Отчёт по лабораторной работе №3

Анализ трафика в Wireshark

Авдадаев Джамал Геланиевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение задания

2.1 Анализ кадров канального уровня в Wireshark

2.1.1 Установка и запуск программы захвата трафика

В ходе выполнения лабораторной работы на домашнем устройстве была установлена программа Wireshark, после чего выбран активный сетевой интерфейс и запущен процесс захвата сетевого трафика. Для отображения только интересующих пакетов в строке фильтра был использован фильтр `arp or icmp`, позволяющий выделить кадры протоколов ARP и ICMP.

Перед началом анализа в консоли операционной системы с помощью команды ipconfig были определены IP-адрес устройства и адрес шлюза по умолчанию. Далее для генерации сетевого трафика был выполнен эхо-запрос к шлюзу.

2.1.2 Проверка доступности шлюза и удалённых узлов

С целью генерации ICMP-трафика была выполнена серия эхо-запросов к шлюзу по умолчанию, а также к внешним сетевым ресурсам.

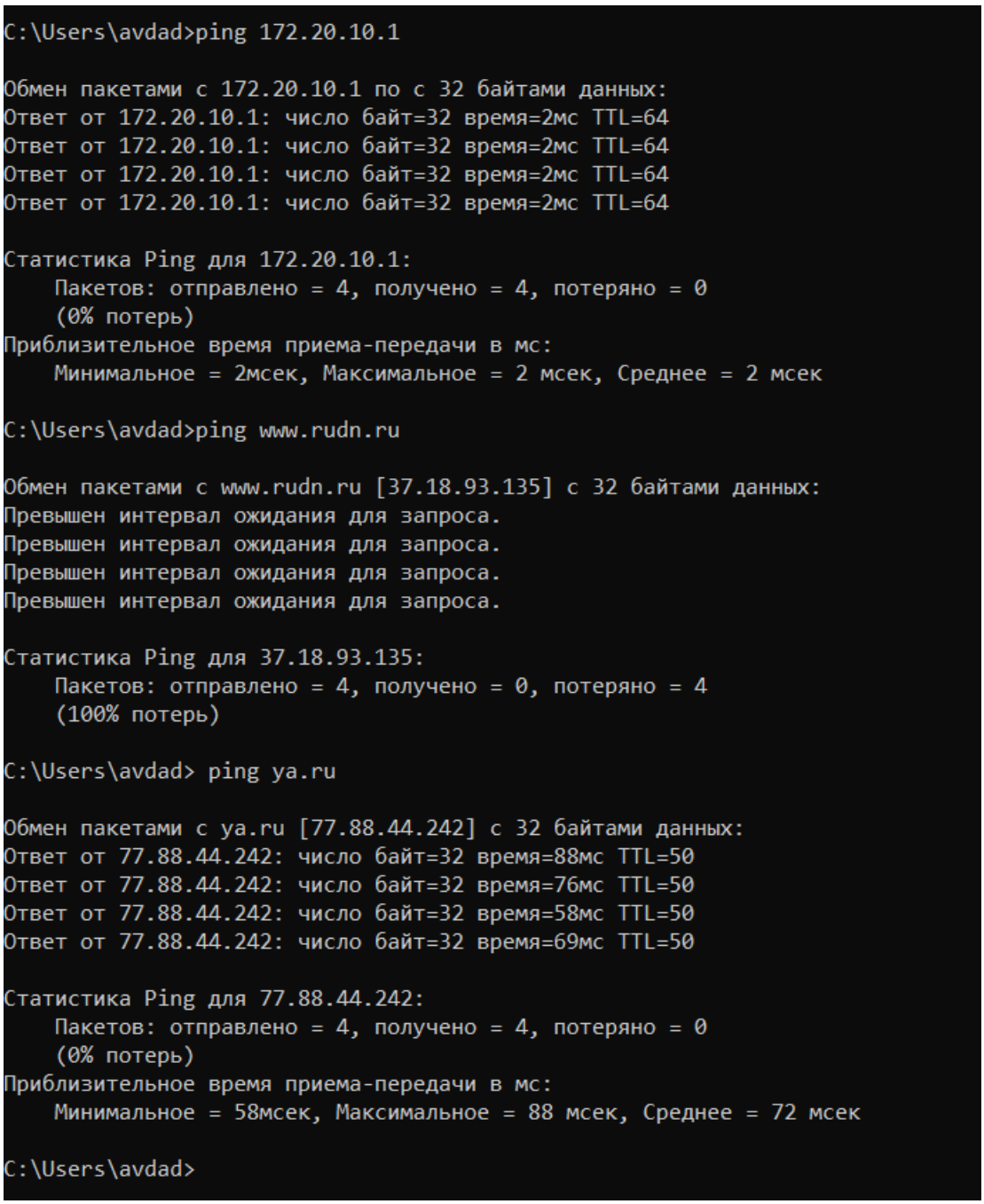

Рис. 2.1: Результаты выполнения команды ping

В результате: - при обращении к адресу шлюза ответы приходят без потерь; - при обращении к одному из внешних ресурсов наблюдается отсутствие ответов; - при обращении к другому доменному имени ответы успешно получены, что подтверждает работоспособность сетевого соединения и прохождение ICMP-

пакетов через шлюз.

2.1.3 Анализ ICMP-кадра (эхо-запрос)

После выполнения команды ping в Wireshark были отфильтрованы ICMP-пакеты. В верхней панели списка пакетов был выбран первый ICMP-кадр — эхо-запрос.

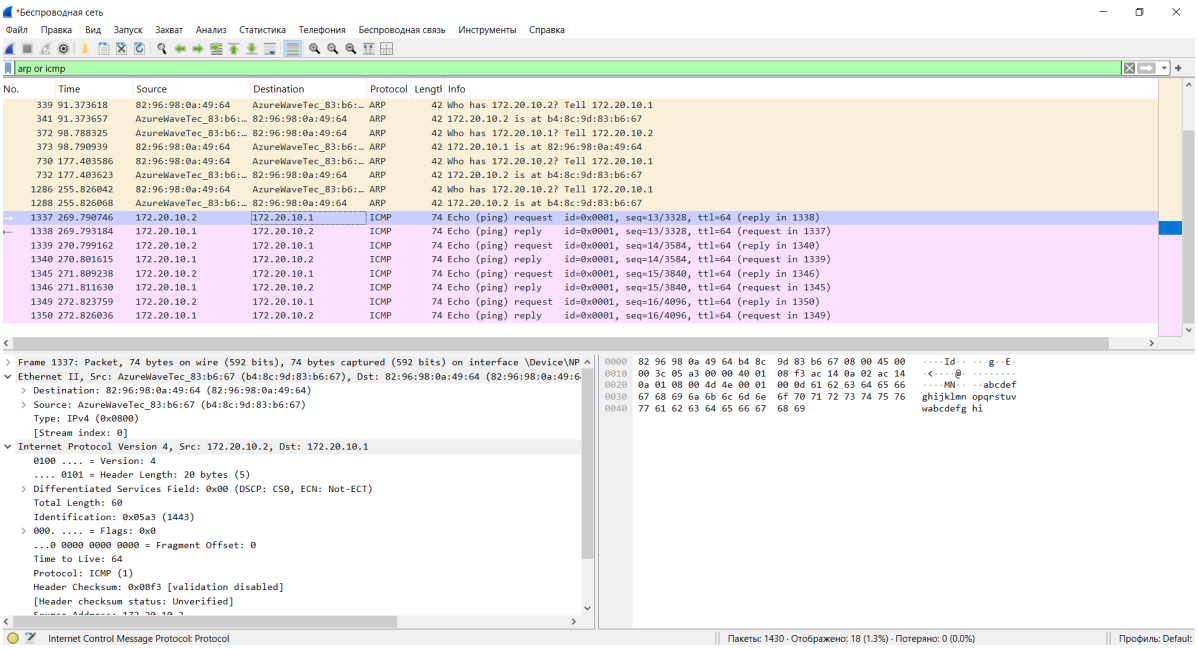

Рис. 2.2: ICMP Echo Request в Wireshark

В результате анализа сведений о пакете установлено:

- длина кадра: 74 байта;
- тип кадра канального уровня: Ethernet II;
- MAC-адрес источника: MAC-адрес локального устройства;
- MAC-адрес назначения: MAC-адрес шлюза по умолчанию;
- тип MAC-адресов: индивидуальные (unicast), так как кадр передаётся конкретному устройству.

В заголовке IPv4 указано, что пакет отправлен с локального IP-адреса на адрес шлюза. Протокол верхнего уровня — ICMP, тип сообщения — Echo Request.

2.1.4 Анализ ICMP-кадра (эхо-ответ)

Далее был выбран следующий ICMP-кадр — ответ на эхо-запрос.

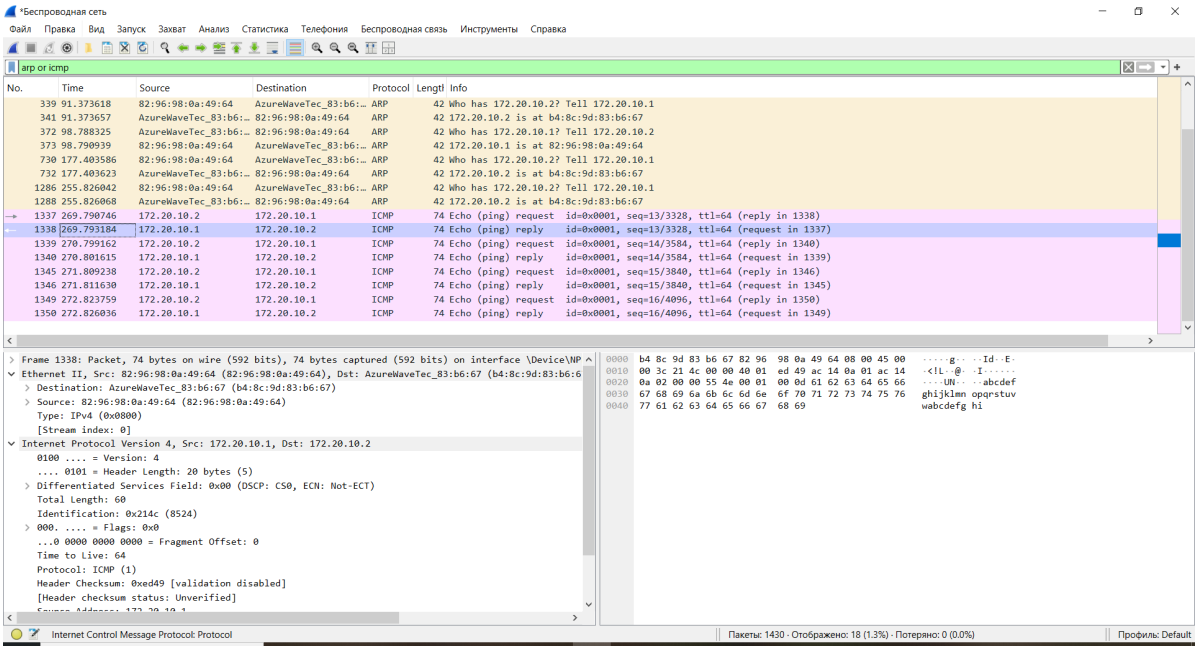

Рис. 2.3: ICMP Echo Reply в Wireshark

В ходе анализа установлено:

- длина кадра: 74 байта;
- тип кадра: Ethernet II;
- MAC-адрес источника: MAC-адрес шлюза;
- MAC-адрес назначения: MAC-адрес локального устройства;
- тип MAC-адресов: индивидуальные (unicast).

2.1.5 Анализ ARP-кадров

В процессе передачи ICMP-пакетов в Wireshark также фиксируются ARP-кадры, используемые для определения соответствия IP- и MAC-адресов.

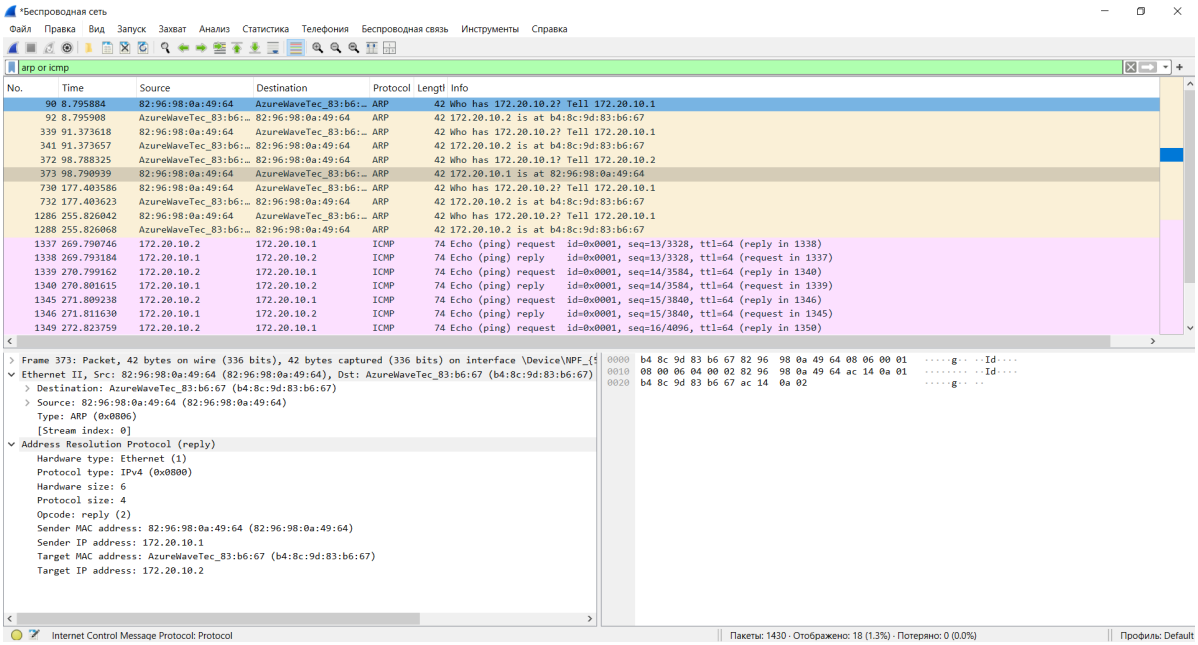

Рис. 2.4: ARP-кадры в Wireshark

В заголовке Ethernet II ARP-кадра можно наблюдать:

- MAC-адрес источника — адрес устройства, отправившего ARP-запрос;
- MAC-адрес назначения — широковещательный адрес (broadcast) при запросе или индивидуальный адрес при ответе;
- тип кадра: ARP (0x0806).

ARP-запрос передаётся широковещательно, поскольку устройство не знает MAC-адрес узла с указанным IP. В ответ ARP-reply направляется уже на конкретный MAC-адрес источника запроса.

2.1.6 Анализ ICMP-трафика при обращении к удалённому узлу

После запуска нового процесса захвата трафика был выполнен эхо-запрос к удалённому доменному имени. В результате в Wireshark были зафиксированы ICMP-запросы и ответы между локальным узлом и удалённым IP-адресом.

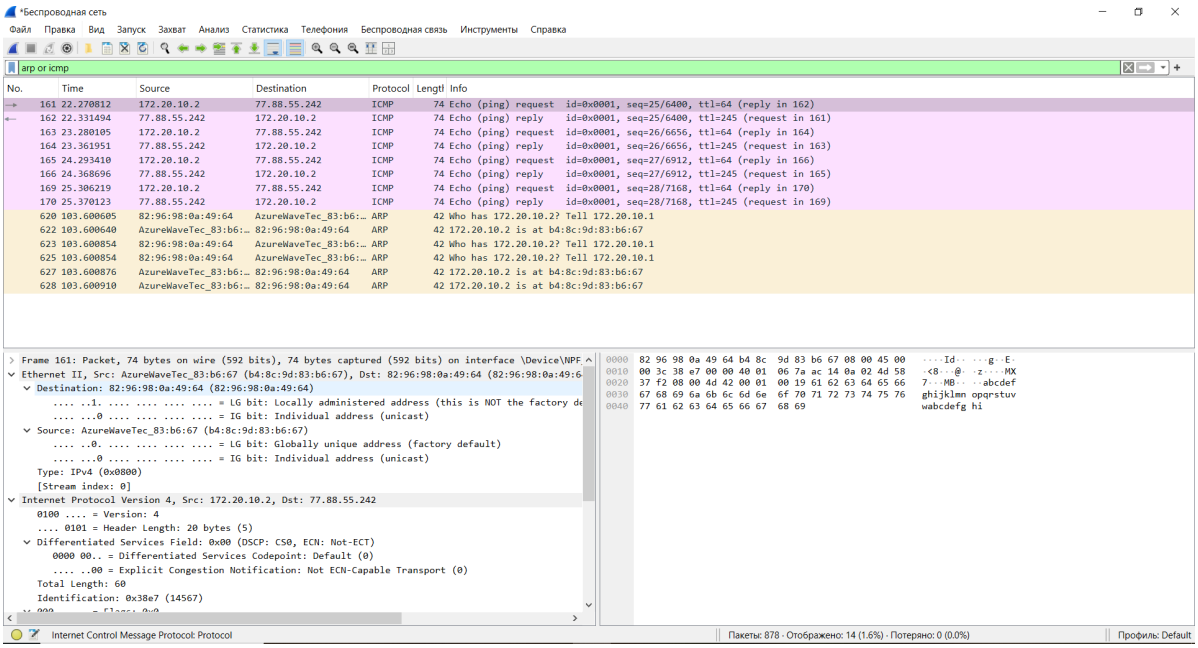

Рис. 2.5: ICMP-трафик к удалённому узлу

В выбранном кадре ICMP-запроса:

- MAC-адрес источника — адрес локального устройства;
- MAC-адрес назначения — MAC-адрес шлюза;
- тип MAC-адресов — индивидуальные (unicast), поскольку передача осуществляется через маршрутизатор.

В кадре ICMP-ответа:

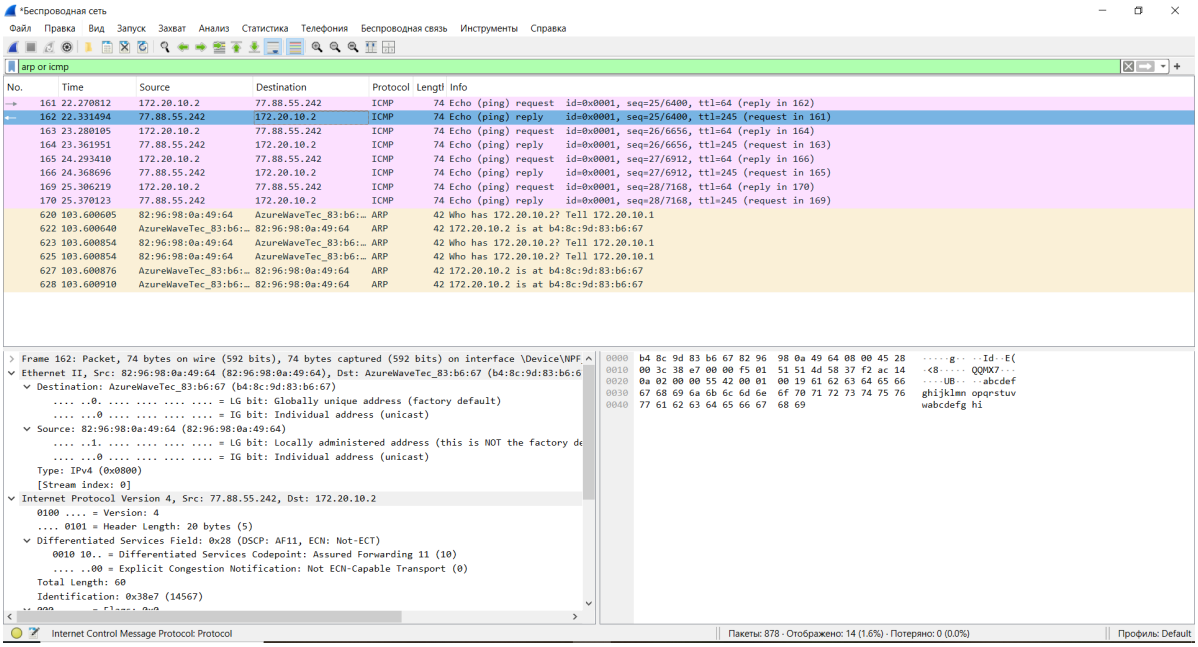

Рис. 2.6: ICMP-ответ от удалённого узла

- MAC-адрес источника — MAC-адрес шлюза;
- MAC-адрес назначения — MAC-адрес локального устройства;
- тип адресации — индивидуальная (unicast).

Это связано с тем, что при передаче пакетов за пределы локальной сети кадры на канальном уровне адресуются не конечному удалённому узлу, а ближайшему маршрутизатору (шлюзу).

2.1.7 Дополнительный анализ ARP при обращении к внешним ресурсам

В процессе обмена трафиком также фиксируются дополнительные ARP-кадры, связанные с обновлением таблицы соответствия IP- и MAC-адресов.

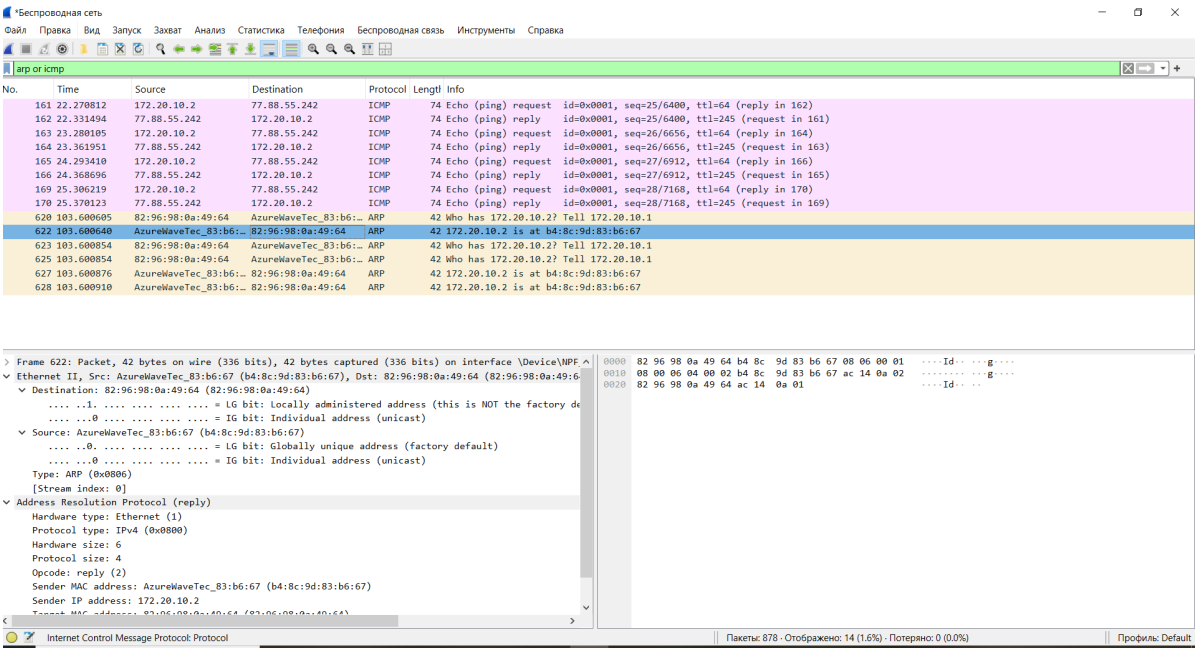

Рис. 2.7: ARP-кадры при работе с внешними узлами

В ARP-запросах MAC-адрес назначения является широковещательным, что указывает на поиск владельца IP-адреса. В ARP-ответах используется индивидуальная адресация, при которой конкретное устройство сообщает свой MAC-адрес инициатору запроса.

2.2 Анализ протоколов транспортного уровня в Wireshark

2.2.1 Захват HTTP-трафика и анализ TCP

В ходе выполнения работы был запущен Wireshark и выбран активный сетевой интерфейс. Для генерации HTTP-трафика в браузере был открыт сайт, работающий по протоколу HTTP, после чего в строке фильтра был применён фильтр `http`.

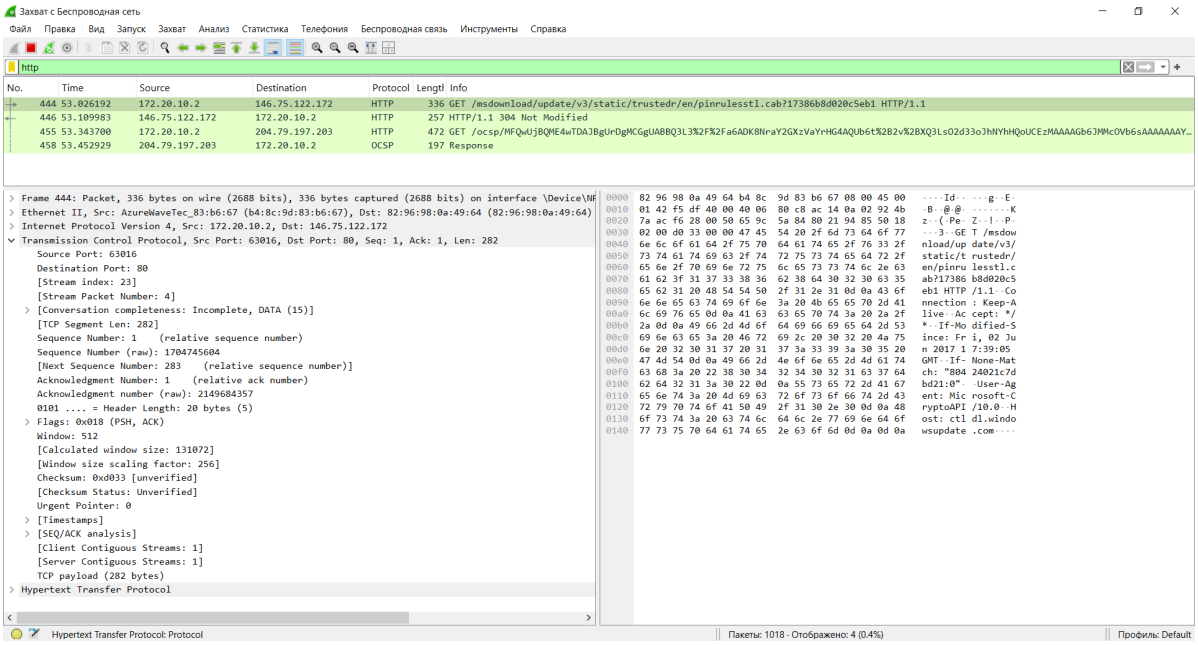

Рис. 2.8: HTTP-трафик в Wireshark

В результате анализа захваченных пакетов были зафиксированы HTTP-запросы и ответы, передаваемые поверх протокола TCP. В выбранном пакете HTTP-запроса видно:

- передача данных осуществляется по TCP;
- порт источника — динамический клиентский порт;
- порт назначения — 80 (HTTP);
- установлен флаг PSH, ACK, указывающий на передачу данных в рамках установленного соединения;
- в полезной нагрузке содержится строка запроса GET.

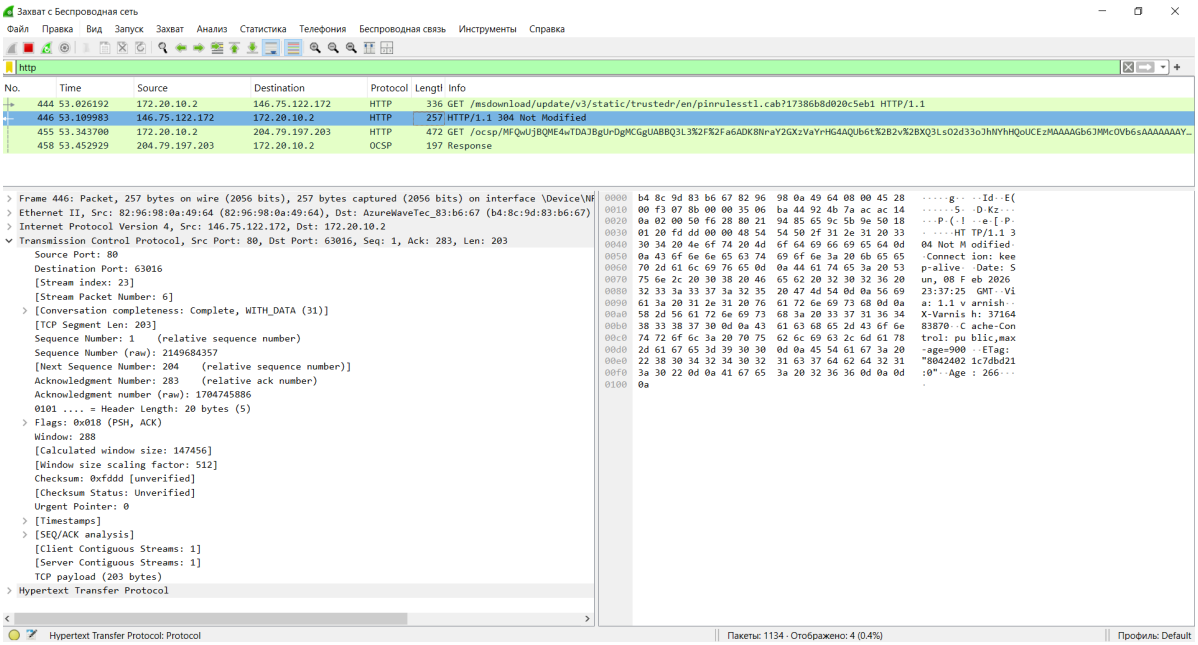

Рис. 2.9: HTTP-ответ в Wireshark

В ответном пакете сервера:

- источник — порт 80;
- назначение — клиентский порт;
- передаётся HTTP-ответ со статусом (например, 304 Not Modified);
- соединение уже установлено, поэтому используются только подтверждения ACK и передача данных.

2.2.2 Анализ DNS-трафика и протокола UDP

Далее в строке фильтра был применён фильтр dns для анализа запросов доменных имён.

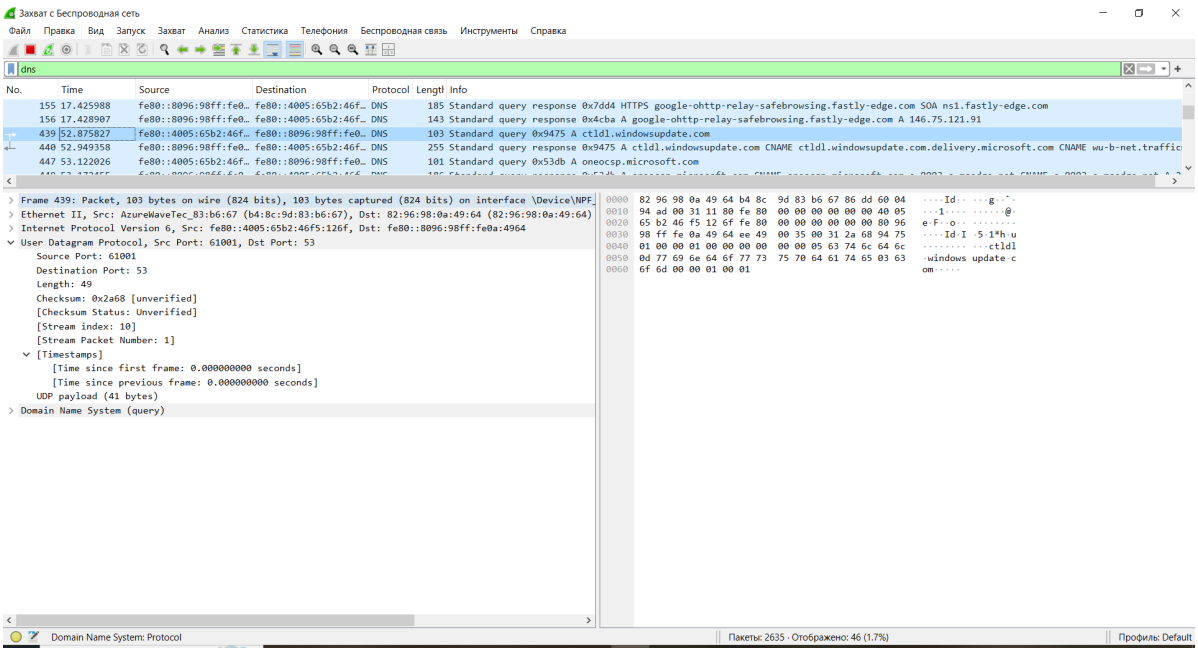

Рис. 2.10: DNS-запрос в Wireshark

В выбранном пакете видно:

- протокол транспортного уровня — UDP;
- порт источника — динамический;
- порт назначения — 53;
- в полезной нагрузке содержится DNS-запрос на разрешение доменного имени.

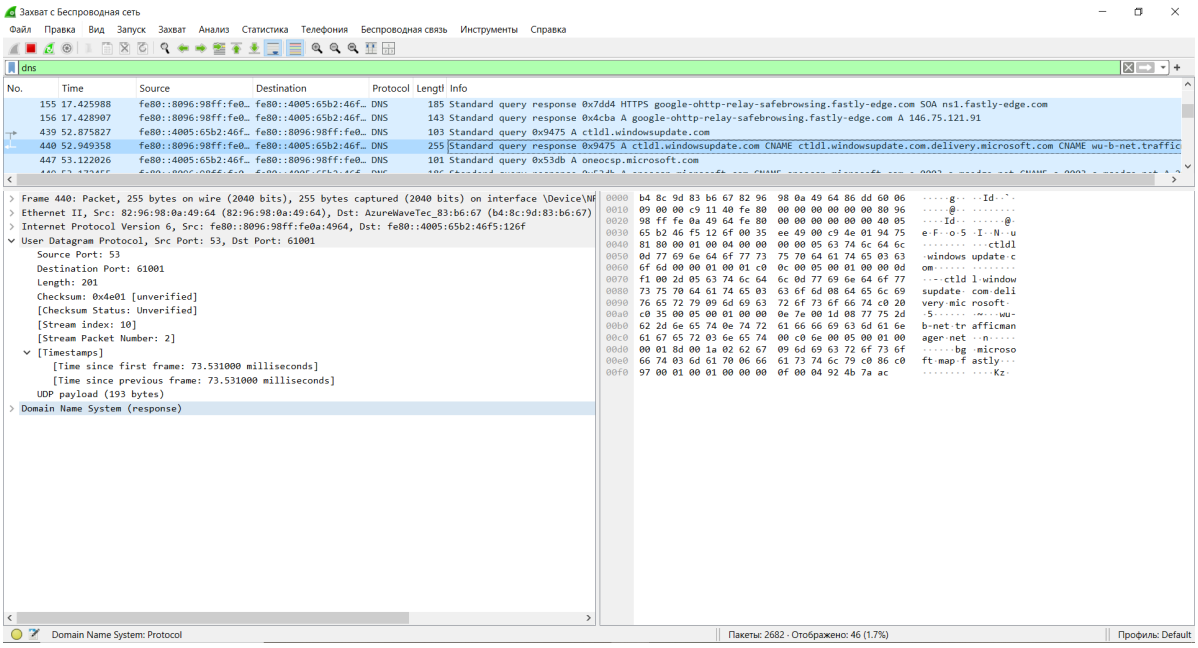

Рис. 2.11: DNS-ответ в Wireshark

В ответном пакете:

- источник — порт 53;
- назначение — клиентский порт;
- содержится DNS-ответ с информацией о сопоставлении доменного имени и IP-адреса;
- передача осуществляется без установления соединения, что характерно для UDP.

2.2.3 Анализ протокола QUIC

В строке фильтра был применён фильтр `quic` для анализа современного транспортного протокола QUIC, используемого браузерами для защищённых соединений.

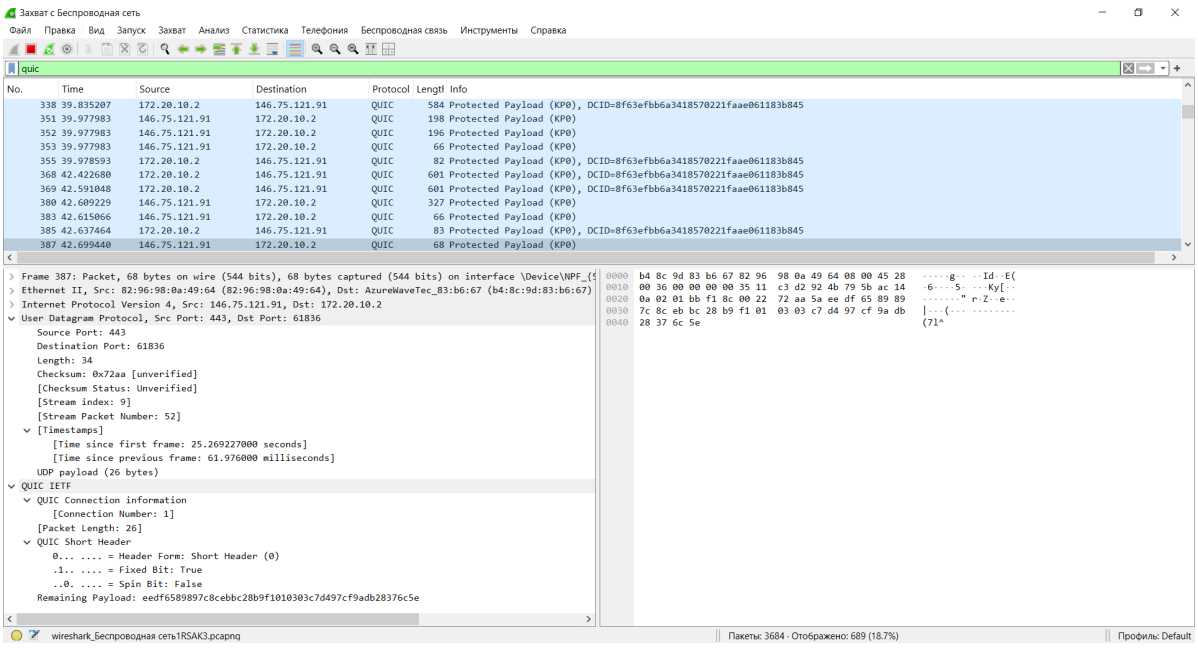

Рис. 2.12: QUIC-трафик в Wireshark

В списке пакетов наблюдаются:

- обмен пакетами между клиентом и удалённым сервером;
- передача данных по UDP-порту 443;
- наличие зашифрованной полезной нагрузки (Protected Payload).

В деталях выбранного пакета видно:

- протокол QUIC работает поверх UDP;
- используется короткий или длинный заголовок;
- в процессе установления соединения выполняется обмен служебными пакетами handshake.

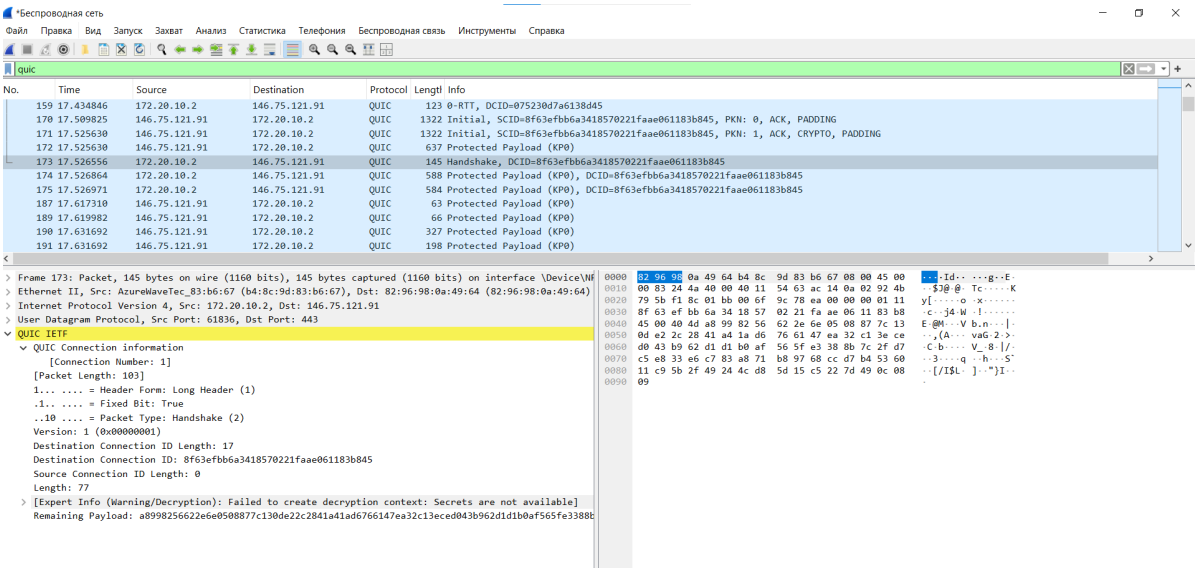

Рис. 2.13: Handshake QUIC в Wireshark

На этапе установления соединения фиксируются пакеты типа Initial и Handshake, содержащие параметры соединения и криптографические данные. После завершения согласования начинается передача защищённых данных.

2.3 Анализ handshake протокола TCP

2.3.1 Установление TCP-соединения

Для анализа процедуры установки TCP-соединения был выполнен захват трафика при обращении к веб-сайту. В Wireshark были найдены пакеты с признаками начала соединения.

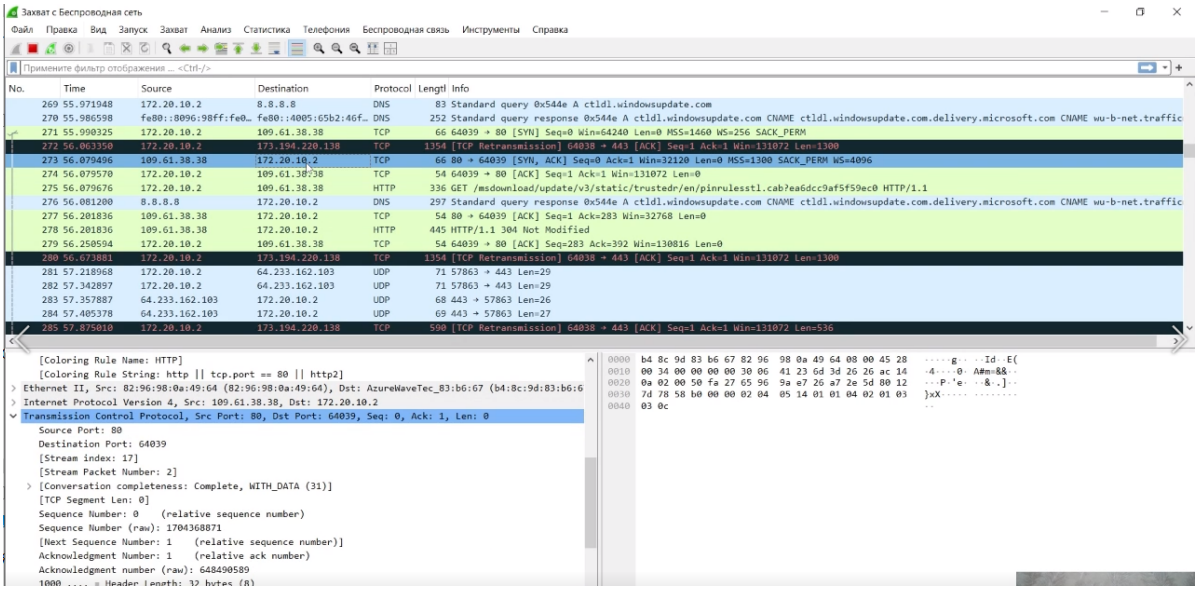

Рис. 2.14: Начало TCP-соединения

Процесс установки соединения TCP включает три этапа (three-way handshake):

1. Клиент отправляет пакет SYN на сервер, инициируя соединение.
2. Сервер отвечает пакетом SYN-ACK, подтверждая готовность принять соединение.
3. Клиент отправляет пакет ACK, подтверждая получение ответа.

На этих этапах наблюдается изменение значений:

- номера последовательности (Sequence Number);
- номера подтверждения (Acknowledgment Number);
- установка соответствующих флагов SYN и ACK.

После завершения этого процесса соединение считается установленным и начинается передача данных.

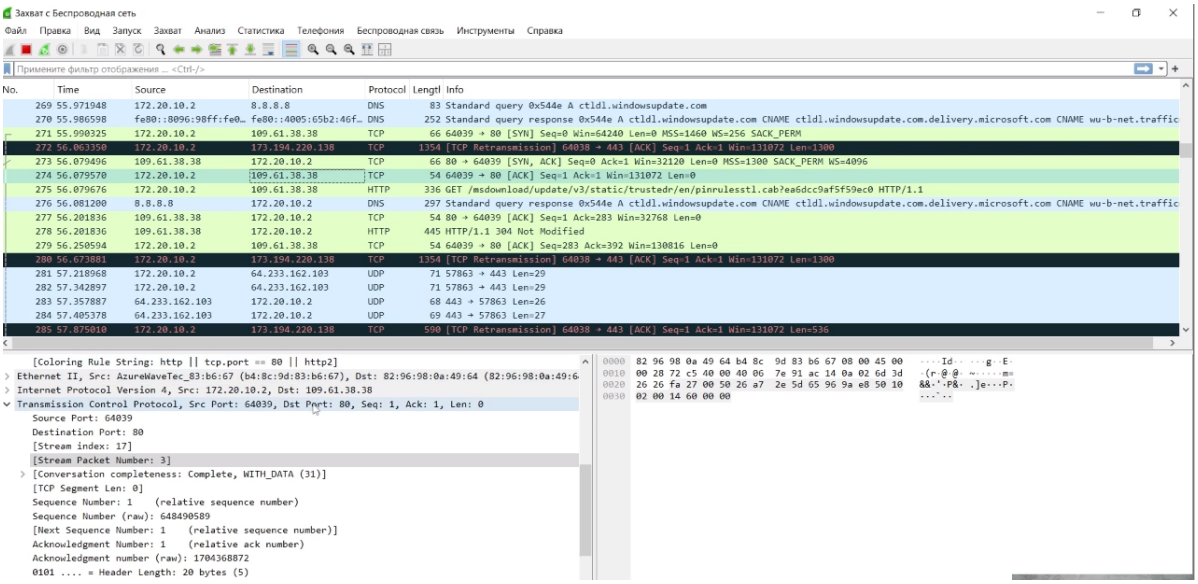

Рис. 2.15: Передача данных после установки соединения

Далее фиксируются пакеты передачи данных, подтверждения ACK и возможные повторные передачи сегментов, что обеспечивает надёжность доставки.

2.3.2 Анализ графика потока TCP

Для наглядного анализа взаимодействия был открыт инструмент «График потока» в разделе «Статистика».

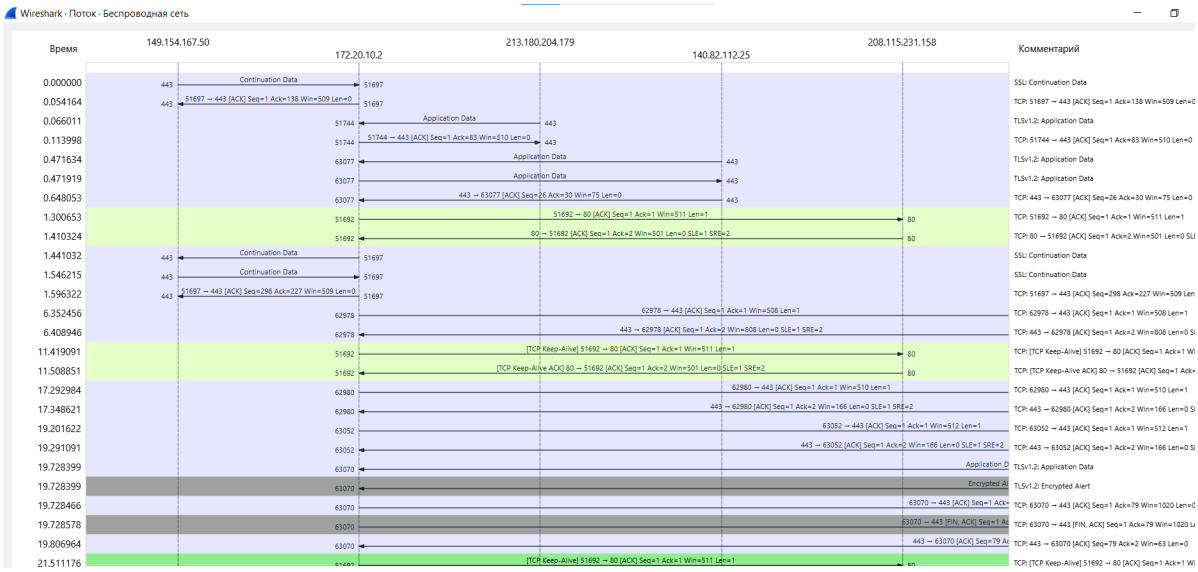

Рис. 2.16: График потока TCP

На графике отображается:

- обмен пакетами между клиентом и несколькими удалёнными узлами;
- последовательность передачи данных;
- подтверждения получения сегментов;
- поддержание соединения с помощью служебных пакетов.

Из графика видно, как после установления соединения происходит регулярный обмен сегментами с подтверждениями, что демонстрирует работу механизма управления потоком и надёжной доставки данных в TCP.

3 Заключение

В ходе выполнения лабораторной работы был выполнен захват и анализ сетевого трафика с использованием программы Wireshark на различных уровнях модели взаимодействия. Были исследованы кадры канального уровня, а также пакеты транспортного и прикладного уровней, что позволило на практике проследить процесс передачи данных в локальной сети и при обращении к внешним ресурсам.

В процессе работы был выполнен анализ ARP- и ICMP-трафика, изучены особенности формирования Ethernet-кадров, определены MAC-адреса источников и получателей, а также рассмотрены принципы широковещательной и индивидуальной адресации. Экспериментально подтверждено, что перед передачей данных в пределах локальной сети выполняется процедура ARP-разрешения, а при взаимодействии с удалёнными узлами кадры направляются на MAC-адрес шлюза по умолчанию.

Дополнительно были исследованы протоколы транспортного уровня. На примере HTTP-трафика рассмотрена передача данных по TCP, изучены структура сегментов и служебные флаги. На примере DNS-запросов проанализирована работа UDP и особенности обмена короткими сообщениями без установления соединения. Также был рассмотрен современный протокол QUIC, функционирующий поверх UDP и обеспечивающий защищённую передачу данных.

Отдельное внимание было уделено процессу установления TCP-соединения. На практике был проанализирован механизм трёхстороннего рукопожатия (SYN, SYN-ACK, ACK), а также изменение номеров последовательности и подтвержде-

ния. С использованием графика потока была наглядно изучена последовательность обмена сегментами между клиентом и сервером.

В результате выполнения работы были закреплены практические навыки захвата, фильтрации и анализа сетевого трафика, а также получено представление о взаимодействии протоколов различных уровней при передаче данных в компьютерных сетях.