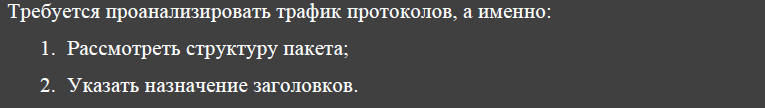
|  |
| --- |
|  |
| Отчет по практике |
| Практическая работа №2 |

|  |
| --- |
| Шемякина Алена БИСО-02-19  10.12.2020 |

# Задание №1



1. Для данного задания был взят 8 пакет.



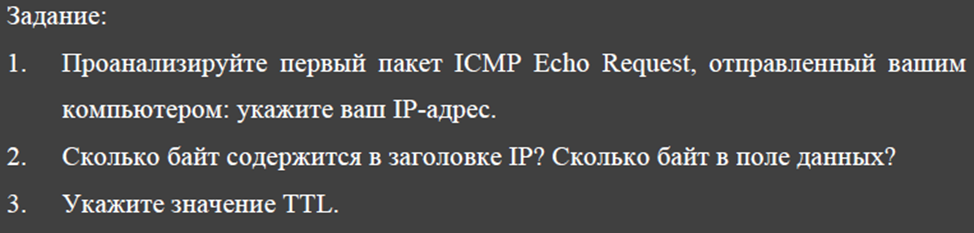
2. Пакет состоит из 4 заголовков:

1. Frame 8 (Протокол физического уровня)
2. Ethernet 2 (Протокол канального уровня)
3. Internet Protocol Version 4 (IPv4, Протокол сетевого уровня)
4. User Datagram Protocol (Протокол пользовательских датаграмм)

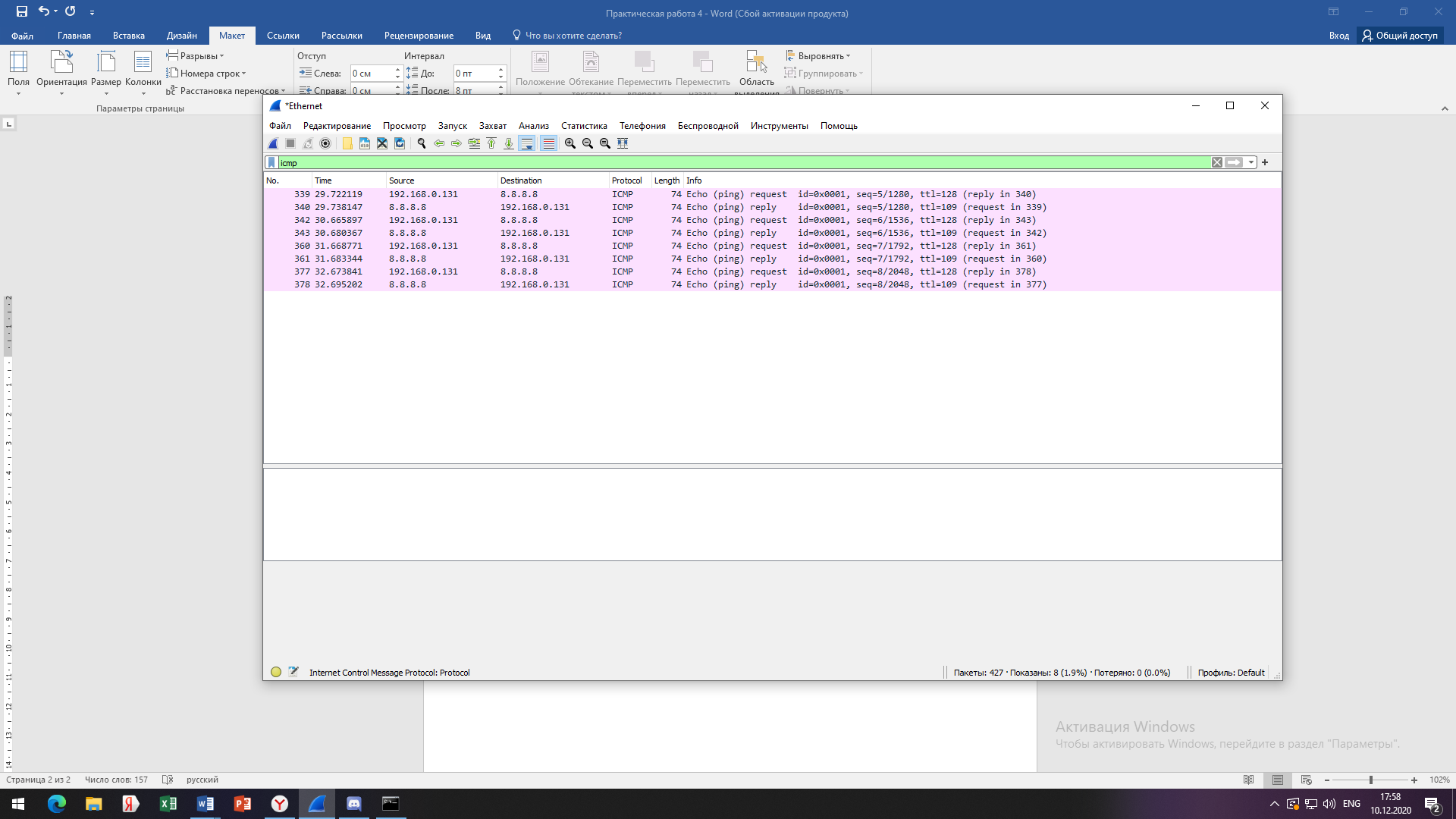
3. Назначение заголовков:

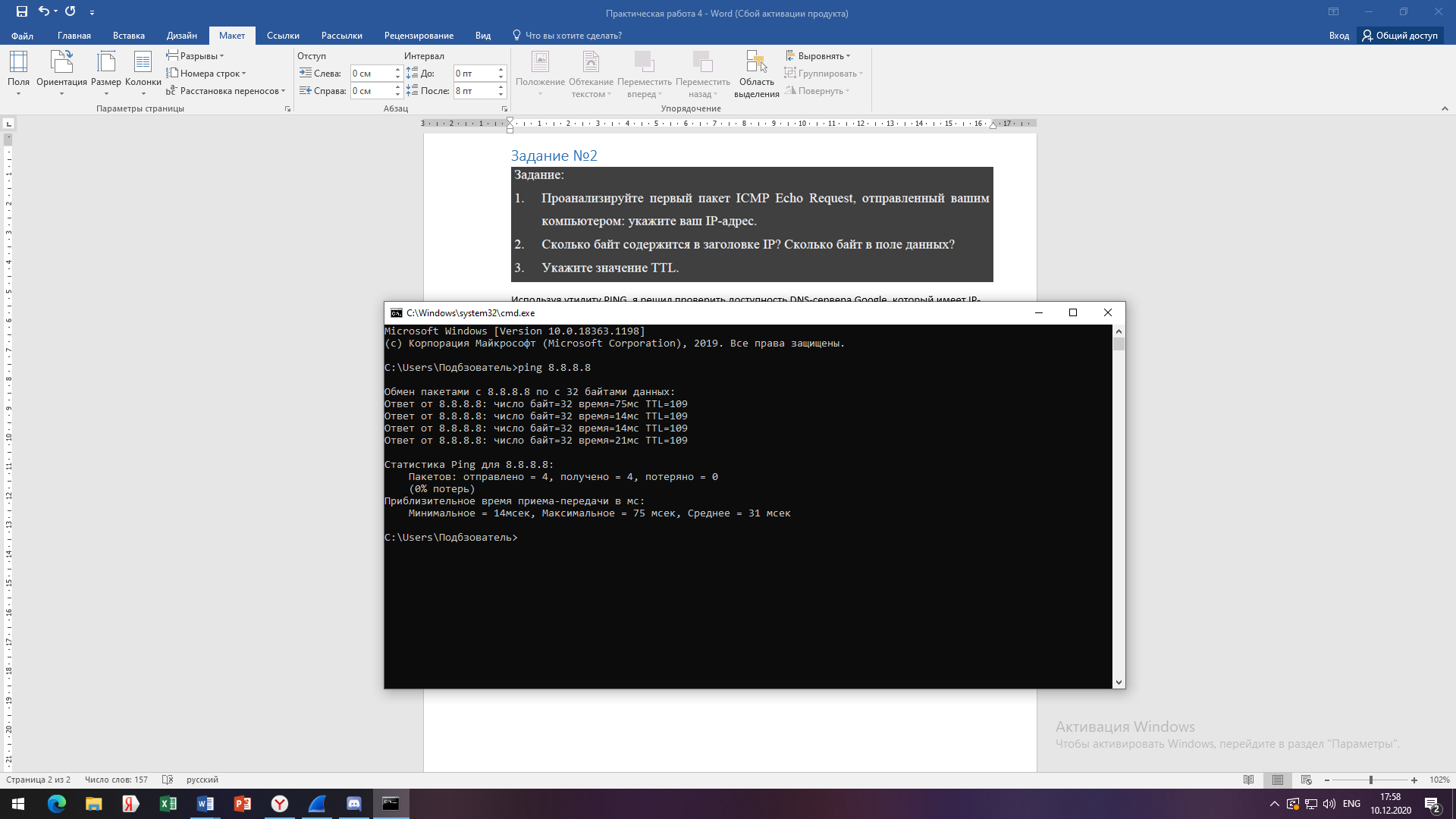
* 1. Frame (Физический уровень) — первый уровень сетевой модели OSI. Физический уровень описывает способы передачи бит (а не пакетов данных) через физические среды линий связи, соединяющие сетевые устройства.
  2. Ethernet – второй уровень сетевой модели OSI. Предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети.
  3. Internet Protocol Version – 3-й уровень сетевой модели OSI. Предназначается для определения пути передачи данных.
  4. UDP — один из ключевых элементов набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.

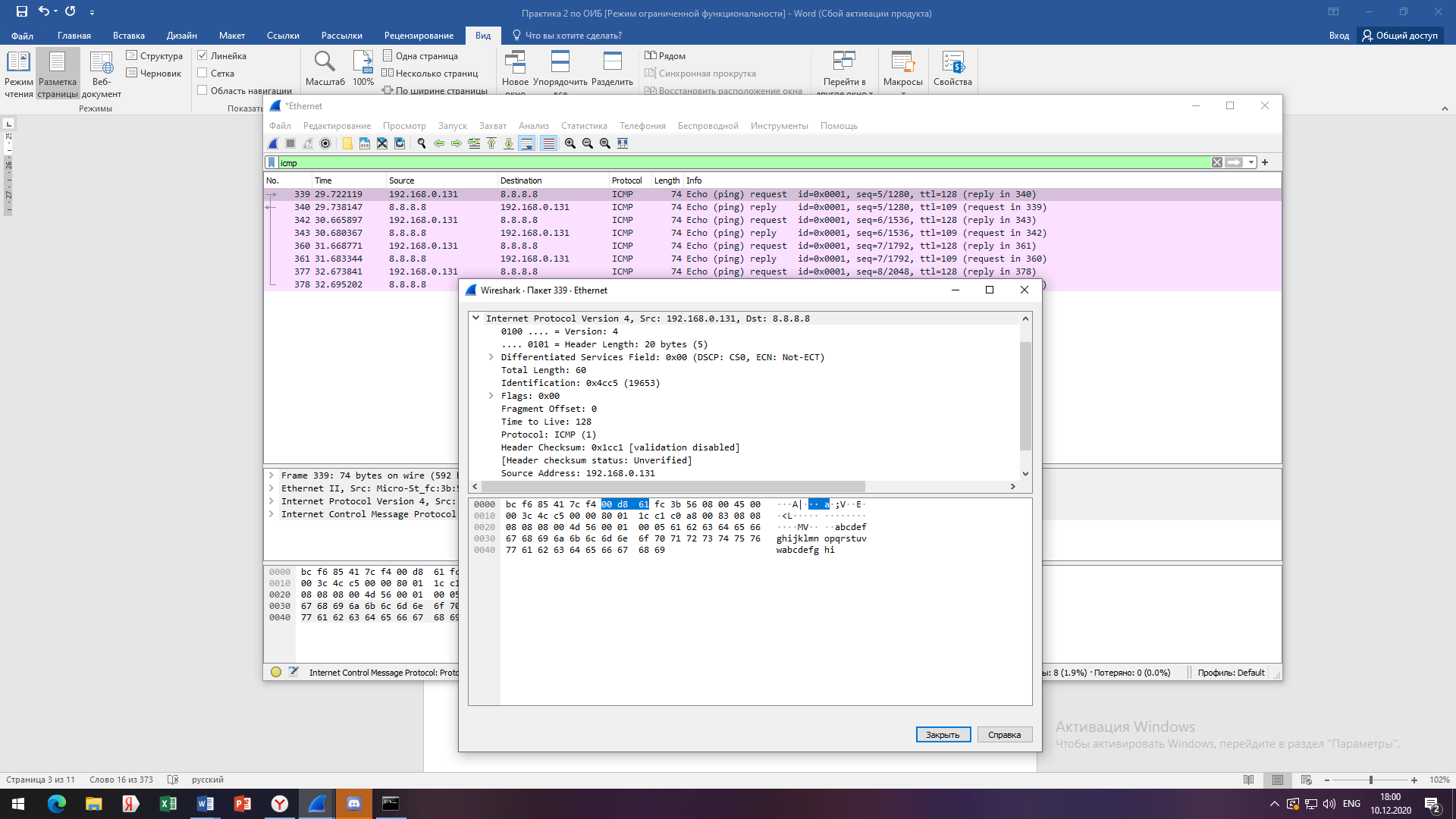
# Задание №2



1. Используя утилиту PING, я решил проверить доступность DNS-сервера Google, который имеет IP-адрес 8.8.8.8

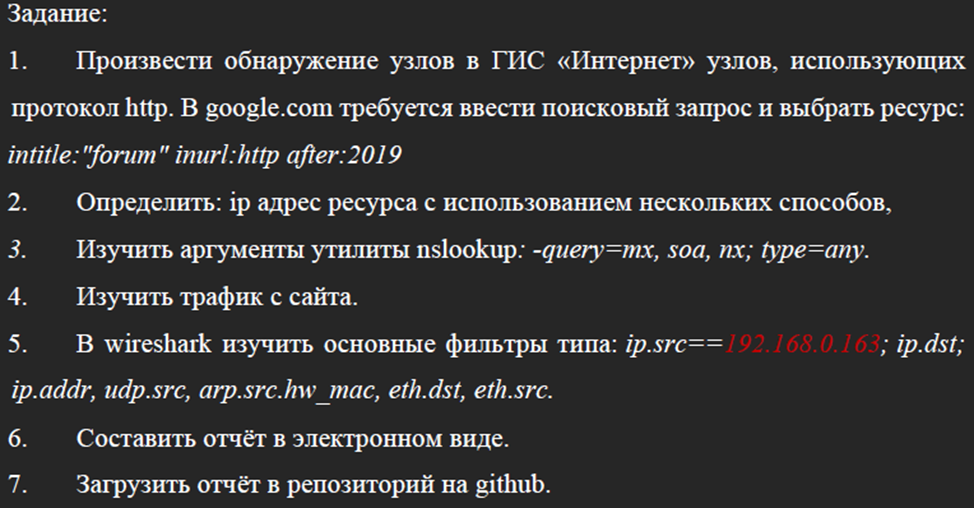




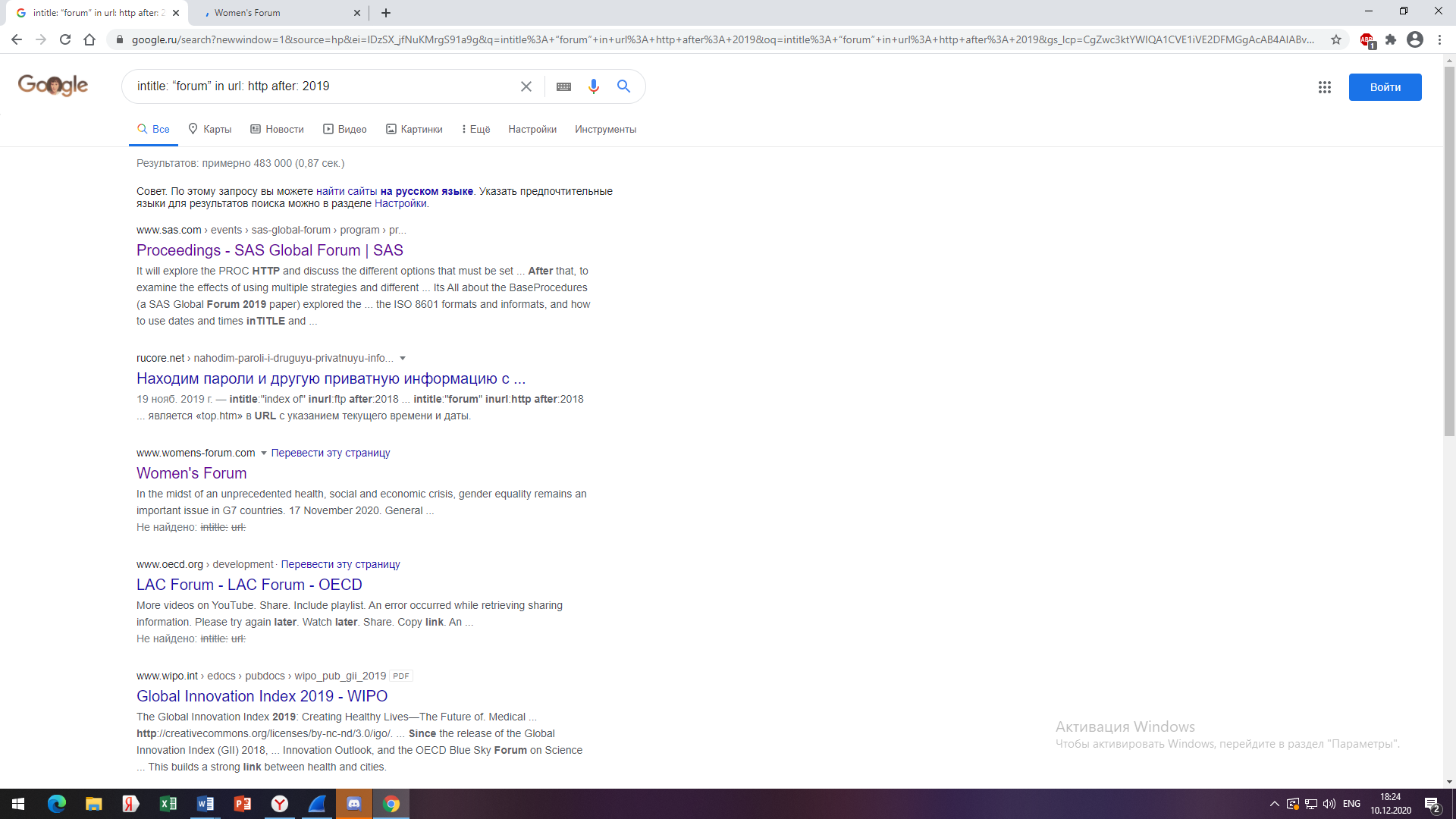


1. Проанализировав первый пакет ICMP, я понял, что мой IP-адрес: 192.168.0.131
2. 20 байт, 4 байта.
3. Time to live составляет 128

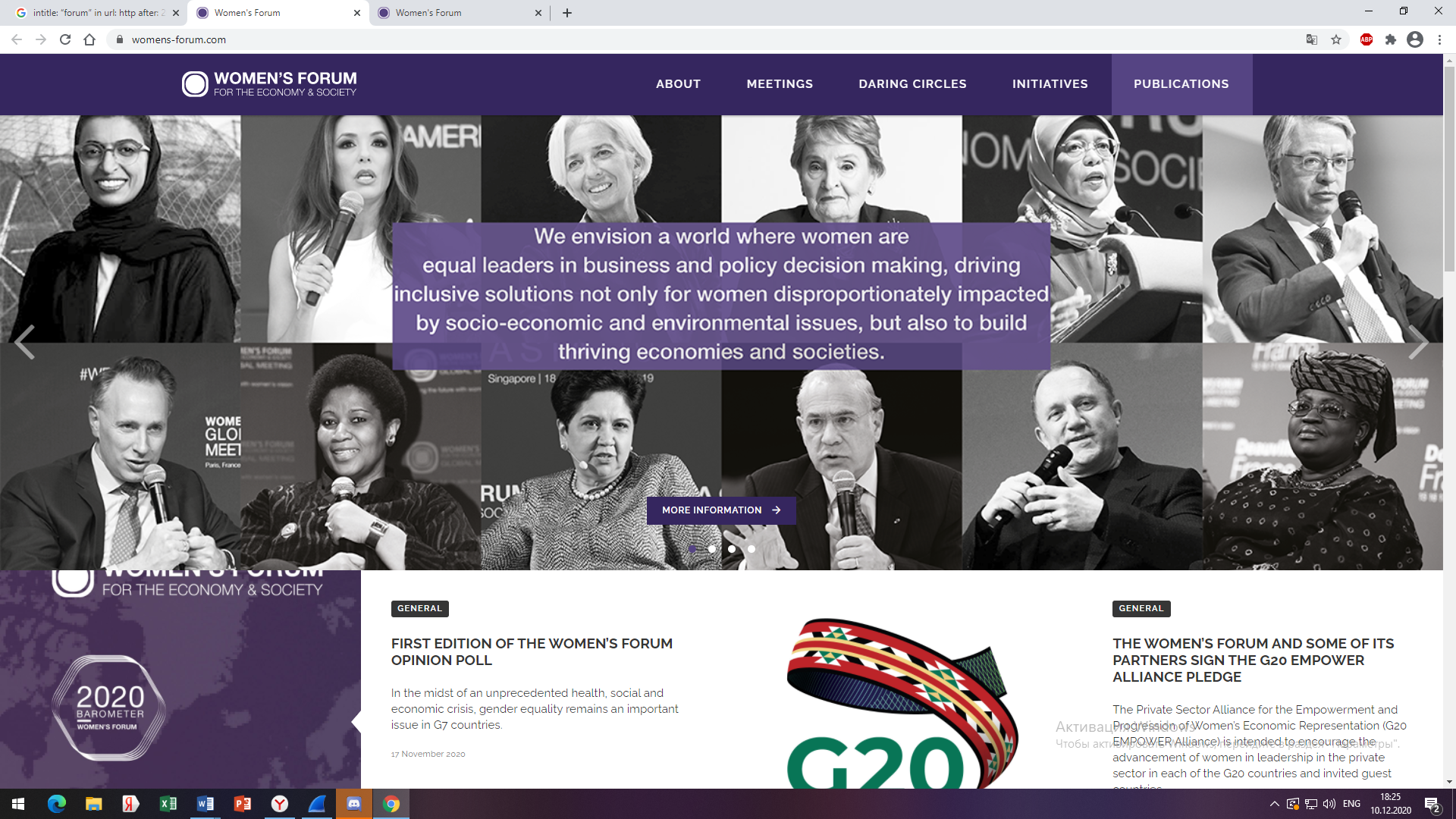
# Задание №3



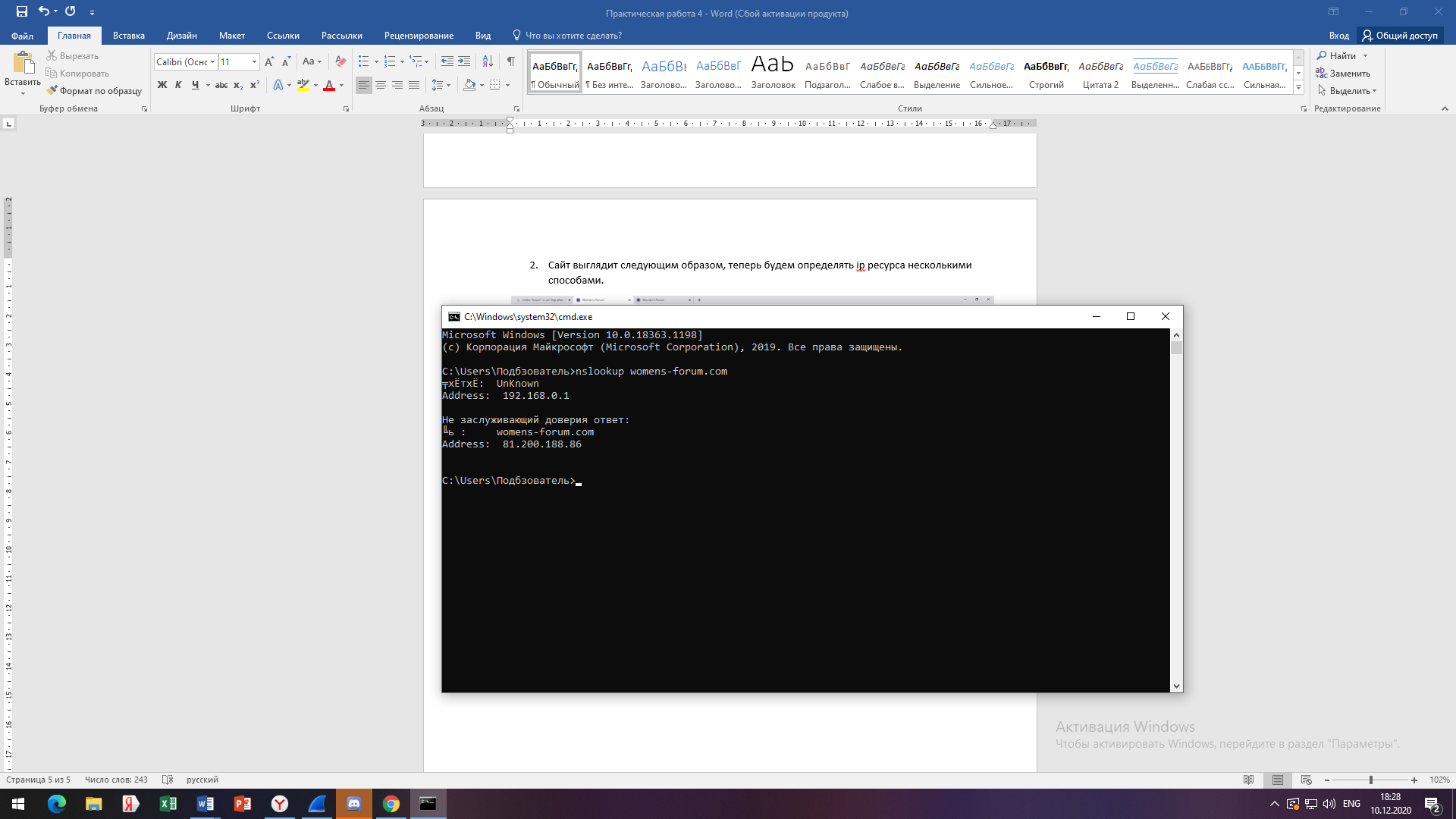
1. Введя в поисковый запрос intitle: “forum” in url: http after: 2019. Этот запрос является строгим, так как мы находим все сайты форумов с протоколом http, которые были проведены или будут проведены после 2019. Я выбираю Woman’s Forum



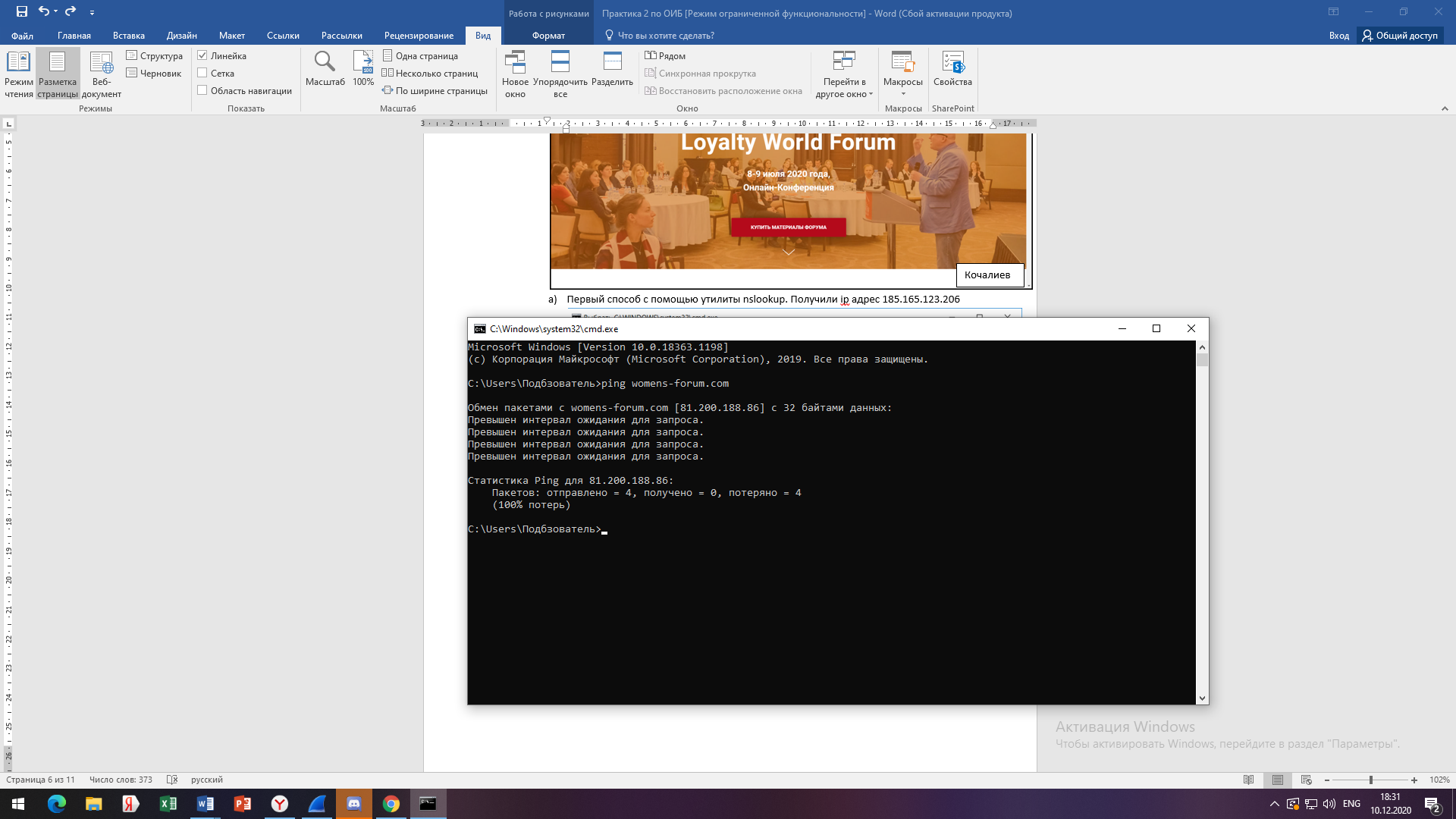
1. Сайт выглядит следующим образом, теперь будем определять ip ресурса несколькими способами.



1. Первый способ с помощью утилиты nslookup. Получили ip адрес 81.200.188.86

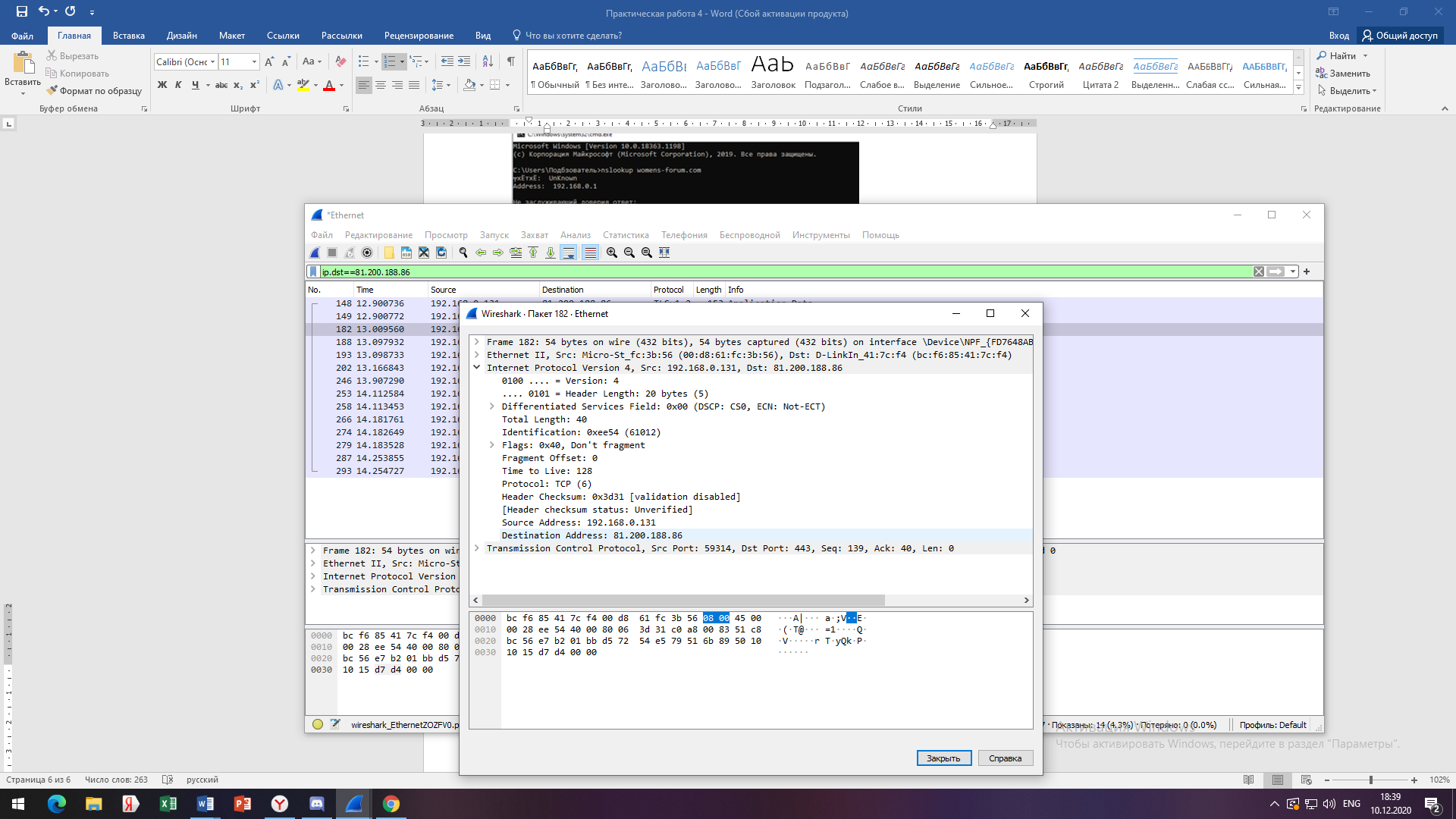


1. Теперь попробуем определить ip адрес при помощи утилиты ping. Неудивителньо, что ip адрес мы получили такой же 81.200.188.86

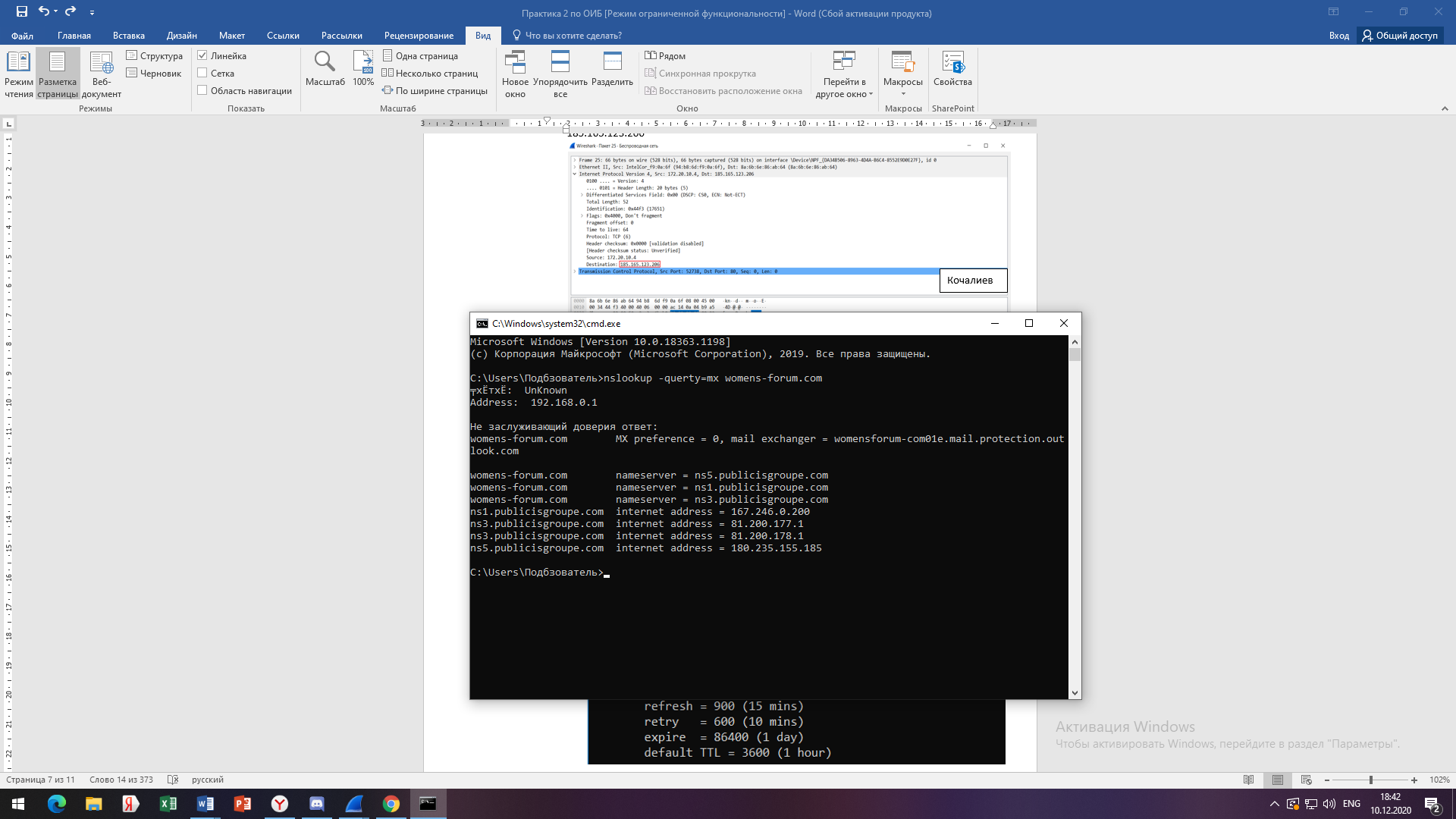


1. И последней способ, это при помощи wireshark.

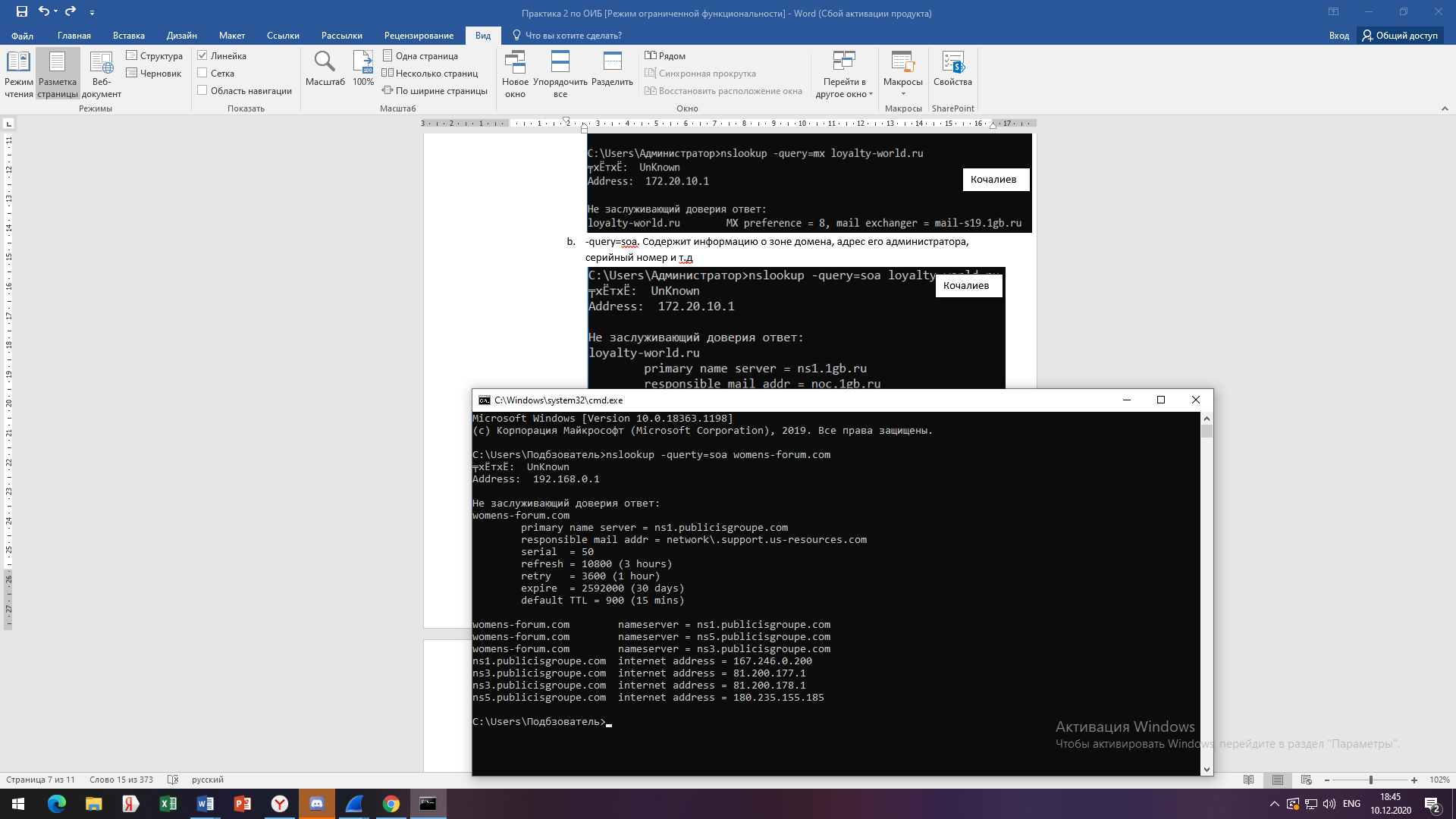
Снова получаем ip адрес равный 81.200.188.86



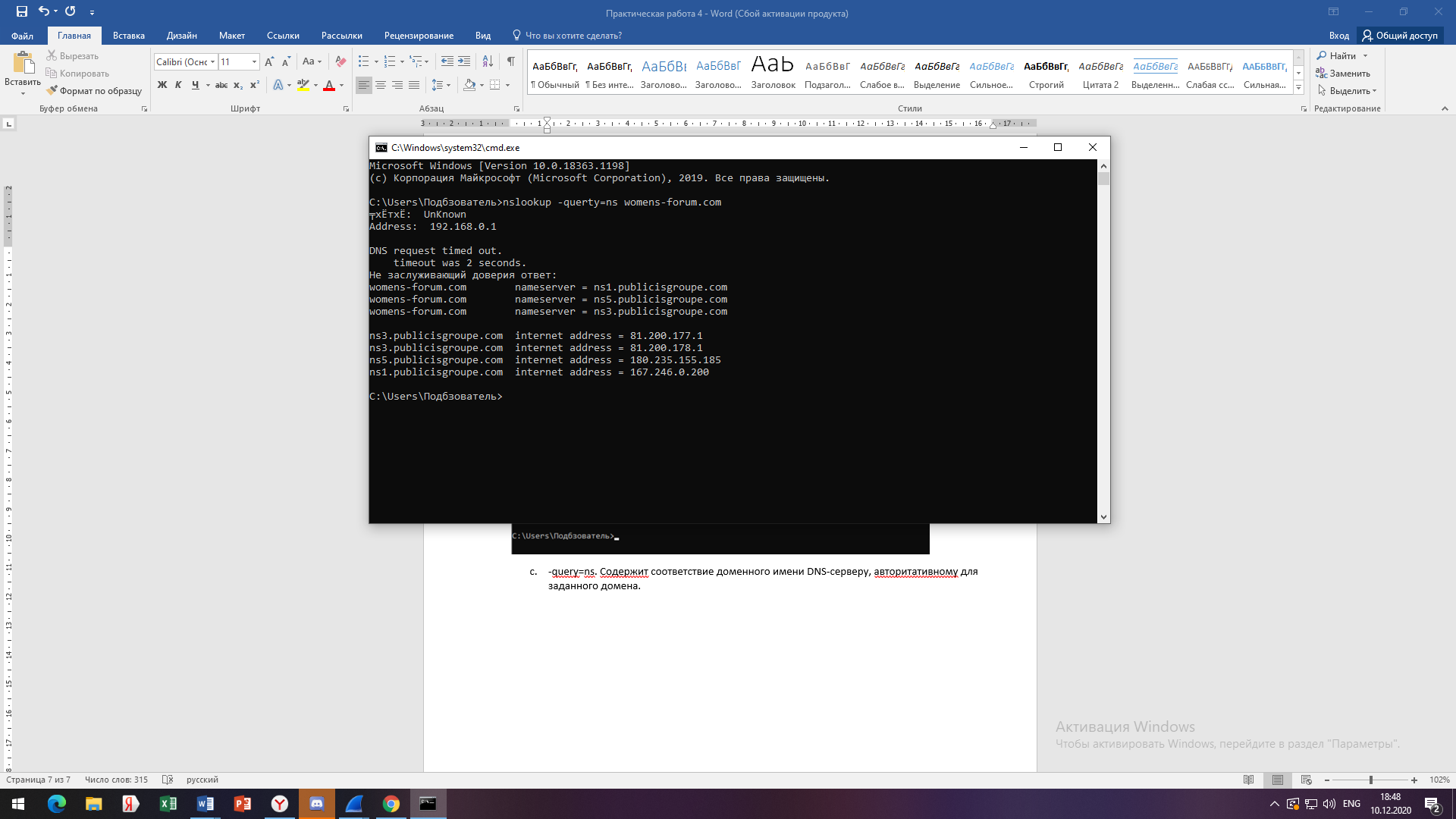
1. Изучение аргументов nslookup
2. -query=mx. Хранит соответствие доменного имени почтовому серверу этого домена.



1. -query=soa. Cодержит информацию о зоне домена, адрес его администратора, серийный номер и т.д

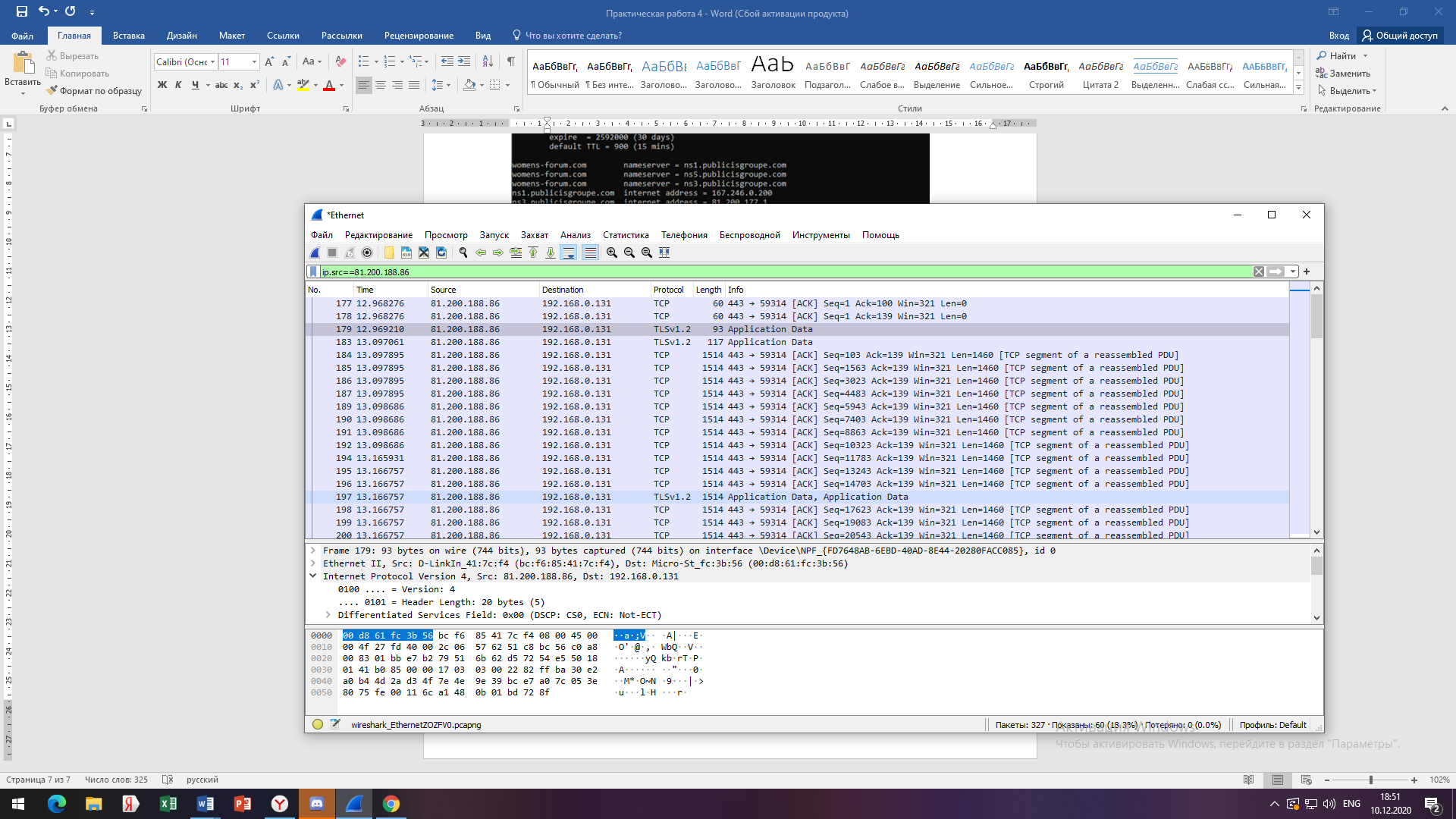


1. -query=ns. Cодержит соответствие доменного имени DNS-серверу, авторитативному для заданного домена.

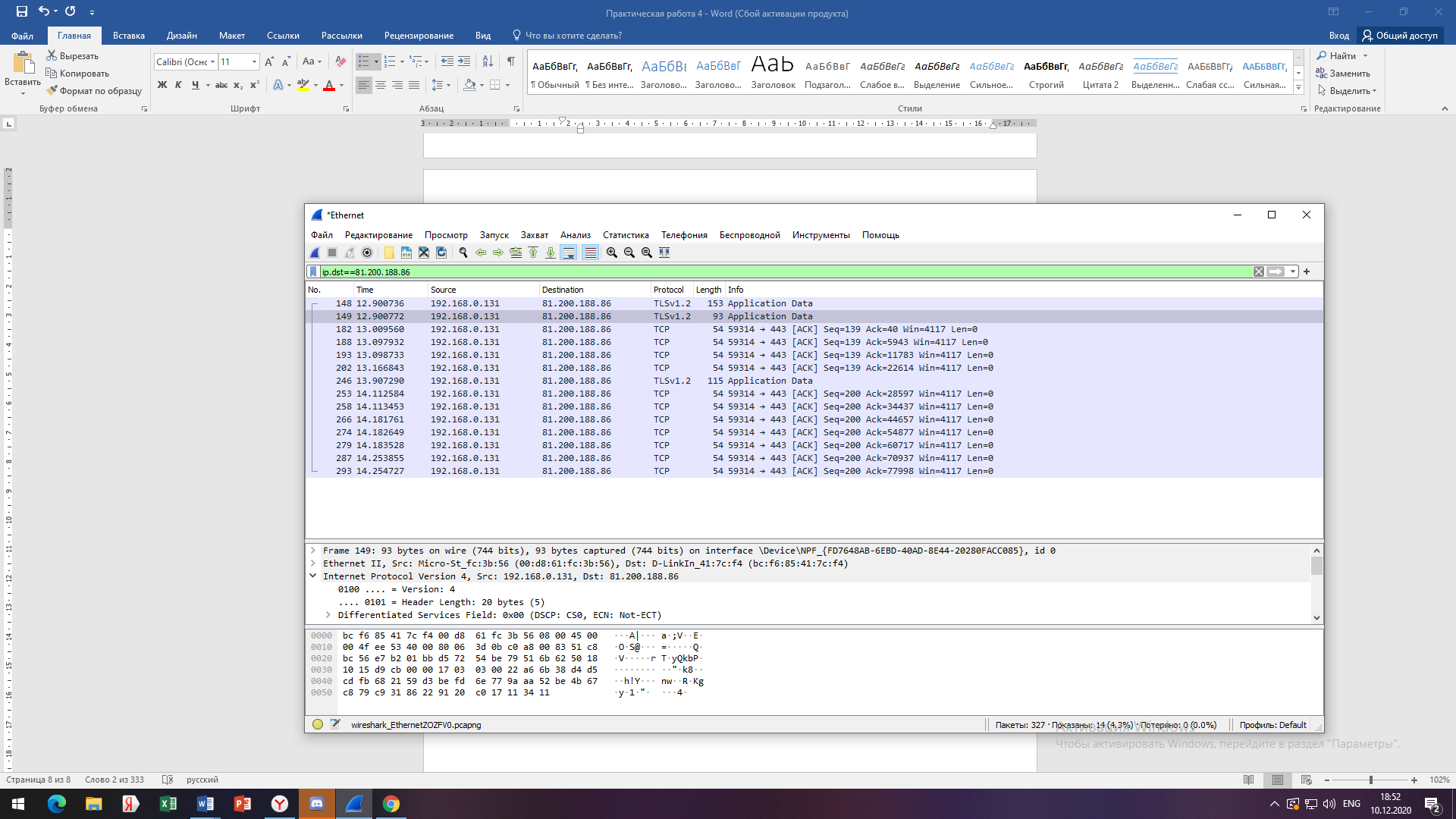


1. Изучение основных фильтров

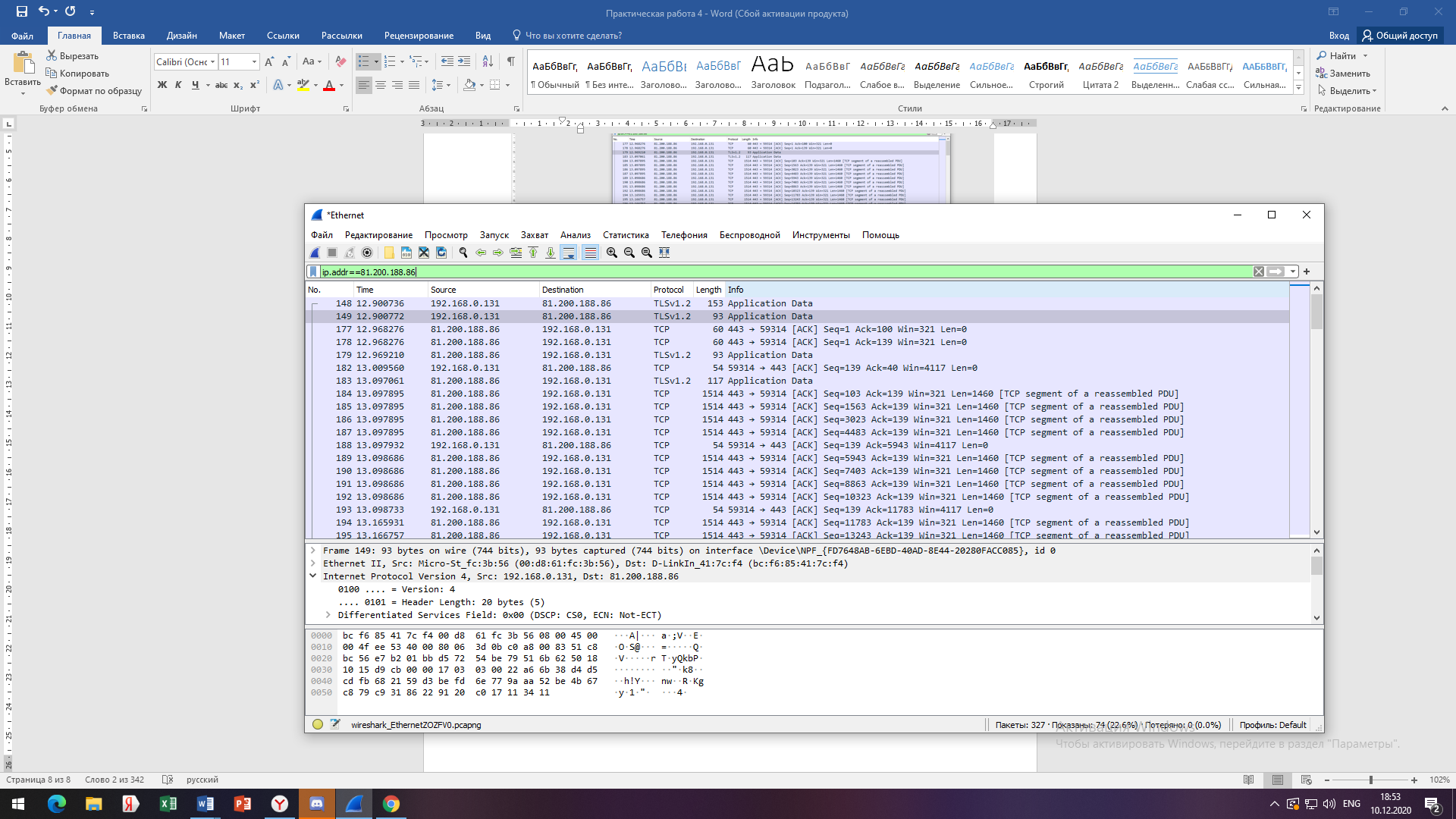
* ip.src==81.200.188.86. Фильтр по IP адресу отправителя



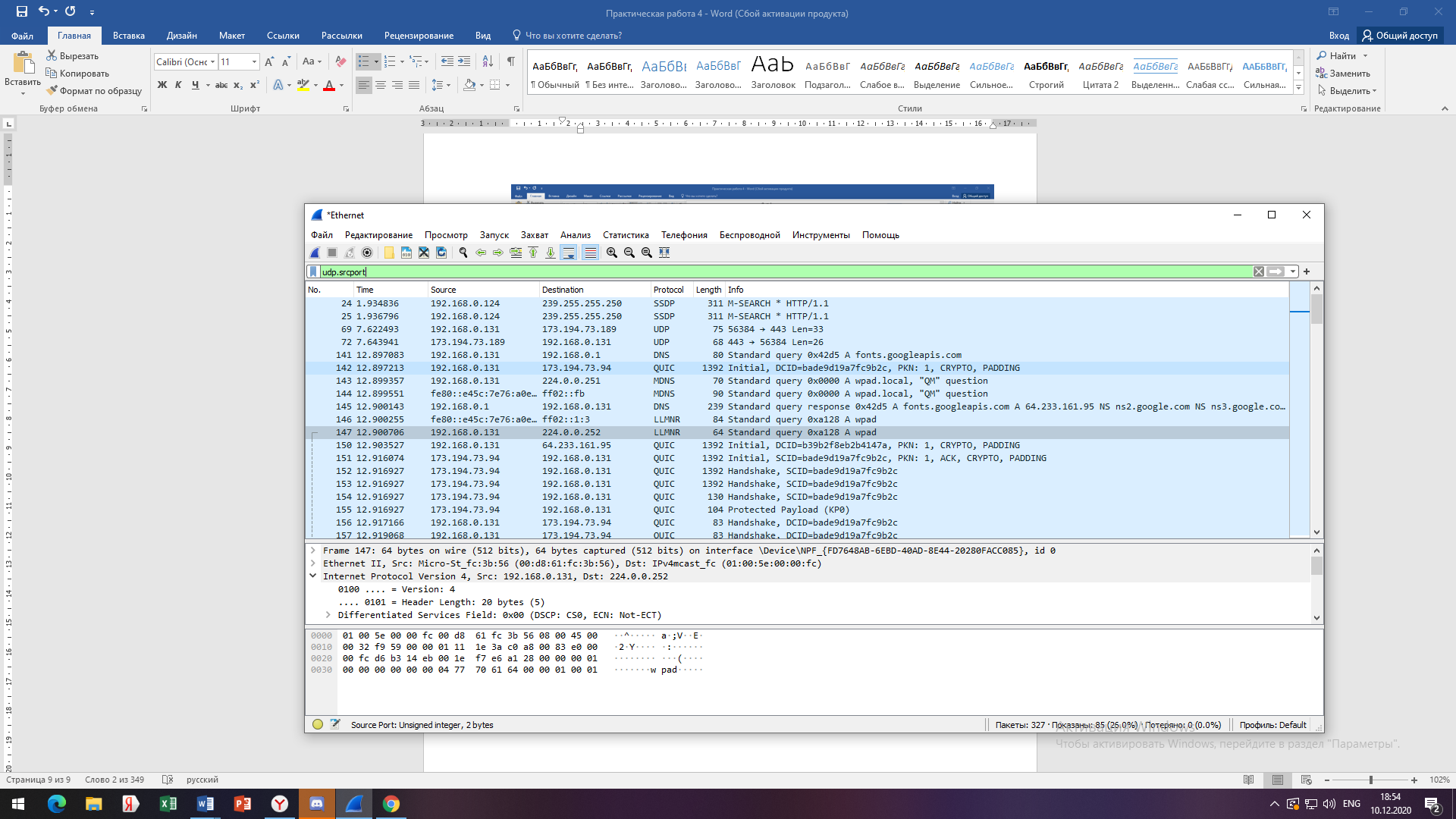
* ip.dst==81.200.188.86. Фильтр по IP адресу получателя



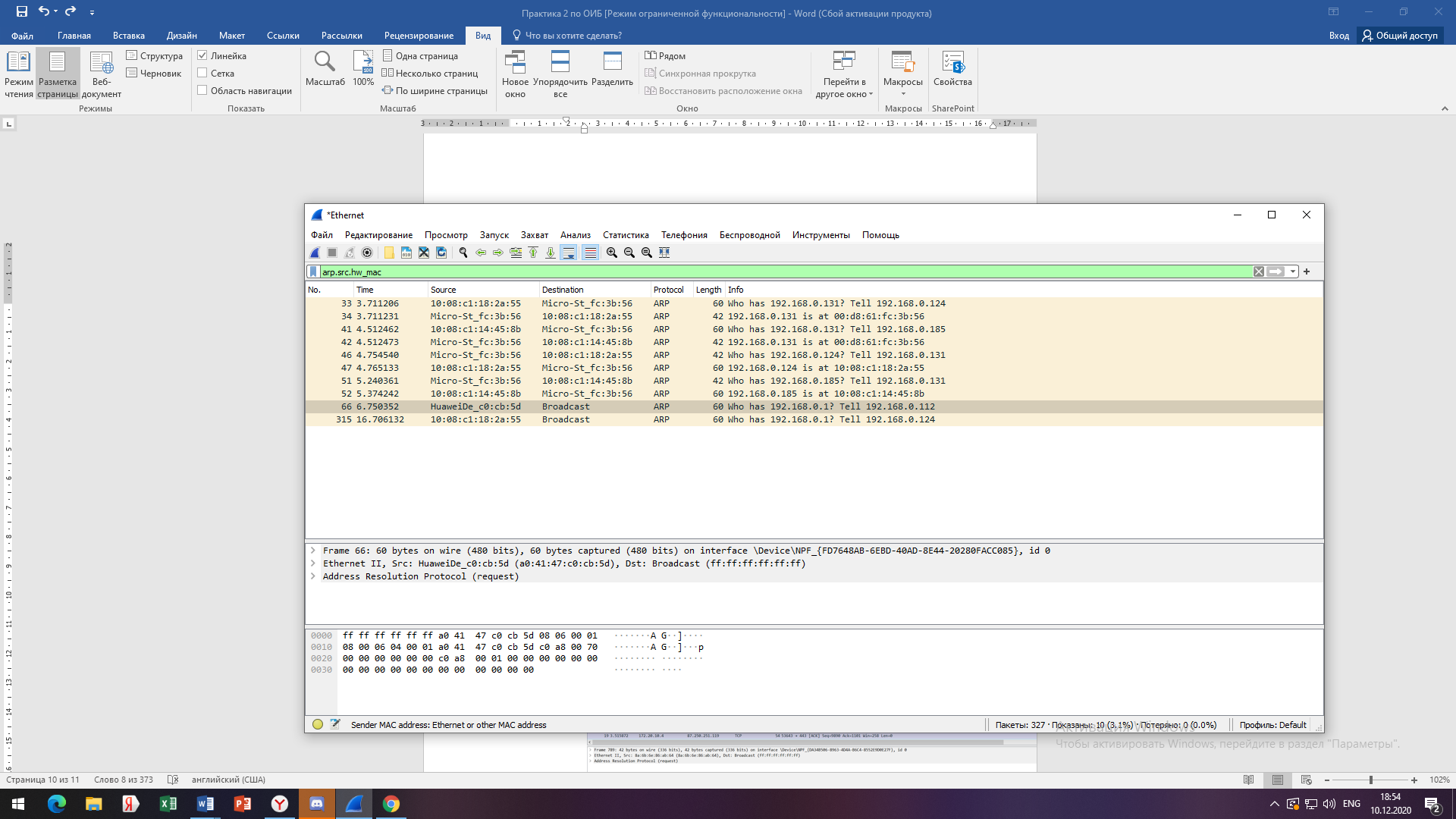
* ip.addr==81.200.188.86. Фильтр по IP адресу получателя и отправителя



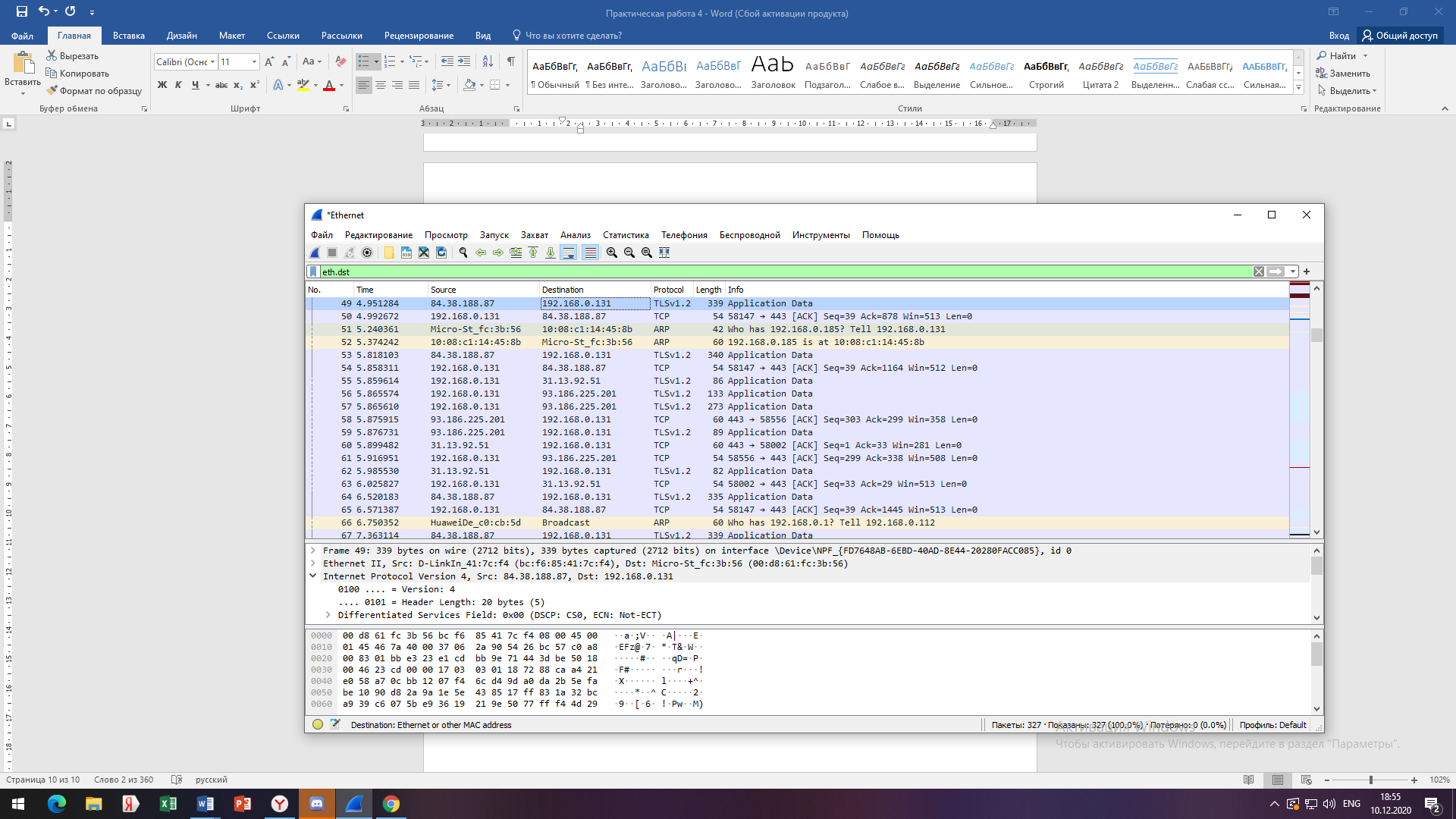
* udp.srcport. Фильтр по UDP порт отправителя



* arp.src.hw\_mac. Протокол ARP – MAC адрес получателя



* eth.dst. MAC-адрес получателя



* eth.src. MAC-адрес оправителя

