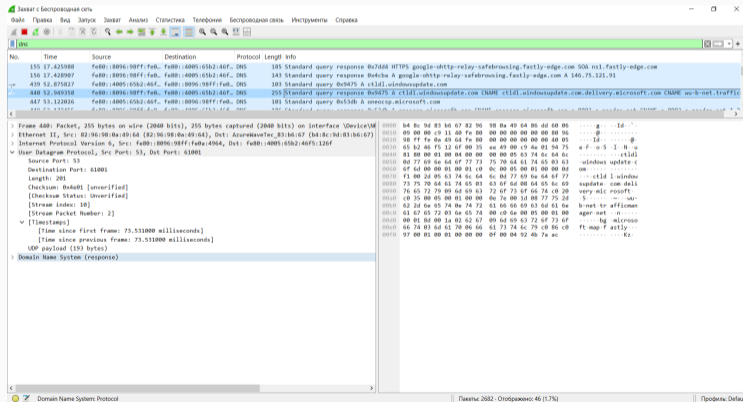
- Сервер отвечает статусом (например 304)
- Используются флаги ACK/PSH
- Передача данных в рамках установленной сессии



- DNS работает поверх UDP
- Порт назначения: 53
- Нет установления соединения
- Быстрая передача коротких сообщений



- Возвращается IP-адрес домена
- Ответ поступает с порта 53
- Минимальные накладные расходы



- Работает поверх UDP (порт 443)
- Использует шифрование
- Включает собственный handshake

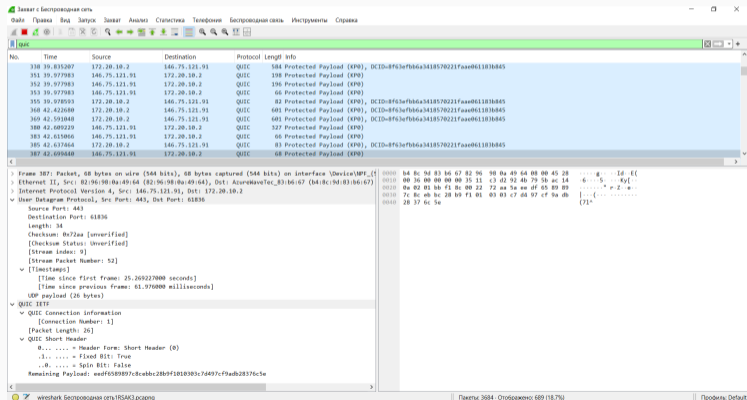


Рис. 10: QUIC-трафик

# QUIC Handshake

- Пакеты Initial и Handshake
- Согласование параметров соединения
- После установления — защищённая передача данных

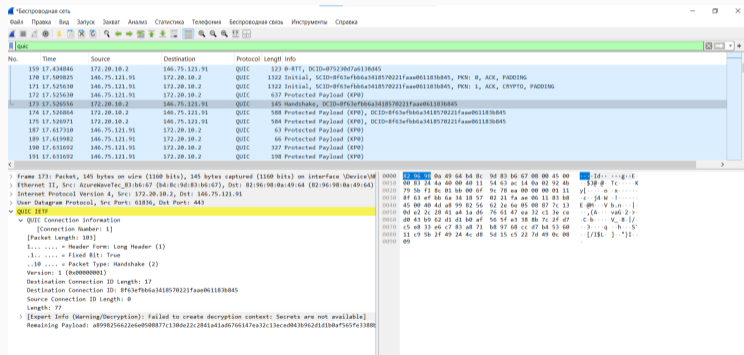


Рис. 11: QUIC handshake

# Установка соединения

## Three-way handshake:

1. SYN — запрос соединения
  2. SYN-ACK — подтверждение сервера
  3. ACK — подтверждение клиента
- Изменяются Sequence и Acknowledgment Number

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets, with the third packet (No. 271) highlighted, representing the SYN-ACK response. The packet details pane on the right shows the 'Transmission Control Protocol' section, indicating 'Seq=64039', 'Ack=1', and 'Len=0'. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
269	55.971948	172.20.10.2	8.8.8.8	DNS	83	Standard query 0x544e A ctld1.windowsupdate.com
270	55.980598	fe80::8096:98ff:fe00::0005:05b2:46f...	fe80::8096:98ff:fe00::0005:05b2:46f...	DNS	252	Standard query response 0x544e A ctld1.windowsupdate.com CHAME ctld1.windowsupdate.com.delivery.microsoft.com CHAME wu-b-net.traffic
271	55.990125	172.20.10.2	109.61.38.38	TCP	60	64039 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1680 S=256 SACK_PERM
272	56.000310	172.20.10.2	172.20.10.2	TCP	1540	[TCP Retransmission] 64039 → 80 [ACK] Seq=0 Ack=1 Win=11072 Len=0
273	56.079456	109.61.38.38	172.20.10.2	TCP	60	80 → 64039 [SYN, ACK] Seq=0 Ack=1 Win=11072 Len=0
274	56.079570	172.20.10.2	109.61.38.38	TCP	54	64039 → 80 [ACK] Seq=1 Ack=1 Win=11072 Len=0
275	56.079676	172.20.10.2	109.61.38.38	HTTP	336	GET /msdownload/update/v3/static/trusted/en/pinruleset1.cab?adddc3af5f59ec0 HTTP/1.1
276	56.081200	8.8.8.8	172.20.10.2	DNS	297	Standard query response 0x544e A ctld1.windowsupdate.com CHAME ctld1.windowsupdate.com.delivery.microsoft.com CHAME wu-b-net.traffic
277	56.201836	109.61.38.38	172.20.10.2	TCP	54	80 → 64039 [ACK] Seq=1 Ack=283 Win=32768 Len=0
278	56.201836	109.61.38.38	172.20.10.2	HTTP	445	HTTP/1.1 300 Not Modified
279	56.250594	172.20.10.2	109.61.38.38	TCP	54	64039 → 80 [ACK] Seq=283 Ack=392 Win=138816 Len=0
300	56.675081	172.20.10.2	172.20.10.2	TCP	1554	[TCP Retransmission] 64039 → 80 [ACK] Seq=1 Ack=1 Win=11072 Len=0
281	57.218968	172.20.10.2	64.233.162.103	UDP	71	57863 → 443 Len=20
282	57.342897	172.20.10.2	64.233.162.103	UDP	71	57863 → 443 Len=29
283	57.357887	64.233.162.103	172.20.10.2	UDP	68	443 → 57863 Len=26
284	57.405378	64.233.162.103	172.20.10.2	UDP	69	443 → 57863 Len=27
285	57.675081	172.20.10.2	172.20.10.2	TCP	508	[TCP Retransmission] 64039 → 80 [ACK] Seq=3 Ack=1 Win=11072 Len=0

[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
> Ethernet II, Src: 82:96:98:0a:49:64 (82:96:98:0a:49:64), Dst: AzureWaveTec\_E3:b6:67 (b4:8c:9d:83:b6:67)  
> Internet Protocol Version 4, Src: 109.61.38.38, Dst: 172.20.10.2  
Transmission Control Protocol, Src Port: 80, Dst Port: 64039, Seq: 0, Ack: 1, Len: 0  
Source Port: 80  
Destination Port: 64039  
[Stream Index: 17]  
[Stream Packet Number: 2]  
> [Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)

# Передача данных

- После handshake начинается обмен сегментами
- Используются подтверждения АСК
- Возможны повторные передачи

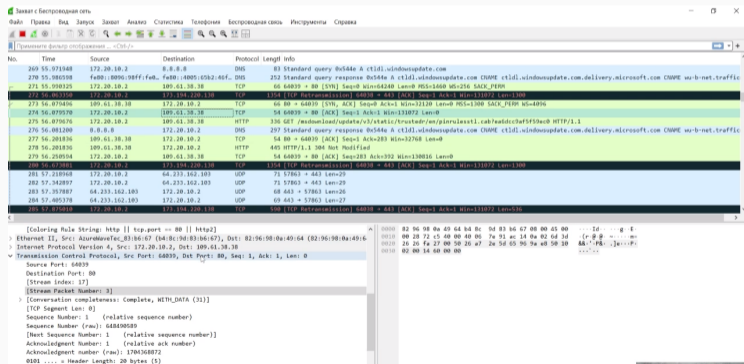


Рис. 13: Передача данных

# График потока TCP

- Отображает последовательность пакетов
- Видны установление и поддержание соединений
- Демонстрирует управление потоком

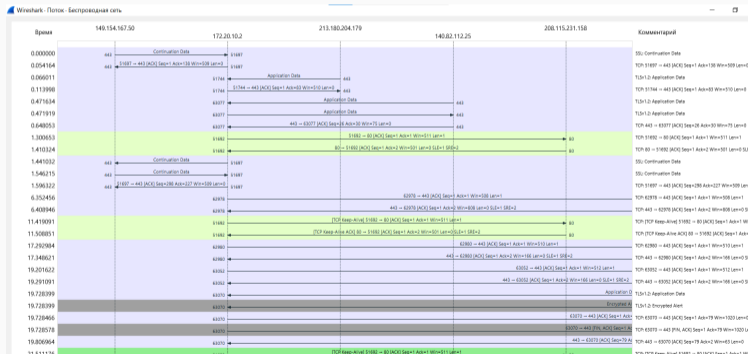


Рис. 14: Flow Graph

## Итоги работы

---

- Выполнен захват сетевого трафика в Wireshark
- Проанализированы протоколы:
  - ARP
  - ICMP
  - HTTP
  - DNS
  - TCP
  - UDP
  - QUIC
- Изучена структура Ethernet-кадров
- Рассмотрен механизм TCP handshake
- Получены практические навыки анализа сетевого взаимодействия