Отчёт по лабораторной работе 3

Анализ трафика в Wireshark

Хамди Мохаммад

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Ход выполнения

2.1 Анализ кадров канального уровня в Wireshark

1. На устройство была установлена программа **Wireshark** и запущен захват трафика на активном сетевом интерфейсе.

2. С помощью команды **ipconfig** были определены параметры сетевого подключения:

    - IP-адрес устройства — **192.168.1.35**

    - Маска подсети — **255.255.255.0**

    - Шлюз по умолчанию — **192.168.1.1**

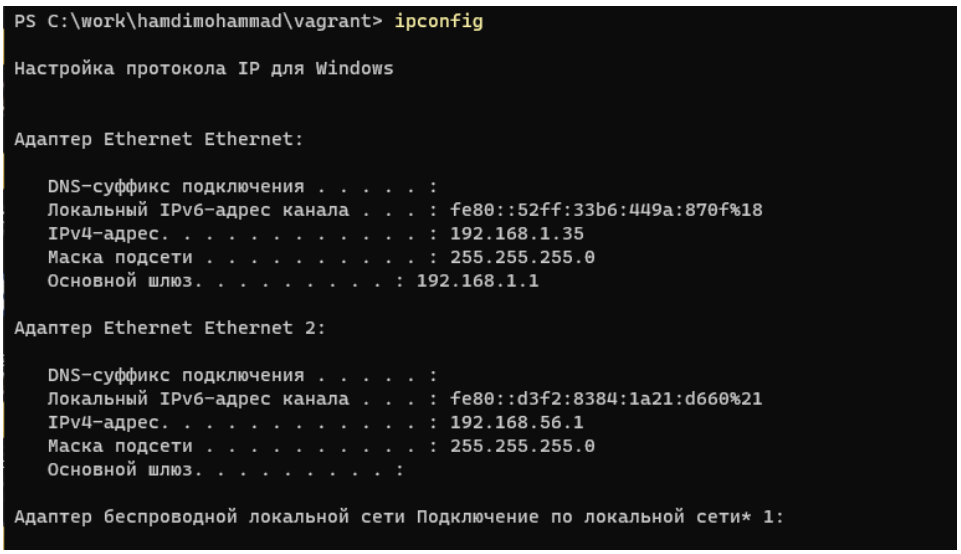


Рис. 2.1: Результат команды ipconfig

3. Для проверки доступности шлюза по умолчанию выполнена команда **ping 192.168.1.1**.

   Ответы получены успешно, потерь пакетов нет.

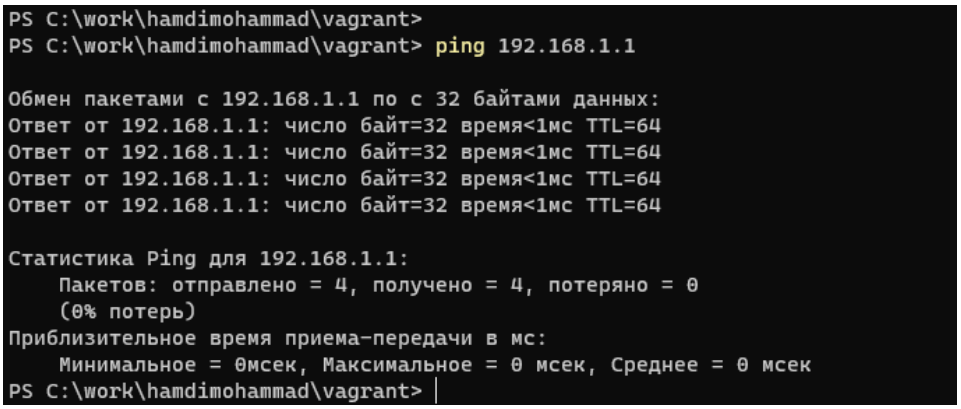
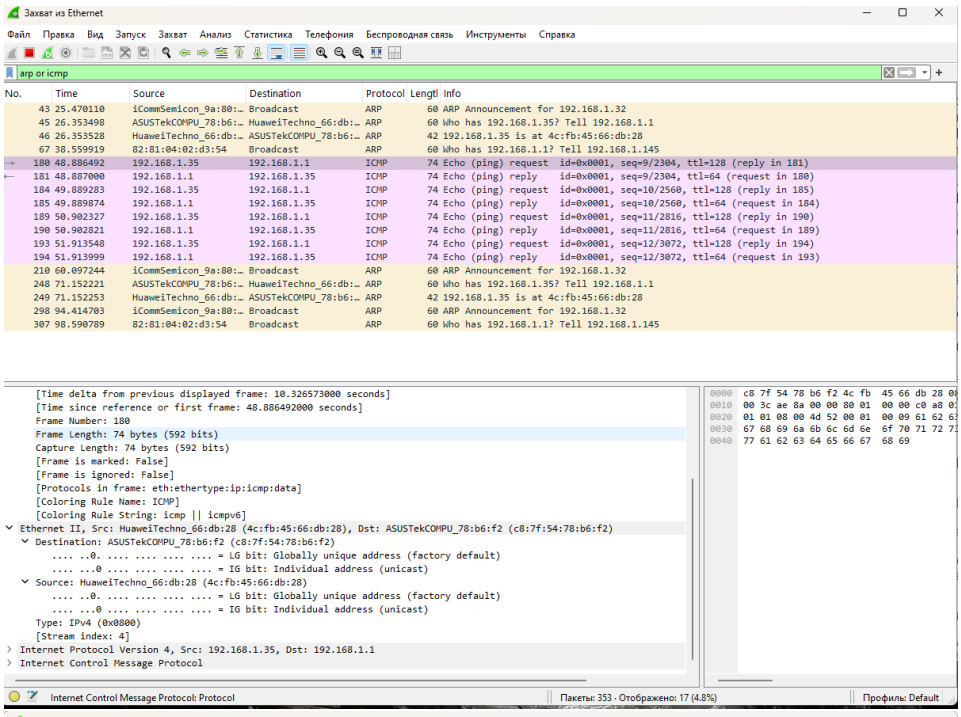
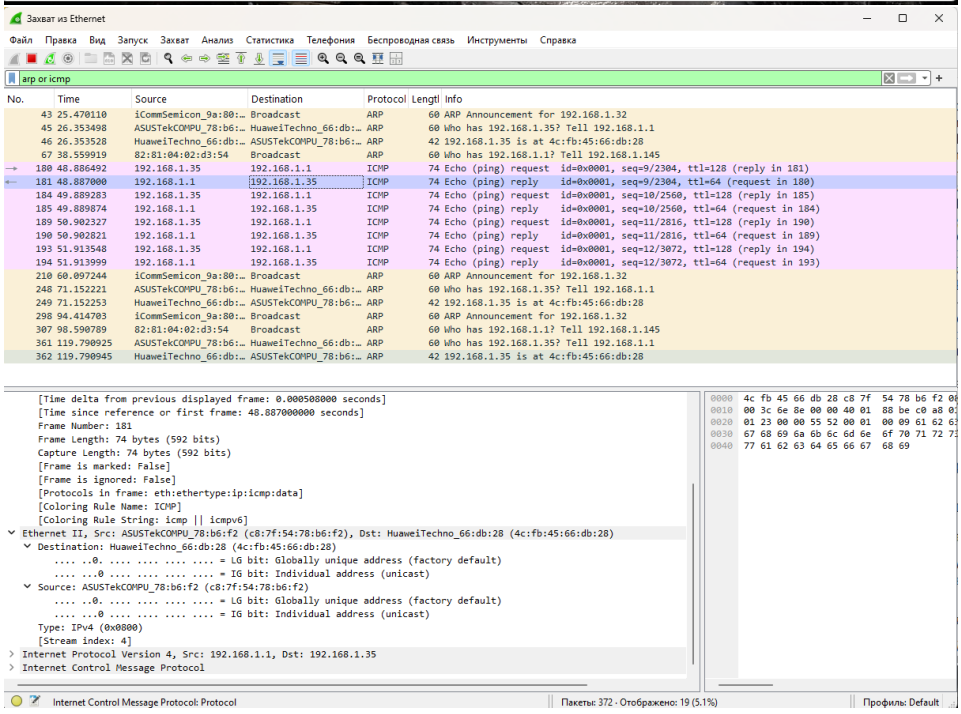
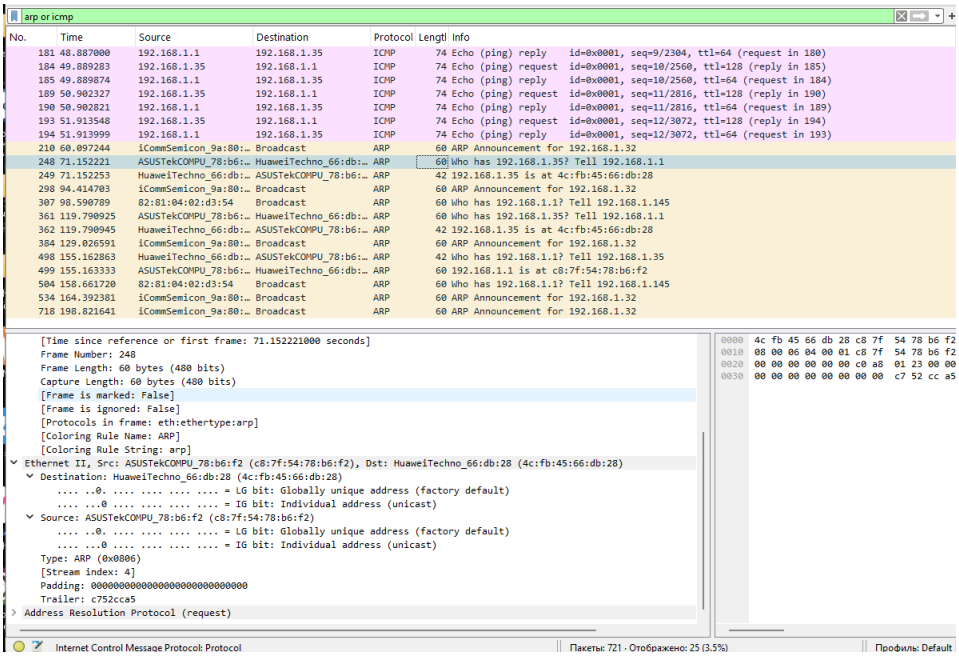


Рис. 2.2: Проверка доступности шлюза

4. В **Wireshark** был применён фильтр `arp or icmp`, после чего зафиксированы ICMP-запросы и ответы между устройством и шлюзом.


Захват из Ethernet
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
arp or icmp
No. Time Source Destination Protocol Lengtl Info
43 25.470110 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
45 26.353498 ASUSTekCOMPU_78:b6:… HuaweiTechno_66:db:… ARP 60 Who has 192.168.1.35? Tell 192.168.1.1
46 26.353528 HuaweiTechno_66:db:… ASUSTekCOMPU_78:b6:… ARP 42 192.168.1.35 is at 4c:fb:45:66:db:28
67 38.559919 82:81:04:02:d3:54 Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.145
180 48.886492 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 181)
181 48.887000 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 180)
184 49.889283 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 185)
185 49.889874 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 184)
189 50.902327 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 190)
190 50.902821 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 189)
193 51.913548 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 194)
194 51.913999 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 193)
210 60.097244 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
248 71.152221 ASUSTekCOMPU_78:b6:… HuaweiTechno_66:db:… ARP 60 Who has 192.168.1.35? Tell 192.168.1.1
249 71.152253 HuaweiTechno_66:db:… ASUSTekCOMPU_78:b6:… ARP 42 192.168.1.35 is at 4c:fb:45:66:db:28
298 94.414703 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
307 98.590789 82:81:04:02:d3:54 Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.145
[Time delta from previous displayed frame: 10.326573000 seconds]
[Time since reference or first frame: 48.886492000 seconds]
Frame Number: 180
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: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 4]
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
Internet Control Message Protocol
0000 c8 7f 54 78 b6 f2 4c fb 45 66 db 28 08
0010 00 3c ae 8a 00 00 80 01 00 00 c0 a8 01
0020 01 01 08 00 4d 52 00 01 00 09 61 62 63
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
0040 77 61 62 63 64 65 66 67 68 69
Internet Control Message Protocol: Protocol
Пакеты: 353 · Отображено: 17 (4.8%)
Профиль: Default


Захват из Ethernet
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
arp or icmp
No. Time Source Destination Protocol Lengtl Info
43 25.470110 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
45 26.353498 ASUSTekCOMPU_78:b6:… HuaweiTechno_66:db:… ARP 60 Who has 192.168.1.35? Tell 192.168.1.1
46 26.353528 HuaweiTechno_66:db:… ASUSTekCOMPU_78:b6:… ARP 42 192.168.1.35 is at 4c:fb:45:66:db:28
67 38.559919 82:81:04:02:d3:54 Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.145
180 48.886492 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 181)
181 48.887000 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 180)
184 49.889283 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 185)
185 49.889874 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 184)
189 50.902327 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 190)
190 50.902821 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 189)
193 51.913548 192.168.1.35 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 194)
194 51.913999 192.168.1.1 192.168.1.35 ICMP 74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 193)
210 60.097244 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
248 71.152221 ASUSTekCOMPU_78:b6:… HuaweiTechno_66:db:… ARP 60 Who has 192.168.1.35? Tell 192.168.1.1
249 71.152253 HuaweiTechno_66:db:… ASUSTekCOMPU_78:b6:… ARP 42 192.168.1.35 is at 4c:fb:45:66:db:28
298 94.414703 iCommSemicon_9a:80:… Broadcast ARP 60 ARP Announcement for 192.168.1.32
307 98.590789 82:81:04:02:d3:54 Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.145
361 119.790925 ASUSTekCOMPU_78:b6:… HuaweiTechno_66:db:… ARP 60 Who has 192.168.1.35? Tell 192.168.1.1
362 119.790945 HuaweiTechno_66:db:… ASUSTekCOMPU_78:b6:… ARP 42 192.168.1.35 is at 4c:fb:45:66:db:28
[Time delta from previous displayed frame: 0.000508000 seconds]
[Time since reference or first frame: 48.887000000 seconds]
Frame Number: 181
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: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
Destination: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 4]
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35
Internet Control Message Protocol
0000 4c fb 45 66 db 28 c8 7f 54 78 b6 f2 08
0010 00 3c 6e 8e 00 00 40 01 88 be c0 a8 01
0020 01 23 00 00 55 52 00 01 00 09 61 62 63
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
0040 77 61 62 63 64 65 66 67 68 69
Internet Control Message Protocol: Protocol
Пакеты: 372 · Отображено: 19 (5.1%)
Профиль: Default



Анализ ICMP-запроса:

- Длина кадра: **74 байта**
- Тип кадра: **Ethernet II**
- MAC-адрес источника: **4c:fb:45:66:db:28** (устройство)
- MAC-адрес получателя (шлюз): **c8:7f:54:78:b6:f2**
- Тип MAC-адресов: **уникальные (unicast)**

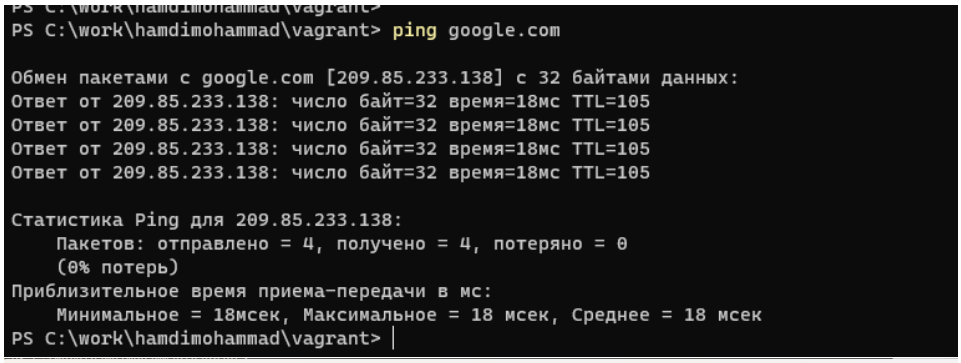
Анализ ICMP-ответа:

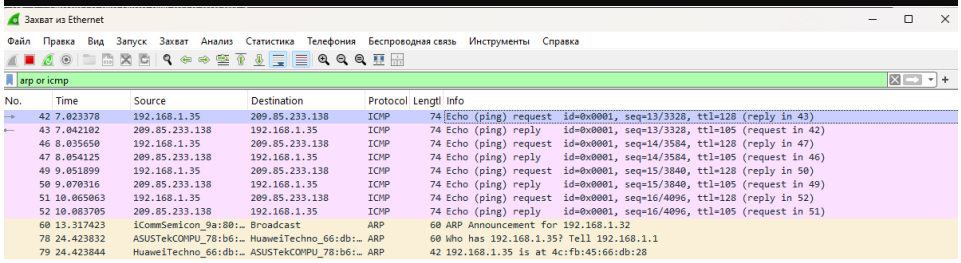
- Длина кадра: **74 байта**
- Тип кадра: **Ethernet II**
- MAC-адрес источника (шлюз): **c8:7f:54:78:b6:f2**

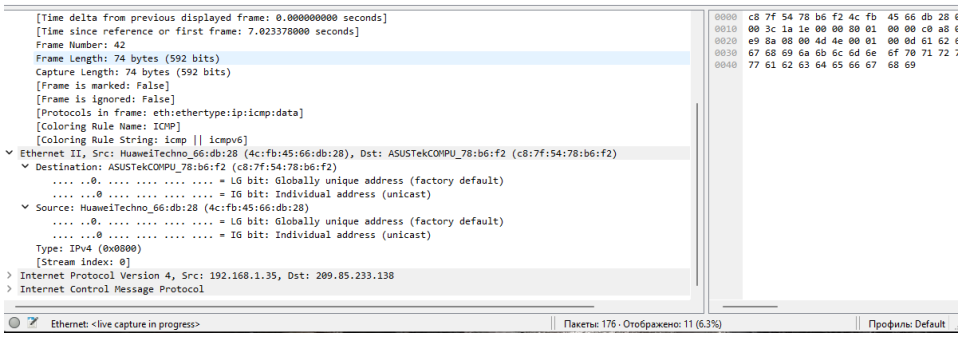
- MAC-адрес получателя (устройство): **4c:fb:45:66:db:28**

- Тип MAC-адресов: **уникальные (unicast)**

5. Далее изучены кадры протокола **ARP**, фиксирующие обмен информацией об IP- и MAC-адресах в сети.







ARP-запрос:

- “Кто имеет IP **192.168.1.35**?”

- Источник: **c8:7f:54:78:b6:f2**

- Адрес назначения: **ff:ff:ff:ff:ff:ff** (широковещательный, broadcast)

ARP-ответ:

- “IP **192.168.1.35** принадлежит MAC **4c:fb:45:66:db:28**”

- Источник: **4c:fb:45:66:db:28**

- Адрес назначения: **c8:7f:54:78:b6:f2**

6. Для анализа взаимодействия с внешними ресурсами был выполнен **ping google.com**.
   Устройство получило ответы от IP-адреса **209.85.233.138**, время отклика составило в среднем **18 мс**.

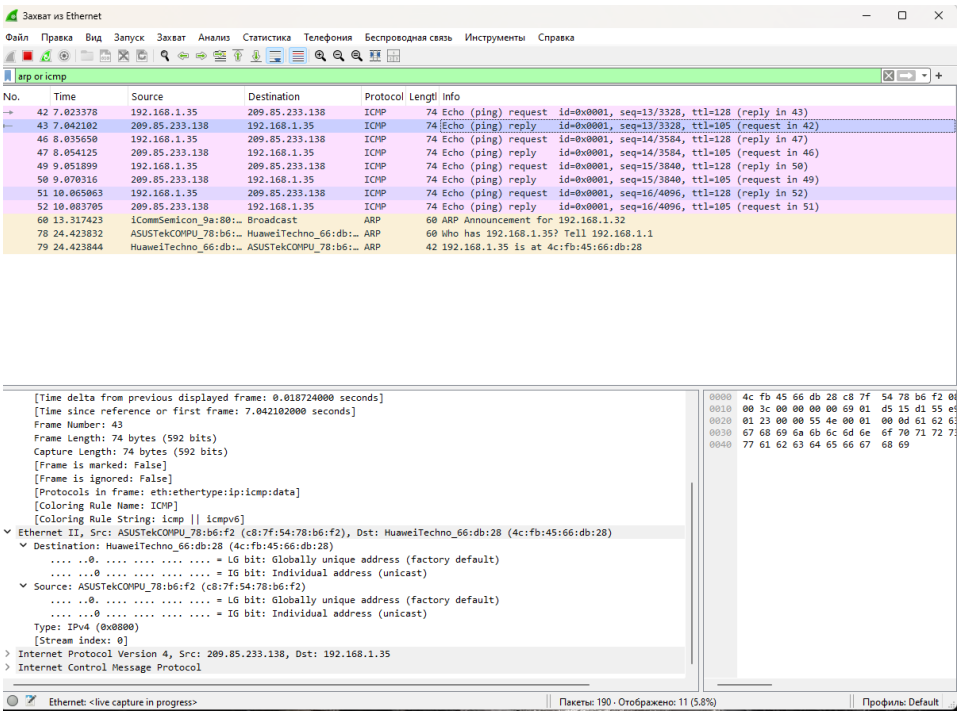


Рис. 2.3: Проверка доступности внешнего ресурса

В Wireshark были зафиксированы соответствующие ICMP-запросы и ответы, а также ARP-обмен для определения адреса шлюза.

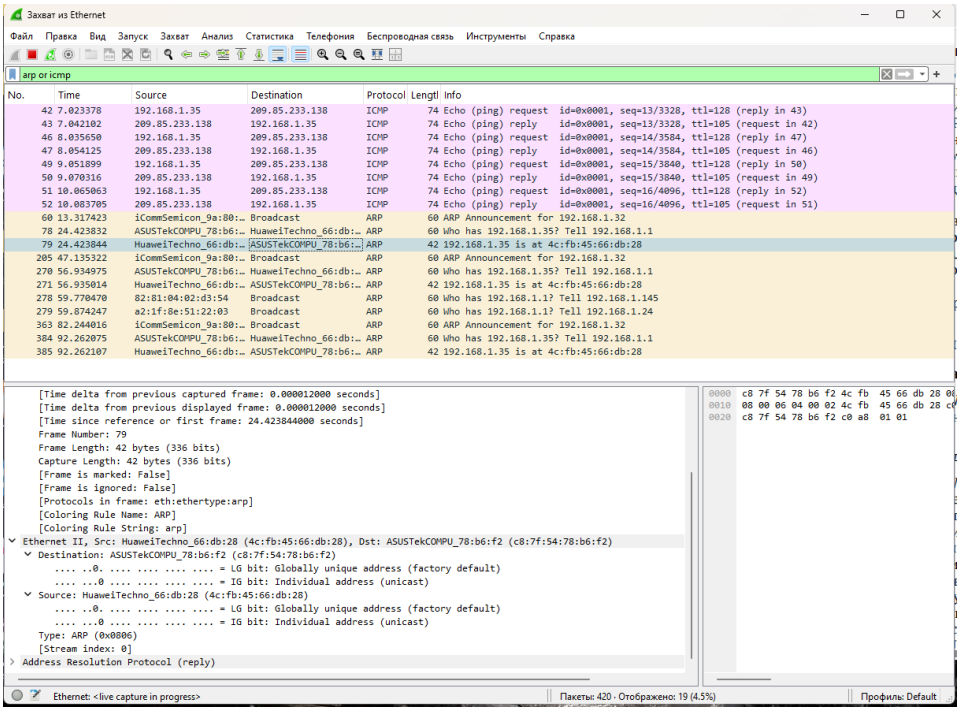
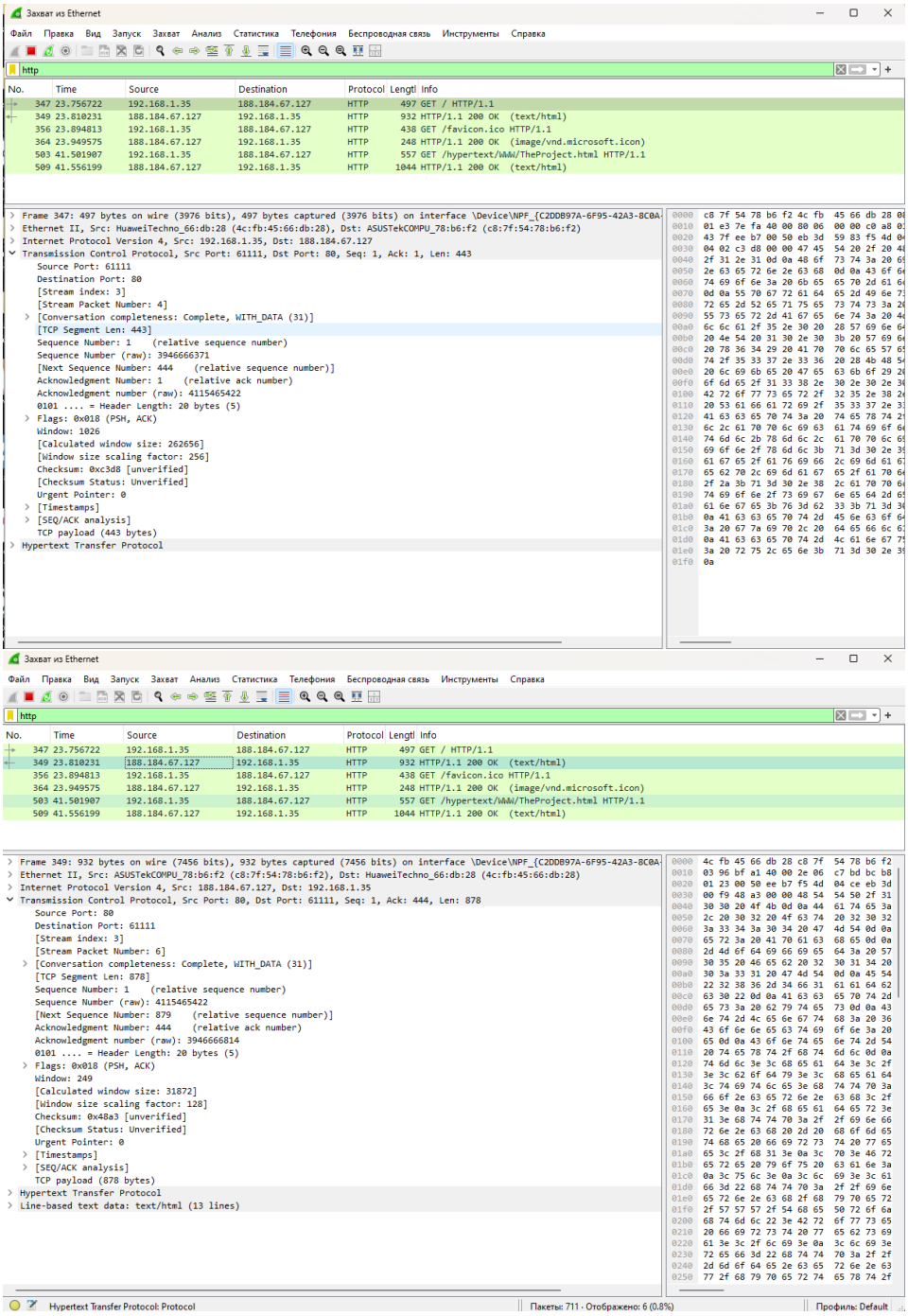


Рис. 2.4: Анализ ICMP-трафика при ping google.com

2.2 Анализ протоколов транспортного уровня в Wireshark

1. В программе **Wireshark** был запущен захват трафика на активном сетевом интерфейсе.
2. В браузере произведён переход на сайт **http://info.cern.ch/**, работающий по протоколу **HTTP**.
3. В Wireshark применён фильтр `http`. Зафиксирован обмен HTTP-запросами и ответами поверх протокола **TCP**.



Пояснение:

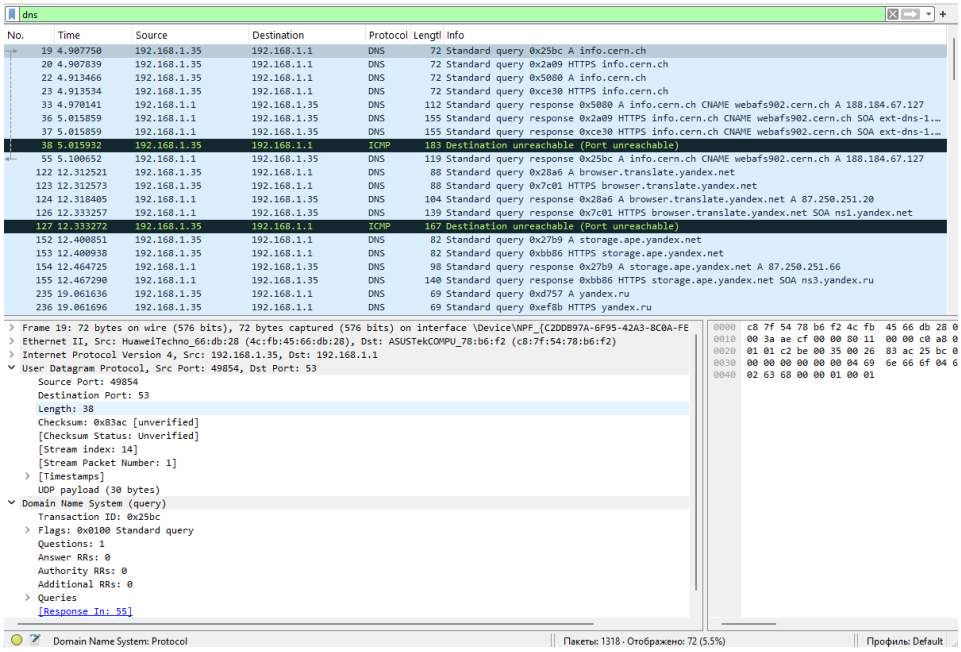
- Запрос отправляется с порта **61111** клиента (192.168.1.35) на порт **80** сервера (188.184.67.127).

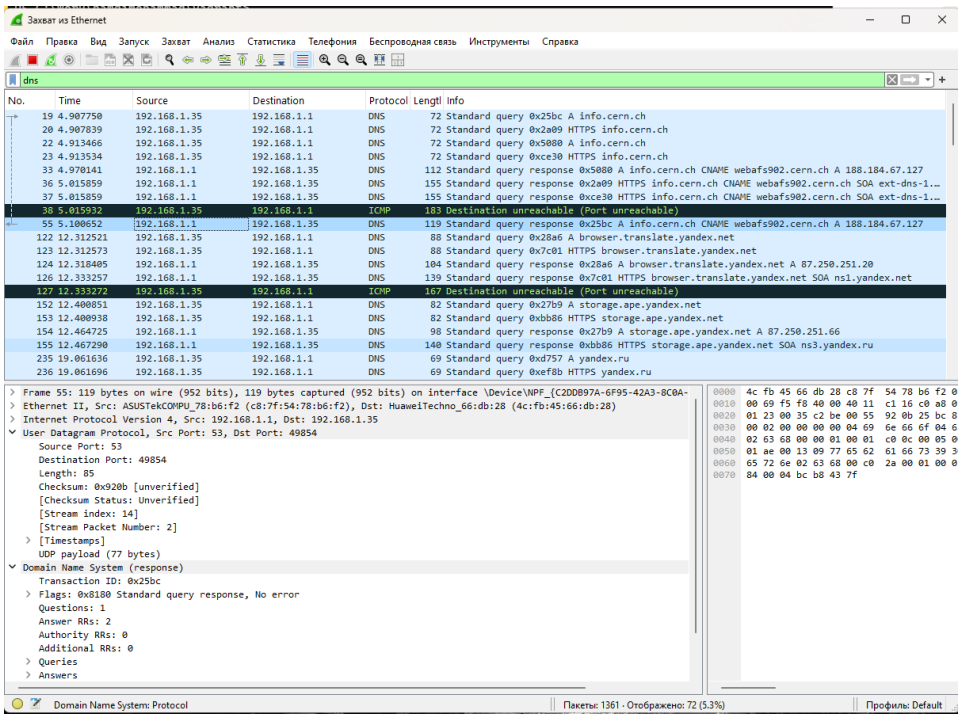
- Используется протокол **Ethernet II → IPv4 → TCP → HTTP**.

- В TCP-сегменте указывается **Sequence Number** и **Acknowledgment Number**, обеспечивающие надёжную доставку данных.

- В кадре видно передачу **HTTP GET-запроса** и ответ **HTTP/1.1 200 OK** с HTML-страницей.

4. В Wireshark применён фильтр `dns`. Зафиксированы запросы и ответы по протоколу **DNS**, работающему поверх **UDP**.





Пояснение:

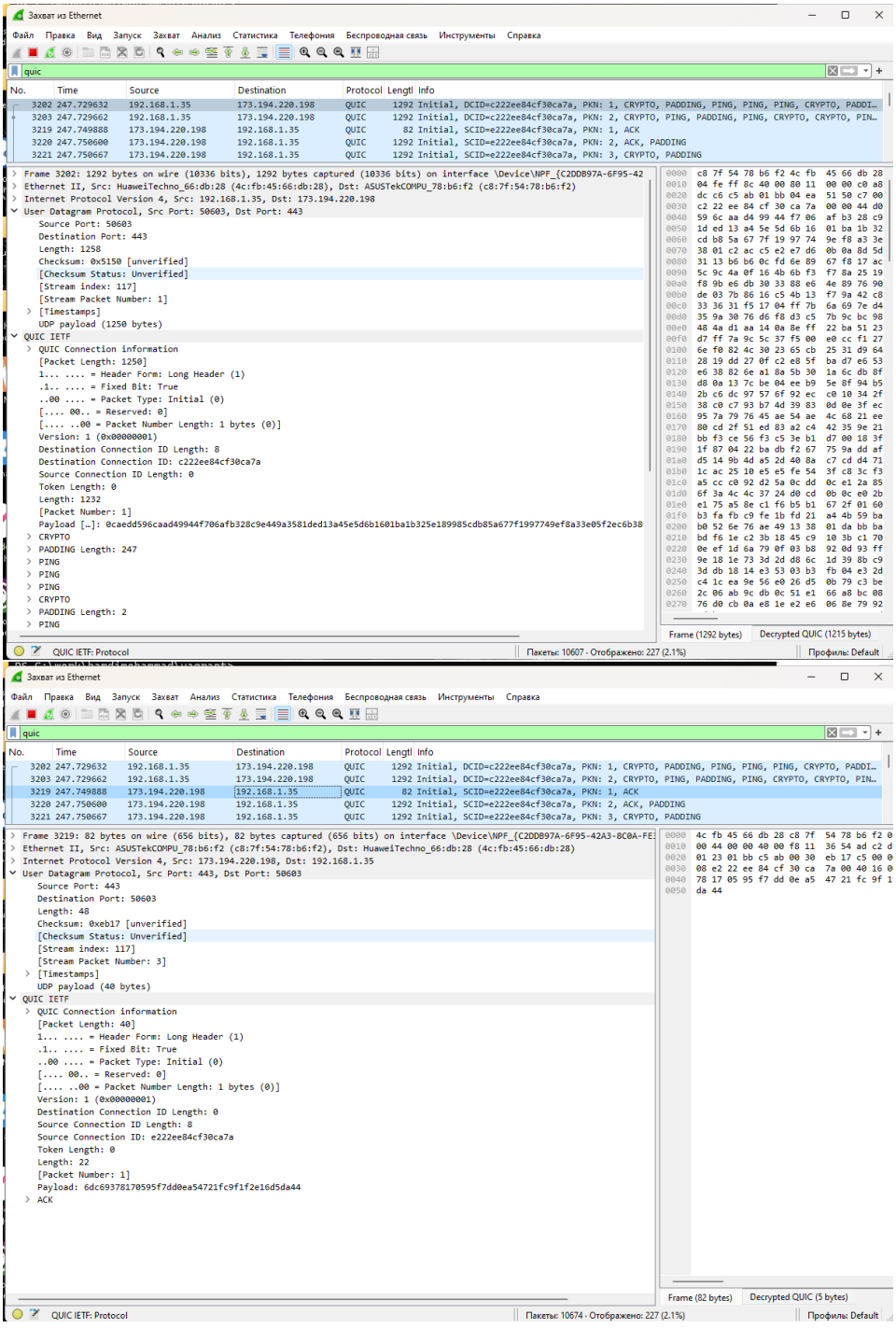
- Запрос отправляется с порта **49854** клиента (192.168.1.35) на порт **53** сервера (192.168.1.1).

- Пример: запрос имени `info.cern.ch` с типом записи **A**.

- В ответ сервер возвращает IP-адрес **188.184.67.127**, что подтверждает успешное разрешение имени.

- Используется структура: **Ethernet II → IPv4 → UDP → DNS**.

5. В Wireshark применён фильтр `quic`. Зафиксирован обмен трафиком по протоколу **QUIC**, работающему поверх **UDP**.



Пояснение:

- Источник: клиент **192.168.1.35**, назначение: сервер **173.194.220.198**, порт **443**.

- Используется протокол: **Ethernet II → IPv4 → UDP → QUIC**.

2.3 Анализ handshake протокола TCP в Wireshark

1. В программе **Wireshark** был запущен захват трафика на активном сетевом интерфейсе.

2. Для генерации TCP-трафика было выполнено соединение с веб-сервером по протоколу **HTTP**.

3. В Wireshark зафиксирован процесс установления TCP-сессии (трёхсторонее рукопожатие).

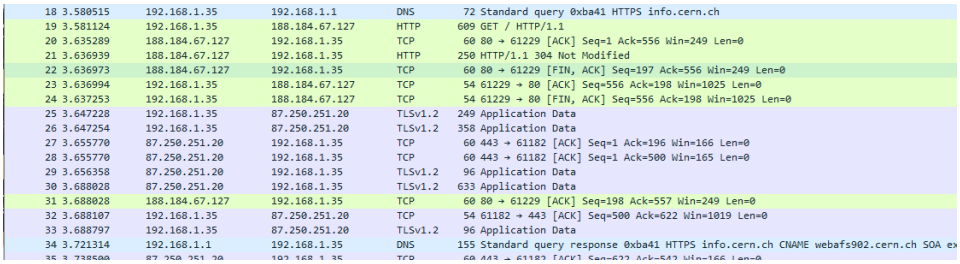


Рис. 2.5: Анализ TCP-сессии

Этапы установления соединения:

- **SYN**: клиент (192.168.1.35) отправляет на сервер (188.184.67.127) запрос на установление соединения с флагом SYN и начальным номером последовательности (**Seq = 1**).

- **SYN + ACK**: сервер отвечает подтверждением с флагами SYN и ACK, устанавливая свой номер последовательности (**Seq = 1**) и подтверждая получение данных клиента (**Ack = 2**).

- **ACK**: клиент подтверждает получение пакета от сервера, устанавливая **Ack = 2**.

После этого соединение считается установленным, и возможна передача данных (HTTP-запрос/ответ).

4. Для анализа был построен **график потока** (Flow Graph) в Wireshark.

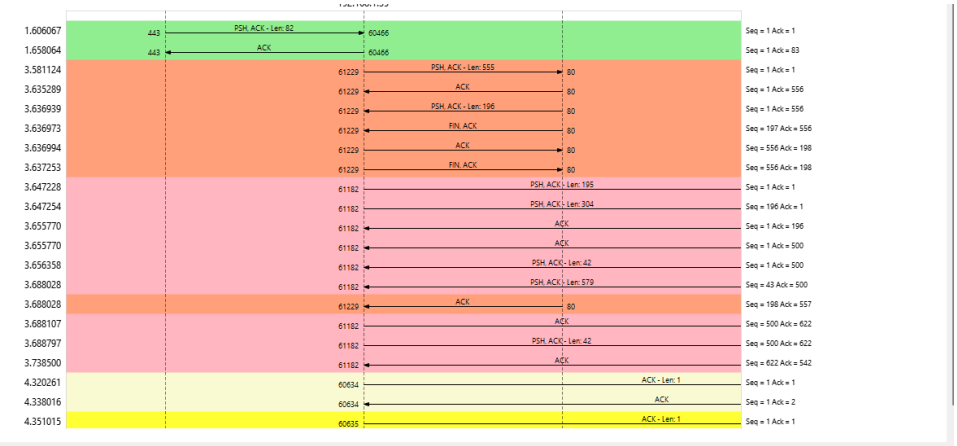


Рис. 2.6: График потока TCP

Пояснение к графику:

- На графике наглядно отображены все этапы TCP-взаимодействия.
- Видно трёхстороннее рукопожатие (SYN → SYN+ACK → ACK).
- После установления соединения фиксируется передача данных (HTTP GET, ответы сервера, обмен ACK).
- Завершение соединения происходит с помощью пакетов **FIN, ACK**, что также отражено на графике.

5. После анализа захват трафика в Wireshark был остановлен.

3 Заключение

В ходе работы был проведён анализ установления соединения по протоколу **TCP** с использованием программы **Wireshark**.
Было зафиксировано трёхстороннее рукопожатие (SYN → SYN+ACK → ACK), подтверждающее успешное начало TCP-сессии.
С помощью графика потока были проанализированы этапы установления и завершения соединения, а также последующая передача данных.