

# Лабораторная работа №3

Сетевые технологии

---

Мишина А. А.

12 октября 2024

## Цели и задачи

---

- Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

## Выполнение лабораторной работы

---

## MAC-адресация

---

# ipconfig

```
C:\Users\nasmi>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet 2:

DNS-суффикс подключения . . . . . : 
IPv4-адрес. . . . . : 192.168.56.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :

Неизвестный адаптер OpenVPN Data Channel Offload:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet 3:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : yandex-team.ru

Адаптер беспроводной локальной сети Беспроводная сеть* 1:

DNS-суффикс подключения . . . . . : wifi.rudn.su
IPv4-адрес. . . . . : 10.200.41.156
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 10.200.0.254

C:\Users\nasmi>
```

Рис. 1: Команда ipconfig

ipconfig /all

```
Адаптер беспроводной локальной сети Подключение по локальной сети* 1:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Физический адрес. . . . . : DC-45-46-63-D4-E6
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : DE-45-46-63-D4-E5
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet 3:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : yandex-team.ru
Описание . . . . . : TAP-Windows Adapter V9
Физический адрес. . . . . : 00-FF-80-8F-B7-06
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:
DNS-суффикс подключения . . . . . : wifi.rudn.su
Описание . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Физический адрес. . . . . : DC-45-46-63-D4-E5
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
IPv4-адрес . . . . . : 10.200.41.156(Основной)
Маска подсети . . . . . : 255.255.0.0
Аренда получена. . . . . : 11 октября 2024 г. 15:23:03
Срок аренды истекает . . . . . : 12 октября 2024 г. 16:05:23
Основной шлюз. . . . . : 10.200.8.254
DHCP-сервер. . . . . : 1.1.1.1
DNS-серверы. . . . . : 10.128.0.240
                                         80.250.174.240
NetBIOS через TCP/IP. . . . . : Включен
```

Рис. 2: Команда ipconfig /all

## Анализ кадров канального уровня в Wireshark

---

# Wireshark

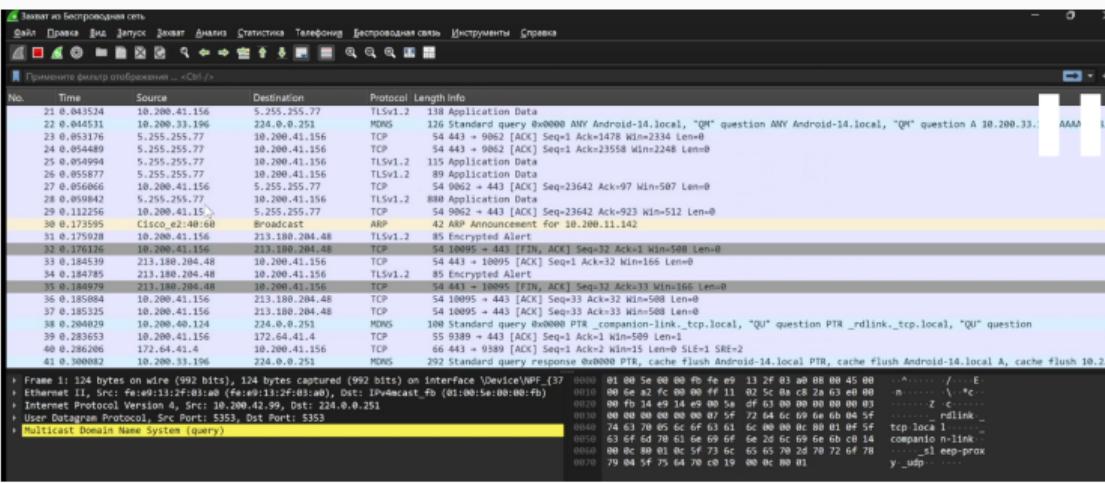


Рис. 3: Запуск захвата трафика

## Пинг

```
Основной шлюз. . . . . : 10.200.0.254
DHCP-сервер. . . . . : 1.1.1.1
DNS-серверы. . . . . : 10.128.0.240
                                         80.250.174.240
NetBIOS через TCP/IP. . . . . : Включен

C:\Users\nasmi>ping 10.200.0.254

Обмен пакетами с 10.200.0.254 по с 32 байтами данных:
Ответ от 10.200.0.254: число байт=32 время=1мс TTL=254
Ответ от 10.200.0.254: число байт=32 время=3мс TTL=254
Ответ от 10.200.0.254: число байт=32 время=2мс TTL=254
Ответ от 10.200.0.254: число байт=32 время=1мс TTL=254

Статистика Ping для 10.200.0.254:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 3 мсек, Среднее = 1 мсек

C:\Users\nasmi>
```

Рис. 4: Пинг шлюза по умолчанию

# Фильтр ICMP

No.	Time	Source	Destination	Protocol	Length	Info
→ 5687	92.963522	10.200.41.156	10.200.0.254	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 5608)
← 5688	92.965219	10.200.0.254	10.200.41.156	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=254 (request in 5607)
5708	93.976866	10.200.41.156	10.200.0.254	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 5709)
5709	93.988367	10.200.0.254	10.200.41.156	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=254 (request in 5708)
5753	94.991985	10.200.41.156	10.200.0.254	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 5754)
5754	94.994239	10.200.0.254	10.200.41.156	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=254 (request in 5753)
5852	96.007988	10.200.41.156	10.200.0.254	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 5853)
5853	96.009507	10.200.0.254	10.200.41.156	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=254 (request in 5852)

- Frame 5607: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{37F84577-9B0A-4D97-8135-C0E8F824A437}  
Section number: 1  
Interface id: 0 (\Device\NPF\_{37F84577-9B0A-4D97-8135-C0E8F824A437})  
Encapsulation type: Ethernet (1)  
Arrival Time: Oct 11, 2024 16:22:34.082690000 RTZ 2 (Эмма)  
UTC Arrival Time: Oct 11, 2024 13:22:34.082690000 UTC  
Epoch Arrival Time: 1728652954.082690000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.040503000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 92.963522000 seconds]  
Frame Number: 5687  
Frame Length: 74 bytes (592 bits)  
Capture Length: 74 bytes (592 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ether:type:ip:icmp:payload]  
[Coloring Rule Name: ICMP]  
[Coloring Rule String: icmp || icmpv6]  
Ethernet II, Src: Intel\_63:d4:e5 (dc:45:46:63:d4:e5), Dst: HuaweiTechno\_7d:d5:b6 (b8:e3:b1:7d:d5:b6)  
Destination: HuaweiTechno\_7d:d5:b6 (b8:e3:b1:7d:d5:b6)  
Source: Intel\_63:d4:e5 (dc:45:46:63:d4:e5)  
Type: IPv4 (0x8000)  
[Stream index: 1]  
Internet Protocol Version 4, Src: 10.200.41.156, Dst: 10.200.0.254  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x4d2e [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 45 (0x02d)  
Sequence Number (LE): 11520 (0x2d00)

0000 b8 e3 b1 7d d5 b6 dc 45 46 63 d4 e5 08 00 45 00  
0010 00 3c c0 d5 00 00 80 01 00 00 0a c8 29 9c 0a c8  
0020 00 fe 08 00 4d 2e 00 01 00 2d 61 62 63 64 65 66  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  
0040 77 61 62 63 64 65 66 67 68 69

Рис. 5: Кадр ICMP - эхо-запрос: информация о длине кадра, типе Ethernet и MAC-адресах

# Фильтр ICMP

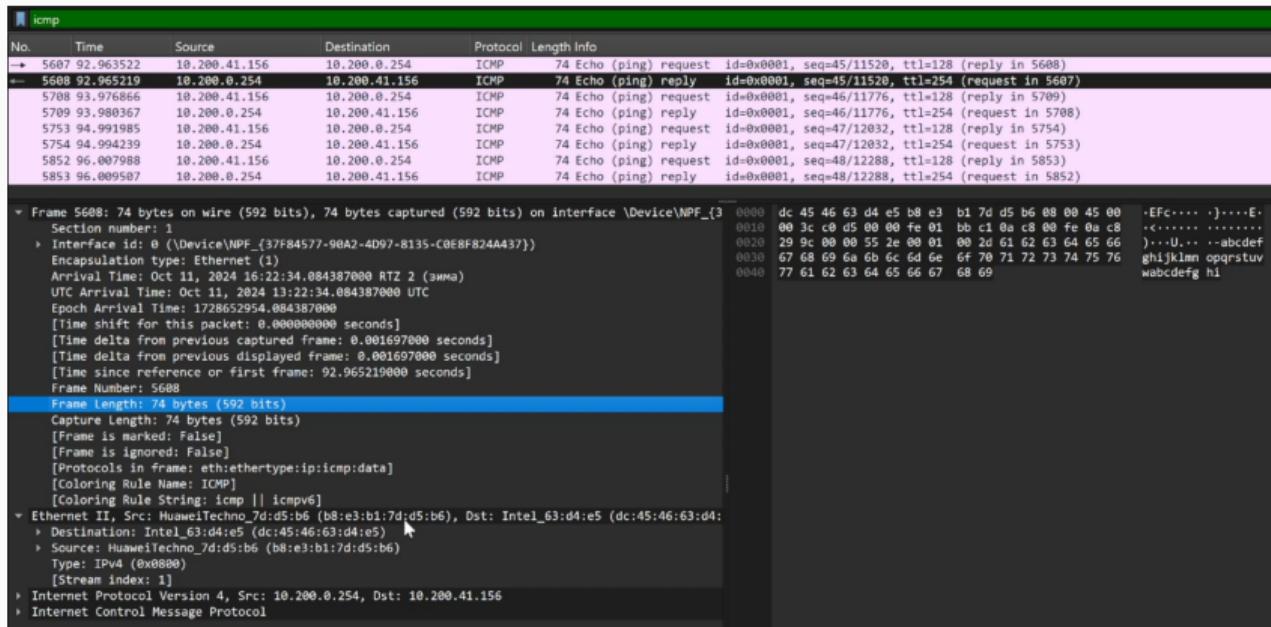


Рис. 6: Кадр ICMP - эхо-ответ: информация о длине кадра, типе Ethernet, MAC-адресах

# Фильтр ARP

No.	Time	Source	Destination	Protocol	Length Info
61	11.08:00:00	Cisco_02:40:60	Broadcast	ARP	42 ARP Announcement for 10.200.11.142
604	11.08:44:77	Cisco_02:40:60	Broadcast	ARP	42 ARP Announcement for 10.200.104.86
3240	20.05:46:20	Cisco_02:40:60	Broadcast	ARP	42 ARP Announcement for 10.200.21.77
3405	22.09:56:16	Intel_03:04:e5	Broadcast	ARP	42 Who has 10.200.42.210? Tell 10.200.41.156
3451	23.56:18:76	Intel_03:04:e5	Broadcast	ARP	42 Who has 10.200.42.210? Tell 10.200.41.156
3521	24.57:38:09	Intel_03:04:e5	Broadcast	ARP	42 Who has 10.200.42.210? Tell 10.200.41.156
3582	26.00:08:09	Intel_03:04:e5	Broadcast	ARP	42 Who has 10.200.42.210? Tell 10.200.41.156
3604	26.57:07:53	Intel_03:04:e5	Broadcast	ARP	42 Who has 10.200.42.210? Tell 10.200.41.156
Frame 1816: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 'DeviceMPF_0' at 00:00:00:00:00:00 [��] (Ethernet II (raw)) Interface Id: 0 (DeviceMPF_0) [378784557-90A2-4D97-8135-C0EBF8244A37] Encapsulation type: Ethernet (1) Arrival Time: Oct 11, 2024 16:21:31.132394000 RTZ 2 (MMYY) UTC Arrival Time: Oct 11, 2024 13:21:31.132394000 UTC Epoch Arrival Time: 178052091.132394000 [Time offset for this packet: 0.000000000 seconds] [Time delta from previous: 0.000000000 seconds] [Time delta from previous displayed frame: 0.558394000 seconds] [Time since reference or first frame: 30.813226000 seconds] Frame Number: 1816 Frame Length: 42 bytes (336 bits) Capture Length: 42 bytes (336 bits) [Frame is marked: False] [Frame is broadcast: True] [Protocols in frame: ethertype:arp] [Coloring Rule Name: arp] [Coloring Rule String: arp] Ethernet II, Src: Intel_03:04:e5 (dc:45:46:63:d4:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff) Destination: Broadcast (ff:ff:ff:ff:ff:ff) Source: Intel_03:04:e5 (dc:45:46:63:d4:e5) Type: ARP (0x0806) [Ether Type index: 133] Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: Request (1) Sender MAC address: Intel_03:04:e5 (dc:45:46:63:d4:e5) Sender IP address: 10.200.41.156 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) Target IP address: 10.200.42.210					

Рис. 7: Кадр ARP: информация о длине кадра, типе Ethernet, MAC-адресах

```
C:\Users\nasmi>
C:\Users\nasmi>ping www.yandex.ru

Обмен пакетами с www.YANDEX.ru [5.255.255.77] с 32 байтами данных:
Ответ от 5.255.255.77: число байт=32 время=79мс TTL=51
Ответ от 5.255.255.77: число байт=32 время=32мс TTL=51
Ответ от 5.255.255.77: число байт=32 время=38мс TTL=51
Ответ от 5.255.255.77: число байт=32 время=51мс TTL=51

Статистика Ping для 5.255.255.77:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 32мсек, Максимальное = 79 мсек, Среднее = 50 мсек

C:\Users\nasmi>
```

Рис. 8: Пинг сайта www.yandex.ru

# Фильтр ICMP

No.	Time	Source	Destination	Protocol	Length Info	Hex	Dec	Description
→ 106	2.769001	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 108)	0000 02 4b 77 4d 6f 6a dc 45	00 00 45 00 46 63 d4 e5 08 00	·KwMo:E Fc--·E
← 108	2.853351	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=65/16640, ttl=51 (request in 106)	0010 00 3c 46 ad 00 00 80 01	00 00 c0 a8 5a 83 05 ff	-F-----Z-
118	3.775840	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (reply in 119)	0020 ff 4d 08 00 4d 1a 00 01	00 41 61 62 63 64 65 66	-M-M---Aabcdef
119	3.830786	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=66/16896, ttl=51 (request in 118)	0030 67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn oppqrstuvwxyz
122	4.792568	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=67/17152, ttl=128 (reply in 125)	0040 77 61 62 63 64 65 66 67	68 69	wabdefghi
125	4.912462	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=67/17152, ttl=51 (request in 122)			
135	5.805744	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=68/17408, ttl=128 (reply in 137)			
137	5.896679	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=68/17408, ttl=51 (request in 135)			

Frame 106: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{37F84577-90A2-4D97-8135-C0E8F824A437}  
Section number: 1  
    > Destination: 0 (\Device\NPF\_{37F84577-90A2-4D97-8135-C0E8F824A437})  
    Encapsulation type: Ethernet (1)  
    Arrival Time: Oct 11, 2024 16:34:02.362148000 RTZ 2 (этива)  
    UTC Arrival Time: Oct 11, 2024 13:34:02.362148000 UTC  
    Epoch Arrival Time: 1728653642.362148000  
    [Time shift for this packet: 0.000000000 seconds]  
    [Time delta from previous captured frame: 0.001189000 seconds]  
    [Time delta from previous displayed frame: 0.000000000 seconds]  
    [Time since reference or first frame: 2.769001000 seconds]  
    Frame Number: 106  
    Frame Length: 74 bytes (592 bits)  
    Capture Length: 74 bytes (592 bits)  
    [Frame is marked: False]  
    [Frame is ignored: False]  
    [Protocols in frame: eth:ethertype:ip:icmp:data]  
    [Coloring Rule Name: ICMP]  
    [Coloring Rule String: icmp || icmpv6]  
    > Ethernet II, Src: Intel\_63:d4:e5 (dc:45:46:63:d4:e5), Dst: 02:4b:77:4d:6f:6a (02:4b:77:4d:6f:6a)  
        > Destination: 02:4b:77:4d:6f:6a (02:4b:77:4d:6f:6a)  
        > Source: Intel\_63:d4:e5 (dc:45:46:63:d4:e5)  
        Type: IPv4 (0x0800)  
        [Stream index: 0]  
    > Internet Protocol Version 4, Src: 192.168.90.131, Dst: 5.255.255.77  
    > Internet Control Message Protocol

Рис. 9: Запрос протокола ICMP

# Фильтр ICMP

No.	Time	Source	Destination	Protocol	Length Info	Hex	Text
→ 106	2.769001	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 108)	0000 dc 45 46 63 d4 e5 92 4b 77 4d 6f 6a 00 00 45 00 .Fc...K WmQ..E:	
← 108	2.853351	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=65/16640, ttl=51 (request in 106)	0010 00 3c 46 ad 00 00 33 01 20 9c 05 ff ff 4d c8 a8 <F...3 ...M:	
118	3.775840	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (reply in 119)	0020 5a 83 00 00 55 1a 00 01 00 41 61 62 63 64 65 66 Z ..U ...Aabcefuv	
119	3.830786	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=66/16896, ttl=51 (request in 118)	0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuvwxyz	
122	4.792568	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=67/17152, ttl=128 (reply in 125)	0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi	
125	4.912462	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=67/17152, ttl=51 (request in 122)		
135	5.808544	192.168.90.131	5.255.255.77	ICMP	74 Echo (ping) request id=0x0001, seq=68/17408, ttl=128 (reply in 137)		
137	5.896679	5.255.255.77	192.168.90.131	ICMP	74 Echo (ping) reply id=0x0001, seq=68/17408, ttl=51 (request in 135)		

Рис. 10: Ответ протокола ICMP

## Фильтр ICMP

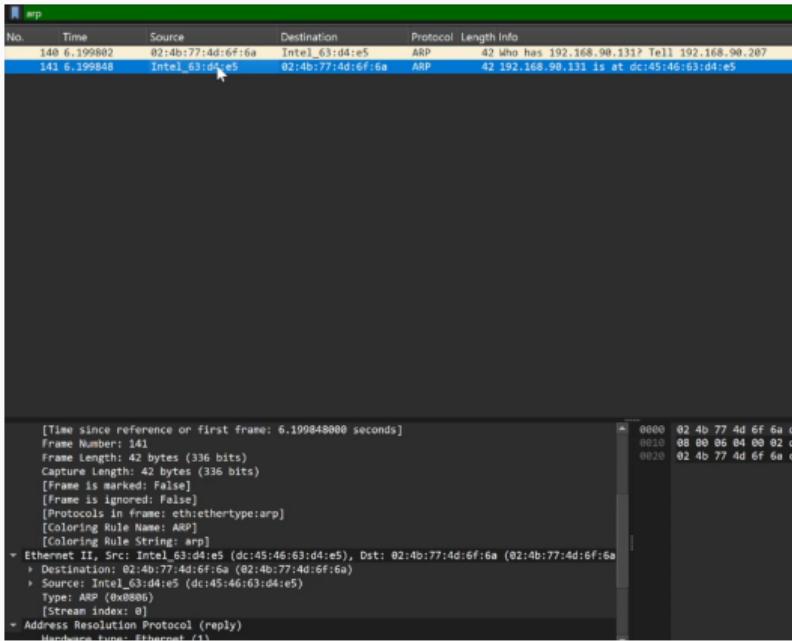


Рис. 11: Кадр ARP - эхо-ответ

## Анализ протоколов транспортного уровня в Wireshark

---

<http://info.cern.ch/>

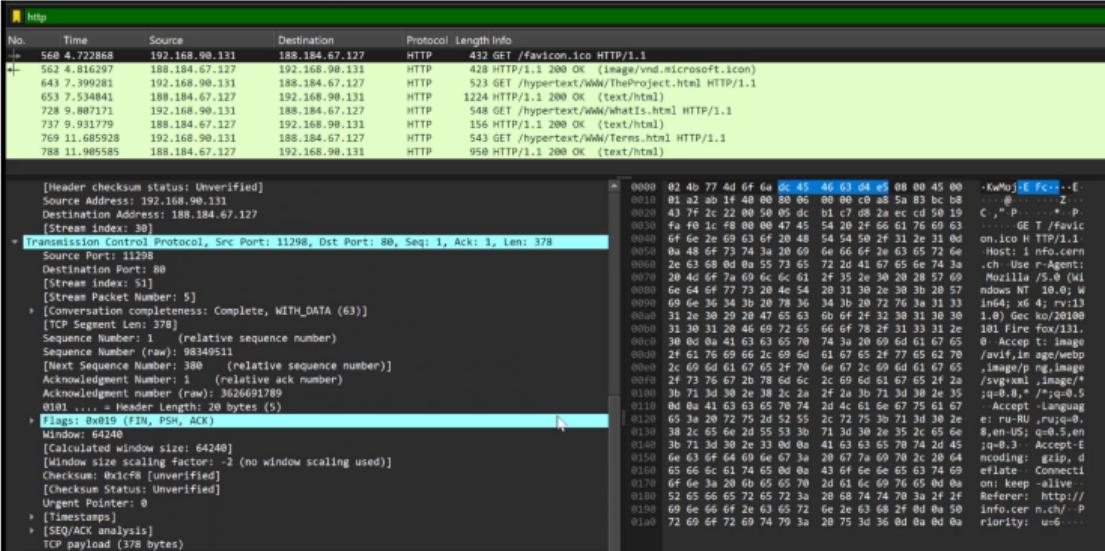


Рис. 12: Кадр http - запрос

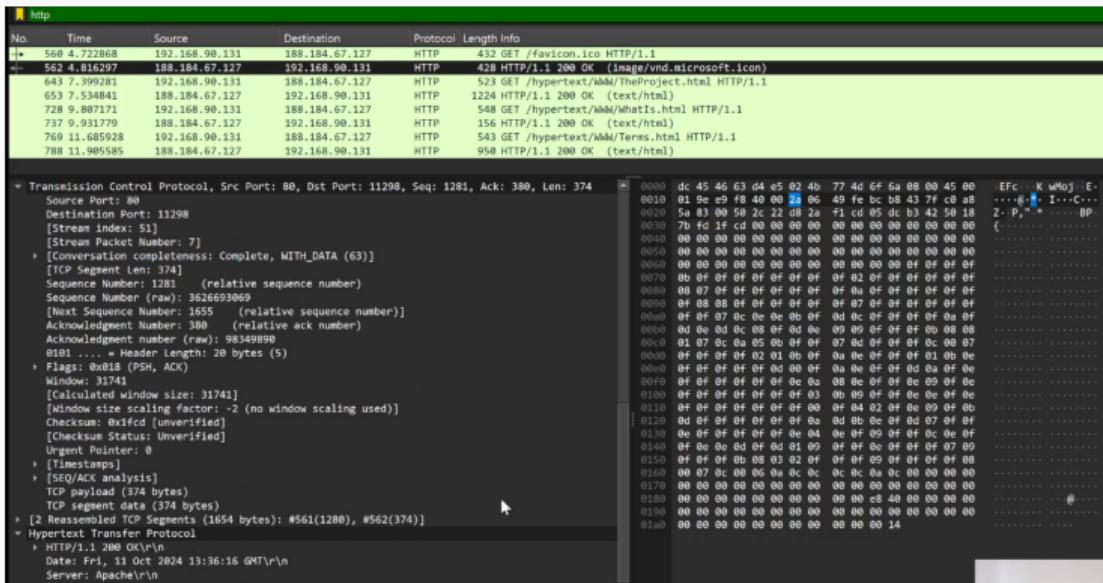


Рис. 13: Кадр http - ответ

## Фильтр dns

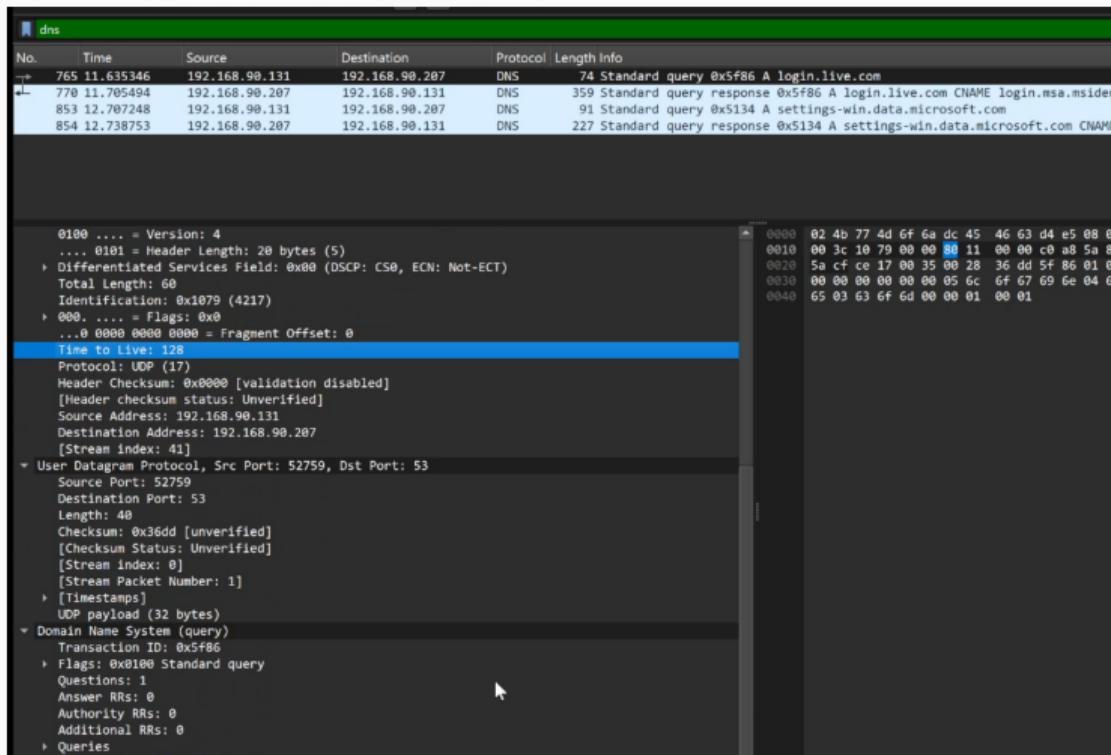


Рис. 14: Кадр dns - запрос

# Фильтр dns

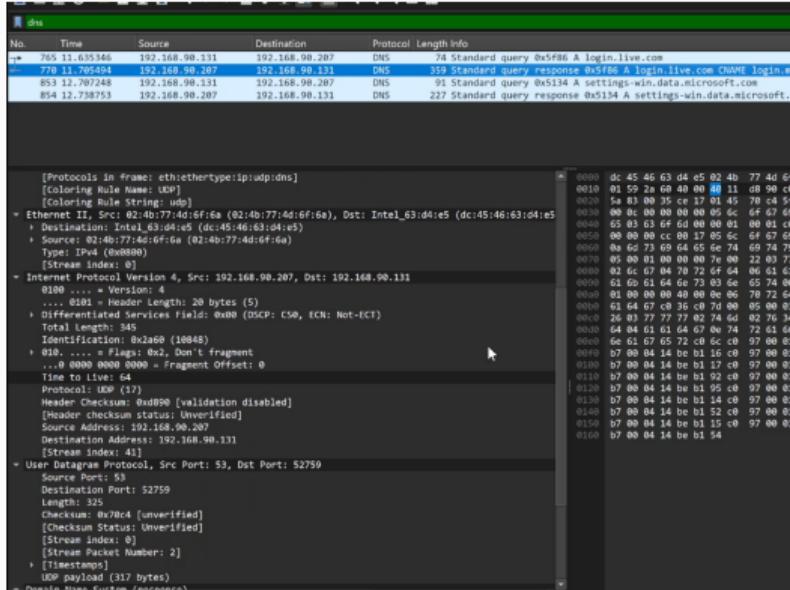


Рис. 15: Кадр dns - ответ

# Фильтр quic

No.	Time	Source	Destination	Protocol	Length Info
- 23999	390.295111	192.168.98.131	173.194.222.84	QUIC	1292 Initial, DCID=221b3a36a59ef3a9, PKN: 1, CRYPTO
+ 24000	390.295238	192.168.98.131	173.194.222.84	QUIC	1292 Initial, DCID=221b3a36a59ef3a9, PKN: 2, CRYPTO, PADDING, PING, PADDING, CRYPTO
24075	390.385848	173.194.222.84	192.168.98.131	QUIC	82 Initial, SCID=e21b3a36a59ef3a9, PKN: 1, ACK
24080	390.389143	173.194.222.84	192.168.98.131	QUIC	1292 Initial, SCID=e21b3a36a59ef3a9, PKN: 2, ACK, PADDING
24084	390.404483	173.194.222.84	192.168.98.131	QUIC	1292 Initial, SCID=e21b3a36a59ef3a9, PKN: 3, CRYPTO, PADDING
24085	390.405795	173.194.222.84	192.168.98.131	QUIC	1292 Initial, SCID=e21b3a36a59ef3a9, PKN: 4, CRYPTO, PADDING
24086	390.406254	192.168.98.131	173.194.222.84	QUIC	1292 Initial, DCID=e21b3a36a59ef3a9, PKN: 5, ACK, PADDING
24087	390.407534	173.194.222.84	192.168.98.131	QUIC	1292 Handshake, SCID=e21b3a36a59ef3a9
24089	390.407534	173.194.222.84	192.168.98.131	QUIC	1292 Handshake, SCID=e21b3a36a59ef3a9
Protocol: UDP (17) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.98.131 Destination Address: 173.194.222.84 [Stream index: 120]					
+ User Datagram Protocol, Src Port: 52268, Dst Port: 443					
Source Port: 52268					
Destination Port: 443					
Length: 1258					
Checksum: 0xac3e [unverified]					
[Checksum Status: Unverified]					
[Stream index: 30]					
[Stream Packet Number: 1]					
+ [timestamps]					
UDP payload (1250 bytes)					
- QUIC IETF					
+ QUIC Connection information					
[Packet Length: 1250]					
1.... .... = Header Form: Long Header (1)					
..1.... .... = Fixed Bit: True					
..00 .... = Packet Type: Initial (0)					
[.... 00.. = Reserved: 0]					
[.... 00.. = Packet Number Length: 1 bytes (0)]					
Version: 1 (0x00000001)					
Destination Connection ID Length: 8					
Destination Connection ID: 221b3a36a59ef3a9					
Source Connection ID Length: 0					
Token Length: 0					
Length: 1232					
[Packet Number: 1]					
Payload [...] : 5c42d330ee166ff95653136883b3471839ee9c51a5f4757d2047428c35ef6338cab4269287aca42;					
+ CRYPTO					

Рис. 16: Кадр quic - запрос

## Анализ handshake протокола TCP в Wireshark

---

# handshake

- 1587 38.361713 192.168.90.131 188.184.99.25 TCP 66 13399 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1588 38.363142 188.184.99.25 192.168.90.131 TCP 66 80 → 13396 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1400 SACK_PERM WS=128
1589 38.363400 192.168.90.131 188.184.99.25 TCP 54 13396 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
1590 38.364674 192.168.90.131 146.75.117.91 TLSv1.3 106 Application Data
1591 38.365258 172.67.174.127 192.168.90.131 TCP 66 443 → 13397 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=819
1592 38.365802 192.168.90.131 172.67.174.127 TCP 54 13397 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
1595 38.371080 192.168.90.131 172.67.174.127 TLSv1.3 571 Client Hello (SNI=cdn.themoneytizer.fr)
1596 38.378282 192.168.90.131 146.75.117.91 TLSv1.3 383 Application Data
1597 38.384621 192.168.90.131 146.75.117.91 TLSv1.3 431 Application Data, Application Data
1598 38.414349 173.194.220.95 192.168.90.131 TCP 54 443 → 13398 [ACK] Seq=1 Ack=518 Win=66816 Len=0
1599 38.416783 173.194.220.95 192.168.90.131 TLSv1.3 1454 Server Hello, Change Cipher Spec
1600 38.417989 173.194.220.95 192.168.90.131 TCP 1454 443 → 13398 [PSH, ACK] Seq=1401 Ack=518 Win=66816 Len=1400 [TCP PDU reassembly]

Frame 1587: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{...}  
Ethernet II, Src: Intel\_63:d4:e5 (dc:45:46:63:d4:e5), Dst: 02:4b:77:4d:6f:6a (02:4b:77:4d:6f:6a)  
Internet Protocol Version 4, Src: 192.168.90.131, Dst: 188.184.99.25  
Transmission Control Protocol, Src Port: 13399, Dst Port: 80, Seq: 0, Len: 0

Source Port: 13399  
Destination Port: 80  
[Stream index: 92]  
[Stream Packet Number: 1]  
↳ [Conversation completeness: Incomplete, ESTABLISHED (7)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 3647781281  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 0  
Acknowledgment Number (raw): 0  
1000 .... = Header Length: 32 bytes (8)  
↳ Flags: 0x002 (SYN)  
Window: 64240  
[Calculated window size: 64240]  
Checksum: 0xb224 [unverified]  
[Checksum Status: Unverified]

0000 02 4b 77 4d 6f 6a dc 45 46 63 d4 e5 08 00 45 0  
0010 00 34 4c d4 40 00 00 06 00 00 c0 a8 5a 83 bc b  
0020 63 19 34 57 00 50 d9 6c b9 a1 00 00 00 00 80 0  
0030 fa fe 3b 24 00 00 02 04 05 b4 01 03 03 08 01 0  
0040 04 02

Рис. 17: Первая ступень handshake TCP

# handshake

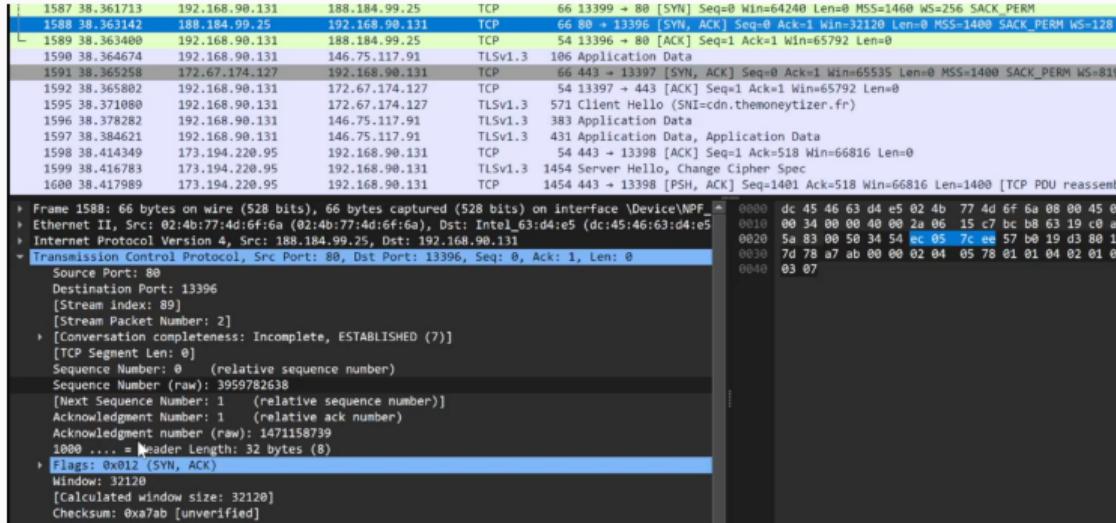


Рис. 18: Вторая ступень handshake TCP

# handshake

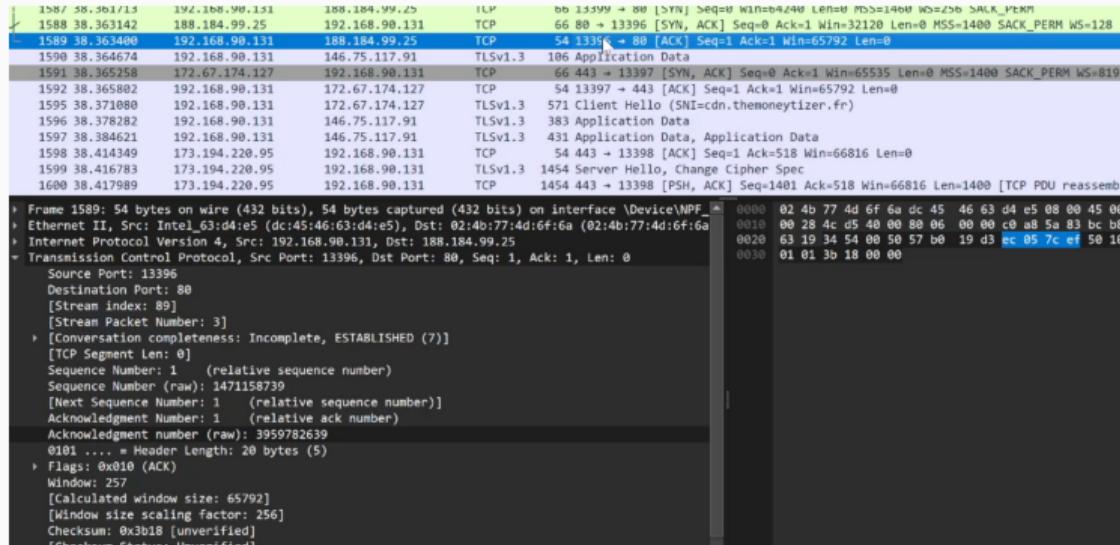


Рис. 19: Третья ступень handshake TCP

# График потока



Рис. 20: График потока

## Вывод

---

- В результате выполнения работы были изучены посредством Wireshark кадры Ethernet, произведен анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.