ГУАП

КАФЕДРА № 42

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		Д. Д. Савельева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ № 2

АНАЛИЗ ТРАФИКА КОМПЬЮТЕРНЫХ СЕТЕЙ УТИЛИТОЙ WIRESHARK

по курсу:

ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ гр. № 4326		Г. С. Томчук
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2025

1 Цель работы

Цель работы: изучить структуру протокольных блоков данных, анализируя реальный трафик с помощью утилиты Wireshark.

2 Задание

В процессе выполнения лабораторной работы выполняются наблюдения за передаваемым трафиком с компьютера пользователя в Интернет и в обратном направлении. Применение специализированной утилиты Wireshark позволяет наблюдать структуру передаваемых кадров, пакетов и сегментов данных различных сетевых протоколов. Требуется анализировать последовательности команд и назначение служебных данных, используемых для организации обмена данными в следующих протоколах: ARP, DNS, FTP, HTTP.

В качестве адреса сайта в заданиях следует использовать один из URL из первой лабораторной работы, свою страницу социальной сети или свой личный сайт. В таблице 1 представлены адреса сайтов, использованные в лабораторной работе № 1.

Таблица 1 — Вариант работы

№ Варианта	Исследуемые узлы
17	www.accounts.google.com www.coub.com www.fstec.ru

3 Ход выполнения работы

3.1 Анализ трафика утилиты ping

Был отслежен и проанализирован утилитой Wireshark трафик, создаваемый утилитой ping при запуске из терминала. Для размера пакета были поочередно использованы значения от 100 до 8000. Не удалось выполнить команду со значением, превышающим 8000.

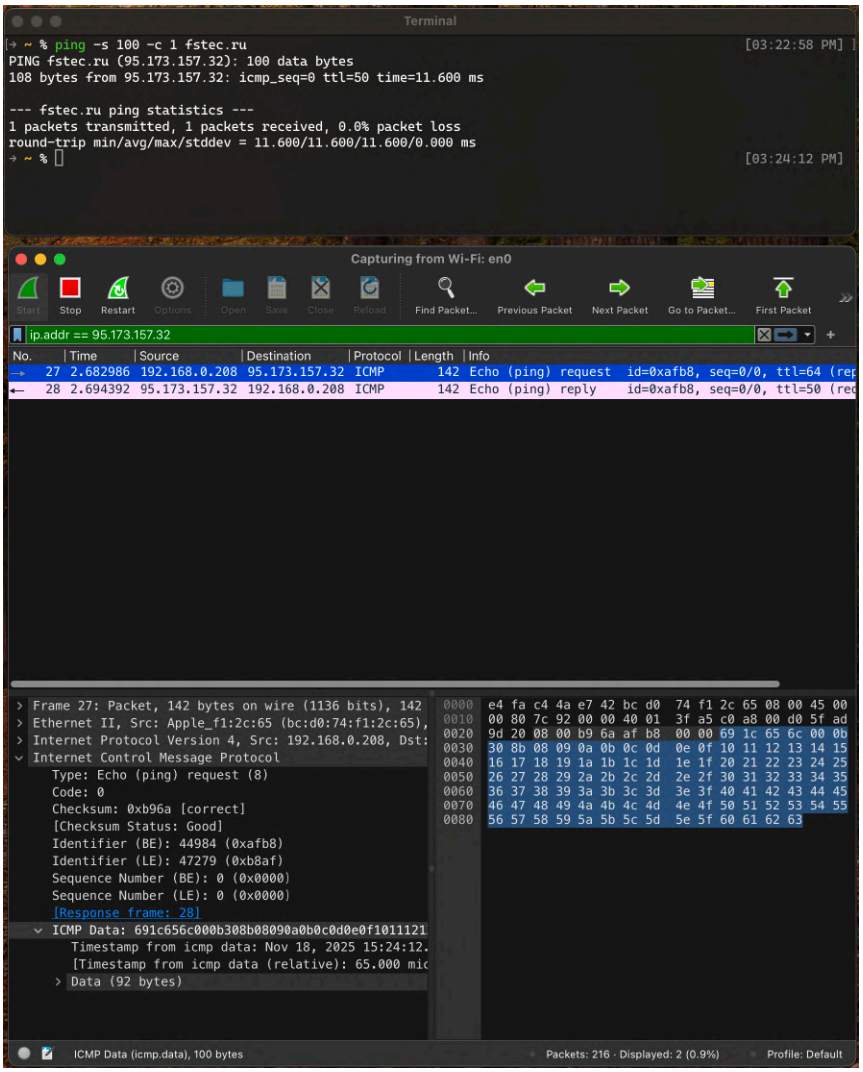

Рисунок 1 — ping с размером пакета 100

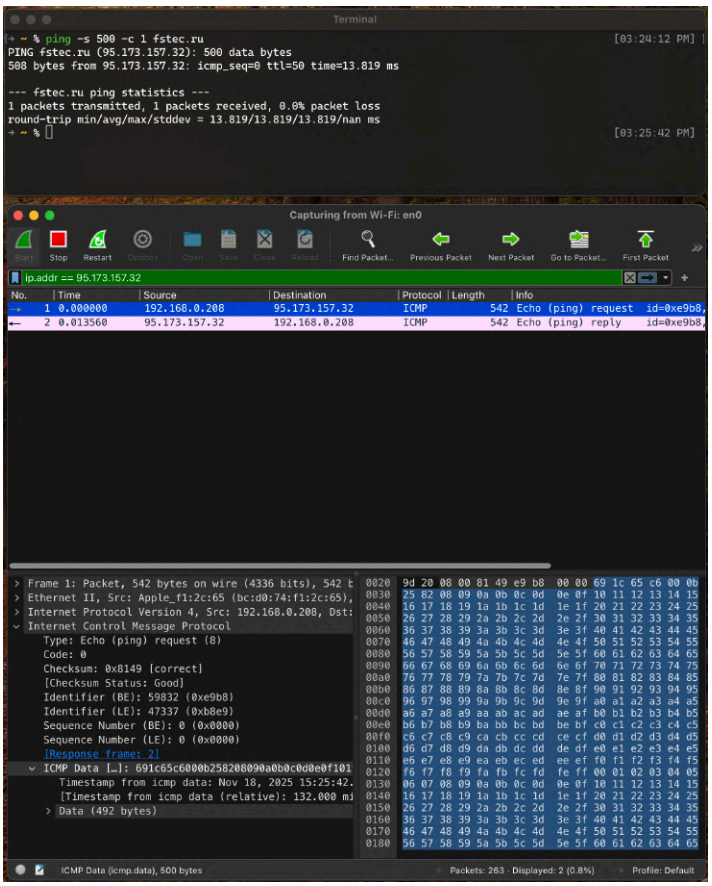

Рисунок 2 — ping с размером пакета 500

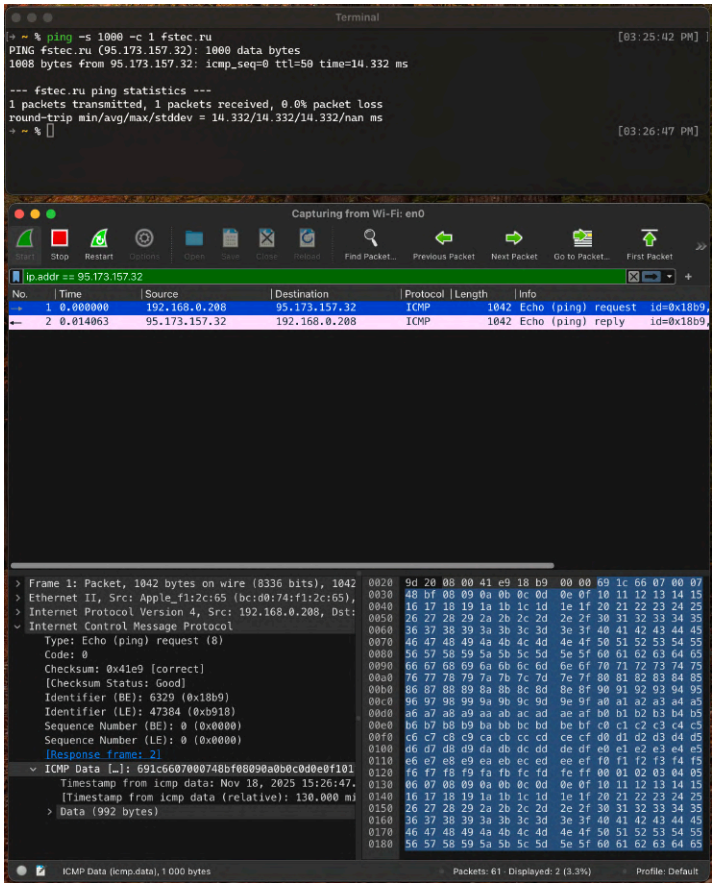

Рисунок 3 — ping с размером пакета 1000

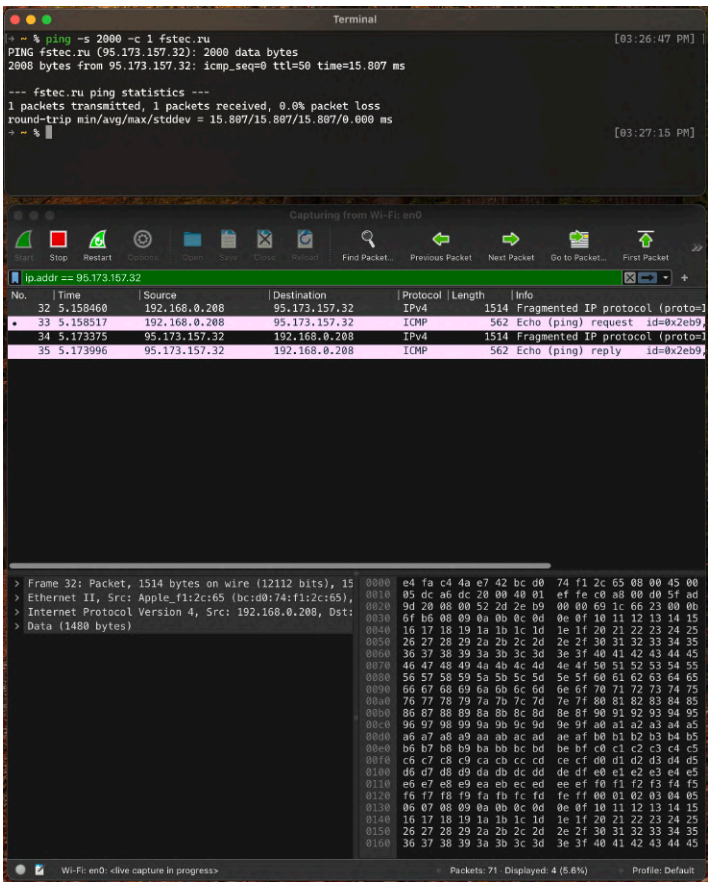

Рисунок 4 — ping с размером пакета 2000

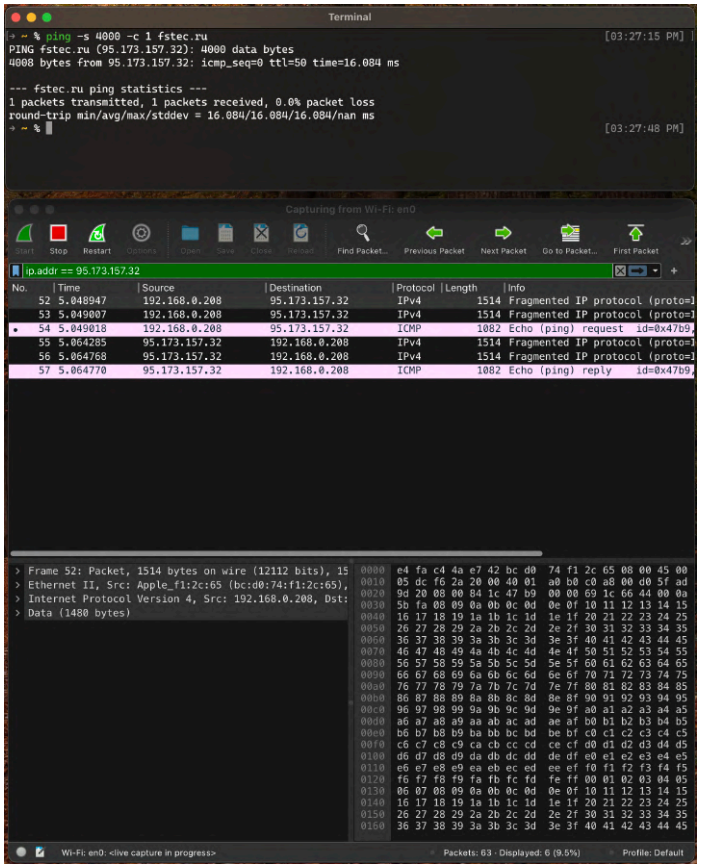

Рисунок 5 — ping с размером пакета 4000

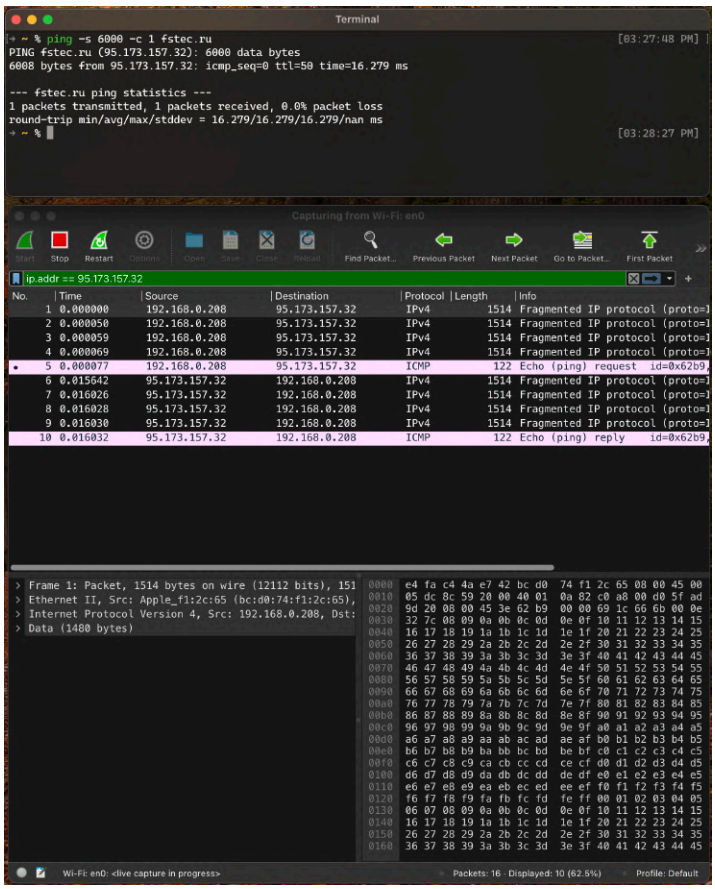

Рисунок 6 — ping с размером пакета 6000

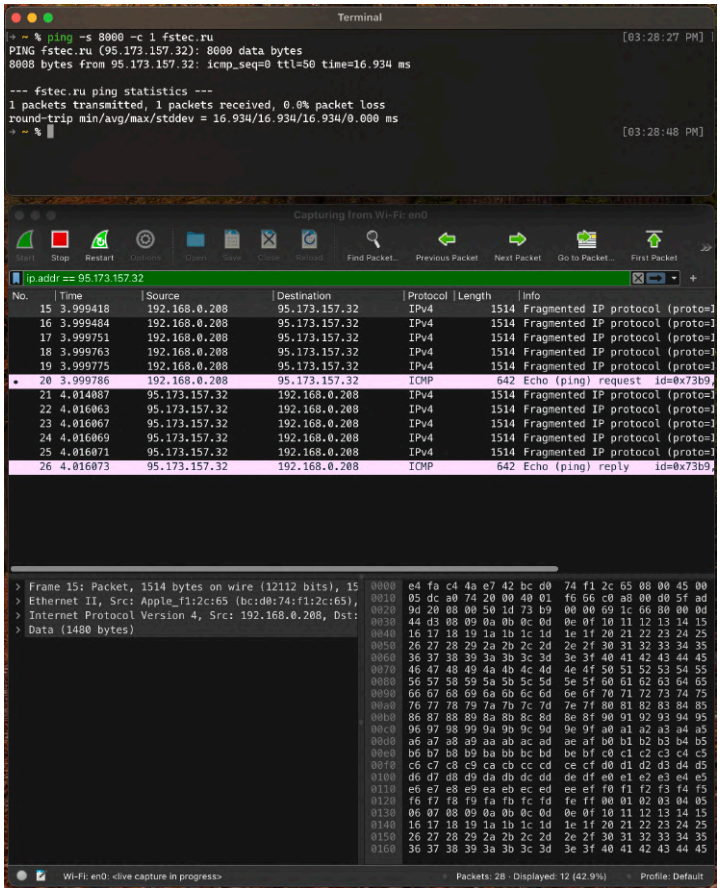

Рисунок 7 — ping с размером пакета 8000

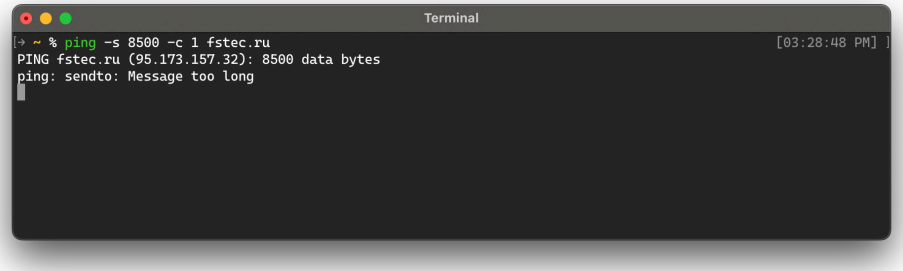

Рисунок 8 — ping с размером пакета 8500, выдающий ошибку

Структура перехваченных PDU (Protocol Data Unit):

1. Канальный уровень: Ethernet Frame с MAC-адресами;
2. Сетевой уровень: IP-пакет с IP-адресами;
3. Транспортный уровень: протокол ICMP;
4. Прикладной уровень: специфичные сообщения (ICMP-запросы).

При фрагментации каждый фрагмент — самостоятельный IP-пакет с данными транспортного уровня.

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает? — Да, в случае если размер пакета превышает MTU. MTU (Maximum Transmission Unit) — максимальный размер блока данных, который может быть передан за один раз без фрагментации. Фрагментация видна по флагу “More fragments” и полю Fragment offset в заголовке IP.

2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным? — Когда бит "MF" установлен в 1, это свидетельствует о том, что текущий фрагмент является промежуточным, и в последующих фрагментах данного IP-пакета будут содержаться дополнительные фрагменты данных. Установка бита"MF" в 0 указывает на то, что данный фрагмент представляет собой завершающий фрагмент в последовательности фрагментов данного IP-пакета. Если бит "DF" установлен в 1, это означает, что IP-пакет не может быть фрагментирован в процессе передачи по сети. Если бит "DF" равен 0, то IP-пакет может быть фрагментирован, если это необходимо в процессе передачи.

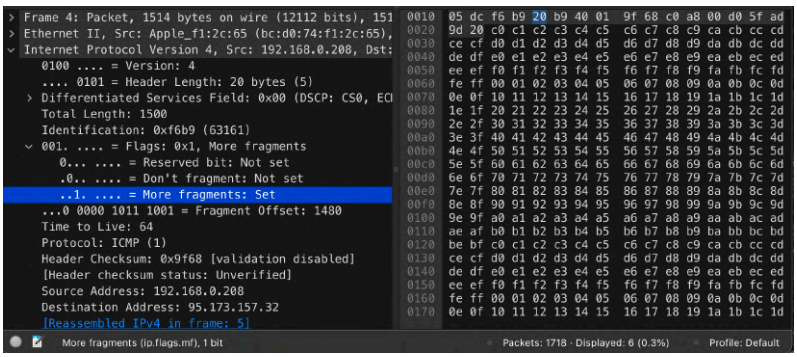

Рисунок 9 — MF=1 для второго фрагмента из трех

3. Чему равно количество фрагментов при передаче ping-пакетов? — В случае, если размер пакета превышает MTU и DF не равен 1, пакет будет поделен на фрагменты равные размеру установленного MTU (в данном случае 1500).

4. Построить график, в котором на оси абсцисс находится размер_пакета, а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет. — На рисунке 10 изображен данный график.

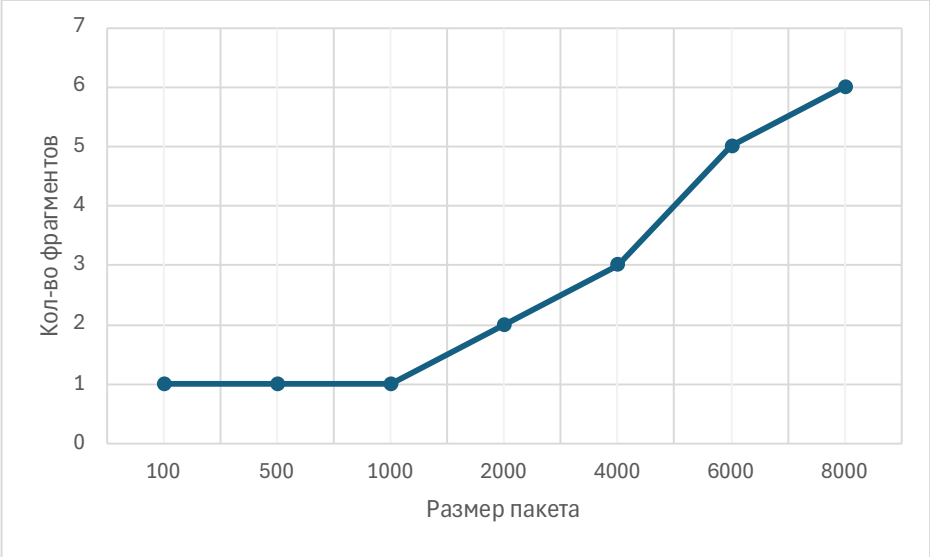

Рисунок 10 — График зависимости количества фрагментов от размера пакета

5. Как изменить поле TTL с помощью утилиты ping? — Нужно добавить аргумент -m (на macOS), значением которого будет TTL в миллисекундах.

6. Что содержится в поле данных ping-пакета? — Содержимое поля данных в ping-пакете представляет собой последовательность букв английского алфавита, которая повторяется до достижения заданного

размера пакета (на macOS).

3.2 Анализ трафика утилиты tracert (traceroute)

Был отслежен и проанализирован трафик, создаваемый утилитой traceroute, при её запуске из терминала.

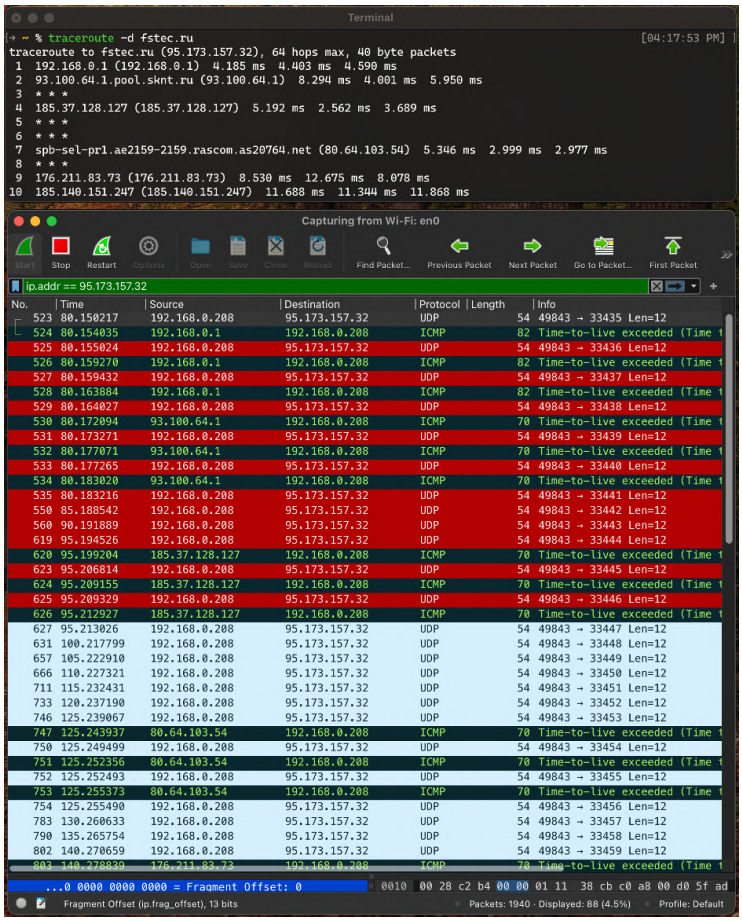

Рисунок 11 — traceroute -d fstec.ru

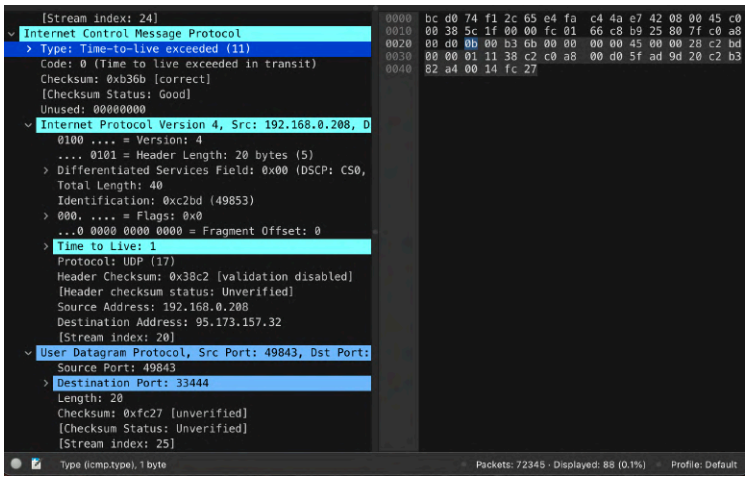

Рисунок 12 — Структура PDU сообщения “Time-to-live exceeded”

Структура перехваченных PDU:

В ICMP-сообщении "Time-to-live exceeded" структура уровней 2–3 аналогична обычным ICMP-пакетам. На транспортном уровне содержится ICMP с данным сообщением об ошибке, которое включает вложенный IP-заголовок исходного пакета. Это позволяет идентифицировать, на каком маршрутизаторе истёк TTL и какой пакет был отправлен.

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных? — Заголовок IP (Internet Protocol) имеет фиксированный размер и состоит из 20 байт (160 бит) для версии IPv4. Поле данных имеет переменную длину, но для ICMP обычно содержит 32 байта.

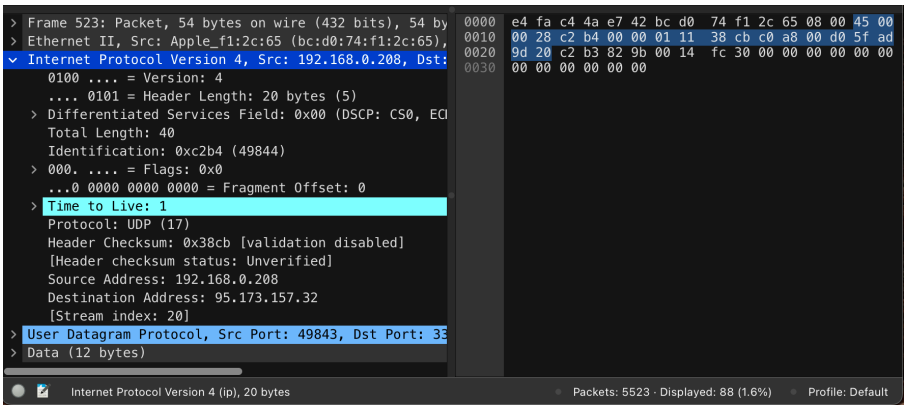

Рисунок 13 — Содержание пакета. Выделен заголовок IP

2. Как и почему изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов. — Поле TTL изменяется для того, чтобы пакеты могли "прыгнуть" от одного маршрутизатора к другому, и изменение TTL позволяет определить, сколько хопов включено в маршрут между исходным компьютером и конечным пунктом назначения. На рисунке 9 отображена эта логика на перехваченном пакете.

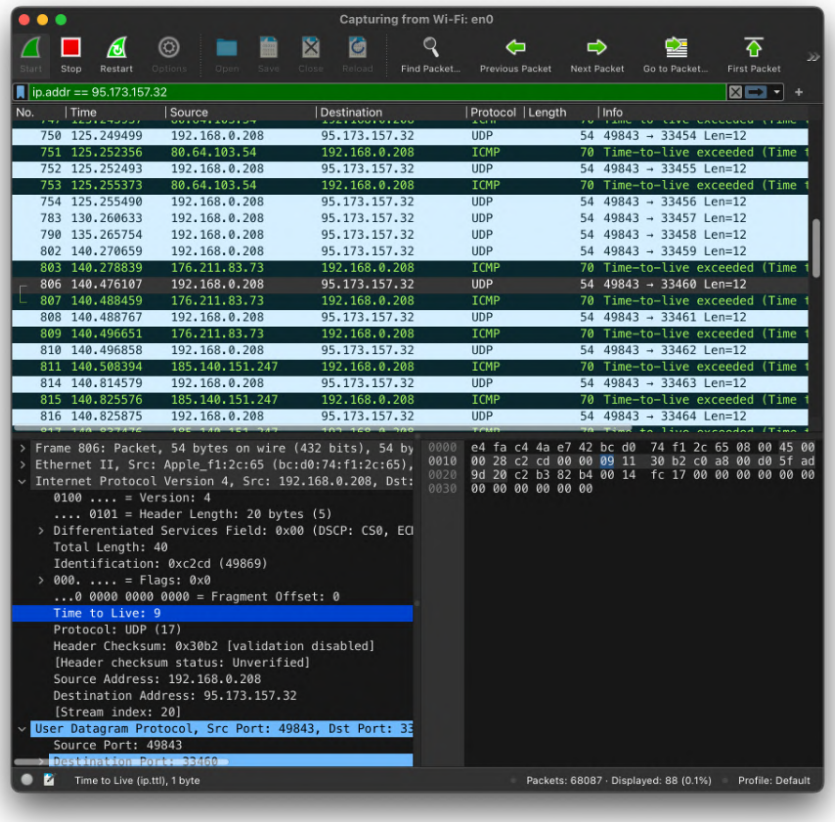

Рисунок 14 — TTL равен 9 для исследования 9-го хопа

3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание). — Утилита ping использует ICMP Echo Request и Echo Reply для проверки доступности узла и измерения времени отклика. В отличие от этого, tracert отправляет пакеты с постепенно увеличивающимся TTL, чтобы получить от каждого промежуточного маршрутизатора ICMP-сообщение "Time Exceeded". Таким образом, ping работает по принципу запрос-ответ для проверки связи, а tracert использует сообщения об ошибках для построения маршрута следования пакетов.

4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов? — Пакеты ICMP Reply являются нормальными ответами на корректные запросы (например, Echo Reply на Echo Request в ping), подтверждая доступность узла. ICMP Error сообщения генерируются при проблемах обработки пакета (недоступность порта, превышение TTL) и служат для диагностики сетевых неисправностей.

Таким образом, ICMP Reply обеспечивает проверку связности, а ICMP Error — диагностику ошибок передачи данных, что в совокупности позволяет эффективно анализировать работу сети.

5. Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться? — Если убрать ключ «-d», то traceroute будет пытаться разрешать имена хостов для промежуточных узлов в пути маршрутизации, что может добавить лишний сетевой трафик и замедлить выполнение команды.

3.3 Анализ HTTP-трафика

Был отслежен и проанализирован HTTP-трафик, создаваемый браузером при посещении Интернет-сайта http://185.202.207.59/ (личный сайт). На рисунках 15–19 представлены полученные данные в результате анализа трафика.

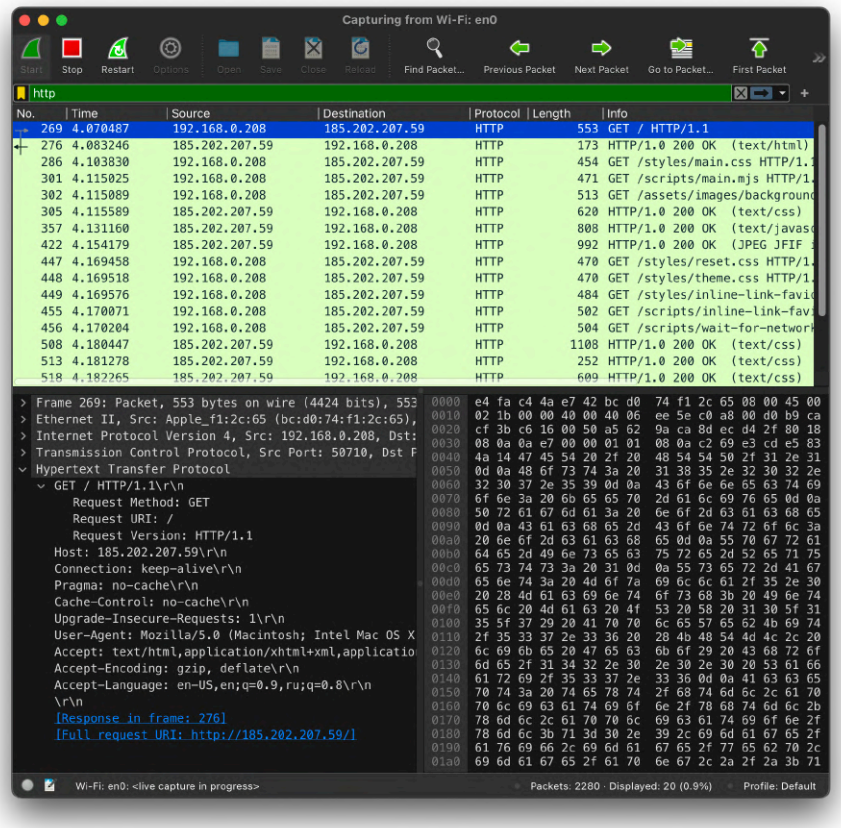

Рисунок 15 — Перехваченные GET-запросы и ответы на них

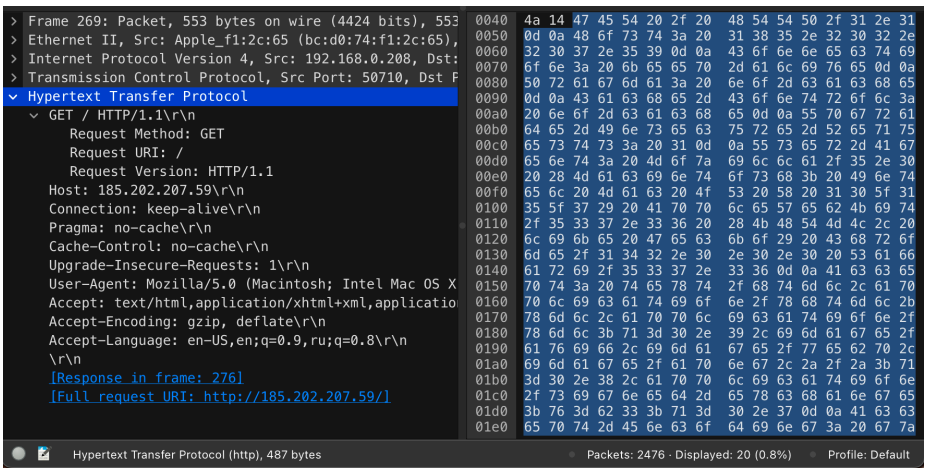

Рисунок 16 — Заголовки GET-запроса

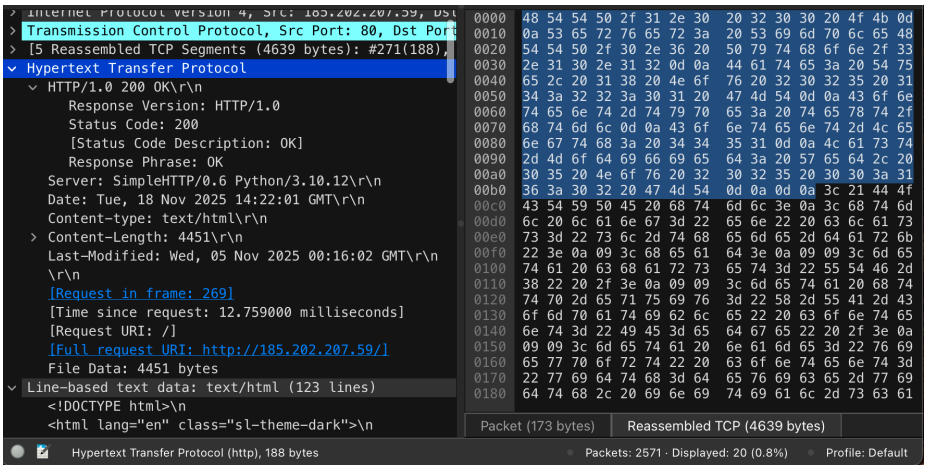

Рисунок 17 — Заголовки HTTP-ответа с кодом 200

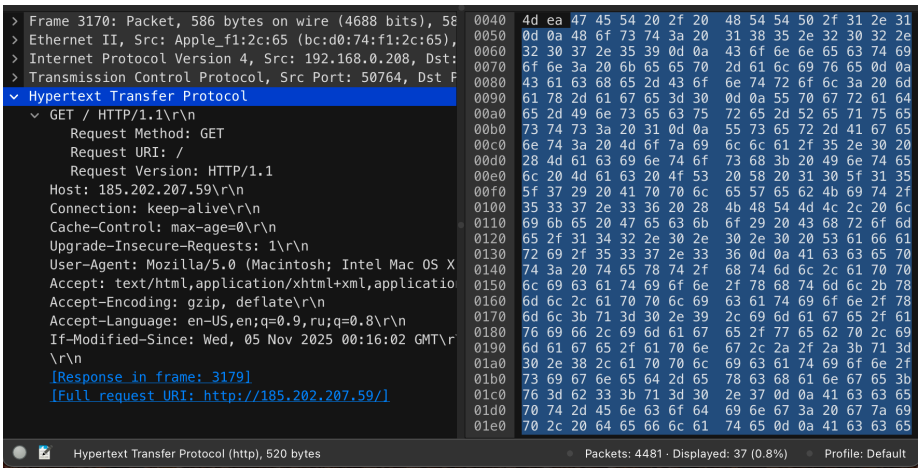

Рисунок 18 — Заголовки условного GET-запроса

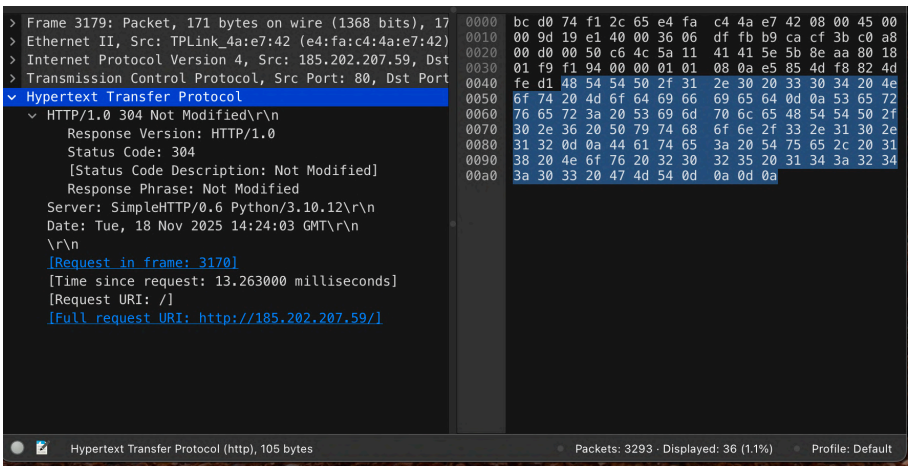

Рисунок 19 — Заголовки HTTP-ответа с кодом 304 (Not Modified)

Структура перехваченных PDU:

1. Канальный уровень: Ethernet Frame с MAC-адресами;
2. Сетевой уровень: IP-пакет с IP-адресами;
3. Транспортный уровень: TCP-сегменты с портами;
4. Прикладной уровень: HTTP-запросы/ответы с заголовками и данными.

Порядок действий при первичном посещении:

1. Установка TCP-соединения;
2. HTTP GET-запрос с заголовками;
3. Сервер формирует ответ (статус 200 (OK) и данные HTML);
4. Браузер отображает страницу.

При вторичном посещении порядок аналогичен первичному, но сервер может вернуть статус 304 (Not Modified) для использования кеша, если контент не изменился.

3.4 Анализ DNS-трафика

Был отслежен и проанализирован трафик протокола DNS, сгенерированный в результате посещения сайта fstec.ru. На рисунке 20 изображены перехваченные DNS-запросы и ответы.

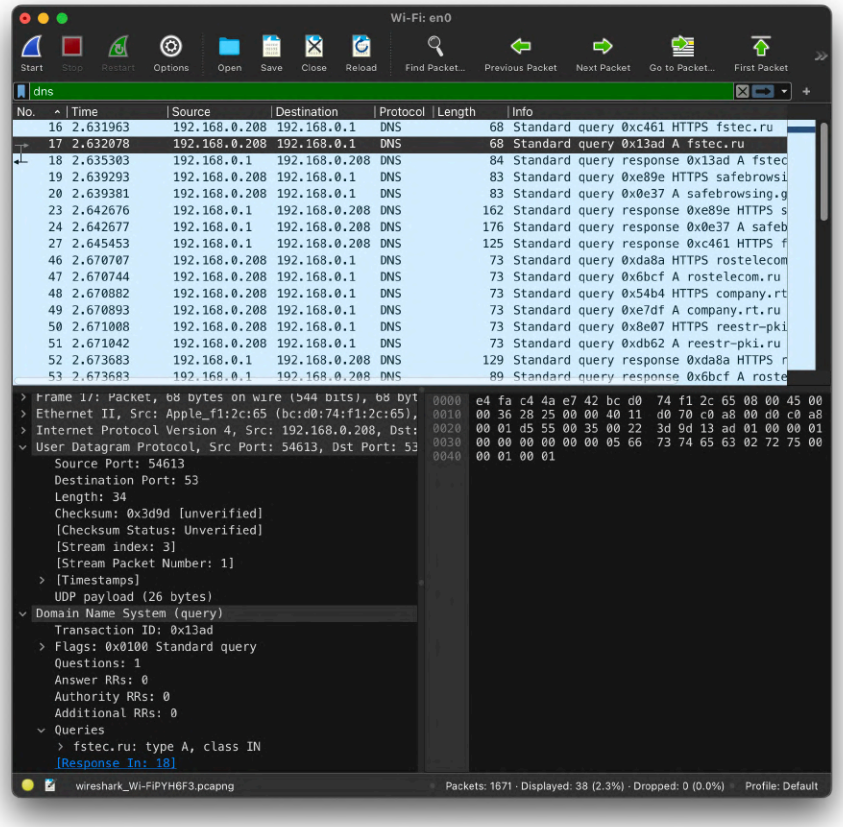

Рисунок 20 — Трафик DNS при заходе на сайт fstec.ru

Структура перехваченных PDU. DNS-запрос:

1. Канальный уровень: Ethernet Frame с MAC-адресами;
2. Сетевой уровень: IP-пакет с адресами отправителя и получателя;
3. Транспортный уровень: UDP-сегменты с портами;
4. Прикладной уровень: DNS-запрос с идентификатором, доменным именем и типом записи (A, AAAA и т.д.).

DNS-ответ имеет аналогичную структуру, но на прикладном уровне содержит запрошенные DNS-записи (IP-адреса или другие данные).

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта? — В таких случаях, как правило, имеют место распределенные DNS-системы, балансировка нагрузки, скрытие инфраструктуры.

2. Какие бывают типы DNS-запросов? — A (IPv4-адрес домена), AAAA (IPv6-адрес), MX (почтовые серверы домена), TXT (текстовая информация), NS (DNS-серверы зоны), PTR (обратное преобразование —

IP-адрес в доменное имя), SRV (нахождение сетевых сервисов).

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений? — В случае, если изображения на сайте хранятся по другому адресу (например, CDN-система — Content Delivery Network, работающая на другой инфраструктуре).

3.5 Анализ ARP-трафика

Был отслежен и проанализирован трафик протокола ARP, сгенерированный в результате посещения сайта fstec.ru. На рисунке 21 изображены перехваченные ARP-пакеты.

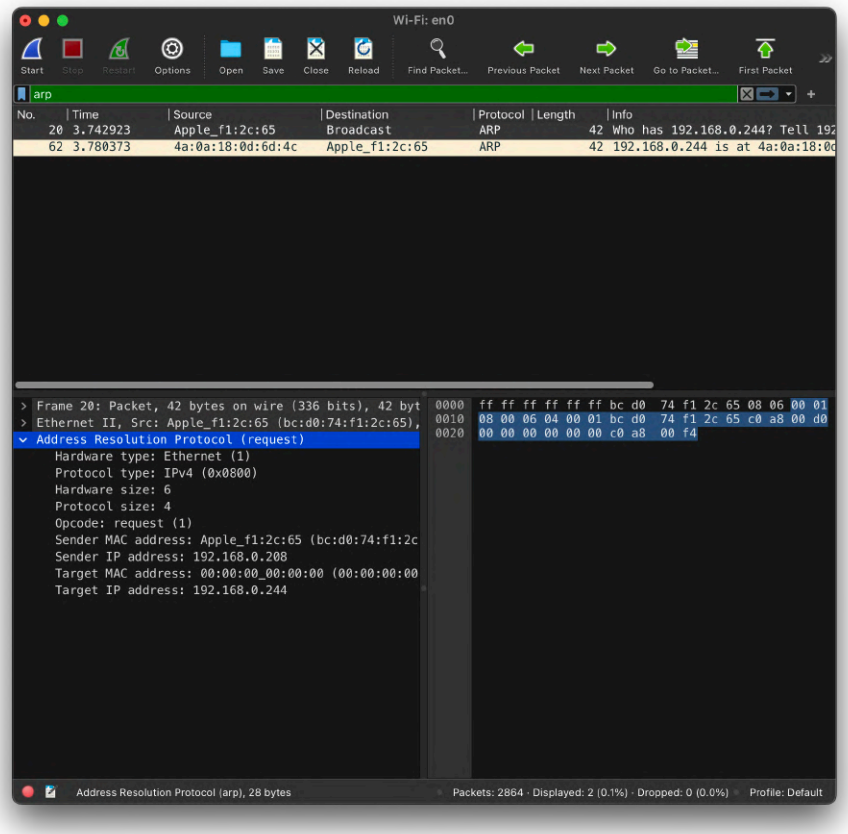

Рисунок 21 — Трафик ARP при заходе на сайт fstec.ru

Структура перехваченных PDU:

1. Канальный уровень: Ethernet Frame с MAC-адресами;
2. Сетевой уровень: информация о типе аппаратного обеспечения, типе протокола, MAC и IP-адреса отправителя и получателя, тип пакета (request 1 или reply 2);

1. Какие MAC-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют? — Sender MAC Address (MAC-адрес отправителя) — это устройство, которое выполнило ARP-запрос или ответ. Это может быть компьютер, маршрутизатор, сервер или любое другое сетевое устройство, которое участвует в процессе разрешения IP-адресов в MAC-адреса. Target MAC Address (MAC-адрес получателя) — в случае ARP-запроса это широковещательный адрес, что означает, что запрос отправляется всем устройствам в сети; а в случае ARP-ответа — это MAC-адрес устройства, которое запрашивало соответствующий IP-адрес.

2. Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Какие устройства они идентифицируют? — В HTTP-пакетах присутствуют MAC-адреса, которые выполняют функцию идентификации отправителя и получателя данных пакетов. В данном контексте на обеих сторонах обмена можно наблюдать MAC-адреса маршрутизатора внутри локальной сети и MAC-адрес компьютера. Эти MAC-адреса указывают, от каких сетевых интерфейсов идут данные HTTP-пакеты и на какие сетевые устройства они направлены.

3. Для чего ARP-запрос содержит IP-адрес источника? — IP-адрес источника в ARP-запросе используется для определения MAC-адреса устройства, связанного с этим IP-адресом в локальной сети.

4 Выводы

В ходе выполнения лабораторной работы была достигнута цель по изучению структуры протокольных блоков данных через анализ реального сетевого трафика с использованием Wireshark. На практике исследованы ключевые протоколы сетевого взаимодействия:

1. ICMP (ping/traceroute). Установлены различия в механизмах работы утилит ping (использующей запросы Echo Request/Reply) и traceroute (основанной на анализе ICMP-ошибок "Time Exceeded"). Определены условия фрагментации пакетов и зависимость количества фрагментов

от размера пакета.

2. HTTP. Проанализирована структура HTTP-запросов и ответов, включая процесс установки TCP-соединения и особенности кеширования при повторных обращениях к ресурсу.
3. DNS. Изучены типы DNS-запросов (A, AAAA, MX и т. д.) и их роль в преобразовании доменных имен в IP-адреса. Продемонстрирована важность DNS-кэширования для оптимизации трафика.
4. ARP. Исследован механизм разрешения IP-адресов в MAC-адреса в локальной сети, а также роль широковещательных запросов в этом процессе.

Работа подтвердила, что анализ сетевого трафика позволяет наглядно изучать архитектуру сетевых протоколов, диагностировать проблемы и оптимизировать сетевое взаимодействие. Полученные навыки использования Wireshark являются основой для дальнейшего освоения методик мониторинга и обеспечения безопасности компьютерных сетей.