**Сетевые технологии**

### Лабораторная работа №3

## Чигладзе Майя Владиславовна

**Содержание**

1. [Цель работы](#_bookmark0) 6
2. [Задание](#_bookmark1) 7
3. [Теоретическое введение](#_bookmark2) 8
4. [Выполнение лабораторной работы](#_bookmark3) 10
5. [Выводы](#_bookmark43) 31

[Список литературы](#_bookmark44) 32

**Список таблиц**

# Цель работы

Целью данной лабораторной работы является приобретение практических навыков посредством Wireshark кадров Ethernet,анализ PDU протоколов транспортного и прикладного уровнейстека TCP/IP.

# Задание

С помощью команды ipconfig для ОС типа Windows или ifconfig для систем типа Linux выведите информацию о текущем сетевом соединении. Ис- пользуйте разные опции команды. В отчёте поясните детально полученную в каждом случае при выводе информацию. Подтвердите свой ответ скриншо- тами.

Определите MAC-адреса сетевых интерфейсов на вашем компьютере. Под- твердите свой ответ скриншотом.

Опишите структуру MAC-адресов вашего устройства. Какая часть адреса иден- тифицирует производителя? Какая часть адреса идентифицирует сетевой интерфейс? Определите, каким является адрес — индивидуальным или груп- повым, глобально администрируемым или локально администрируемым. Поясните свой ответ. Используйте шестнадцатеричную запись MAC-адреса для пояснения.

# Теоретическое введение

Wireshark — анализатор трафика сетей на базе технологии Ethernet ([https:](https://www.wireshark.org/)

[//www.wireshark.org/](https://www.wireshark.org/)). По функциональности Wireshark аналогичен утили- те tcpdump (<http://www.tcpdump.org/>), но имеет графический интерфейс. В основе используется библиотека Pcap.

Wireshark может использоваться для анализа и устранения неполадок в сети, определения угроз безопасности сети и их источников, выявления некорректной работы сетевых приложения в процессе их разработки, отладки реализации протоколов, для изучения внутренней структуры протоколов.

Рекомендуется для установки Wireshark в ОС Windows использовать мене- джер пакетов Chocolatey (<https://chocolatey.org/>). Потребуется установить Wireshark и драйвер WinPcap:

choco install wireshark choco install winpcap

Wireshark для сбора данных в реальном времени использует драйвер WinPcap

(NPF), для работы которого требуются права администратора. При установке драйвера WinPcap через Chocolatey он устанавливается для автоматического запуска с полномочиями администратора и не требует дальнейшей настройки.

Если установка Wireshark и WinPcap проводилась вручную, то для запуска потребуется вручную запустить NPT из-под записи администратора:

runas /u:administrator "net start npf"

После этого можно работать с Wireshark.

Для остановки NPF из-под записи администратора следует ввести:

runas /u:administrator "net stop npf"

Для запуска драйвера NPF под администратором автоматически при старте системы следует из-под учётной записи администратора ввести:

sc config npf start=auto

Альтернативный вариант— воспользоваться Device Manager, выбрать View-

>Show hidden devices, открыть Non-Plug and Play Drivers. Затем настро- ить запуск NetGroup Packet Filter Driver.

# Выполнение лабораторной работы

Запустите Wireshark.Выберите активный на вашем устройстве сетевой ин терфейс.Убедитесь,что начался процесс захвата трафика.

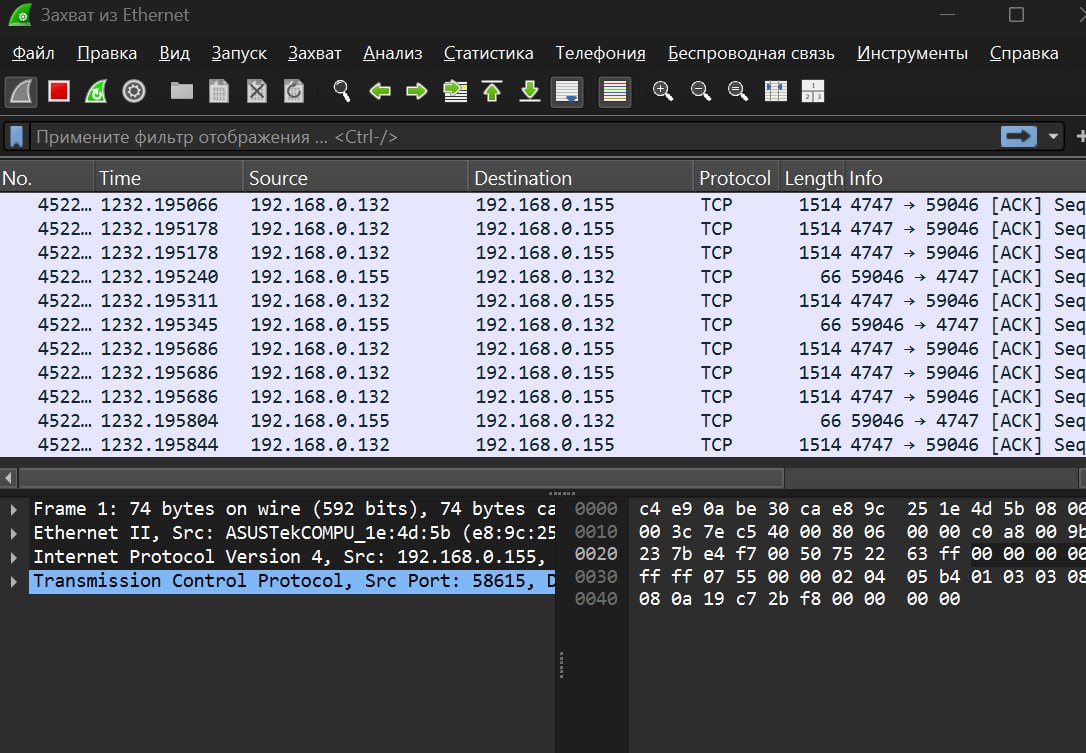
****

Рис. 1.1. Процесс захвата трафика

С помощью команды ipconfig выведем информацию о текущем сетевом соединении:



Рис. 1.2. Вывод информации о текущем сетевом соединении.

На вашем устройстве в консоли с помощью команды ping адрес\_шлюза

пропингуйте шлюз по умолчанию.

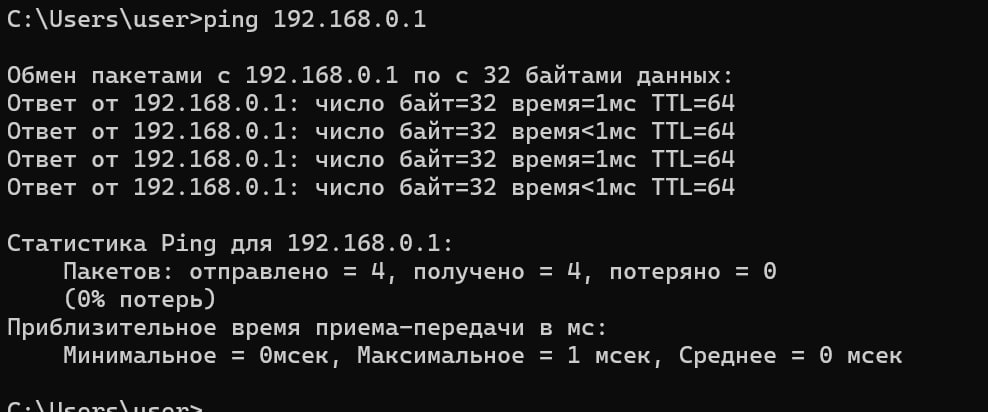


Рис. 1.3. Пингуем шлюз

В Wireshark остановим захват трафика. В строке фильтра пропишем фильтр arp or icmp и убедимся, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с нашего устройства на шлюз по умолчанию (Рис. 2.5).

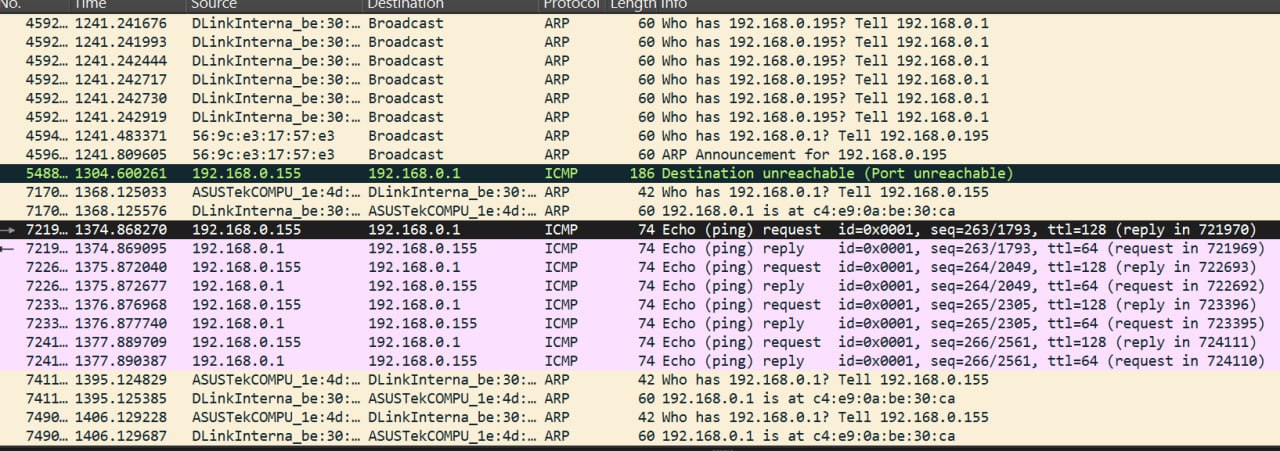


Рис. 1.4. Остановка захвата трафика. Фильтр arp or icmp.

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark:

– На панели списка пакетов выберем первый указанный кадр ICMP — эхо-запрос. 08-71-90-86-95-BB - MAC-адрес. Globally unique address, individual address (Рис. 2.6).

– На панели списка пакетов выберем второй указанный кадр ICMP — эхо-ответ. 04-D9-F5-E9-81-B8 - MAC-адрес. Globally unique address, individual address (Рис. 2.7).

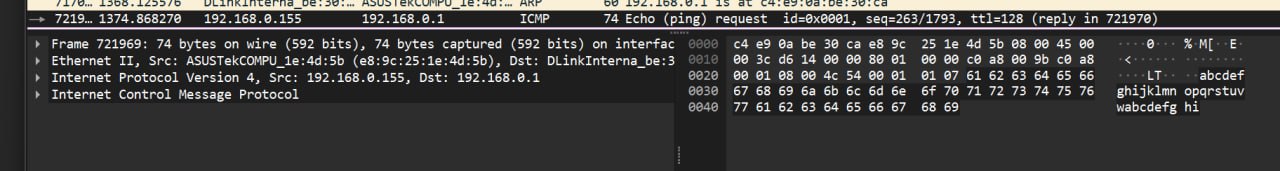


Рис. 1.5. Кадр ICMP — эхо-запрос.

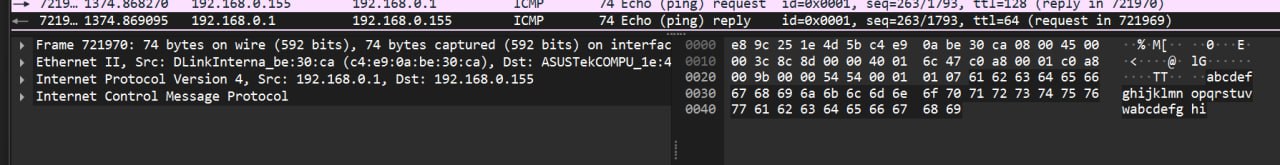


Рис. 1.6. Кадр ICMP — эхо-ответ.

Изучим кадры данных протокола ARP и данные в полях заголовка Ethernet II (Рис. 2.8).

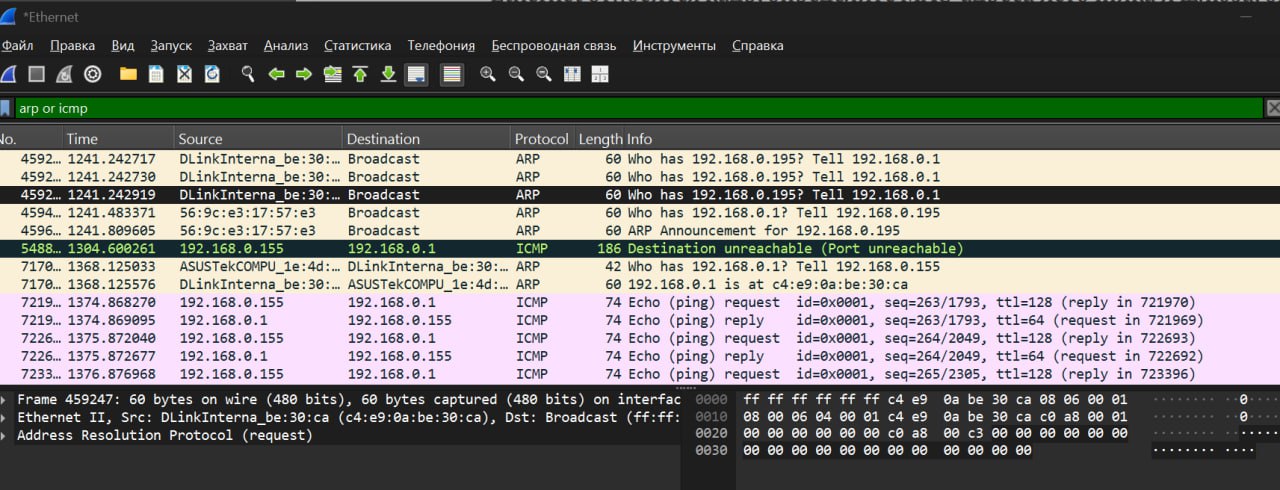


Рис. 1.7. Изучение кадров данных протокола ARP и данных в полях заголовка Ethernet II.

Начнём новый процесс захвата трафика в Wireshark. На нашем устройстве в консоли пропингуем по имени адрес ping rudn.ru (Рис. 2.9).

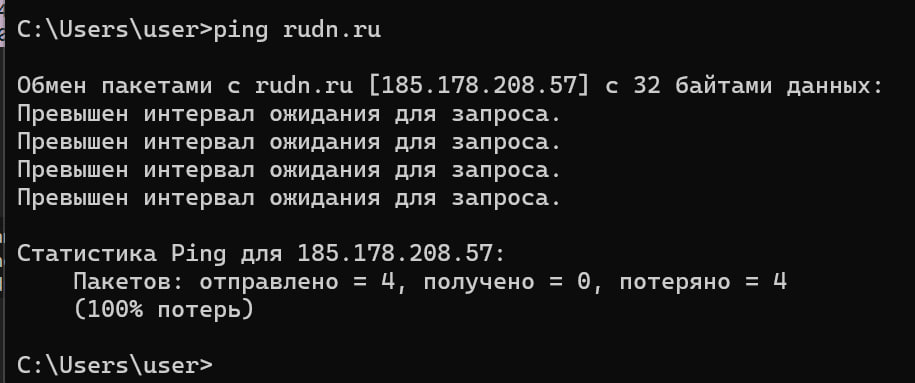


Рис. 1.9. Пингуем по имени адрес rudn.ru.

В Wireshark остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP.

08-71-90-86-95-BB - MAC-адрес источника, Globally unique address, individual address (Рис. 2.10).

04-D9-F5-E9-81-B8 - MAC-адрес получателя, Globally unique address, individual address (Рис. 2.11).

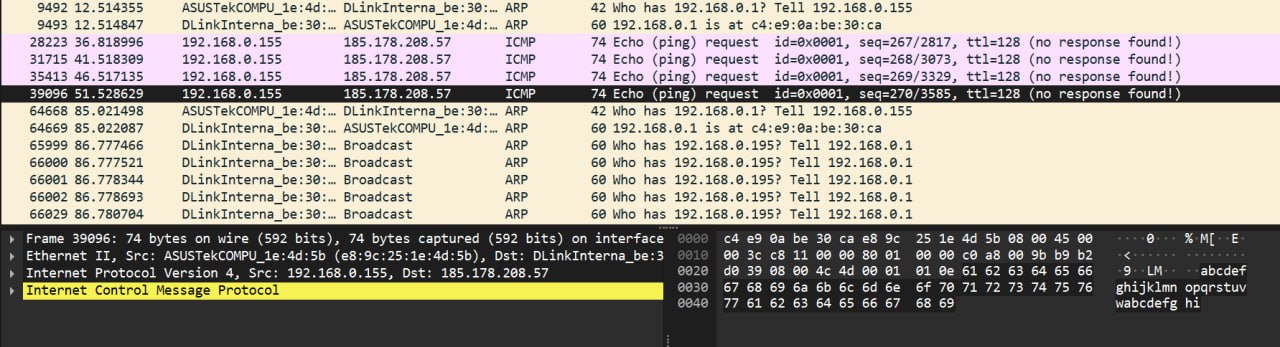


Рис. 1.10. MAC-адрес

Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (Рис. 3.1).

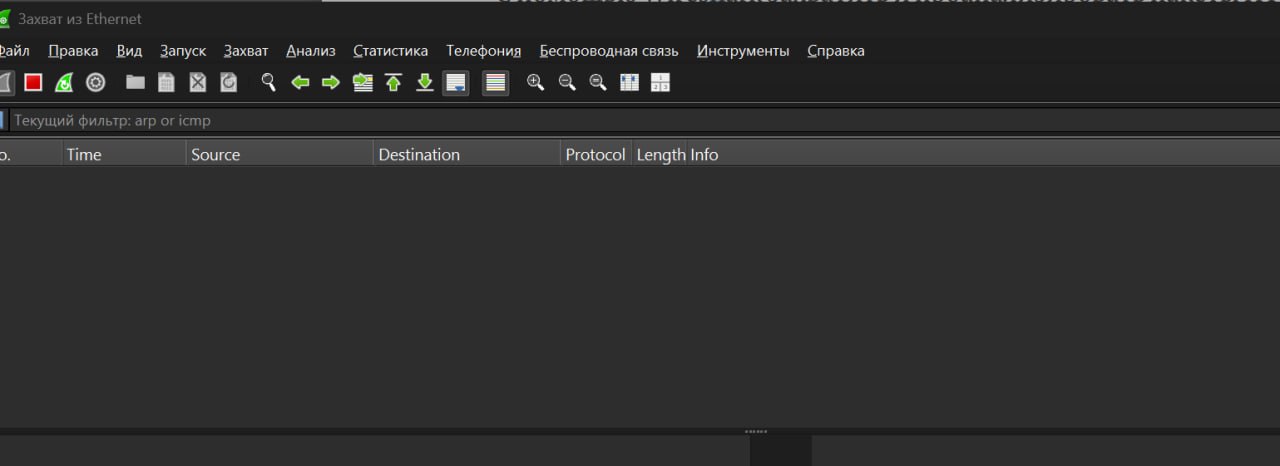
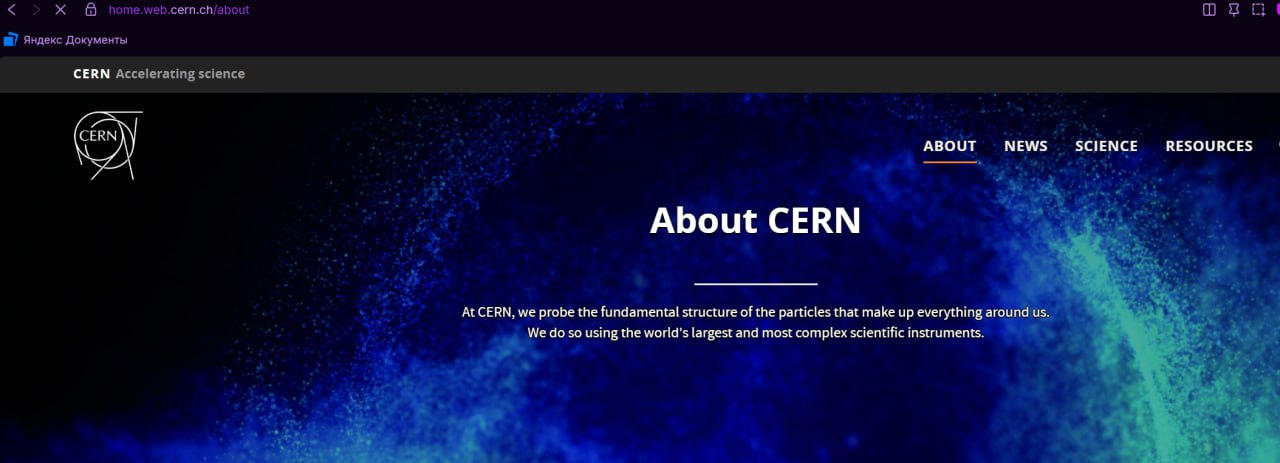


Рис. 2.1. Остановила Вайршарк.

На устройстве в браузере перейдём на сайт, работающий по протоколу HTTP (<http://info.cern.ch/>) и поперемещаемся по ссылкам и разделам сайта в браузере (Рис. 3.2).

Рис. 2.2. Открытие в браузере сайта CERN.

В Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов и ответов (Рис. 3.3).

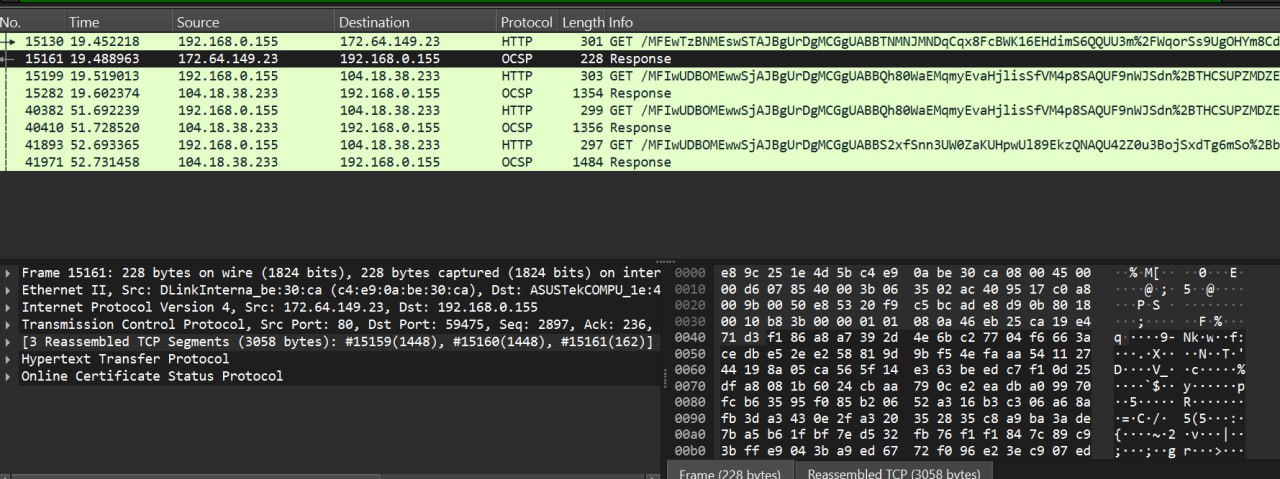


Рис. 2.3. Анализ информации по протоколу TCP.

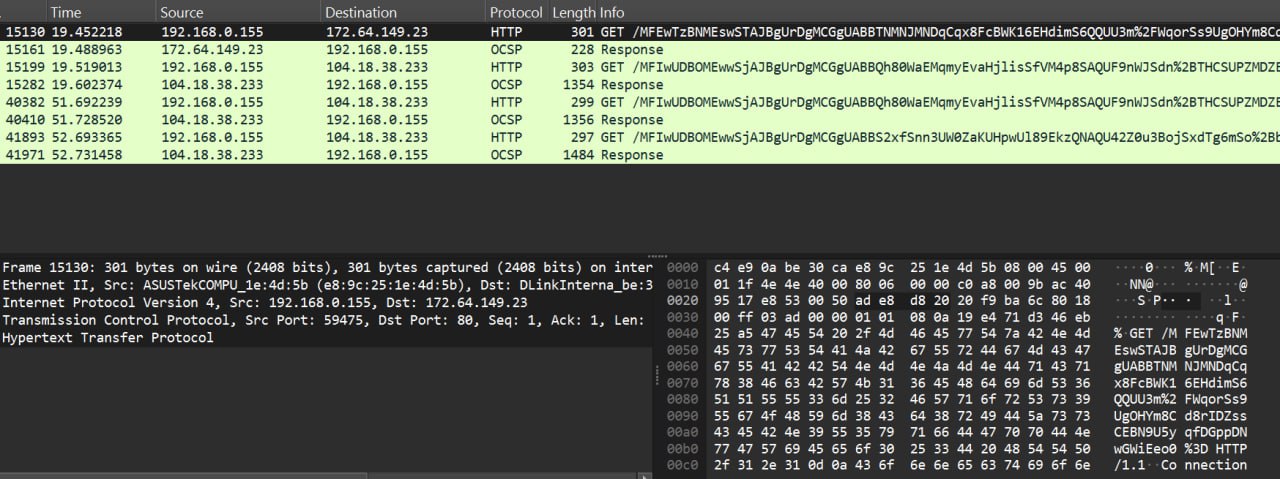


Рис. 2.4 Анализ информации по протоколу TCP1.

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов (Рис. 3.4).

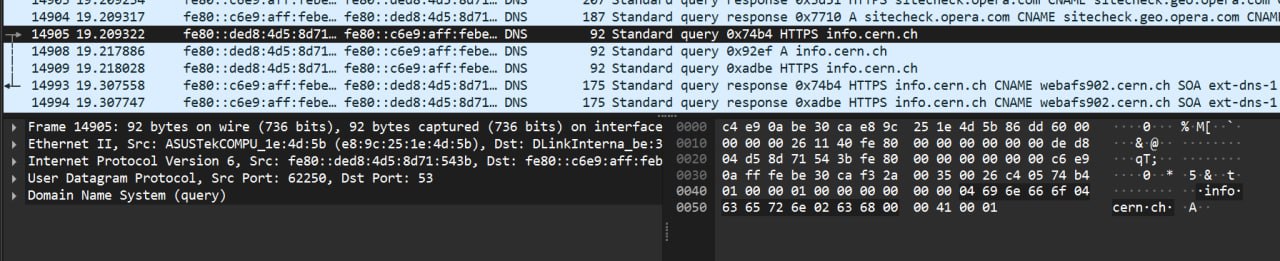


Рис. 2.5. Анализ информации по протоколу UDP.

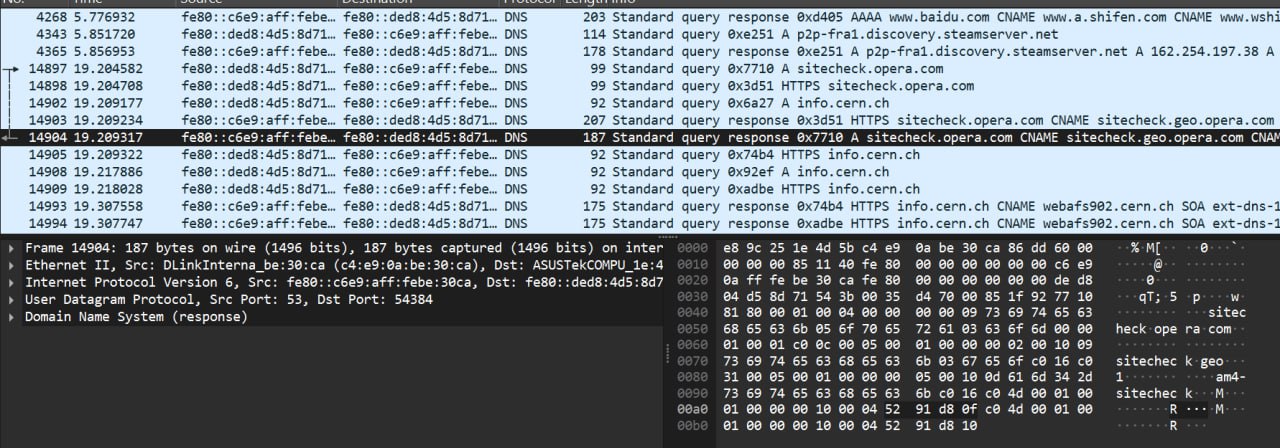


Рис. 2.6 Анализ информации по протоколу UDP2.

В Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов (Рис. 3.5).

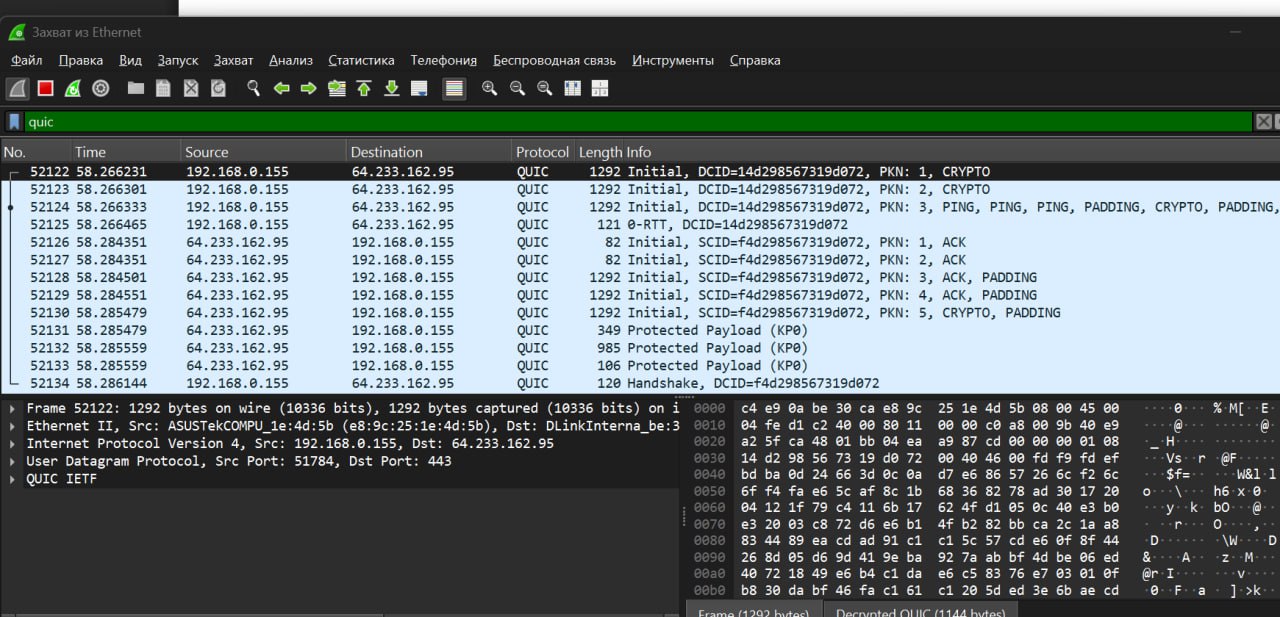


Рис. 2.7. Анализ информации по протоколу QUIC.

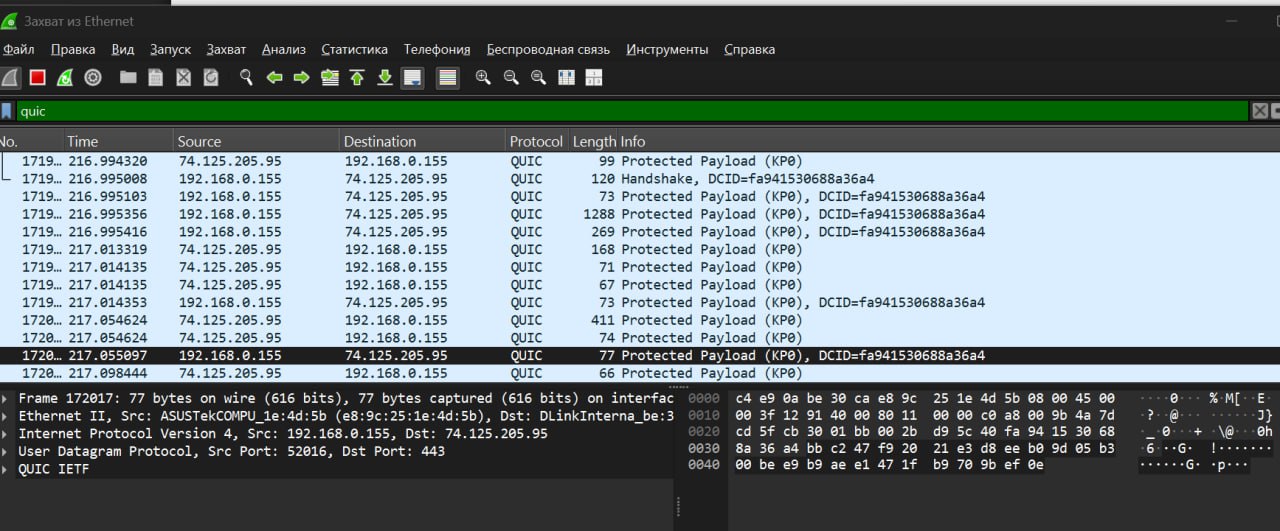


Рис. 2.8 Анализ информации по протоколу QUIC 2

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (Рис. 4.1).

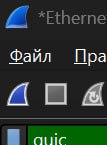


Рис. 3.1. Запуск Wireshark.

На устройстве используем соединение по HTTP с сайтом CERN для захвата в Wireshark пакетов TCP (Рис. 4.2).



Рис. 3.2. Использование соединения по HTTP с сайтом CERN.

В Wireshark проанализируем handshake протокола TCP (Рис. 4.3).

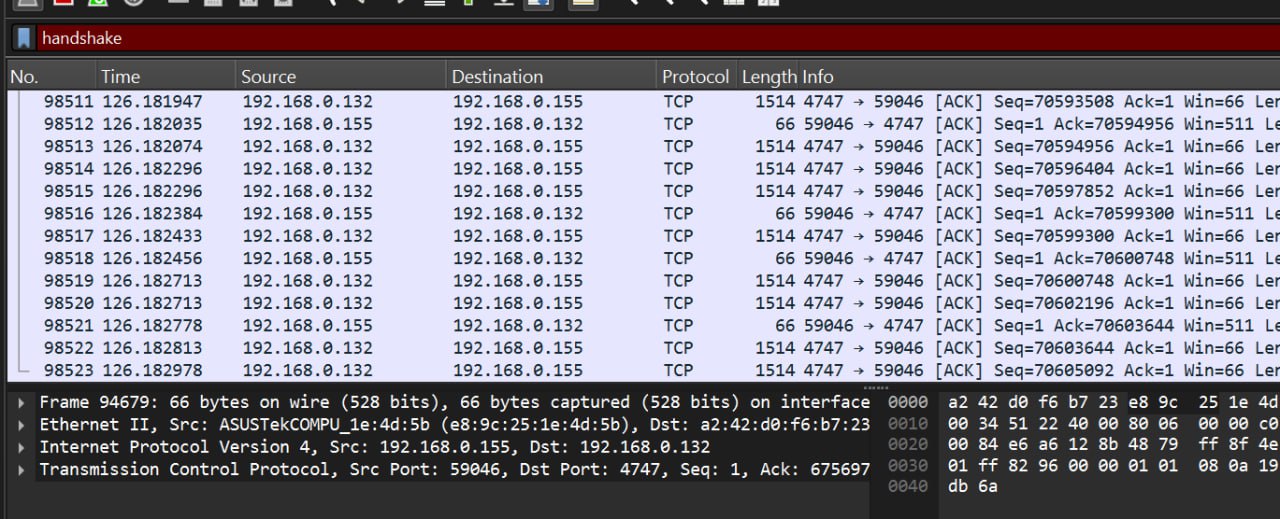


Рис. 3.3. Анализ handshake протокола TCP.

В Wireshark в меню «Статистика» выберем «График Потока» (Рис. 4.4).

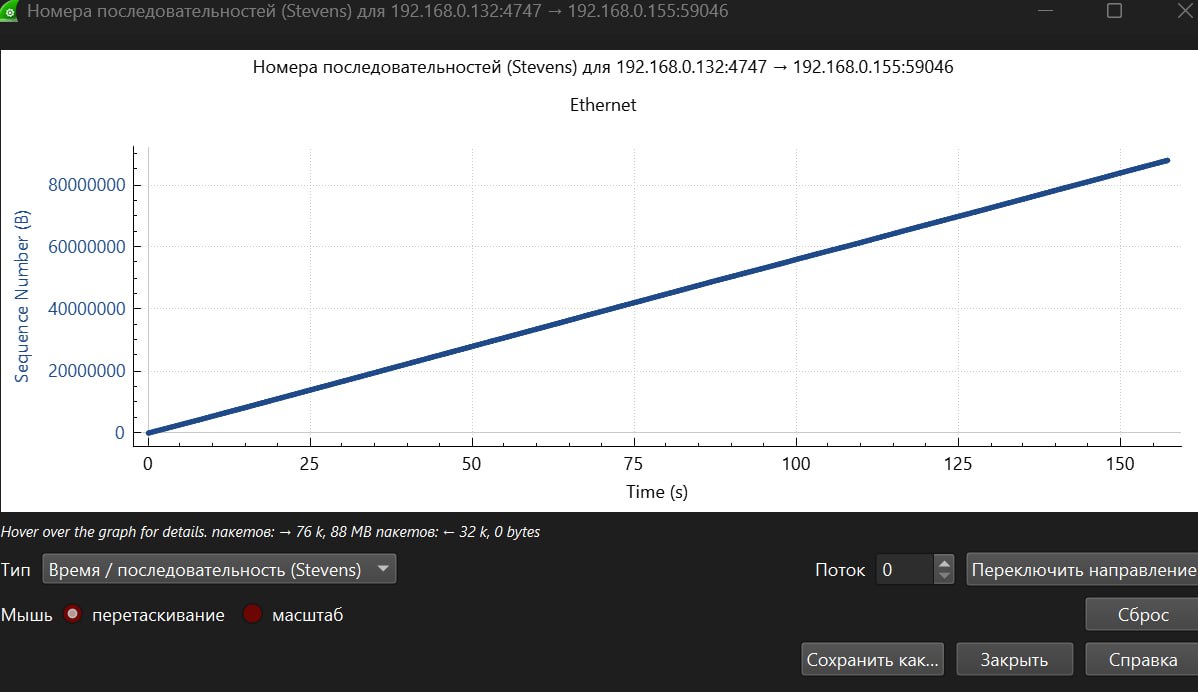


Рис. 3.4. График потока.

Вывод:

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

# Выводы

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

# Список литературы

* 1. Barr D. Common DNS Operational and Configuration Errors: RFC / RFC Editor.

—02/1996. — DOI: 10.17487/rfc1912.

* 1. Security-Enhanced Linux. Linux с улучшенной безопасностью: руковод- ство пользователя / M. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris. — URL: https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security- Enhanced\_Linux/index.html (дата обр.13.09.2021).
  2. Systemd. — 2015. — URL: https:/ /wiki .archlinux .org /index .php /Systemd (visited on 09/13/2021).
  3. Костромин В. А. Утилита lsof — инструмент администратора. — URL: http : / / rus linux.net/kos.php?name=/papers/lsof/lsof.html (дата обр. 13.09.2021).
  4. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: http : wiki.opennet.ru/Systemd (дата обр. 13.09.2021).
  5. Сайт проекта NetworkManager. — URL: https : / / wiki . gnome . org / Projects / NetworkManager (visited on 09/13/2021).
  6. Сайт проекта nmcli. — URL: https://developer.gnome.org/NetworkManager/stable/ nmcli.html (visited on 09/13/2021).