

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ**

**«Национальный исследовательский университет ИТМО»
(Университет ИТМО)**

Факультет инфокоммуникационных технологий

О Т Ч Е Т

по практической работе №5
курса "Компьютерные сети"

Выполнил:

Привалов Кирилл Алексеевич
К3242

Проверил:

к.т.н. Харитонов Антон Юрьевич

Санкт-Петербург, 2024

Содержание

1 Введение	3
1.1 Цель работы	3
1.2 Задания к лабораторной работе	3
2 Основная часть	4
2.1 Начало работы с Wireshark	4
2.2 Сбор и углубленный анализ данных протокола ICMP	9
2.3 Анализ полей TCP	13
3 Вывод	16

1 Введение

1.1 Цель работы

Разобраться со стеком TCP/IP, анализируя пакеты, которые отправляются и принимаются с помощью данного стека. Научиться собирать сетевой трафик с помощью программы Wireshark. Научиться фильтровать собранный трафик, находить и просматривать соединения.

1.2 Задания к лабораторной работе

1. Начало работы с Wireshark.
2. Сбор и углубленный анализ данных протокола ICMP.
 - (a) Сбор и анализ данных протокола ICMP по локальным узлам.
 - (b) Сбор и анализ данных протокола ICMP по удаленным узлам.
3. Анализ полей TCP.

2 Основная часть

2.1 Начало работы с Wireshark

Выставим лимит захвата трафика - 5 мб.

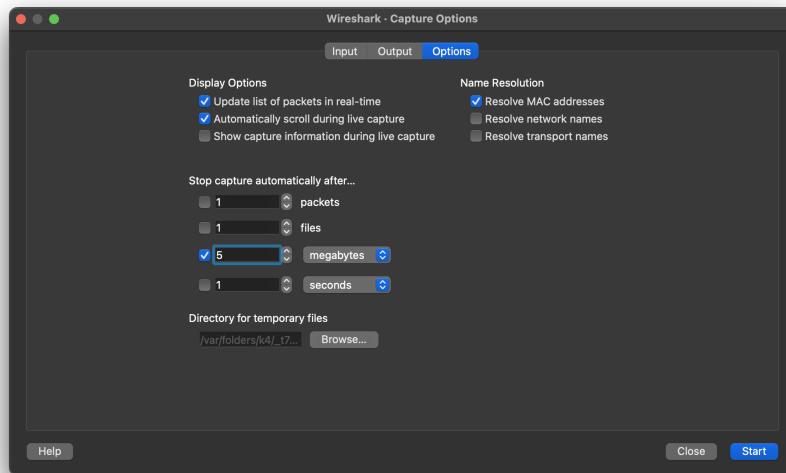


Рис. 1: Настройка лимита захвата трафика

Определили узел с максимальной активностью:

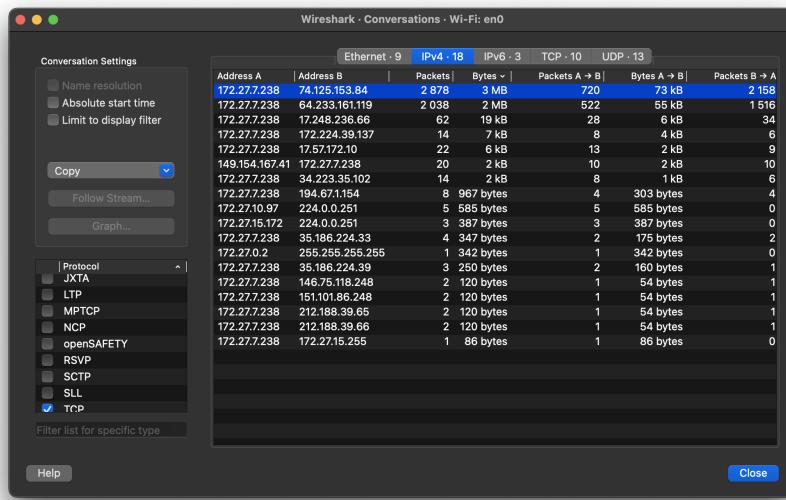


Рис. 2: Узел с максимальной активностью

Узел с наибольшим количеством широковещательных рассылок найден при помощи фильтра:

```
ip.dst == 255.255.255.255 || eth.dst == ff:ff:ff:ff:ff:ff || icmpv6.type == 134
```

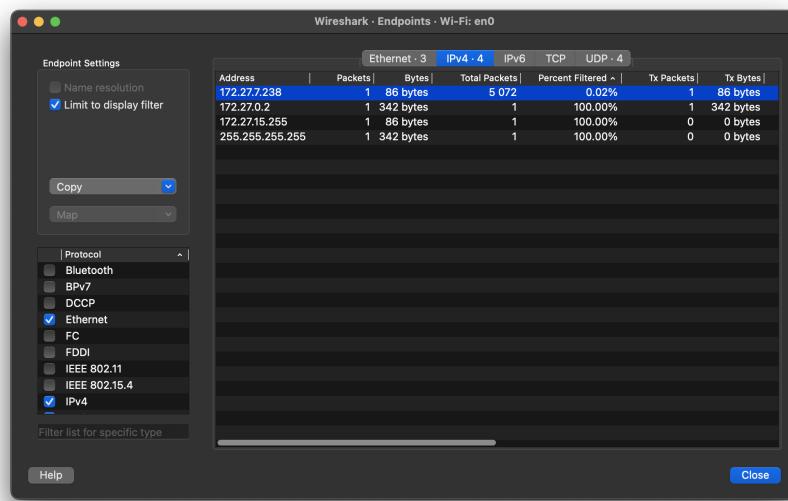


Рис. 3: Узел, осуществивший наибольшее количество широковещательных рассылок

Узел с максимальным количеством переданных пакетов:

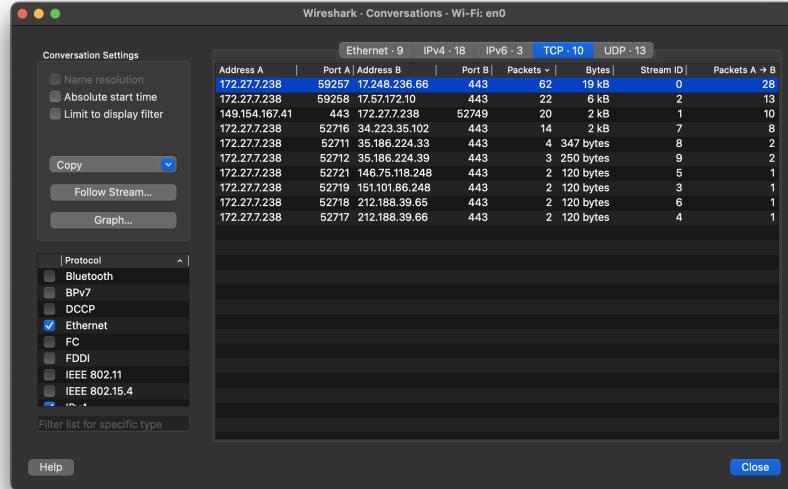


Рис. 4: Самый активный TCP-порт на хосте

Построим график интенсивности TCP и UDP:

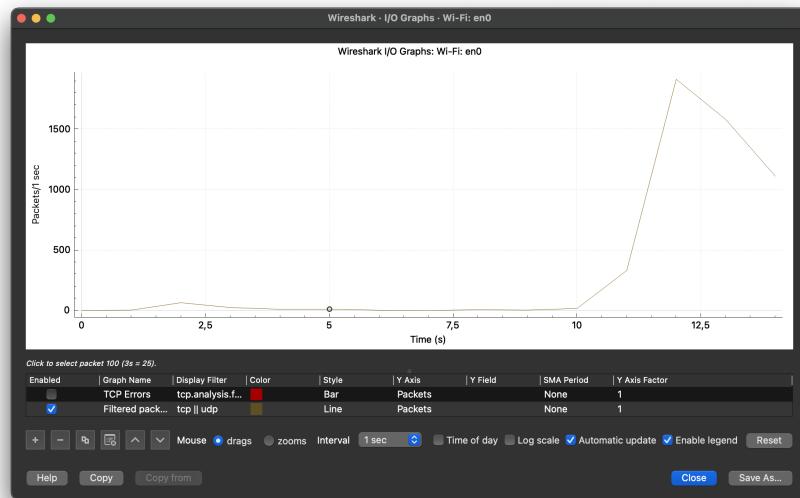


Рис. 5: График интенсивности трафика TCP и UDP

Отфильтруем по протоколу tls

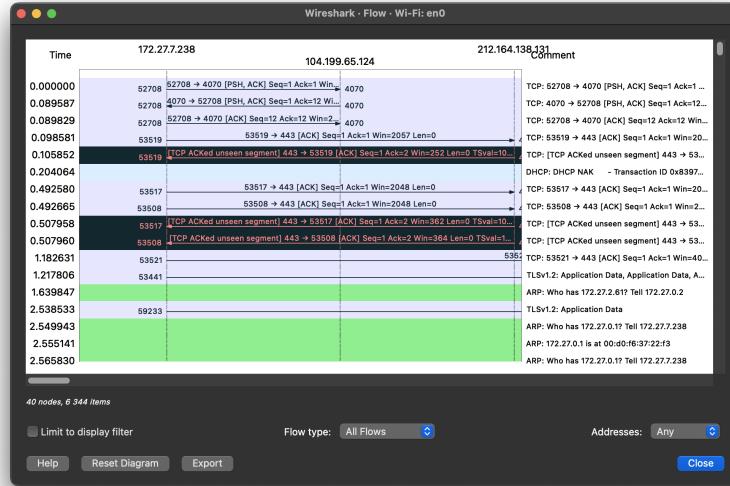


Рис. 6: Диаграмма связей только для пакетов, содержащих сообщения протокола HTTPS

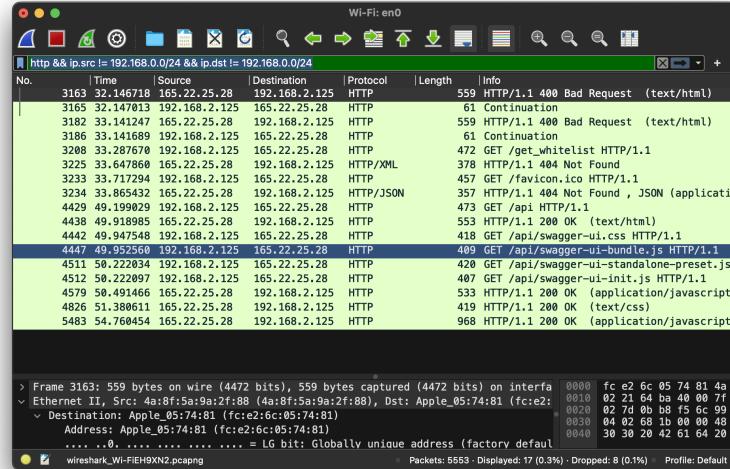


Рис. 7: Протоколы HTTP: локальные клиенты и внешние сервера

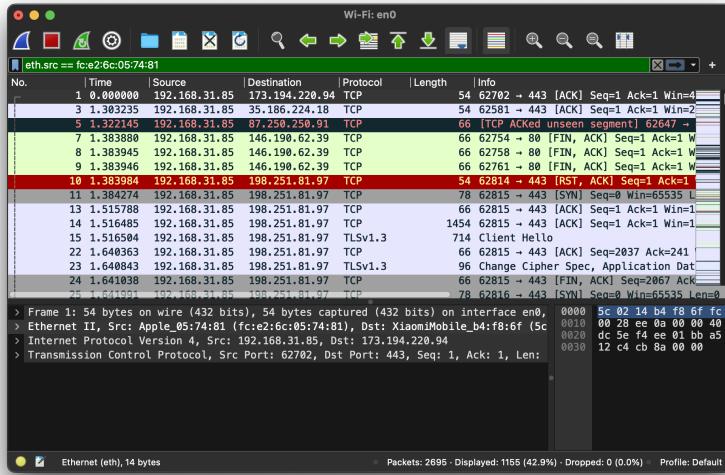


Рис. 8: Все кадры Ethernet, отправленные с сетевого интерфейса хоста

В следующем скриншоте видно, что ARP и UDP являются наиболее распространеными широковещательными сообщениями в моей сети в связи с тем, что технологии "Умного дома" регулярно общаются друг с другом (напр., умные лампочки). Если говорить о протоколах, которые часто "общаются" в широковещательном режиме, то к ним относятся: DHCP, SSDP и т.д.

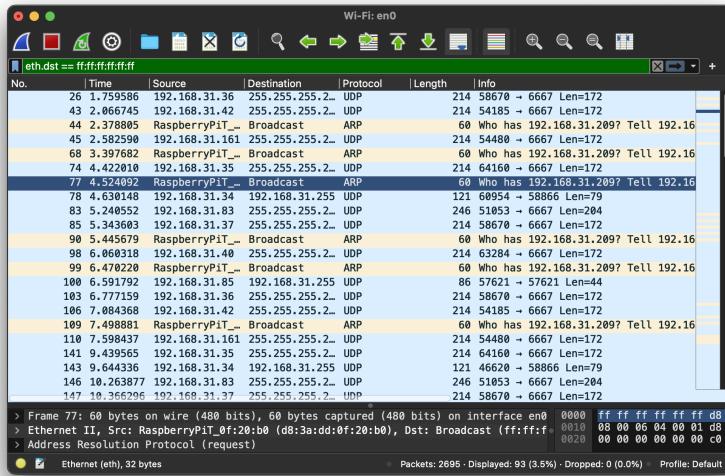


Рис. 9: Широковещательные сообщения

Для определения адресов, на которые поступают кадры, можем использовать следующие фильтры. Для определения адресов на канальном уровне - eth. На сетевом уровне - ip.

Фильтры для широковещательных рассылок: `arp.opcode == 1`, `udp.port == 1900`, `bootp.type == 1`.

На основе статистики и полученных данных в Wireshark, можно сделать вывод, что устройство принадлежит к маршрутизатору, так как видны IP адреса, а маршрутизатор как раз-таки работает на сетевом уровне.

2.2 Сбор и углубленный анализ данных протокола ICMP

Начнем с анализа локальных узлов. Я взял адреса ноутбука и моего телефона. Пропишем команду `ping` в терминале с адресом телефона. В Wireshark посмотрим на первый отправленный пакет:

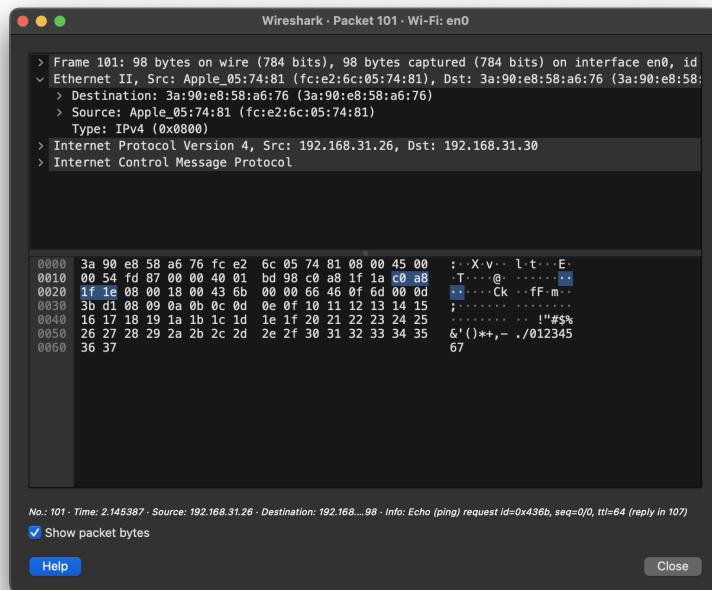


Рис. 10: Анализ пакета в Wireshark

MAC-адреса ноутбука и телефона совпадают с теми адресами, которые прописаны в Wireshark.

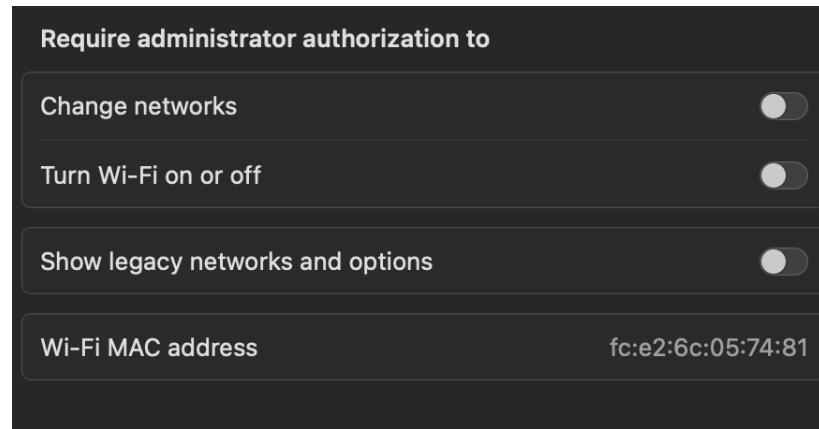


Рис. 11: MAC-адрес ноутбука

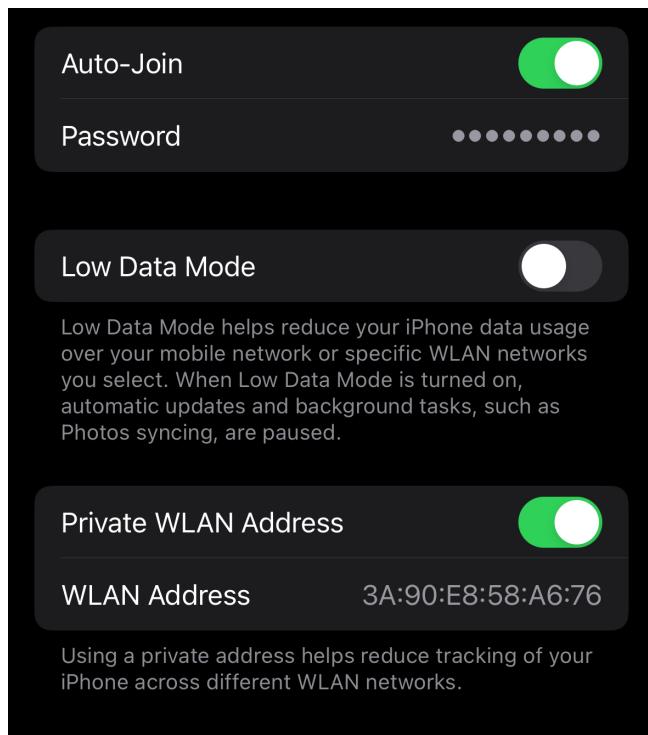


Рис. 12: MAC-адрес телефона

Далее проанализируем удаленные узлы. Составим таблицу с ссылками, ip-адресами сайтов.

IP-адрес	Сайт
140.82.121.4	github.com
31.13.72.36	facebook.com
142.250.74.46	youtube.com

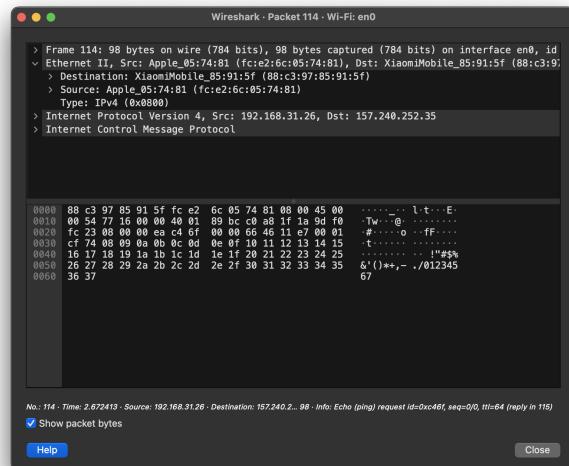


Рис. 13: GitHub анализ в Wireshark

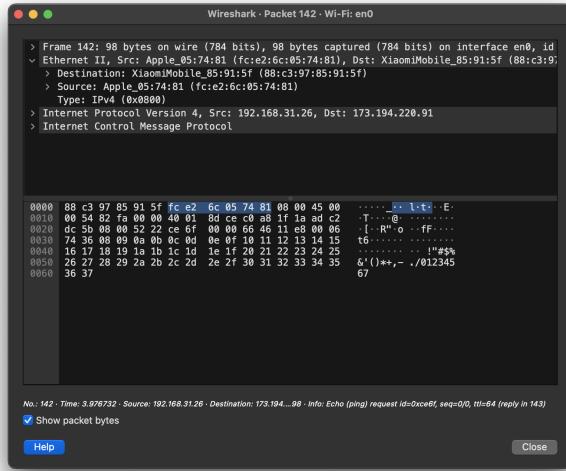


Рис. 14: YouTube анализ в Wireshark

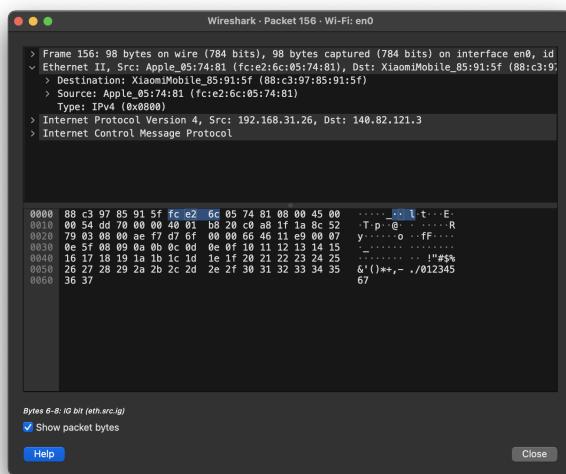


Рис. 15: Facebook анализ в Wireshark

При выполнении команды ping для устройства в локальной сети, компьютер сначала отправляет ARP-запрос для определения MAC-адреса устройства, получает ARP-ответ с этим MAC-адресом, обновляет свой ARP-кэш и затем отправляет ICMP-эхо-запрос.

Программа Wireshark показывает фактические MAC-адреса локальных узлов, поскольку они включены в Ethernet-кадры в пределах локальной сети, но не показывает фактические MAC-адреса удаленных узлов, так как передача через маршрутизаторы заменяет исходные MAC-адреса на свои собственные при каждой передаче (hop).

2.3 Анализ полей TCP

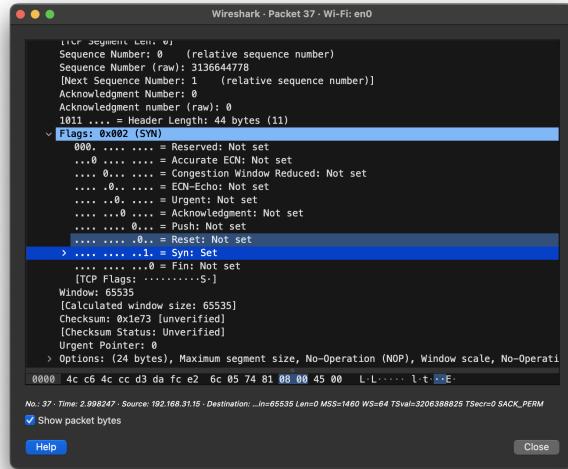


Рис. 16: Запрос от компьютера к серверу

Название поля	Значение поля
IP-адрес источника	192.168.31.15
IP-адрес назначения	158.160.35.173
Номер порта источника	63409
Номер порта назначения	443
Порядковый номер	0
Номер подтверждения	0
Длина заголовка	44 bytes
Размер окна	65535

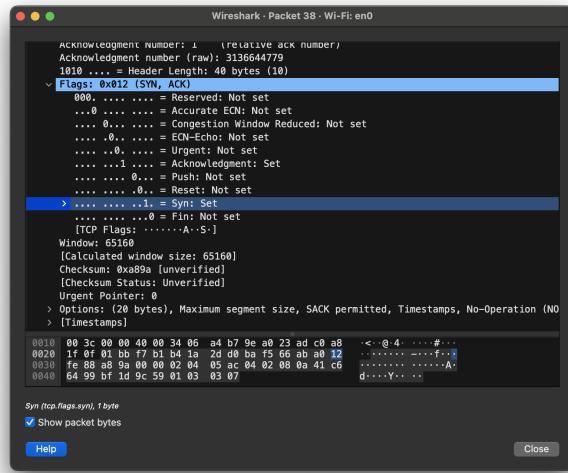


Рис. 17: Ответ от сервера

Название поля	Значение поля
IP-адрес источника	158.160.35.173
IP-адрес назначения	192.168.31.15
Номер порта источника	443
Номер порта назначения	63409
Порядковый номер	0
Номер подтверждения	1
Длина заголовка	40 bytes
Размер окна	65160

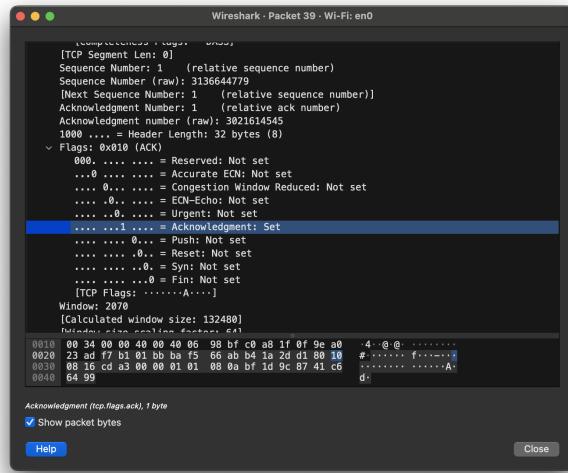


Рис. 18: Повторный запрос компьютера к серверу

Название поля	Значение поля
IP-адрес источника	192.168.31.15
IP-адрес назначения	158.160.35.173
Номер порта источника	63409
Номер порта назначения	443
Порядковый номер	1
Номер подтверждения	1
Длина заголовка	32 bytes
Размер окна	132480

3 Вывод

В ходе лабораторной работы с программой Wireshark я разобрал структуру и функционирование стека TCP/IP, анализируя перехваченные пакеты данных. Я научился собирать сетевой трафик. Это позволило мне глубже понять взаимодействие различных уровней стека TCP/IP и выявить потенциальные проблемы в сетевом трафике.