

Отчёт по лабораторной работе 3

Анализ трафика в Wireshark

Метвалли Ахмед Фарг Набеев

Содержание

1	Цель работы	5
2	Выполнение	6
3	Выполнение	7
3.1	Анализ кадров канального уровня в Wireshark	7
3.2	Анализ протоколов транспортного уровня в Wireshark	13
3.3	Анализ handshake протокола TCP в Wireshark	18
4	Заключение	20

Список иллюстраций

3.1	Результат ipconfig	7
3.2	Фильтр arp or icmp	8
3.3	ICMP Echo Request	9
3.4	ICMP Echo Reply	10
3.5	ARP Request	11
3.6	Ping ya.ru	11
3.7	TCP Handshake	18
3.8	График потока TCP	19

Список таблиц

1 Цель работы

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

2 Выполнение

3 Выполнение

3.1 Анализ кадров канального уровня в Wireshark

1. На устройство установлен и запущен **Wireshark**. Для анализа был выбран активный беспроводной сетевой интерфейс, начат захват трафика.
2. С помощью команды **ipconfig** в консоли Windows определён IP-адрес устройства и шлюз по умолчанию.

Устройство имеет адрес 192.168.212.42, а шлюз по умолчанию — 192.168.212.16.

```
Адаптер Ethernet Ethernet 2:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . : fe80::d3f2:8384:1a21:d660%21
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

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 беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . : fe80::da3b:4057:9ef4:1e28%7
    IPv4-адрес. . . . . : 192.168.212.42
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.212.16
PS C:\> |
```

Рис. 3.1: Результат ipconfig

3. Выполнена команда **ping** шлюза по умолчанию (192.168.212.16). На экране

отобразились ответы от шлюза.

- В Wireshark был применён фильтр `arp or icmp`. В списке пакетов отображались только пакеты ARP и ICMP.

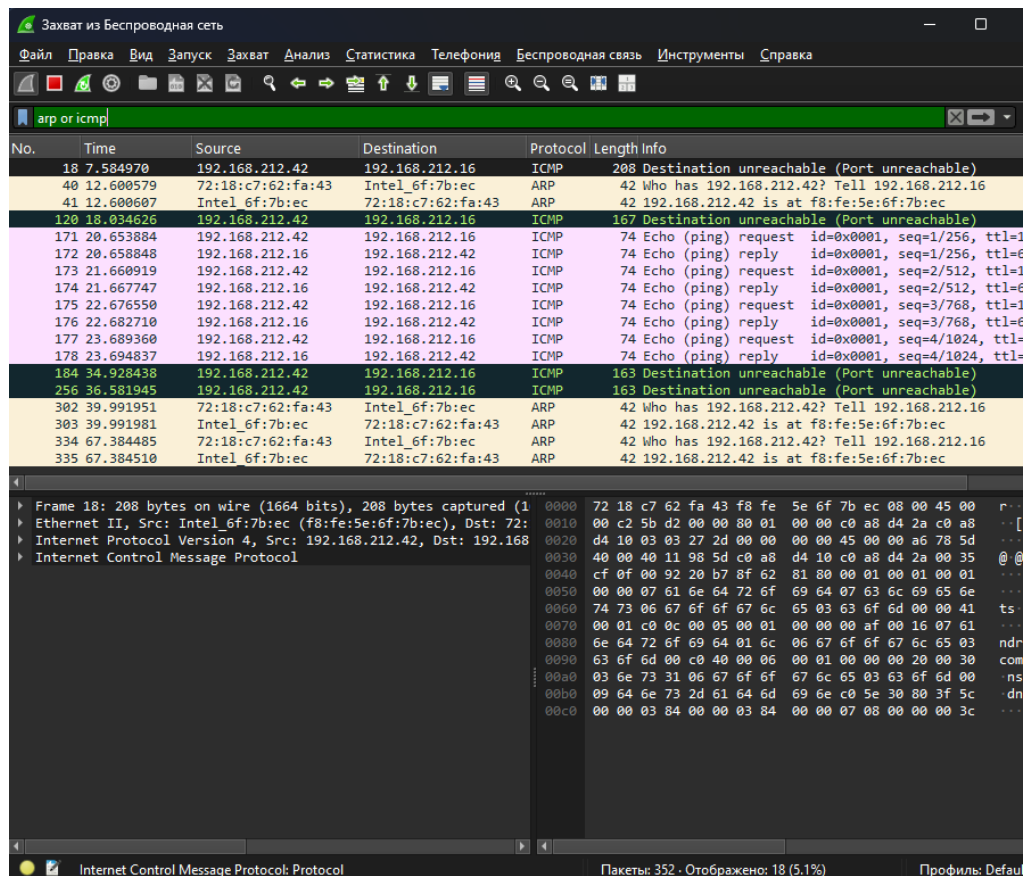


Рис. 3.2: Фильтр `arp or icmp`

- Анализ ICMP эхо-запроса:

- Длина кадра — 74 байта.
- Тип кадра Ethernet II.
- MAC-адрес источника: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec).

- MAC-адрес шлюза: 72:18:c7:62:fa:43.
- Тип MAC-адресов — индивидуальные (unicast).

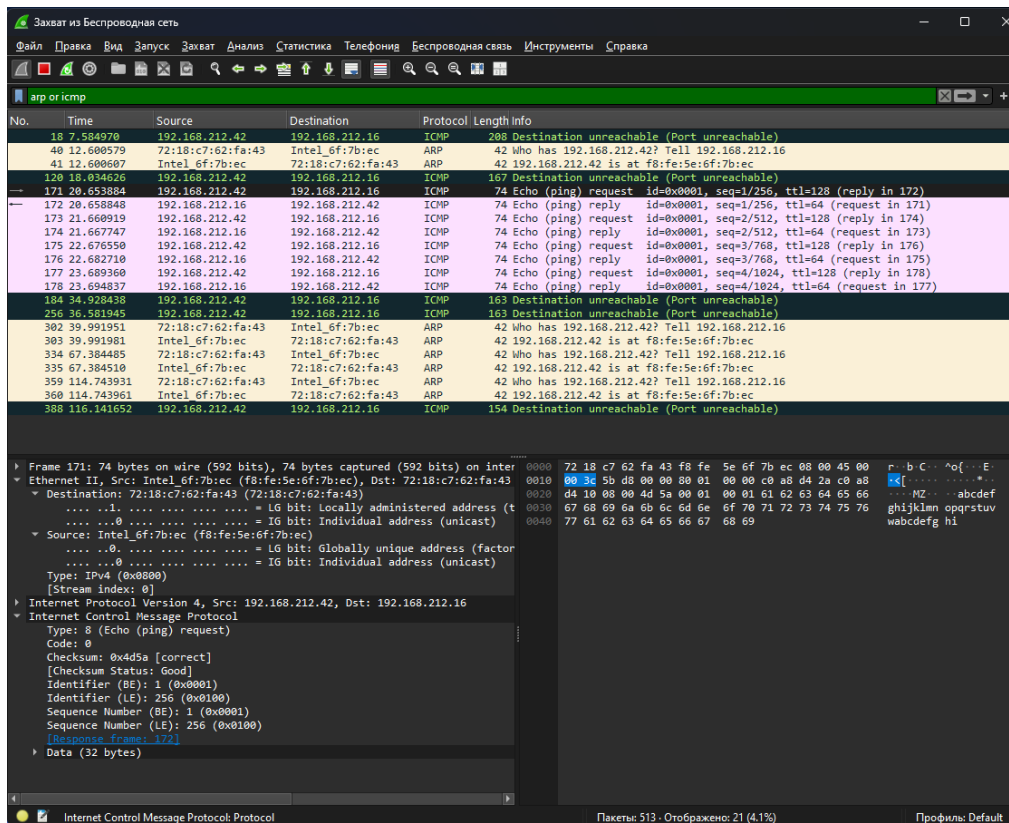


Рис. 3.3: ICMP Echo Request

6. Анализ ICMP эхо-ответа:

- Длина кадра — 74 байта.
- Тип кадра Ethernet II.
- MAC-адрес источника: 72:18:c7:62:fa:43.
- MAC-адрес получателя: f8:fe:5e:6f:7b:ec.

- Тип MAC-адресов — индивидуальные (unicast).

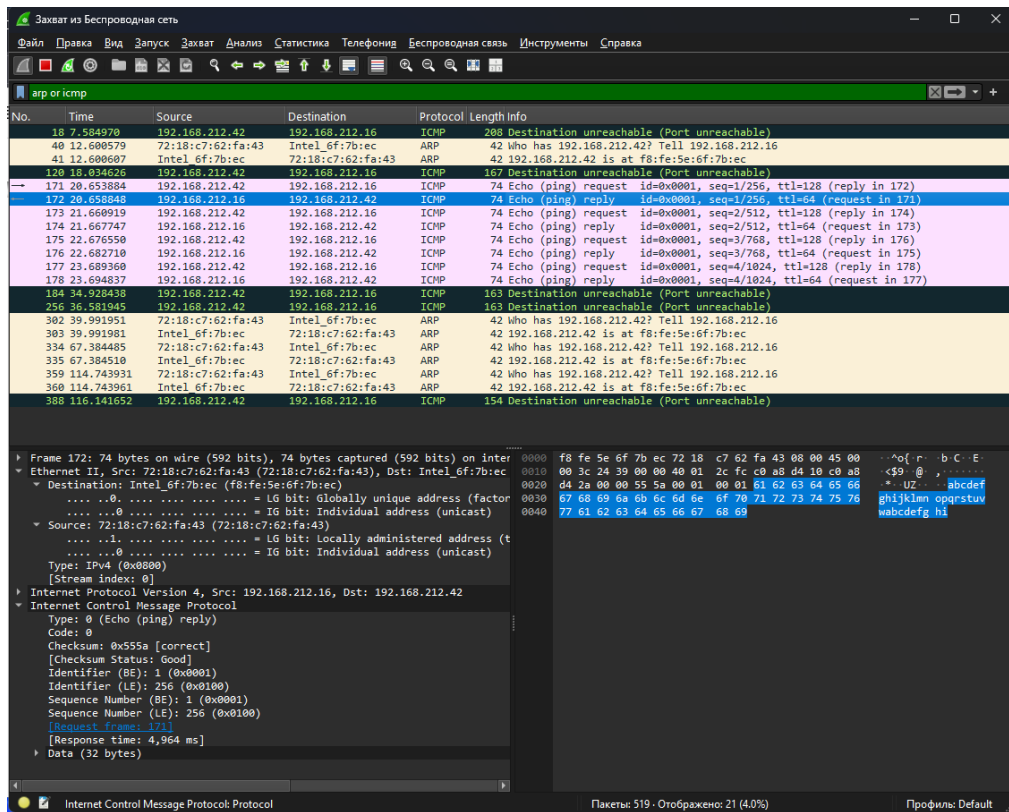


Рис. 3.4: ICMP Echo Reply

7. Анализ ARP-запроса:

- Длина кадра — 42 байта.
- Отправитель: 192.168.212.42.
- Запрос: «Кто имеет IP 192.168.212.16?»
- Тип MAC-адресов — индивидуальные.

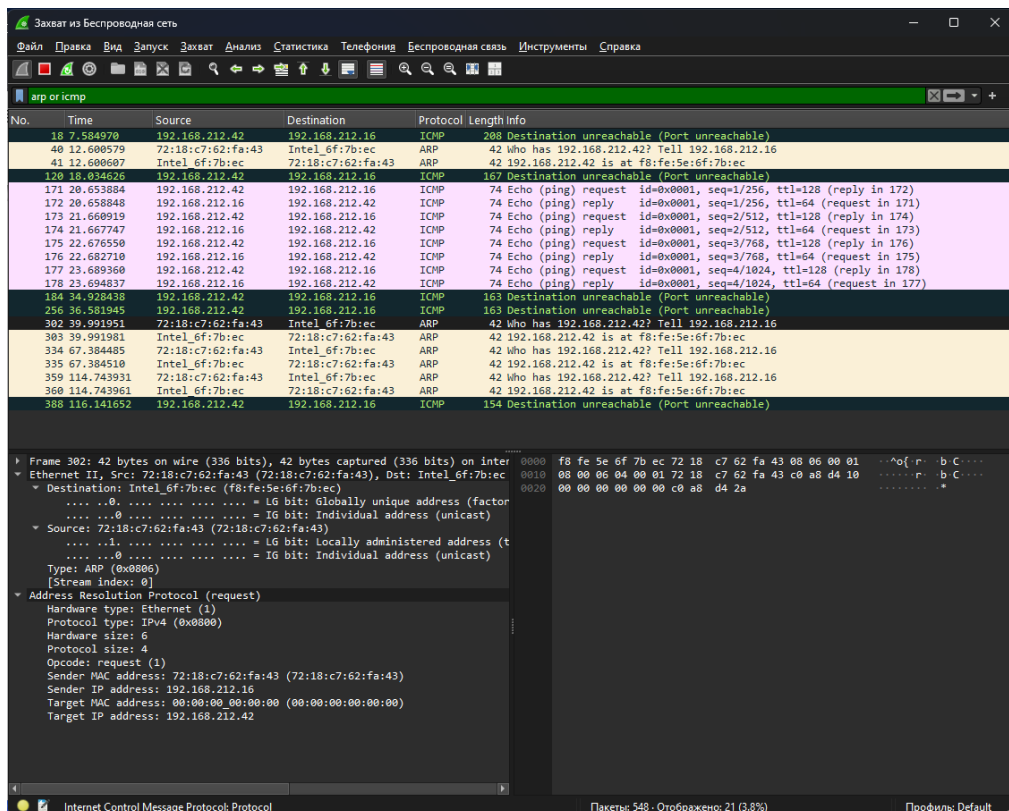


Рис. 3.5: ARP Request

8. Далее был выполнен ping внешнего узла ya.ru. Ответы пришли успешно, что подтверждает работоспособность соединения.

```
PS C:\> ping ya.ru

Обмен пакетами с YA.ru [5.255.255.242] с 32 байтами данных:
Ответ от 5.255.255.242: число байт=32 время=25мс TTL=246
Ответ от 5.255.255.242: число байт=32 время=52мс TTL=246
Ответ от 5.255.255.242: число байт=32 время=65мс TTL=246
Ответ от 5.255.255.242: число байт=32 время=67мс TTL=246

Статистика Ping для 5.255.255.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 25мсек, Максимальное = 67 мсек, Среднее = 52 мсек
PS C:\> |
```

Рис. 3.6: Ping ya.ru

9. В Wireshark зафиксированы пакеты ICMP при обмене с внешним сервером (5.255.255.242). Отображены эхо-запросы и ответы, а также промежуточ-

ные ARP-запросы.

The image displays a Wireshark packet capture of ICMP Echo (ping) traffic. The top pane shows a list of packets, with packet 563 selected. The middle pane shows the details of the selected packet, which is an ICMP Echo (ping) reply from 192.168.212.16 to 192.168.212.42. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
178	23.694837	192.168.212.16	192.168.212.42	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 177)
184	34.928438	192.168.212.42	192.168.212.16	ICMP	163	Destination unreachable (Port unreachable)
256	36.581945	192.168.212.42	192.168.212.16	ICMP	163	Destination unreachable (Port unreachable)
302	39.991951	72:18:c7:62:fa:43	Intel_6f:7b:ec	ARP	42	Who has 192.168.212.42? Tell 192.168.212.16
303	39.991981	Intel_6f:7b:ec	72:18:c7:62:fa:43	ARP	42	192.168.212.42 is at f8:fe:5e:6f:7b:ec
334	67.384485	72:18:c7:62:fa:43	Intel_6f:7b:ec	ARP	42	Who has 192.168.212.42? Tell 192.168.212.16
335	67.384510	Intel_6f:7b:ec	72:18:c7:62:fa:43	ARP	42	192.168.212.42 is at f8:fe:5e:6f:7b:ec
359	114.743931	72:18:c7:62:fa:43	Intel_6f:7b:ec	ARP	42	Who has 192.168.212.42? Tell 192.168.212.16
360	114.743961	Intel_6f:7b:ec	72:18:c7:62:fa:43	ARP	42	192.168.212.42 is at f8:fe:5e:6f:7b:ec
388	116.741652	192.168.212.42	192.168.212.16	ICMP	163	Destination unreachable (Port unreachable)
554	230.451080	72:18:c7:62:fa:43	Intel_6f:7b:ec	ARP	42	Who has 192.168.212.42? Tell 192.168.212.16
555	230.452006	Intel_6f:7b:ec	72:18:c7:62:fa:43	ARP	42	192.168.212.42 is at f8:fe:5e:6f:7b:ec
563	243.373315	192.168.212.42	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 564)
564	243.398454	5.255.255.242	192.168.212.42	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=246 (request in 563)
567	244.380150	192.168.212.42	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 568)
568	244.432816	5.255.255.242	192.168.212.42	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=246 (request in 567)
569	245.396538	192.168.212.42	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 570)
570	245.461865	5.255.255.242	192.168.212.42	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=246 (request in 569)
571	246.412186	192.168.212.42	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 572)
572	246.479762	5.255.255.242	192.168.212.42	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=246 (request in 571)
586	254.981702	192.168.212.42	192.168.212.16	ICMP	168	Destination unreachable (Port unreachable)
610	260.144683	72:18:c7:62:fa:43	Intel_6f:7b:ec	ARP	42	Who has 192.168.212.42? Tell 192.168.212.16
611	260.144712	Intel_6f:7b:ec	72:18:c7:62:fa:43	ARP	42	192.168.212.42 is at f8:fe:5e:6f:7b:ec

Packet Details (Packet 563):

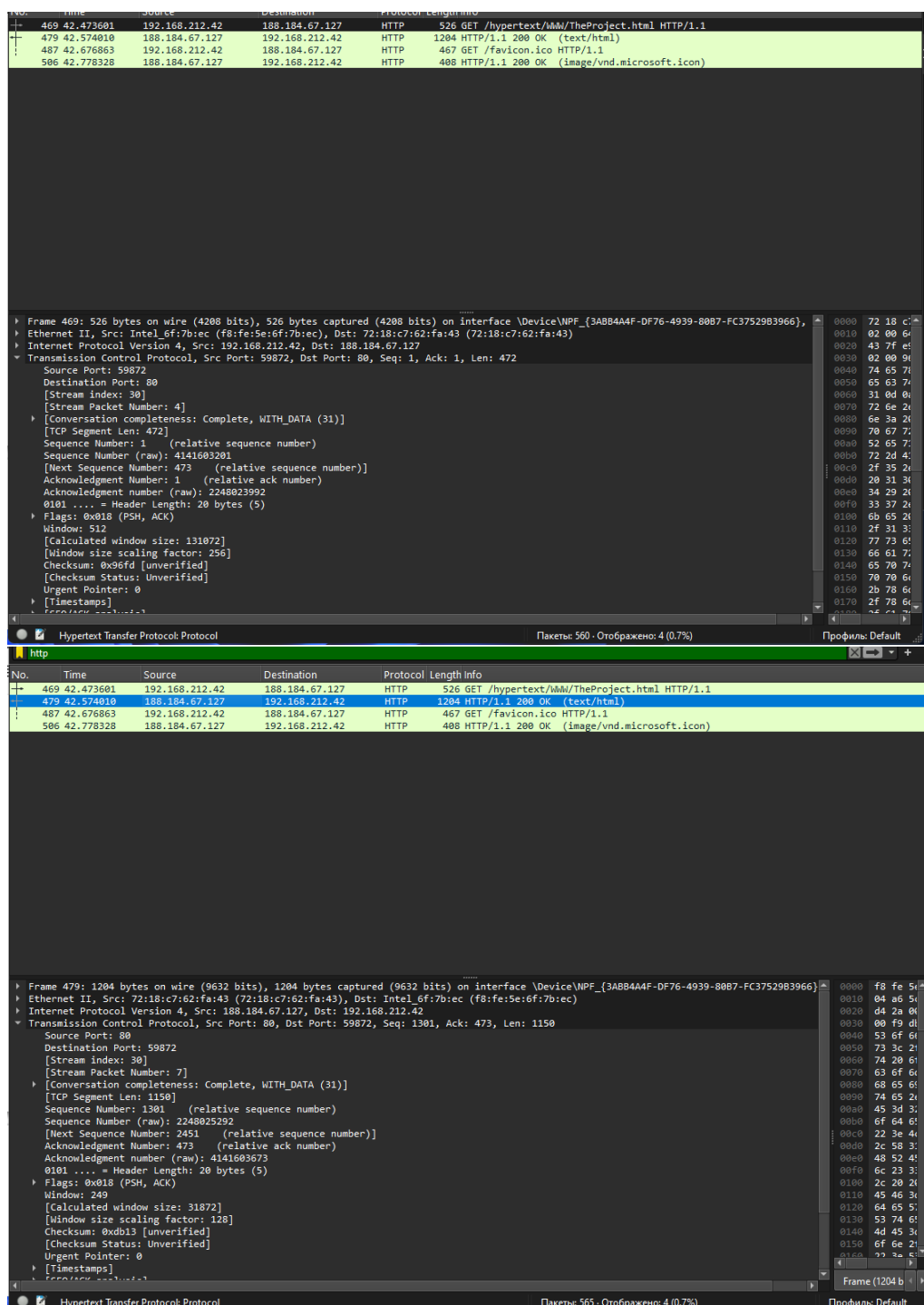
- Frame 563: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3AB84A4F-DF76-4939-8087-FC37529B3966}, id 0
- Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: 72:18:c7:62:fa:43 (72:18:c7:62:fa:43)
- Destination: 72:18:c7:62:fa:43 (72:18:c7:62:fa:43)
- Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.212.42, Dst: 5.255.255.242
- Internet Control Message Protocol
- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d56 [correct]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 5 (0x0005)
- Sequence Number (LE): 1280 (0x0500)
- Response time: 561 ms
- Data (32 bytes)

Packet Details (Packet 564):

- Frame 564: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3AB84A4F-DF76-4939-8087-FC37529B3966}, id 0
- Ethernet II, Src: 72:18:c7:62:fa:43 (72:18:c7:62:fa:43), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
- Destination: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
- Source: 72:18:c7:62:fa:43 (72:18:c7:62:fa:43)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 5.255.255.242, Dst: 192.168.212.42
- Internet Control Message Protocol
- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x5556 [correct]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 5 (0x0005)
- Sequence Number (LE): 1280 (0x0500)
- Response time: 25.139 ms
- Data (32 bytes)

3.2 Анализ протоколов транспортного уровня в Wireshark

1. На устройстве был запущен **Wireshark**, выбран активный сетевой интерфейс и начат захват трафика.
2. В браузере был открыт сайт, работающий по протоколу **HTTP**. Для получения достаточного количества пакетов осуществлён переход по разделам сайта.
3. В Wireshark применён фильтр `http`. На экране отобразились HTTP-запросы и ответы, передаваемые по протоколу **TCP**:
 - Зафиксирован запрос `GET /hypertext/WWW/TheProject.html`.
 - Сервер ответил кодом `200 OK` и передал HTML-документ.
 - Дополнительно передавались файлы: `favicon.ico` и графические данные.
 - Для каждого пакета видны исходные и целевые порты TCP, порядковые и подтверждающие номера сегментов.



4. Далее был применён фильтр dns. В захвате зафиксированы **UDP-пакеты** с DNS-запросами и ответами:

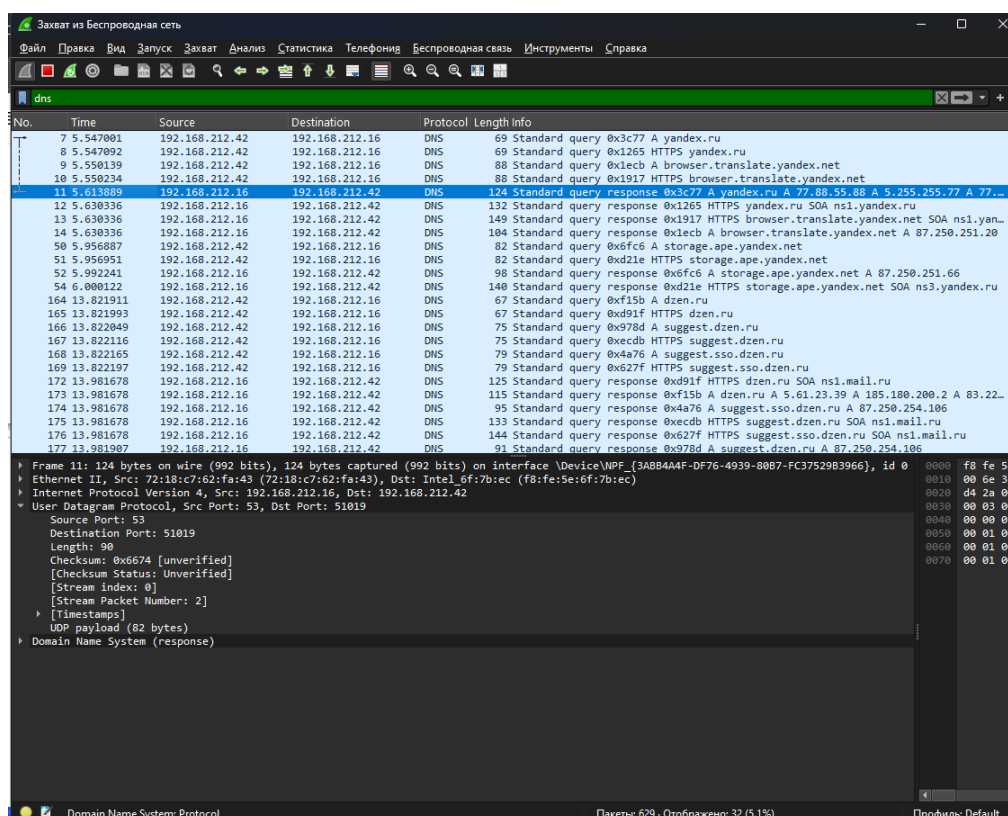
- Запросы на разрешение имени yandex.ru и других доменов.

- Ответы содержат несколько IP-адресов для одного доменного имени.
- Применялись стандартные порты: источник — динамический порт клиента, назначение — 53/UDP.

No.	Time	Source	Destination	Protocol	Length	Info
7	5.547001	192.168.212.42	192.168.212.16	DNS	69	Standard query 0x3c77 A yandex.ru
8	5.547092	192.168.212.42	192.168.212.16	DNS	69	Standard query 0x1265 HTTPS yandex.ru
9	5.550139	192.168.212.42	192.168.212.16	DNS	88	Standard query 0x1ecb A browser.translate.yandex.net
10	5.550234	192.168.212.42	192.168.212.16	DNS	88	Standard query 0x1917 HTTPS browser.translate.yandex.net
11	5.613089	192.168.212.16	192.168.212.42	DNS	124	Standard query response 0x3c77 A yandex.ru A 77.88.55.88 A 5.255.255.77 A 77...
12	5.630336	192.168.212.16	192.168.212.42	DNS	132	Standard query response 0x1265 HTTPS yandex.ru SOA ns1.yandex.ru
13	5.630336	192.168.212.16	192.168.212.42	DNS	149	Standard query response 0x1917 HTTPS browser.translate.yandex.net SOA ns1.yan...
14	5.630336	192.168.212.16	192.168.212.42	DNS	104	Standard query response 0x1ecb A browser.translate.yandex.net A 87.250.251.20
50	5.956887	192.168.212.42	192.168.212.16	DNS	82	Standard query 0x6fc6 A storage.ape.yandex.net
51	5.956951	192.168.212.42	192.168.212.16	DNS	82	Standard query 0xd21e HTTPS storage.ape.yandex.net
52	5.992241	192.168.212.16	192.168.212.42	DNS	98	Standard query response 0x6fc6 A storage.ape.yandex.net A 87.250.251.66
54	6.000122	192.168.212.16	192.168.212.42	DNS	140	Standard query response 0xd21e HTTPS storage.ape.yandex.net SOA ns3.yandex.ru
164	13.821911	192.168.212.42	192.168.212.16	DNS	67	Standard query 0xf15b A dzen.ru
165	13.821993	192.168.212.42	192.168.212.16	DNS	67	Standard query 0xd91f HTTPS dzen.ru
166	13.822049	192.168.212.42	192.168.212.16	DNS	75	Standard query 0x978d A suggest.dzen.ru
167	13.822116	192.168.212.42	192.168.212.16	DNS	75	Standard query 0xecdb HTTPS suggest.dzen.ru
168	13.822165	192.168.212.42	192.168.212.16	DNS	79	Standard query 0x4a76 A suggest.sso.dzen.ru
169	13.822197	192.168.212.42	192.168.212.16	DNS	79	Standard query 0x627f HTTPS suggest.sso.dzen.ru
172	13.981678	192.168.212.16	192.168.212.42	DNS	125	Standard query response 0xd91f HTTPS dzen.ru SOA ns1.mail.ru
173	13.981678	192.168.212.16	192.168.212.42	DNS	115	Standard query response 0xf15b A dzen.ru A 5.61.23.39 A 185.180.200.2 A 83.22...
174	13.981678	192.168.212.16	192.168.212.42	DNS	95	Standard query response 0x4a76 A suggest.sso.dzen.ru A 87.250.254.106
175	13.981678	192.168.212.16	192.168.212.42	DNS	133	Standard query response 0xecdb HTTPS suggest.dzen.ru SOA ns1.mail.ru
176	13.981678	192.168.212.16	192.168.212.42	DNS	144	Standard query response 0x627f HTTPS suggest.sso.dzen.ru SOA ns1.mail.ru
177	13.981907	192.168.212.16	192.168.212.42	DNS	91	Standard query response 0x978d A suggest.dzen.ru A 87.250.254.106

▶ Frame 7: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \DeviceNPF_{3A8B44AF-DF76-4939-8067-FC3752983966}, id 0
 ▶ Ethernet II, Src: Intel_E7:70:ec (f8:fe:5e:ef:7b:ec), Dst: 72:18:c7:62:fa:43 (72:18:c7:62:fa:43)
 ▶ Internet Protocol Version 4, Src: 192.168.212.42, Dst: 192.168.212.16
 ▶ User Datagram Protocol, Src Port: 51019, Dst Port: 53
 Source Port: 51019
 Destination Port: 53
 Length: 35
 Checksum: 0x29c1 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 0]
 [Stream Packet Number: 1]
 [Timestamps]
 UDP payload (27 bytes)
 Domain Name System (query)

Domain Name System Protocol Пакеты: 625 · Отображено: 32 (5.1%) Профиль: Default



5. После этого был применён фильтр quic. В списке пакетов отобразились сессии по протоколу **QUIC** (поверх UDP):

- Видны начальные пакеты соединения Initial с идентификаторами сессий.
- Присутствуют зашифрованные сегменты Protected Payload.
- Передача данных осуществляется через порт 443/UDP.
- QUIC обеспечивает функции транспортного уровня, аналогичные TCP, но с более высокой производительностью.

The image displays a Wireshark packet capture analysis of QUIC traffic. The top pane shows a list of packets with details for packet 1258, including QUIC connection information and protected payloads. The bottom pane shows a detailed view of packet 902, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and QUIC connection information.

Packet 1258 Details:

- Length: 1258
- Checksum: 0x7f16 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 30]
- [Stream Packet Number: 2]
- [Timestamps]
- UDP payload (1258 bytes)
- QUIC IETF
 - QUIC Connection information
 - [Packet Length: 1258]
 - 1... .. = Header Form: Long Header (1)
 - 1... .. = Fixed Bit: True
 - ..00 = Packet Type: Initial (0)
 - [... ..00.. = Reserved: 0]
 - [... ..01.. = Packet Number Length: 2 bytes (1)]
 - Version: 1 (0x00000001)
 - Destination Connection ID Length: 8
 - Destination Connection ID: b44232ab7d0c5a9a
 - Source Connection ID Length: 0
 - Token Length: 70
 - Token: 0049ef0765945e4701d31db938a8c75f54b1741b74e812df8170af582963ebf95c0694a157a21e1942987b40fbd0159d31a65d6d2dd4af9e4cee572bdc228
 - Length: 1161
 - [Packet Number: 2]
 - Payload [-]: cdc27d01530322f1b10c0e5386357f460c45a933c92cdc7649c8cbe63b4ad009133a8d6be619f21f2177bb7f370a9e6478e07859581a3b04256c2b0

Packet 902 Details:

- Frame 902: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{3AB84A4F-DF76-4939-8087-FC37529B3966}, id 0
- Ethernet II, Src: Intel_Gf7b0ec (f8:fe:5e:6f:7b:ec), Dst: 72:18:c7:62:fa:43 (72:18:c7:62:fa:43)
- Internet Protocol Version 4, Src: 192.168.212.42, Dst: 64.233.164.94
- User Datagram Protocol, Src Port: 51952, Dst Port: 443
- Source Port: 51952
- Destination Port: 443
- Length: 39
- Checksum: 0x7a53 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 30]
- [Stream Packet Number: 14]
- [Timestamps]
- UDP payload (31 bytes)
- QUIC IETF
 - QUIC Connection information
 - [Packet Length: 31]
 - QUIC Short Header DCID=f44232ab7d0c5a9a
 - Remaining Payload: d674a6f471bf9a3aa6bac898cee151c6190c6bc2e3f0

6. Захват трафика был завершён.

3.3 Анализ handshake протокола TCP в Wireshark

1. На устройстве был запущен **Wireshark**, выбран активный сетевой интерфейс и начат захват пакетов.
2. Для анализа установленного соединения было выполнено обращение к сайту по протоколу **HTTP**. В процессе обмена зафиксированы пакеты TCP, включая этап установки соединения (handshake).
3. Анализ TCP handshake:
 - Первое сообщение (SYN) инициирует соединение, устанавливается начальный порядковый номер (Sequence Number).
 - Второе сообщение (SYN, ACK) подтверждает приём SYN от клиента и устанавливает собственный порядковый номер.
 - Третье сообщение (ACK) завершает процесс трёхстороннего рукопожатия, соединение считается установленным.

На скриншоте ниже виден процесс установления соединения по TCP, включая SYN, SYN-ACK и ACK:

The image shows a Wireshark packet capture with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
25	4.101214	77.88.21.232	192.168.212.42	TLSv1.2	495	Application Data
26	4.108710	188.184.67.127	192.168.212.42	TCP	66	80 → 59891 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1300 SACK_PERM WS=...
27	4.108768	192.168.212.42	188.184.67.127	TCP	54	59891 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
28	4.108995	192.168.212.42	188.184.67.127	HTTP	638	GET /hypertext/WWW/TheProject.html HTTP/1.1
29	4.116132	188.184.67.127	192.168.212.42	TCP	66	80 → 59890 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1300 SACK_PERM WS=...
30	4.116187	192.168.212.42	188.184.67.127	TCP	54	59890 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
31	4.146548	192.168.212.42	77.88.21.232	TCP	54	59850 → 443 [ACK] Seq=1935 Ack=883 Win=511 Len=0
32	4.184953	188.184.67.127	192.168.212.42	TCP	54	80 → 59891 [ACK] Seq=1 Ack=585 Win=31872 Len=0
33	4.188782	188.184.67.127	192.168.212.42	HTTP	250	HTTP/1.1 304 Not Modified
34	4.188782	188.184.67.127	192.168.212.42	TCP	54	80 → 59891 [FIN, ACK] Seq=197 Ack=585 Win=31872 Len=0
35	4.188841	192.168.212.42	188.184.67.127	TCP	54	59891 → 80 [ACK] Seq=585 Ack=198 Win=131072 Len=0
36	4.189122	192.168.212.42	188.184.67.127	TCP	54	59891 → 80 [FIN, ACK] Seq=585 Ack=198 Win=131072 Len=0
37	4.200755	192.168.212.42	77.88.21.232	TLSv1.2	1059	Application Data
38	4.201349	192.168.212.42	192.168.212.16	DNS	88	Standard query 0xc301 A browser.translate.yandex.net
39	4.201429	192.168.212.42	192.168.212.16	DNS	88	Standard query 0x91a8 HTTPS browser.translate.yandex.net
40	4.201534	192.168.212.42	87.250.251.20	TLSv1.2	249	Ignored Unknown Record
41	4.201567	192.168.212.42	87.250.251.20	TLSv1.2	100	Application Data
42	4.201576	192.168.212.42	87.250.251.20	TLSv1.2	1116	Application Data
43	4.259376	188.184.67.127	192.168.212.42	TCP	54	80 → 59891 [ACK] Seq=198 Ack=586 Win=31872 Len=0

Рис. 3.7: TCP Handshake

4. В ходе обмена были также зафиксированы HTTP-запросы и ответы поверх установленного TCP-соединения. Например:

- GET /hypertext/WWW/TheProject.html HTTP/1.1

- Ответ сервера: HTTP/1.1 304 Not Modified

5. Для наглядности в меню **Статистика → График Потока** был построен график TCP-сессии. На нём отображается трёхстороннее рукопожатие:

- Первый сегмент SYN от клиента.
- Ответный сегмент SYN, ACK от сервера.
- Заключительный сегмент ACK от клиента.

После этого происходит передача HTTP-запроса и ответа.

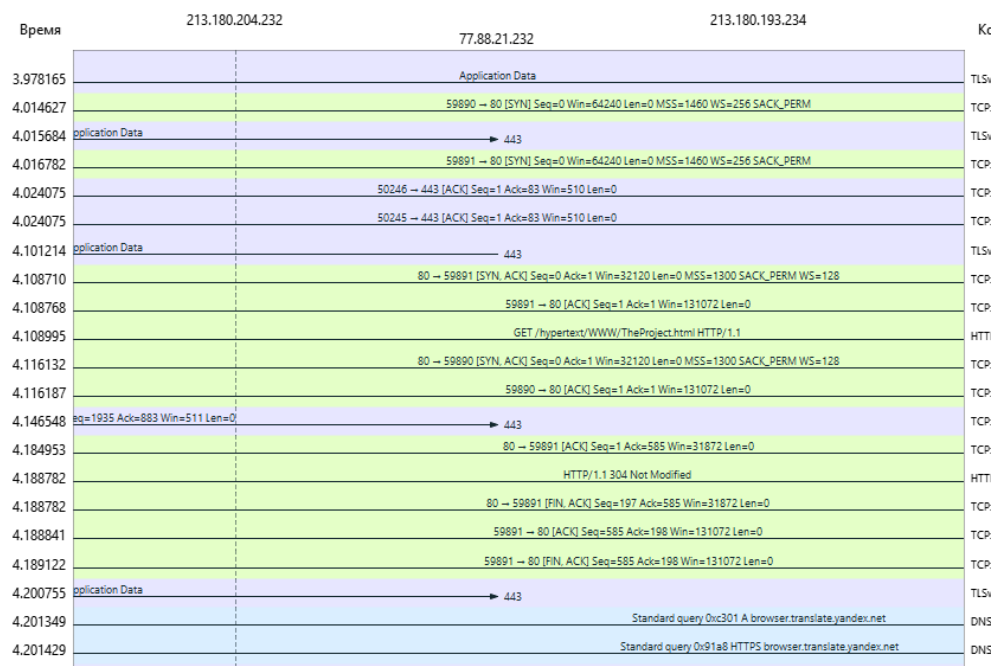


Рис. 3.8: График потока TCP

6. Захват трафика был остановлен.

4 Заключение

В ходе работы был проанализирован процесс установления соединения по протоколу TCP.

С помощью Wireshark зафиксированы пакеты трёхстороннего рукопожатия (SYN, SYN-ACK, ACK), а также последующая передача данных HTTP.