Федеральное государственное образовательное бюджетное   
учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЕТ   
по лабораторной работе**

**Лабораторная работа №11:** «Использование программы Wireshark для просмотра сетевого трафика**»**

**Студента:** Пузачёвой Ольги

**Дисциплина /Профессиональный модуль:** Компьютерные сети

|  |  |  |
| --- | --- | --- |
| **Группа:** 2ИСИП-221 |  | **Преподаватель:** |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.В.Сибирев/ |
|  |  | **Дата выполнения:** |
|  |  | 22.05.2023 г. |
|  |  | **Оценка за работу: \_\_\_\_\_\_\_\_\_\_\_\_** |

Москва   
2023

Содержание

[Задачи 3](#_Toc137849130)

[1. Теоретическая часть 4](#_Toc137849131)

[2. Практическая часть 5](#_Toc137849132)

[Заключение 11](#_Toc137849133)

# Задачи

1. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark;

2. Сбор и анализ данных протокола ICMP по удаленным узлам в программе Wireshark.

# Теоретическая часть

**Общие сведения:**

Wireshark — это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор «захватывает» каждую единицу данных протокола (PDU), после чего расшифровывает или анализирует ее содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark — полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства лабораторных работ в рамках курсов CCNA. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для захвата IP-адресов пакетов данных ICMP и МАС-адресов Ethernet-кадров.

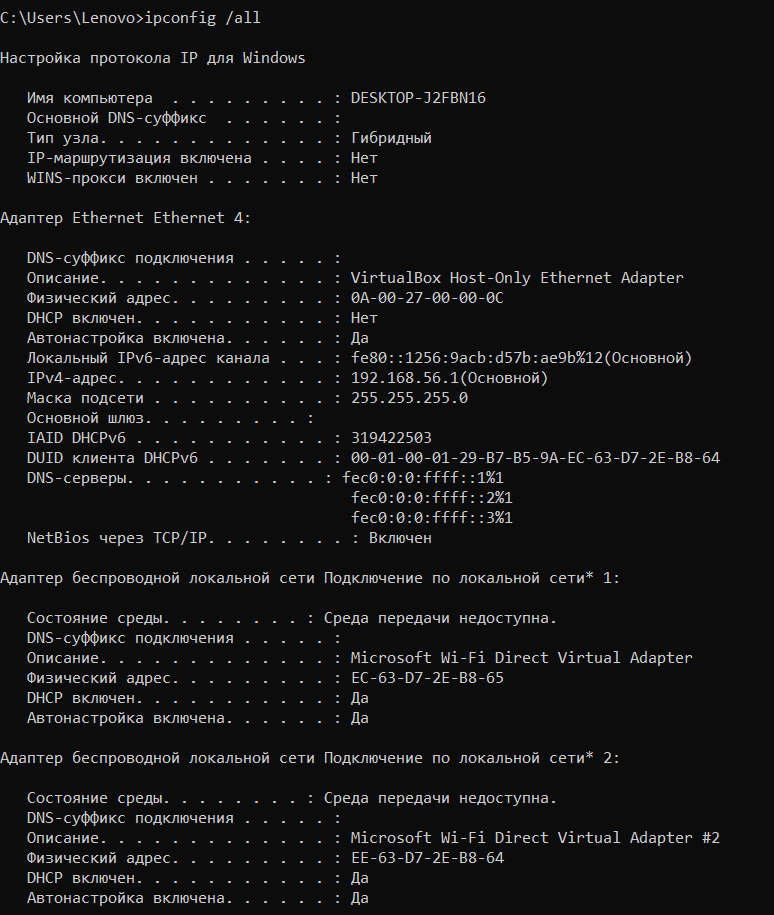
**Необходимые ресурсы:**

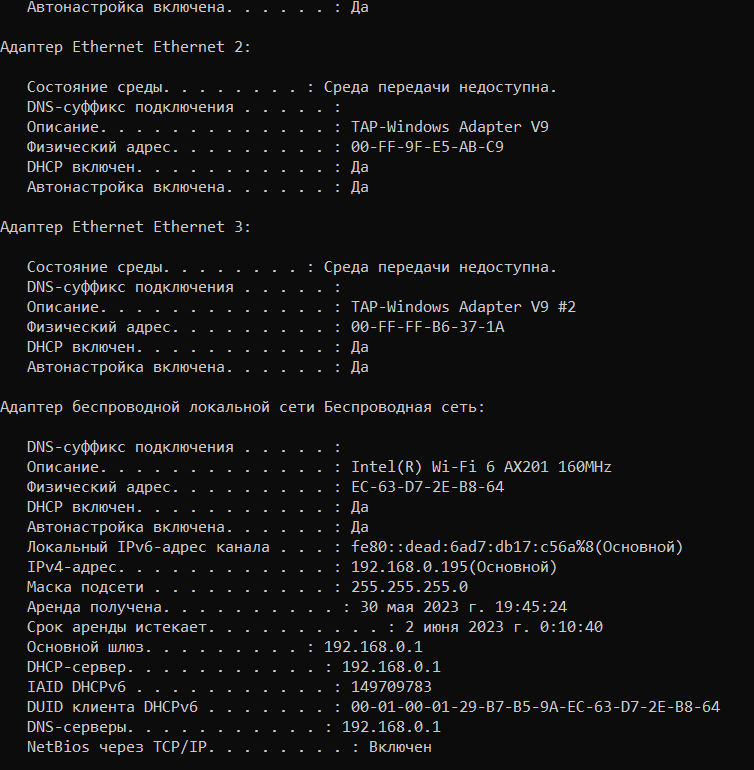
* 1 ПК (Windows с доступом в Интернет)
* Дополнительные ПК в локальной сети будут использоваться для ответов на ping-запросы.

# Практическая часть

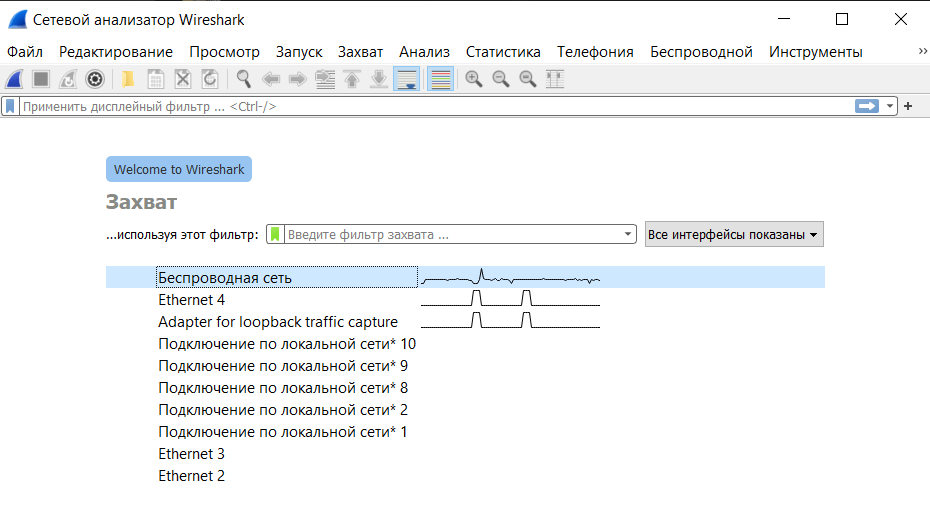
**Часть 1. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark**

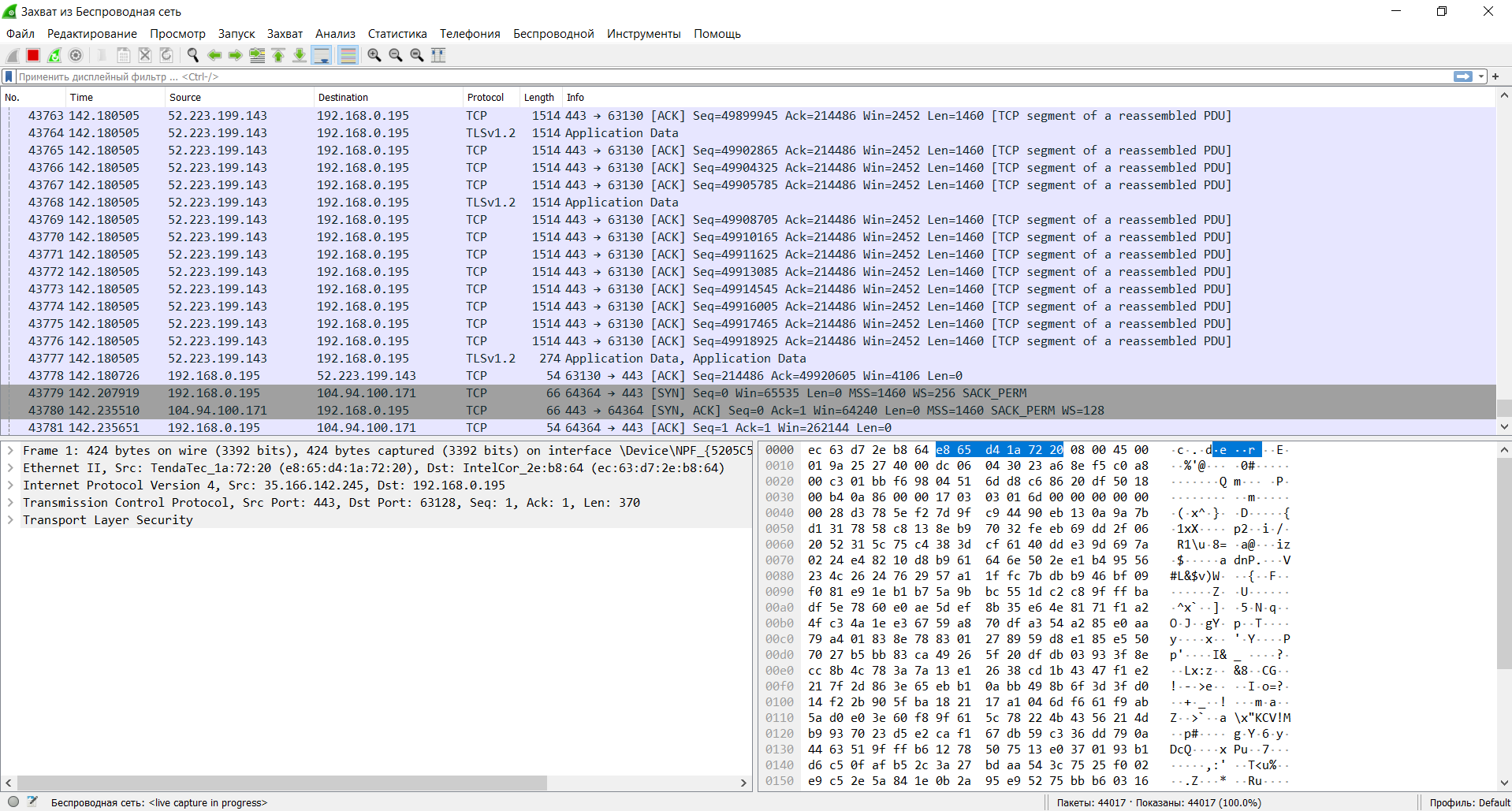
**Шаг 1. Узнать адреса интерфейсов своего ПК**

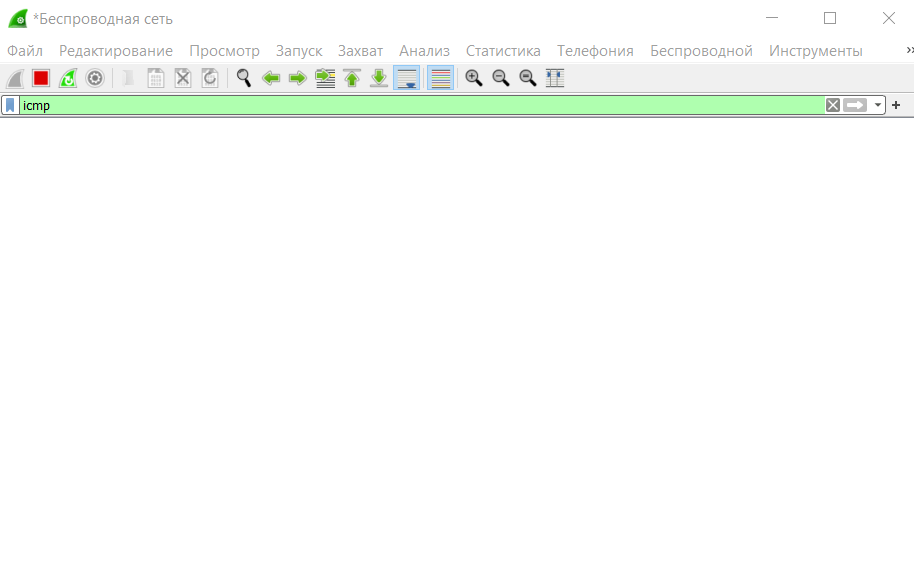


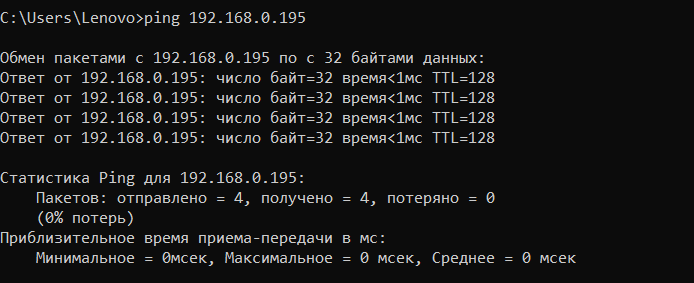


**Шаг 2. Запустить программу Wireshark и начать сбор данных**

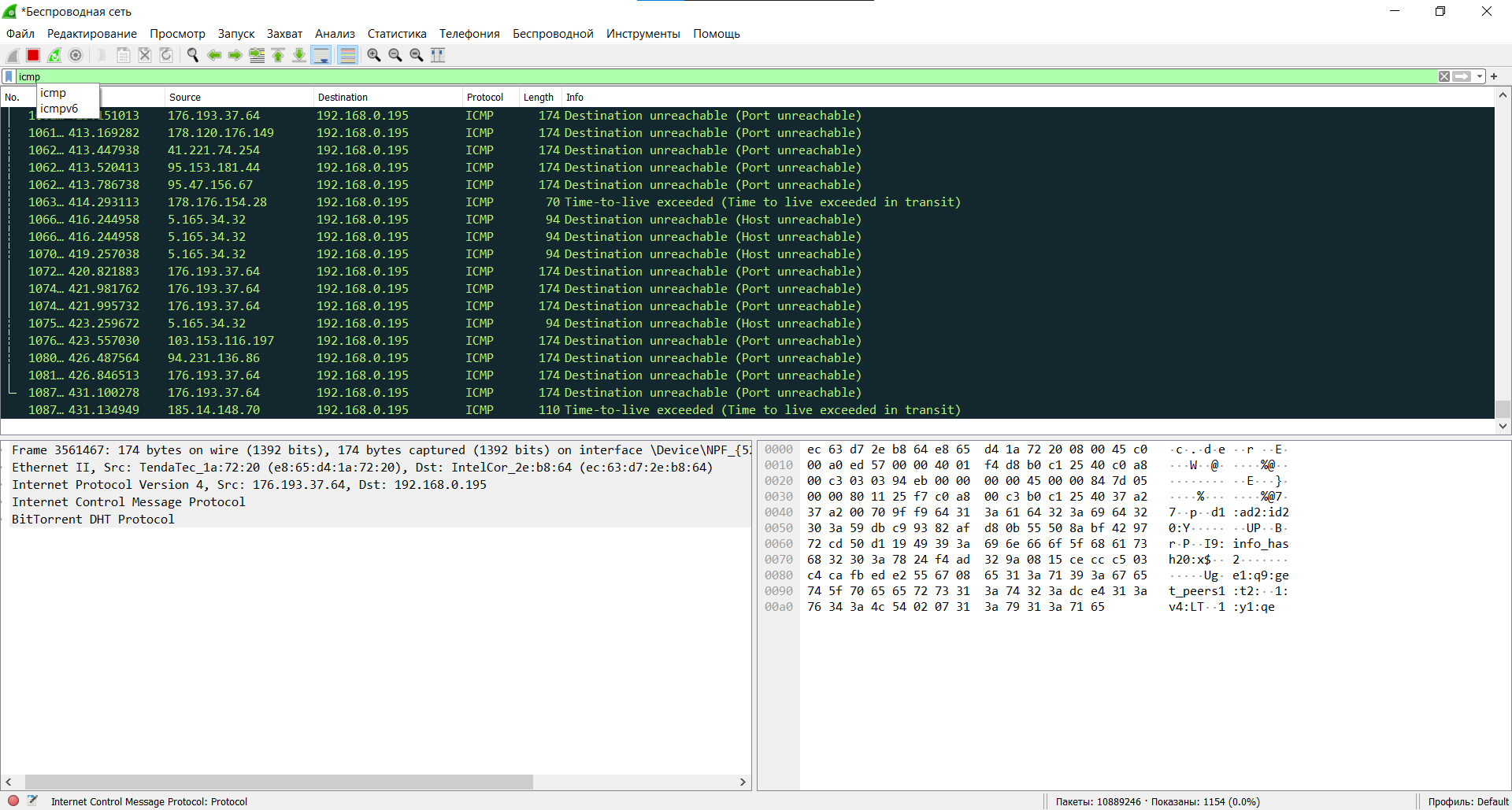
****

****

****Фильтрация по icmp, все данные в верхнем окне исчезли

****

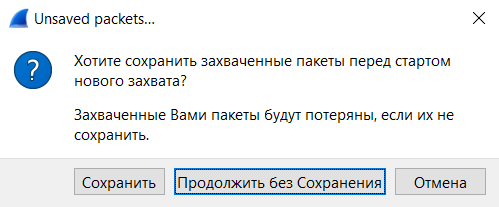
Эхо-запрос с помощью команды ping на IP-адрес другого человека

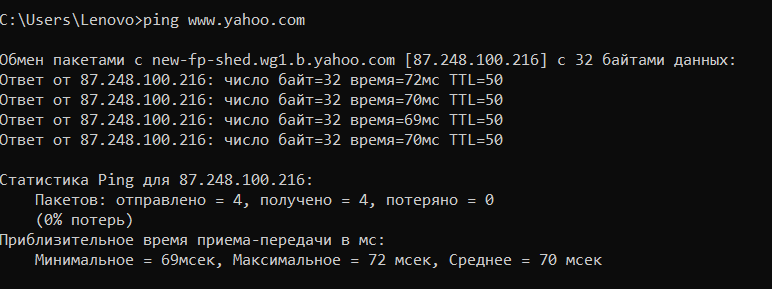


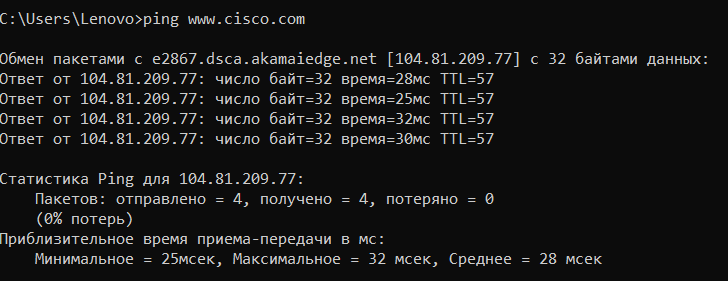
В верхней части окна программы Wireshark снова появились данные

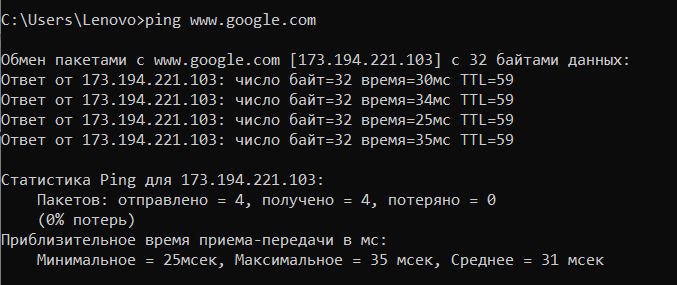
**Часть 2. Сбор и анализ данных протокола ICMP по удаленным узлам в программе Wireshark**

**Шаг 2. Запустить захват данных в интерфейсе**

****

****

****

****

**Шаг 2.** Изучить и проанализировать данные, полученные от удаленных узлов.

IP-адрес для URL-адреса [www.yahoo.com](http://www.yahoo.com): 87.248.100.216

MAC-адрес для URL-адреса [www.yahoo.com](http://www.yahoo.com): e8:65:d4:1a:72:20

IP-адрес для URL-адреса [www.cisco.com](http://www.cisco.com): 104.81.209.77

MAC-адрес для URL-адреса [www.cisco.com](http://www.cisco.com): e8:65:d4:1a:72:20

IP-адрес для URL-адреса [www.google.com](http://www.google.com): 173.194.221.103

MAC-адрес для URL-адреса [www.google.com](http://www.google.com): e8:65:d4:1a:72:20

MAC-адреса всех трех веб-сайтов совпадают.

# Заключение

В результате выполнения работы осуществлены сбор и анализ данных протокола ICMP по локальным и по удаленным узлам в программе Wireshark.