Федеральное государственное образовательное бюджетное   
учреждение высшего образования

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

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЕТ   
по практической работе**

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

**Студентки:** Кузьмичевой Полины

**Дисциплина /Профессиональный модуль:** Компьютерные сети

|  |  |  |
| --- | --- | --- |
| **Группа:** 2ИСИП-221 |  | **Преподаватель:** |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_/И. В. Сибирев/ |
|  |  | **Дата выполнения:** |
|  |  | 06.06.2023 г. |
|  |  | **Оценка за работу: \_\_\_\_\_\_\_\_\_\_\_\_** |

Москва   
2023

Содержание

[Цель работы: 3](#_Toc137328896)

[Задачи: 3](#_Toc137328897)

[Необходимые ресурсы: 3](#_Toc137328898)

[Теоретические сведения 3](#_Toc137328899)

[Практическая часть 3](#_Toc137328900)

[Контрольные вопросы: 8](#_Toc137328901)

[Заключение 9](#_Toc137328902)

[Используемые источни 9](#_Toc137328903)

Цель работы:

Научиться собирать и анализировать данные протокола ICMP в программе Wireshark при передаче данных в локальной сети и при передаче данных в удаленную сеть.

Задачи:

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

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

Необходимые ресурсы:

1 ПК (Windows с доступом в Интернет)

Дополнительные ПК в локальной сети будут использоваться для ответов на ping-запросы.

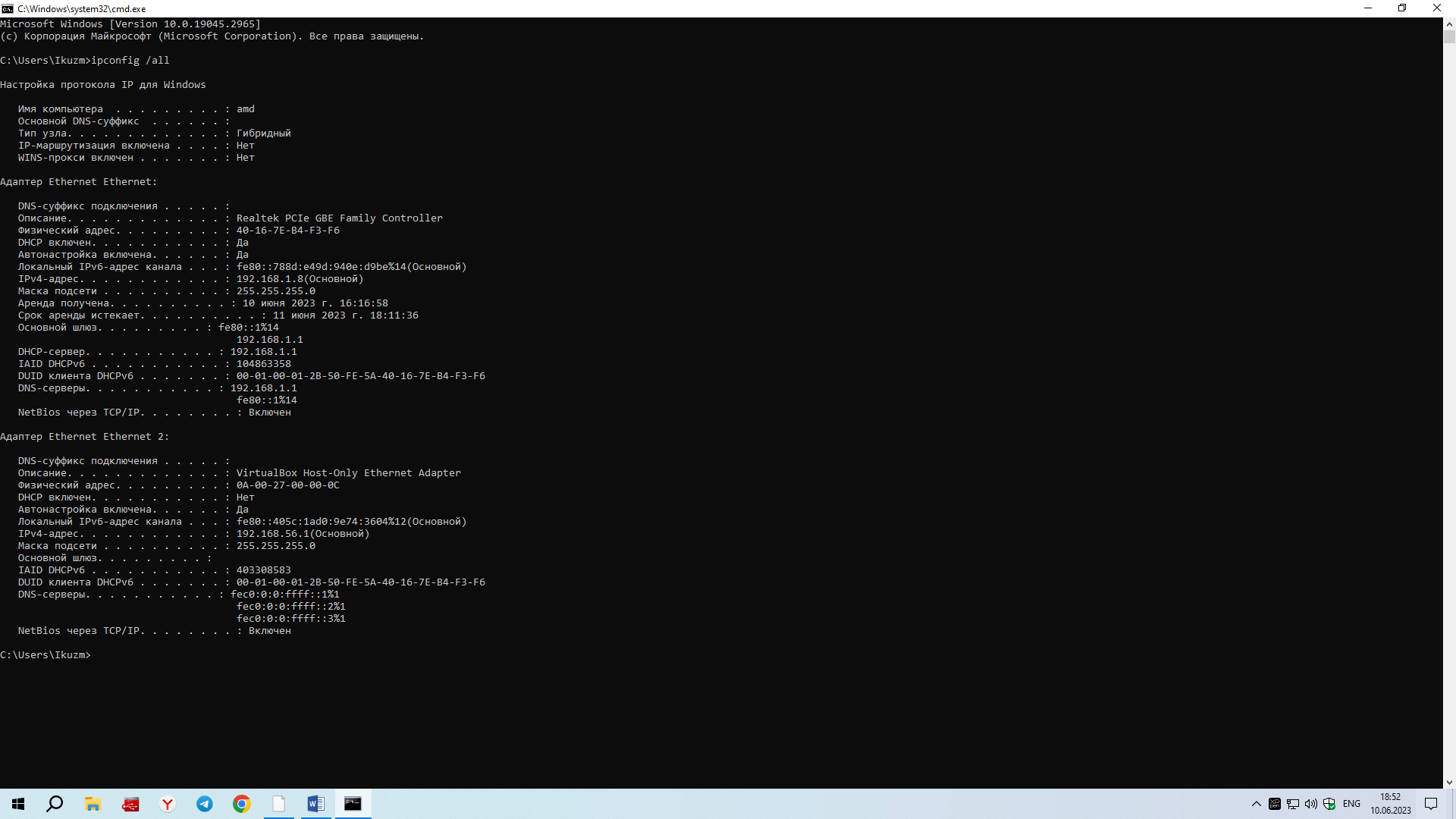
Теоретические сведения

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.

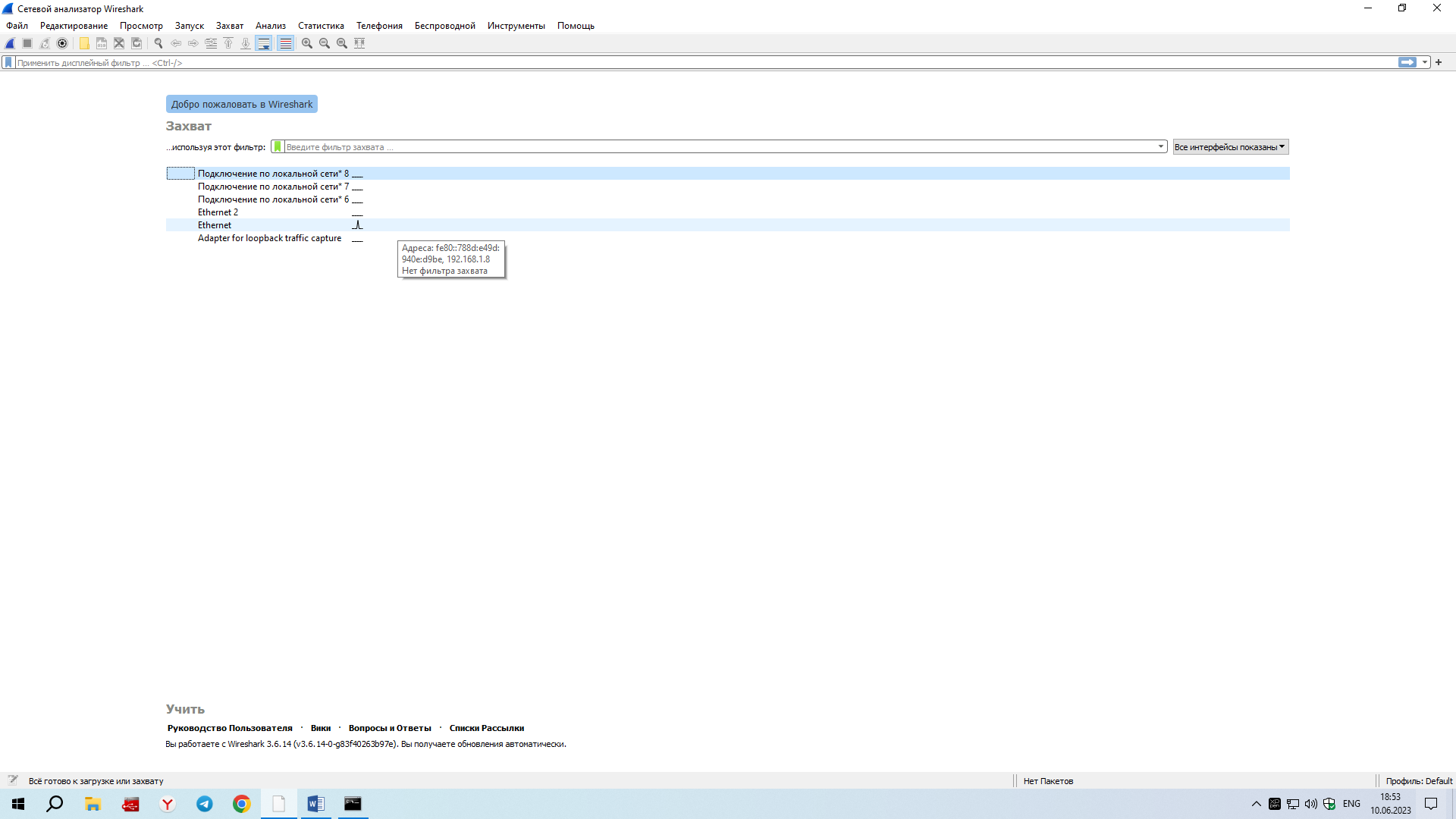
Практическая часть

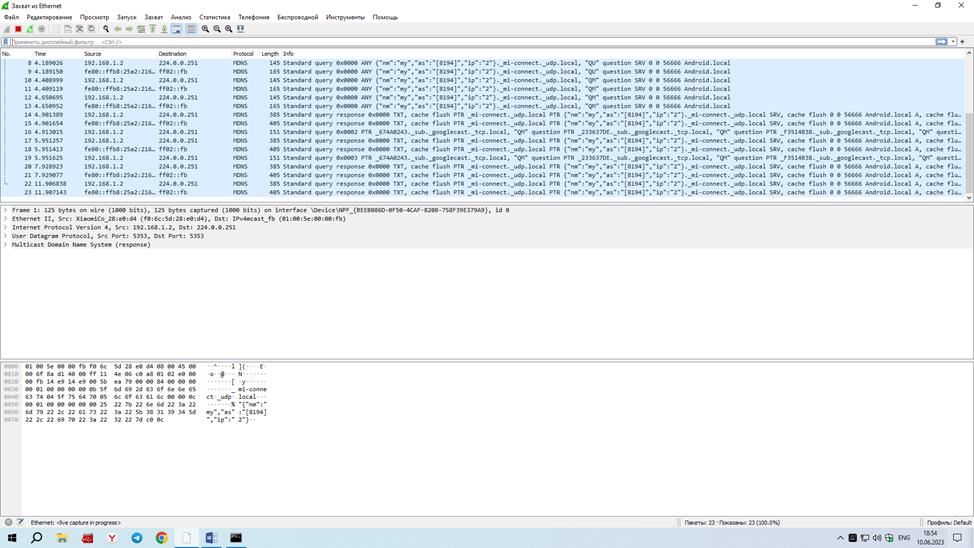
Часть 1. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

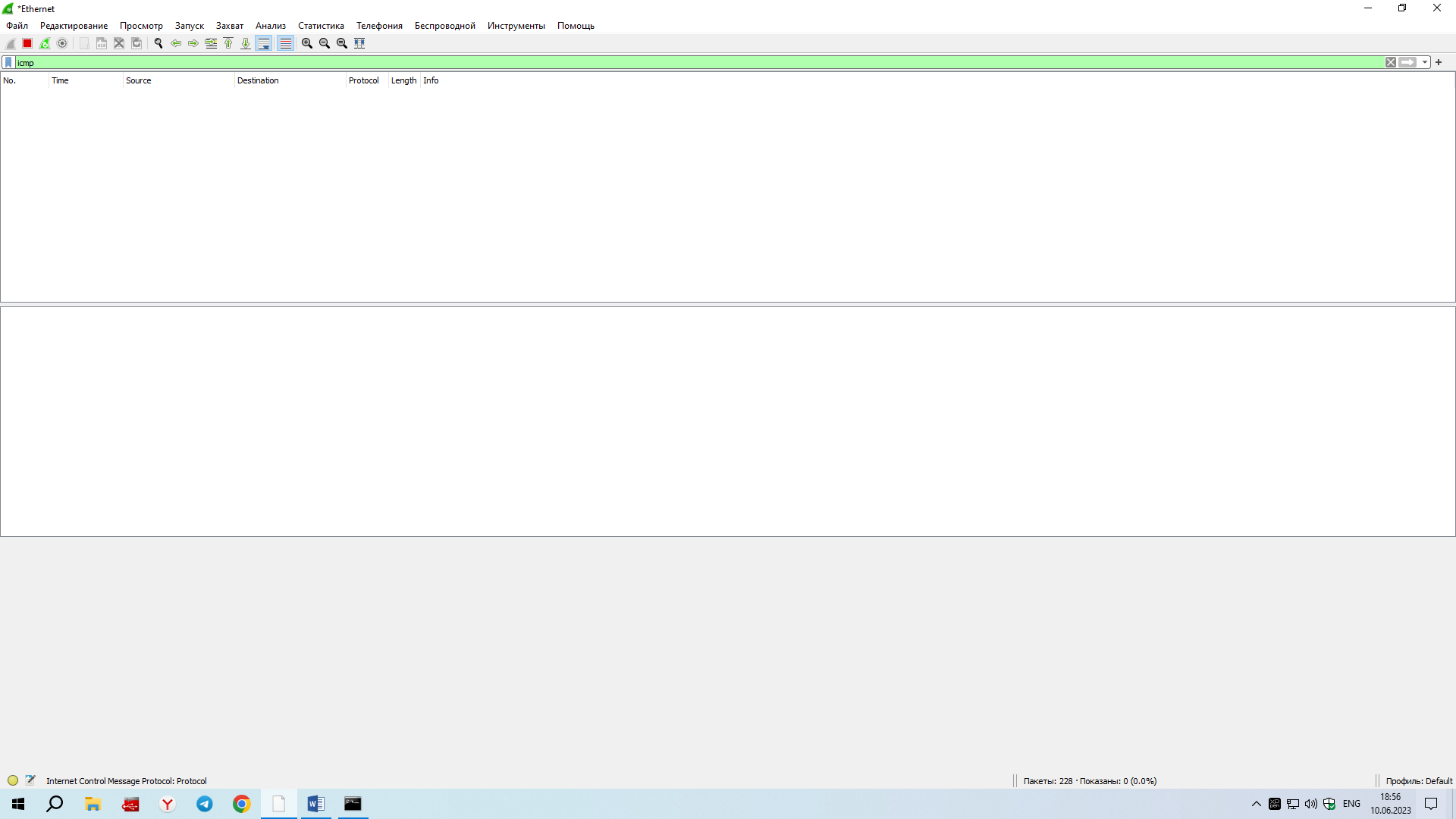
Шаг 1. Узнайте адреса интерфейсов своего ПК

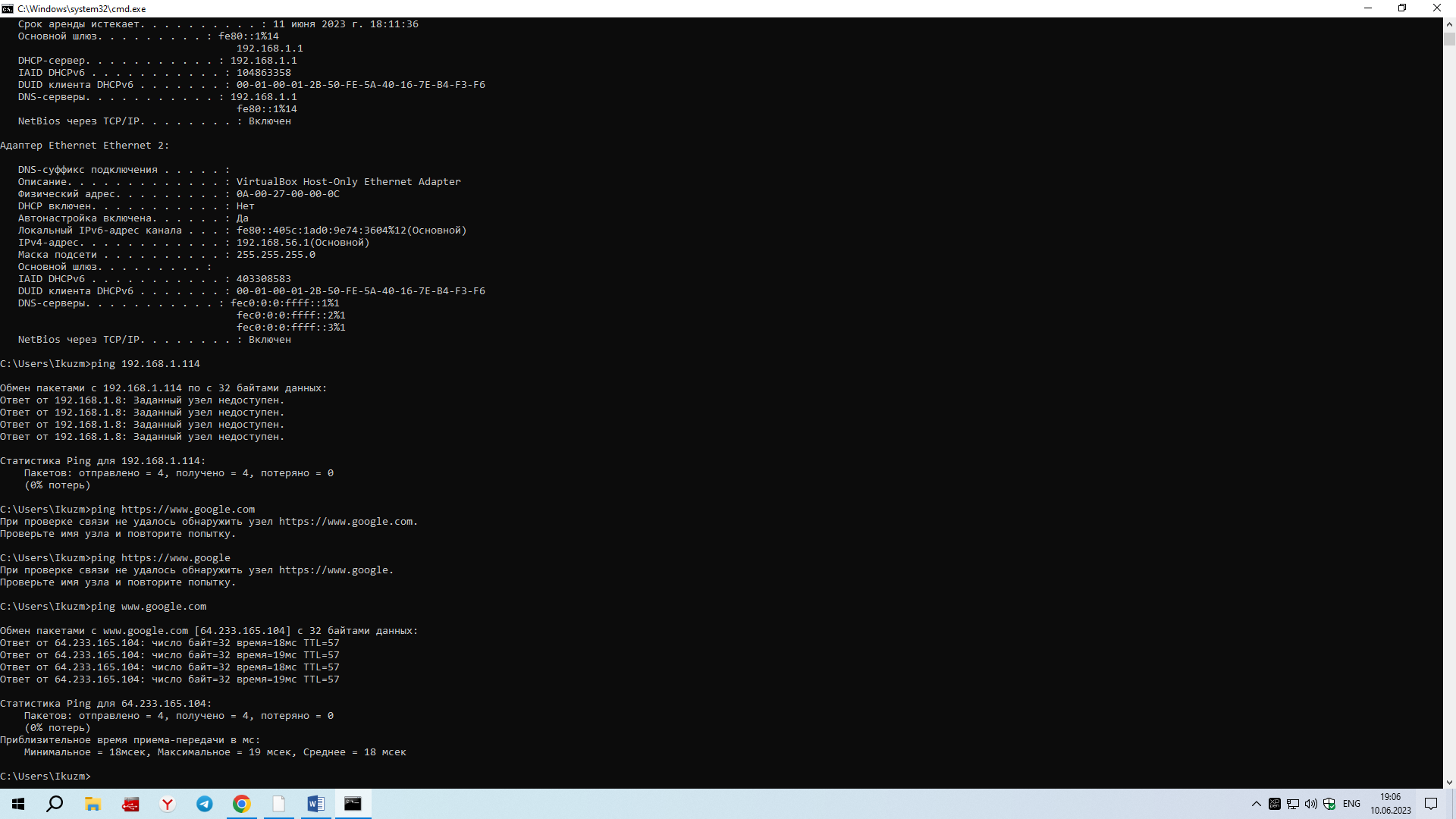


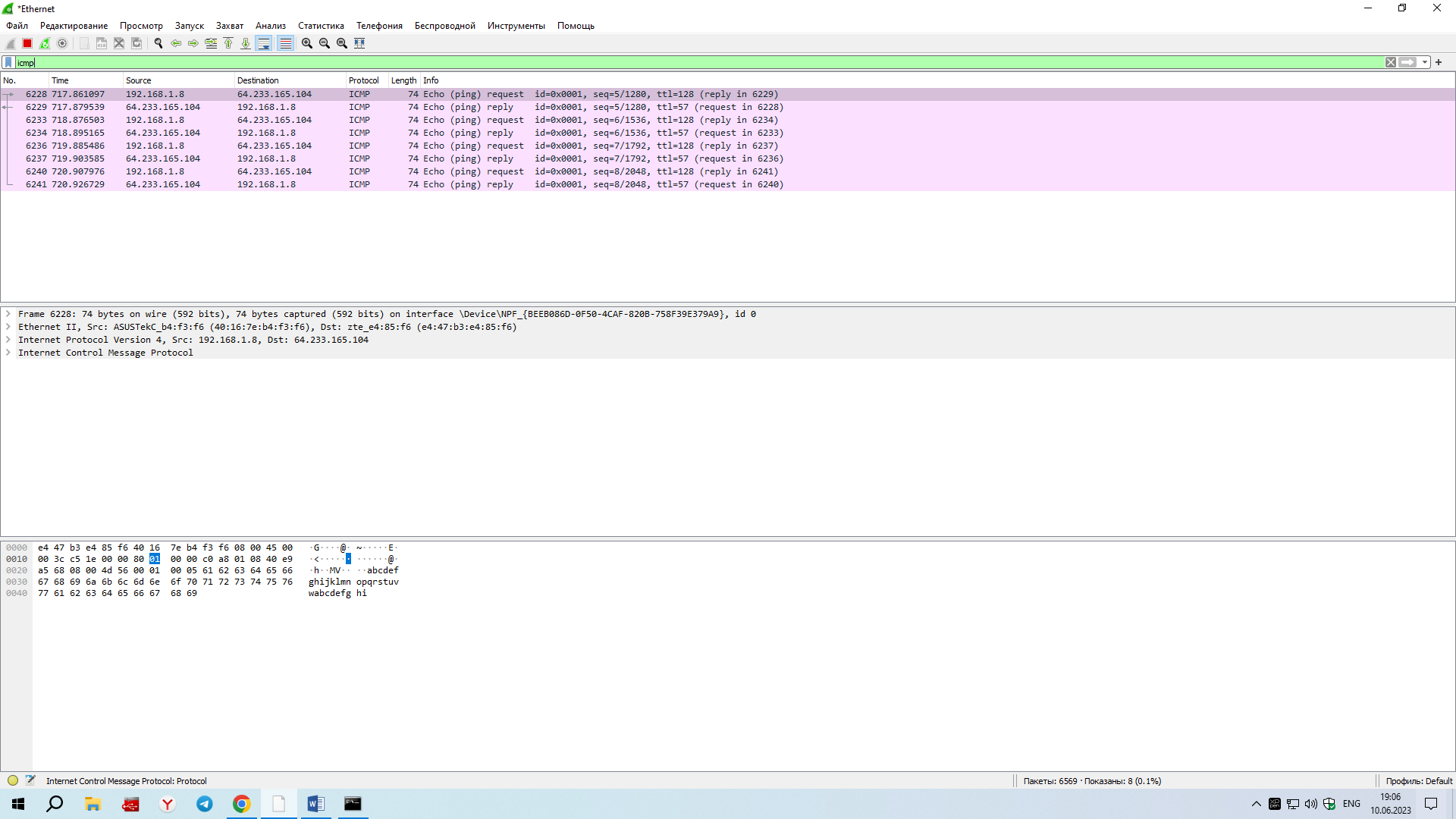
Шаг 2. Запустите программу Wireshark и начните сбор данных.

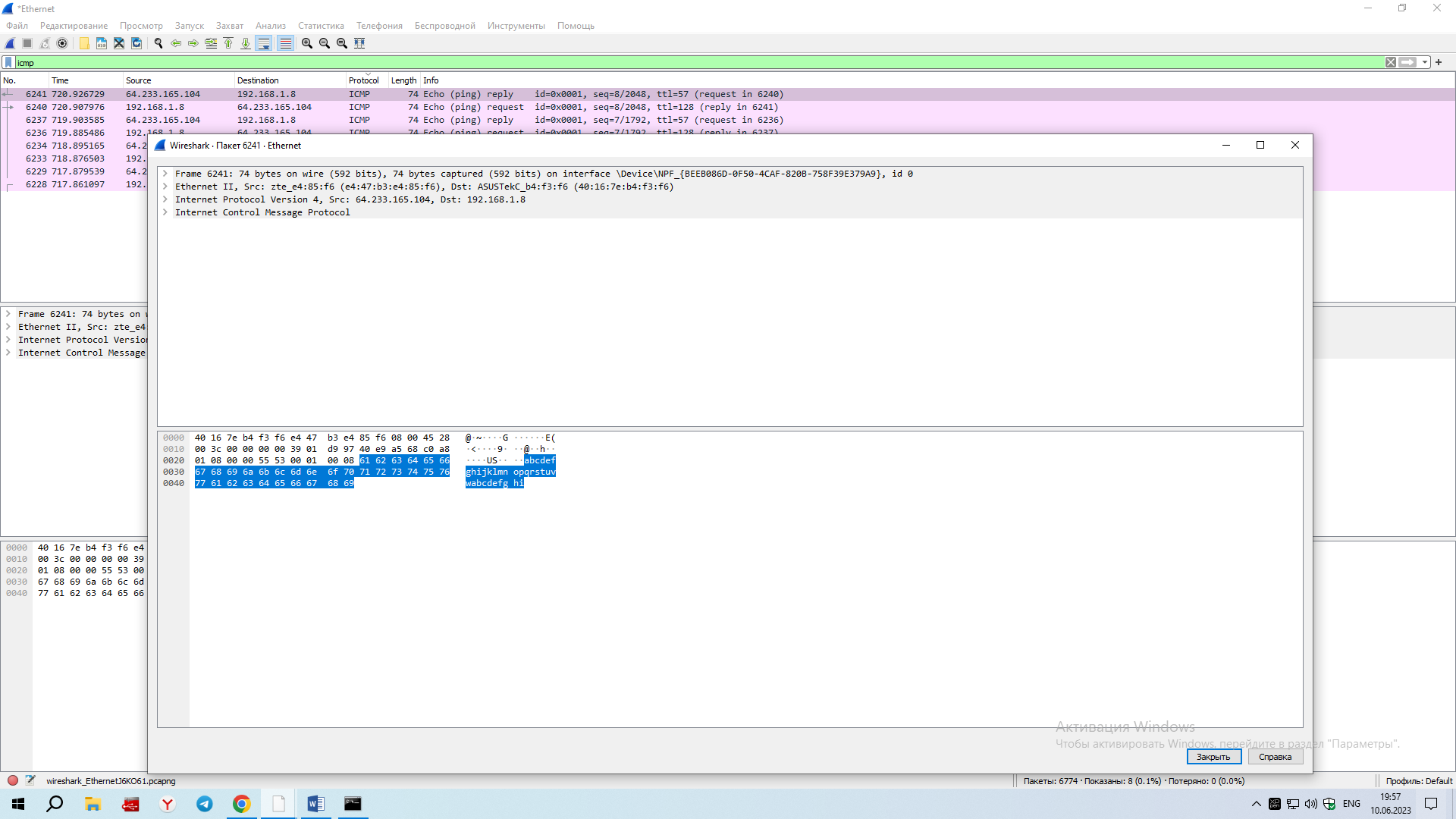




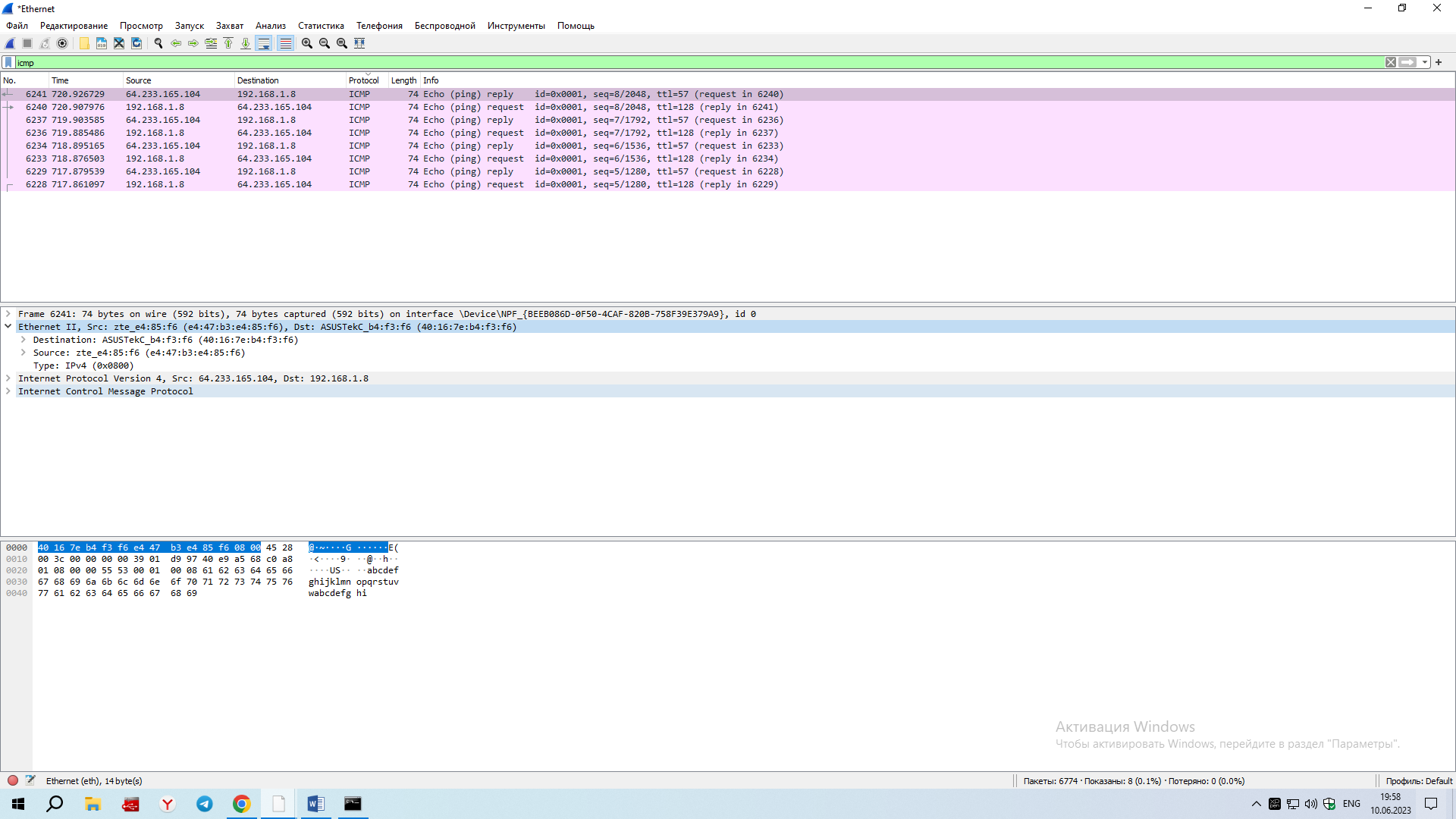








Шаг 3. Изучите полученные данные.



Совпадает ли MAC-адрес источника с интерфейсом компьютера?

Ответ: да

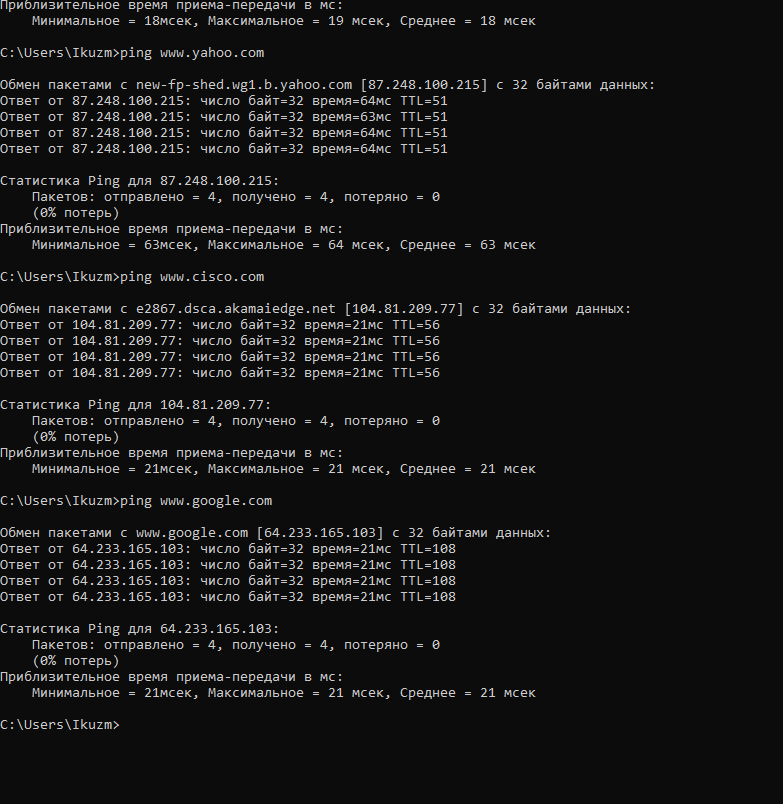
Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого участника рабочей группы?

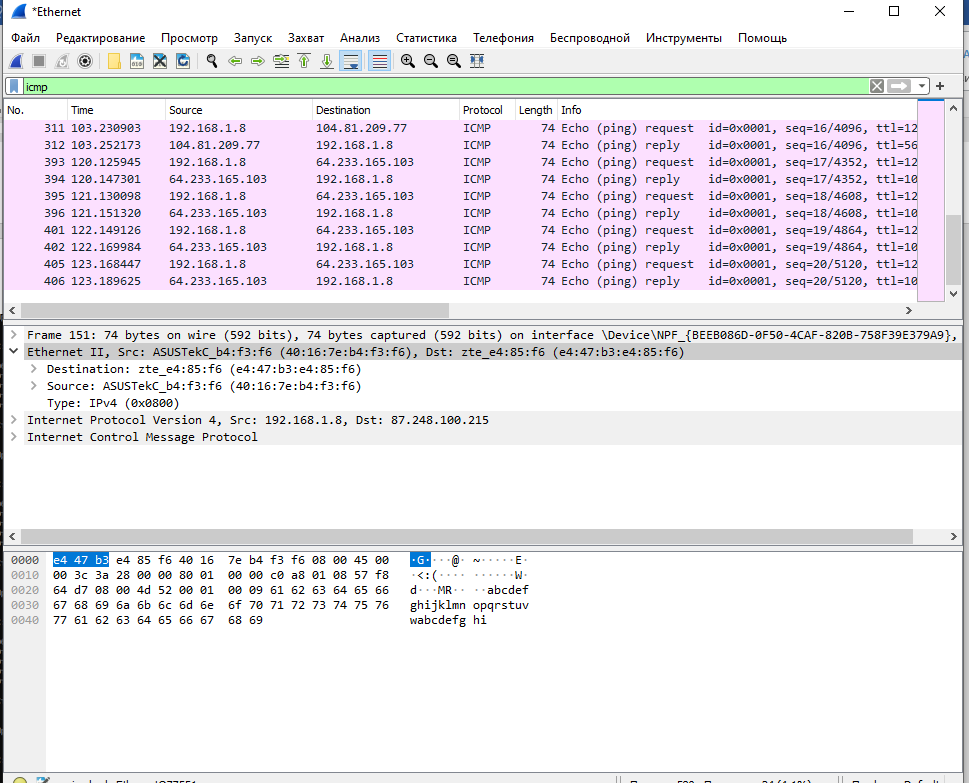
Ответ: да

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?

Ответ: При помощи протокола ARP. Для того, чтобы обменяться данными по сети Ethernet компьютерам нужно знать МАС адрес друг друга, так как сеть Ethernet не работает с IP-адресами. При запросе компьютер №1 обращается по IP к компьютеру №2, сообщает свой MAC-адрес и запрашивает MAC-адрес компьютера №2.

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





Шаг 2. Изучите и проанализируйте данные, полученные от удаленных узлов.

IP-адрес для www.yahoo.com: 87.248.100.215

MAC-адрес для www.yahoo.com: e4:47:b3:e4:85:f6

IP-адрес для www.cisco.com: 104.81.209.77

MAC-адрес для www.cisco.com: e4:47:b3:e4:85:f6

IP-адрес для www.google.com: 64.233.165.103

MAC-адрес для www.google.com: e4:47:b3:e4:85:f6

Какова существенная особенность этих данных?

Ответ: Все адреса имеют одинаковый МАС-адрес.

Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

Ответ: В 1 части показывается МАС-адрес компьютера в локальной сети, во 2 части отображается МАС-адрес сетевого шлюза.

Контрольные вопросы:

Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?

Ответ: Потому что IP-адрес на который отправляется ping находится в  
другой сети доступ к которой осуществляется через локальный узел.

Заключение

Вывод:

1. Я собрала и проанализировала данные протокола ICMP по локальным узлам в программе Wireshark
2. Совершила сбор и анализ данных протокола ICMP по удаленным узлам в программе Wireshark

Используемые источни

<https://demo.ciscostr.ru/static/courses/img/ITN_RU/module03/3.7/3.7.10-lab---use-wireshark-to-view-network-traffic_ru-RU.pdf>