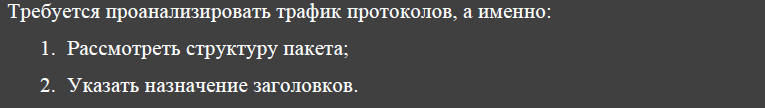
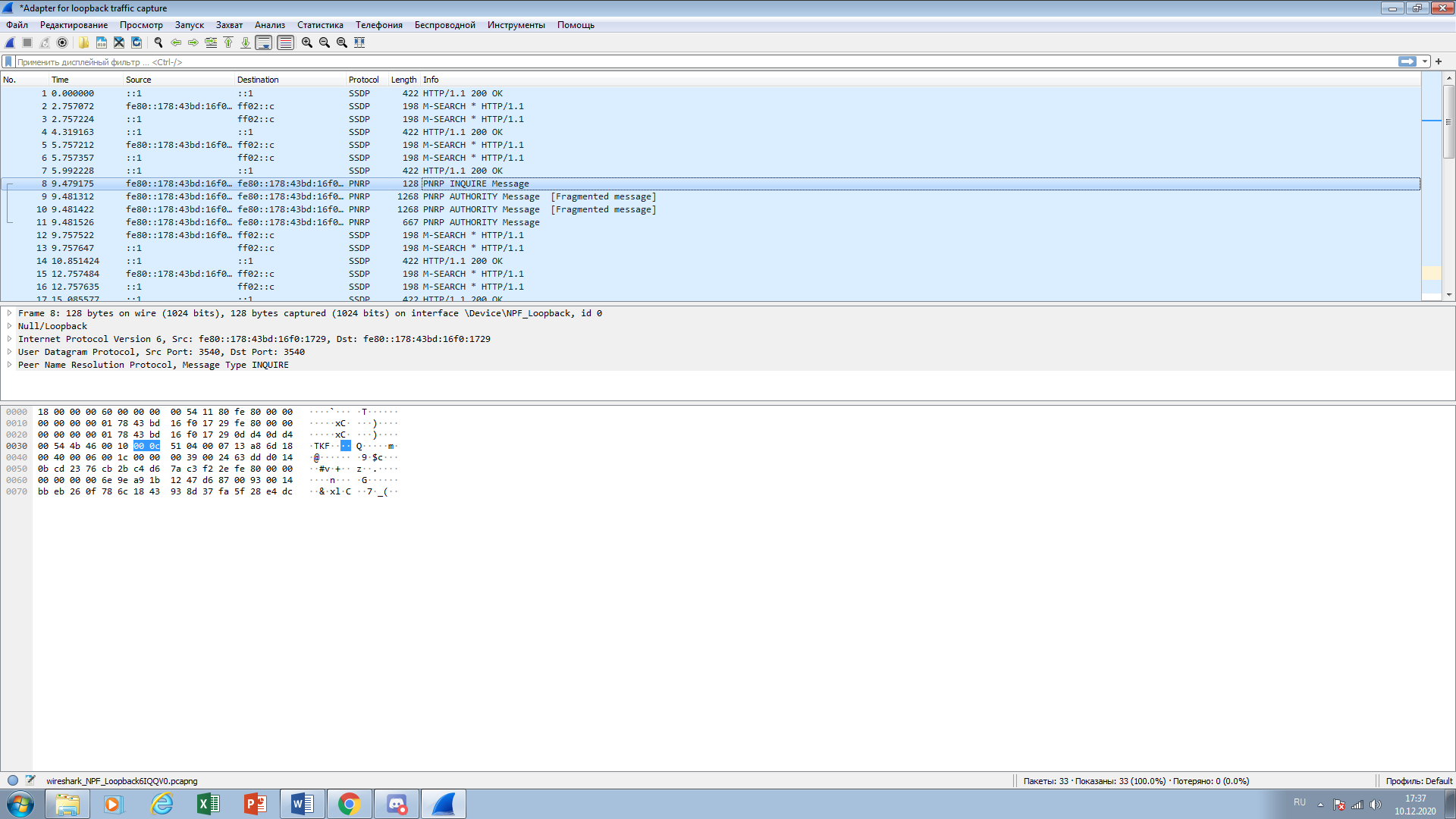
|  |
| --- |
|  |
| Отчёт по ОИБ |
| Практика №2 |

|  |
| --- |
| Кузьмина Надежда  11.12.2020 |

# Задание №1

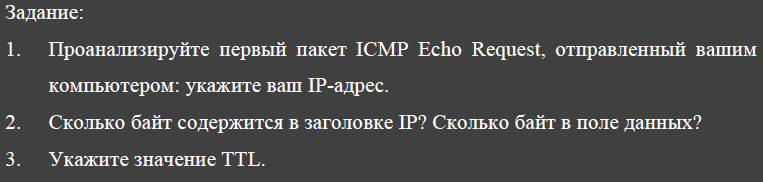


1. Для данного задания был взят 8 пакет.

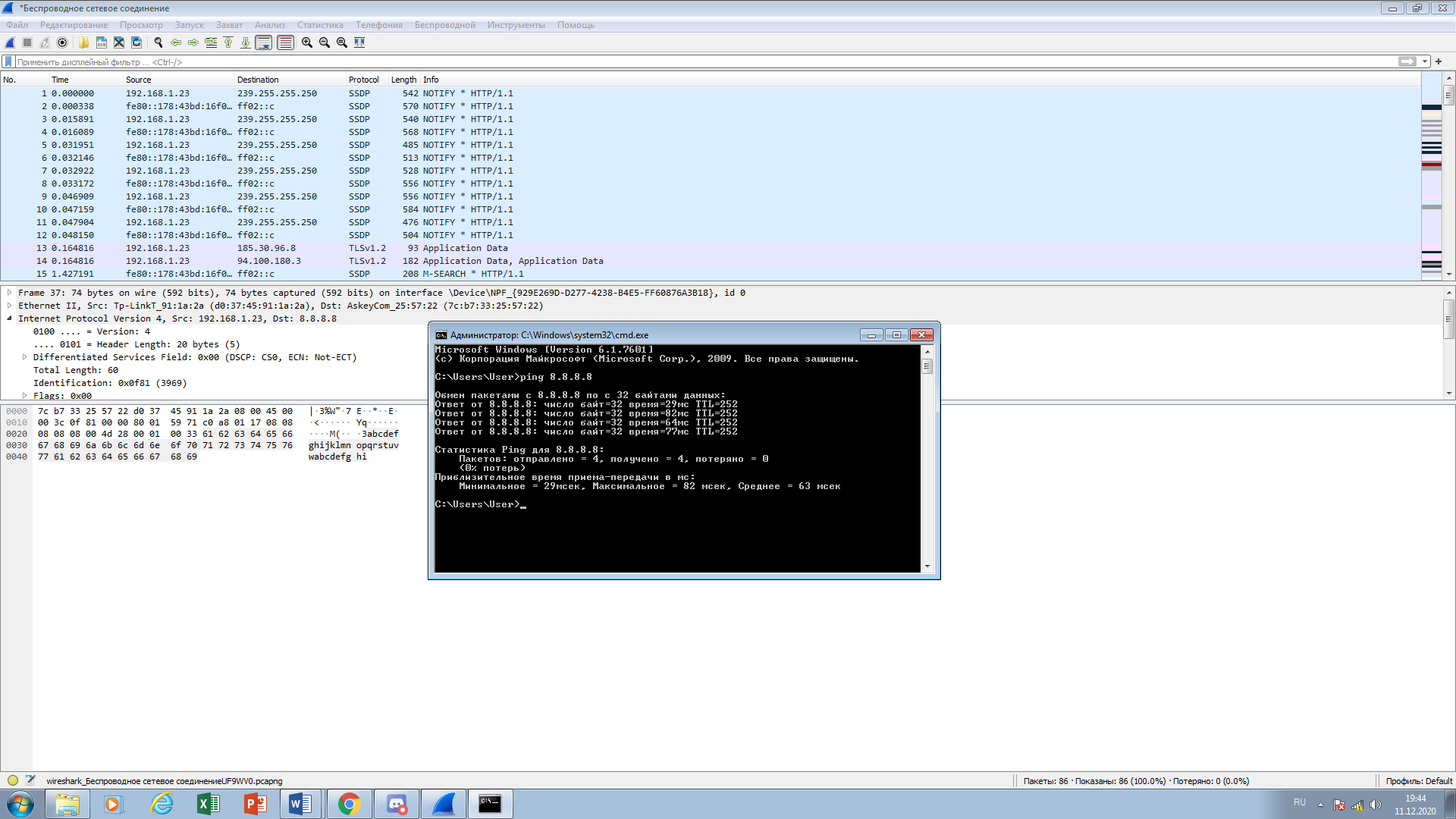


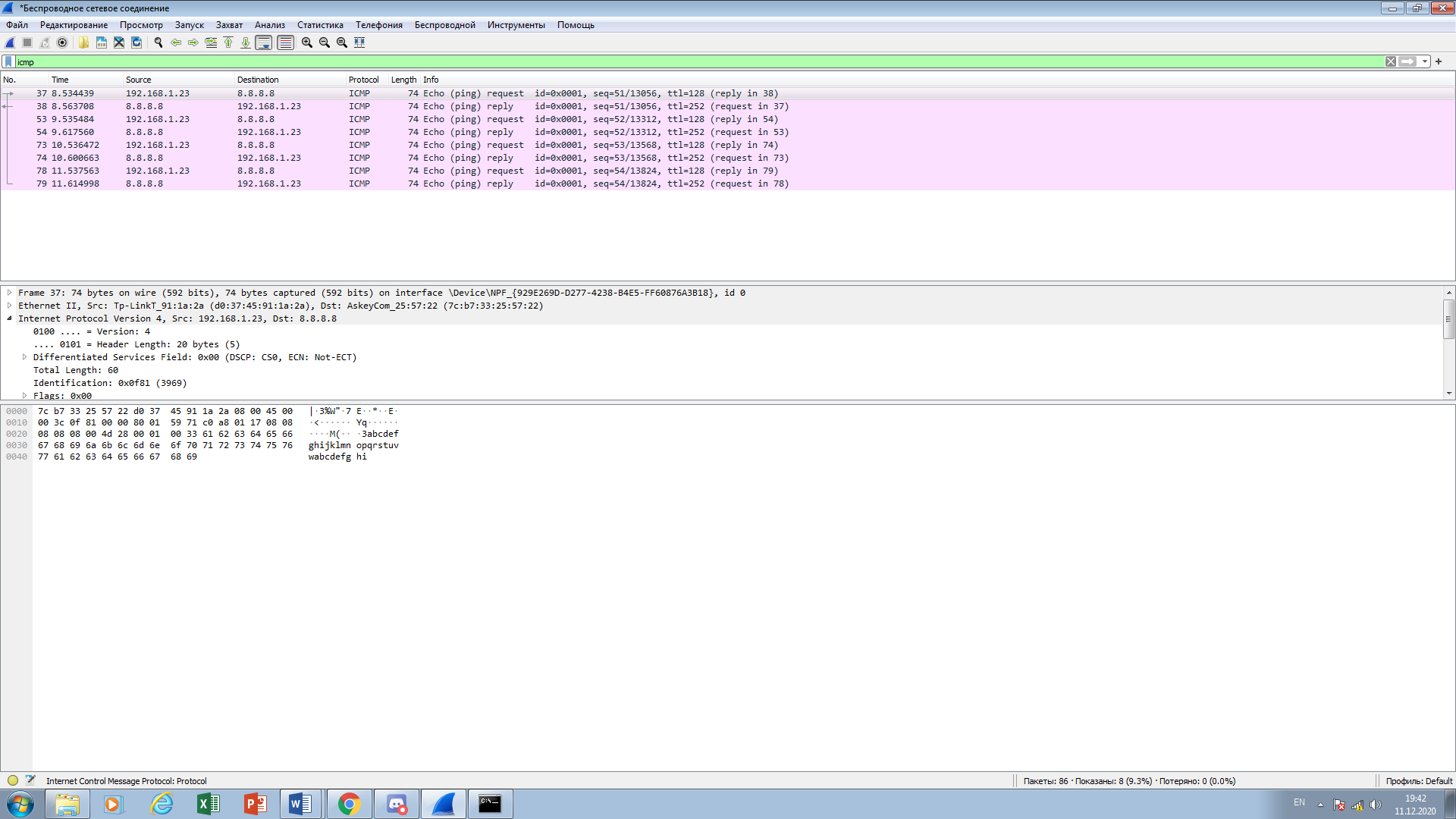
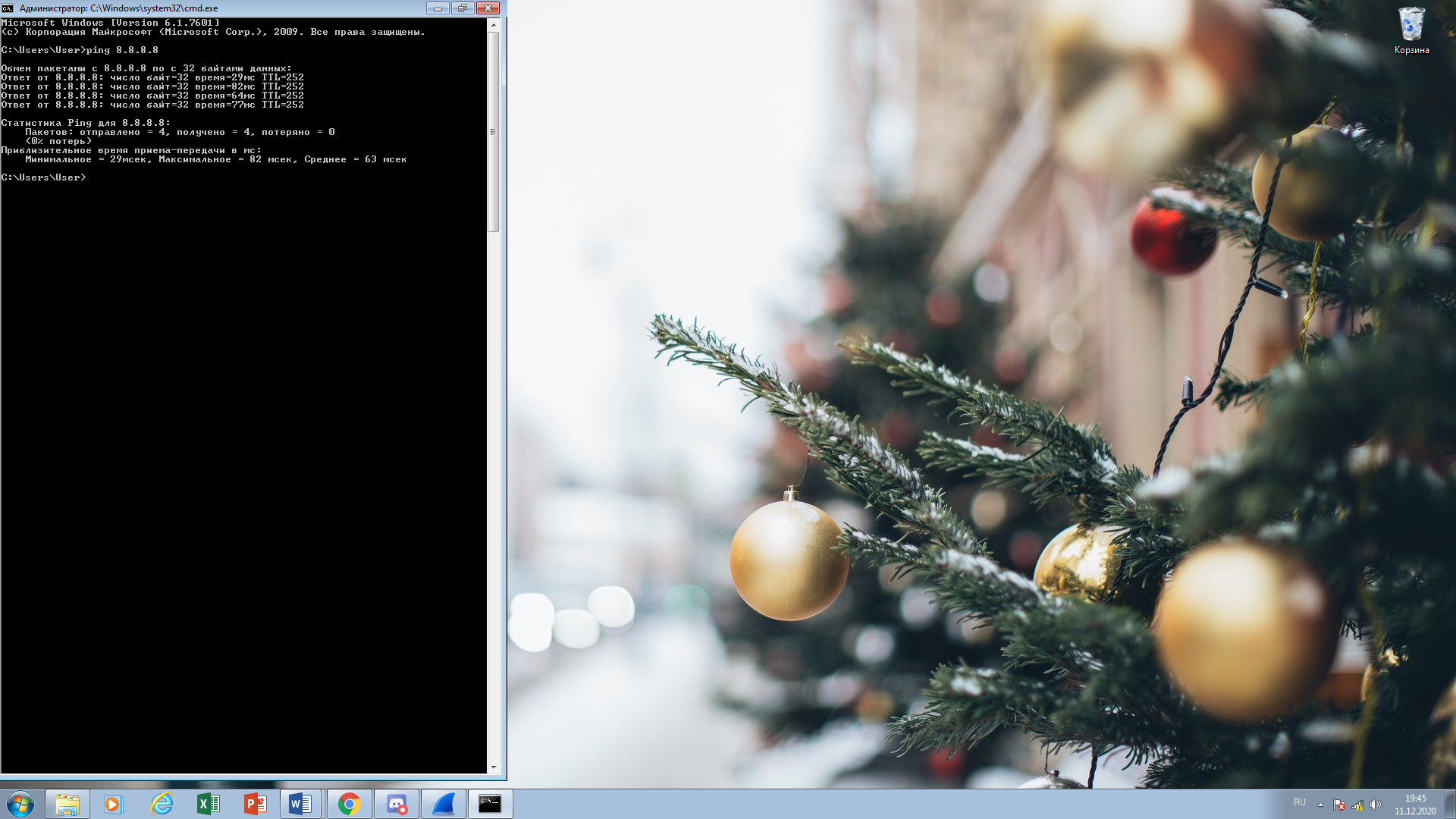
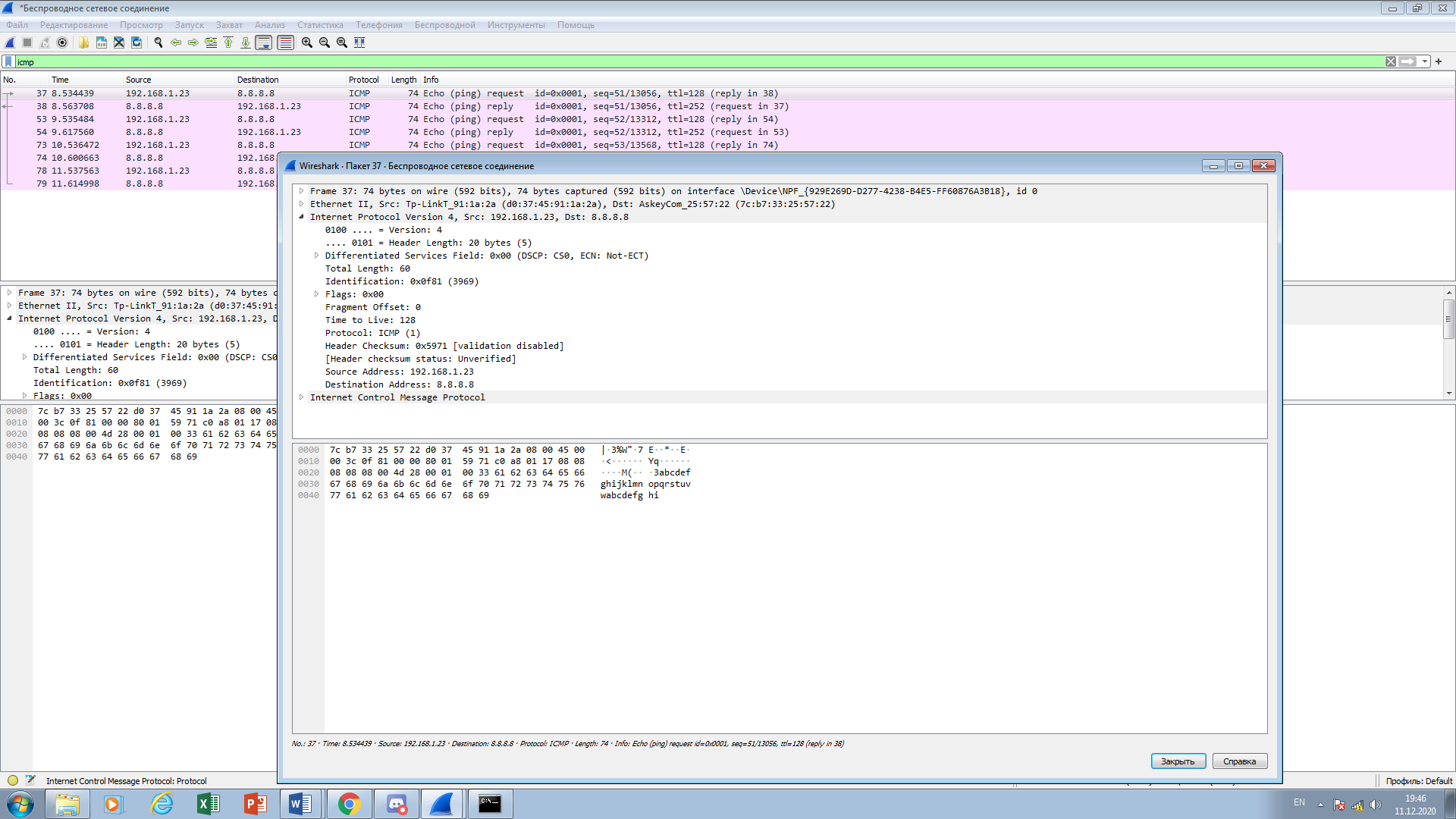
1. Пакет состоит из 4 заголовков:
   1. Frame 8 (Протокол физического уровня)
   2. Ethernet 2 (Протокол канального уровня)
   3. Internet Protocol Version 6 (IPv4, Протокол сетевого уровня)
   4. User Datagram Protocol, Src Port
   5. Peer Name Resolution, Message Type INQUIRE
2. Назначение заголовков:
   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.
   5. Peer Name Resolution Protocol — протокол, разработанный компанией Microsoft, применяющийся в одноранговой компьютерной сети с целью обращения к узлам сети по имени узла, которое связано с адресом IPv6.

# Задание №2

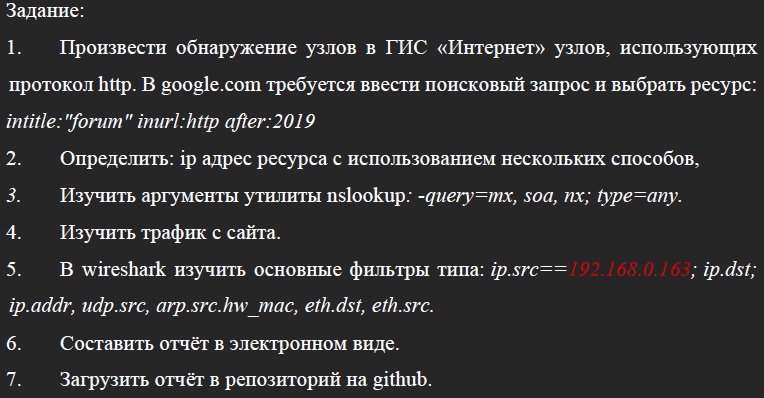


1. Используя утилиту PING, я решил проверить доступность DNS-сервера Google, который имеет IP-адрес 8.8.8.8

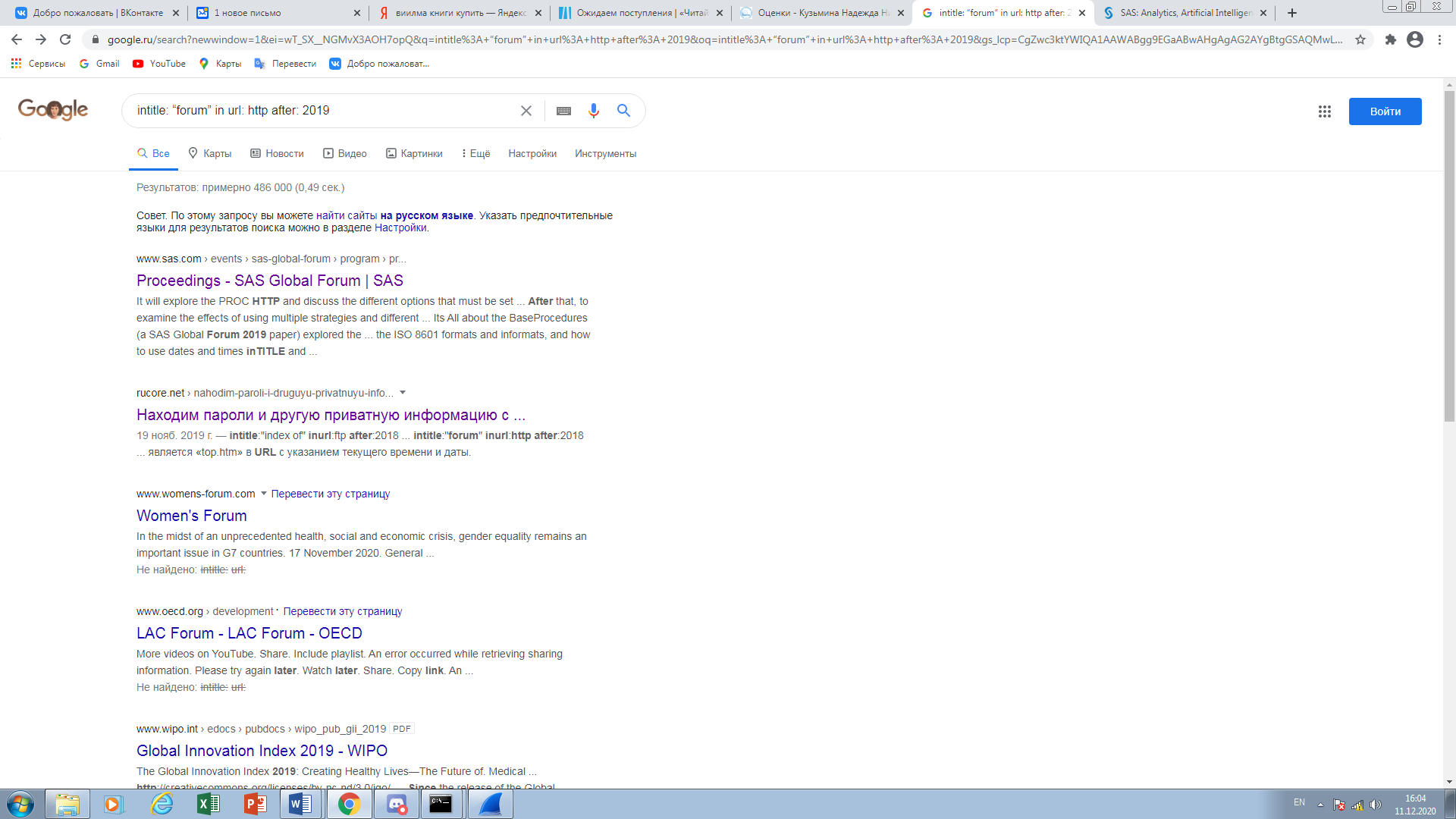


1. 
2. 
3. 
4. Проанализировав первый пакет ICMP, я понял, что мой IP-адрес: 192.168.1.23
5. 20 байт, 4 байта.
6. Time to live составляет 128

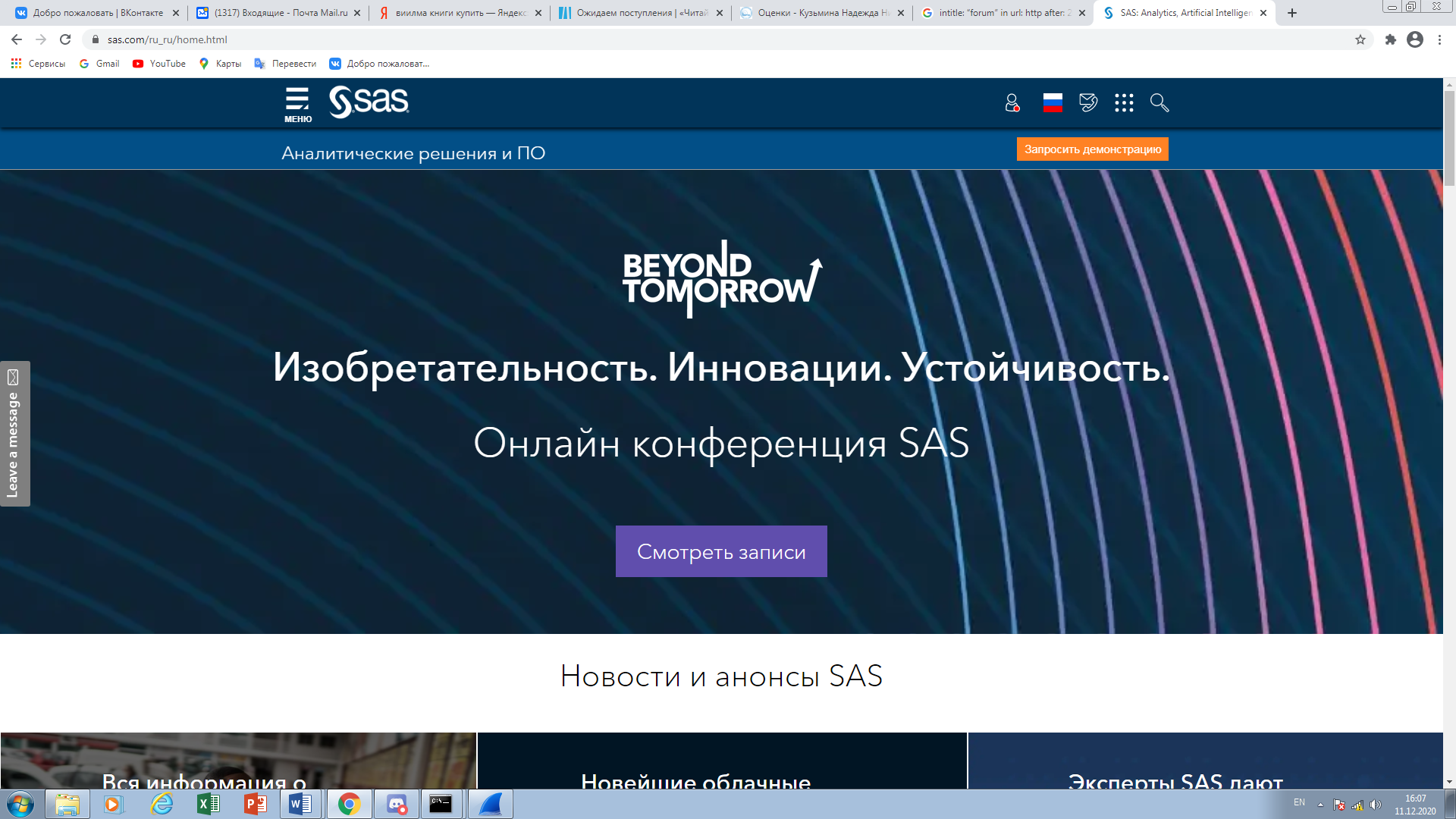
# Задание №3



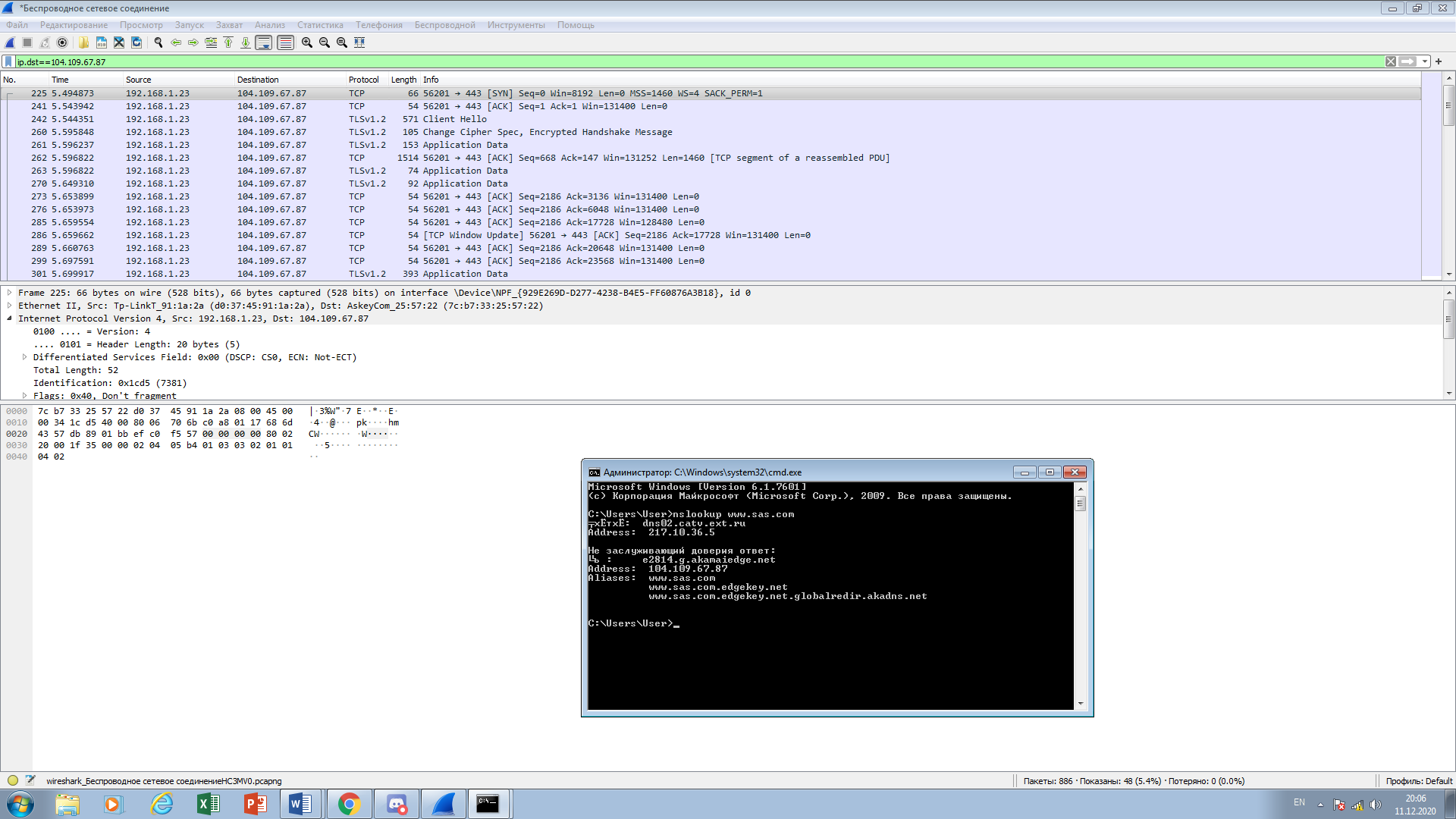
1. Введя в поисковый запрос intitle: “forum” in url: http after: 2019. Этот запрос является строгим, так как мы находим все сайты форумов с протоколом http, которые были проведены или будут проведены после 2019. Я выбираю самый первый SAS Global Forum.



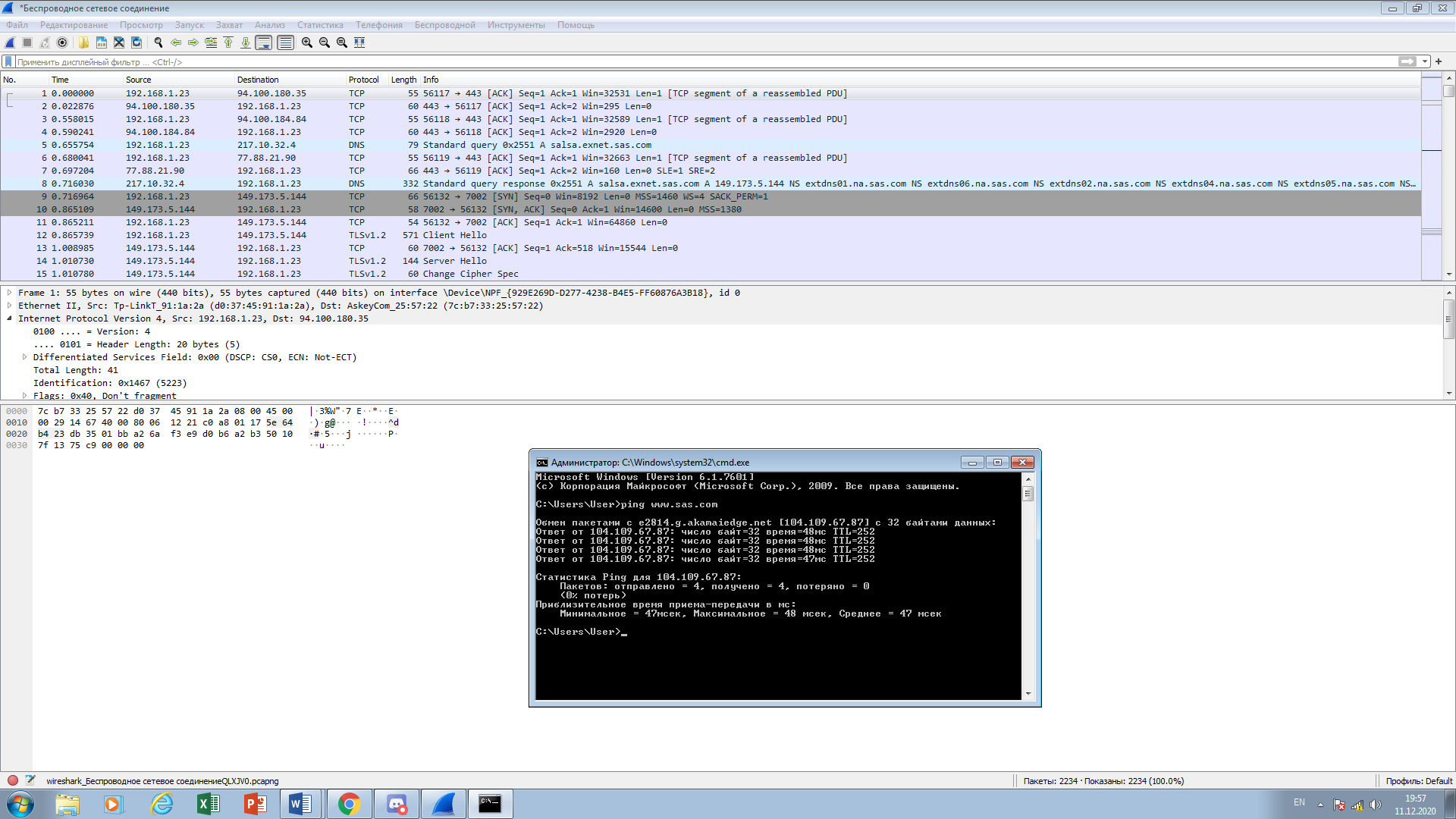
1. Сайт выглядит следующим образом, теперь будем определять ip ресурса несколькими способами.



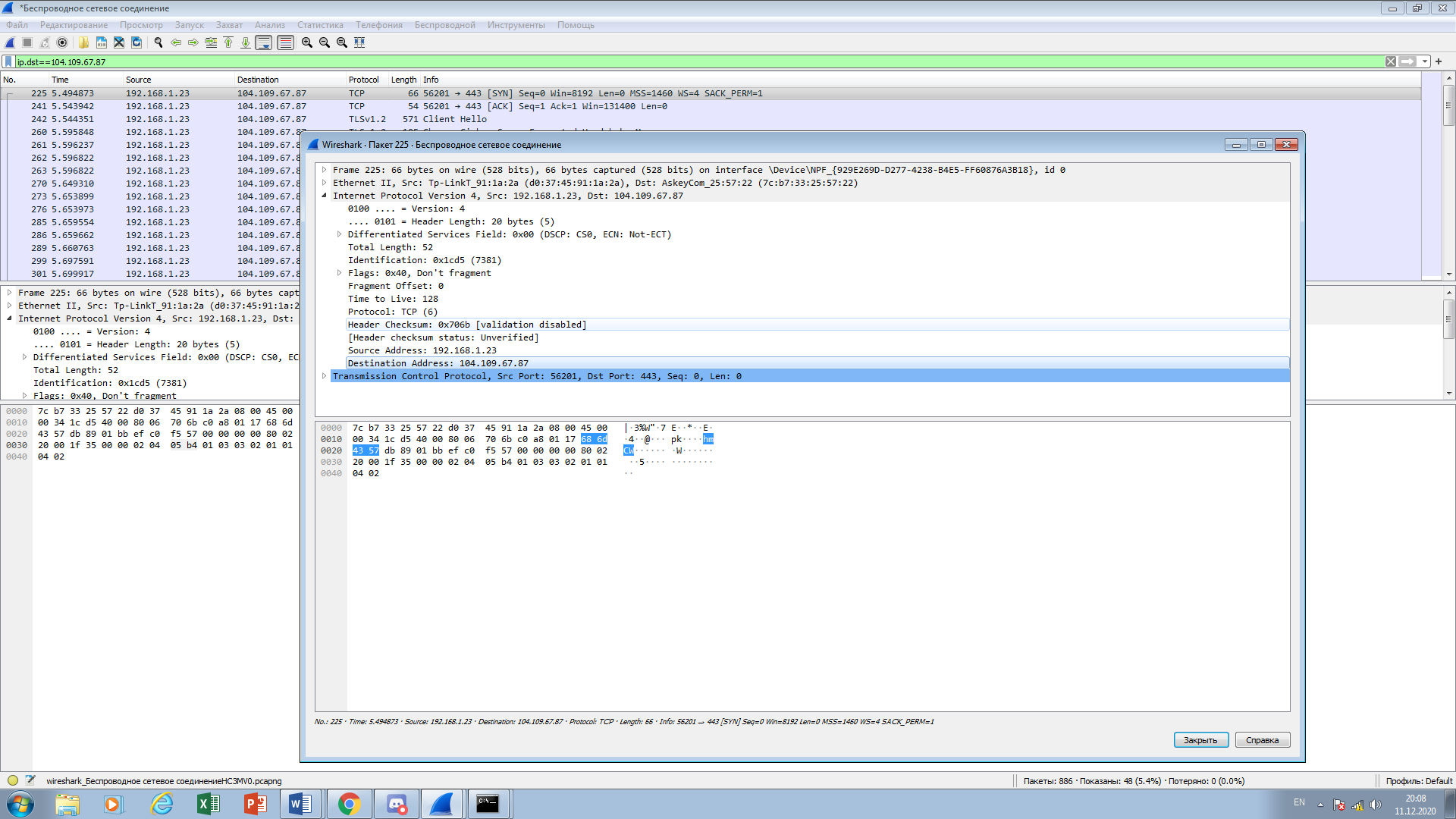
1. Первый способ с помощью утилиты nslookup. Получили ip адрес 104.109.67.87



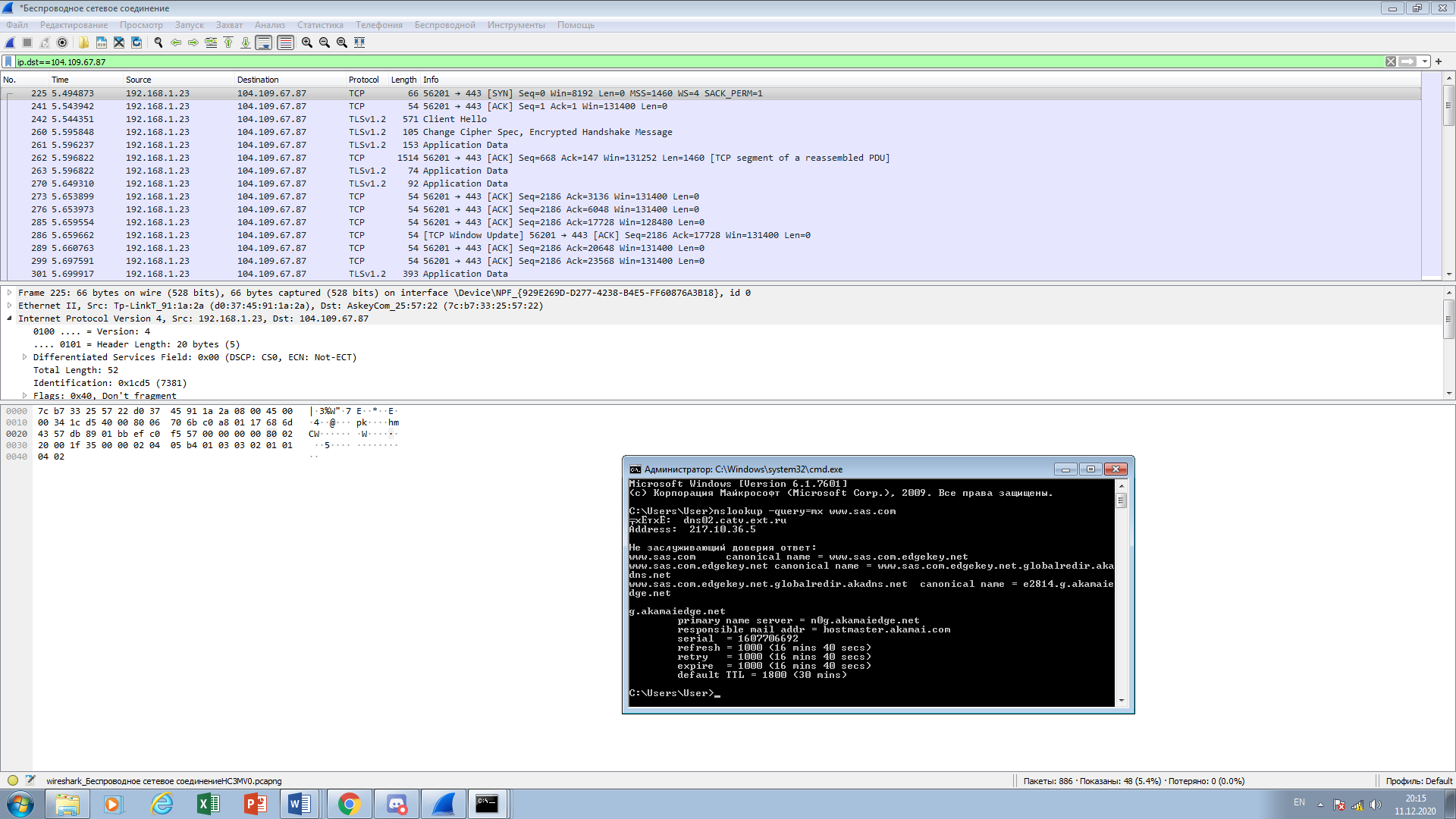
1. Теперь попробуем определить ip адрес при помощи утилиты ping. Неудивителньо, что ip адрес мы получили такой же 104.109.67.87



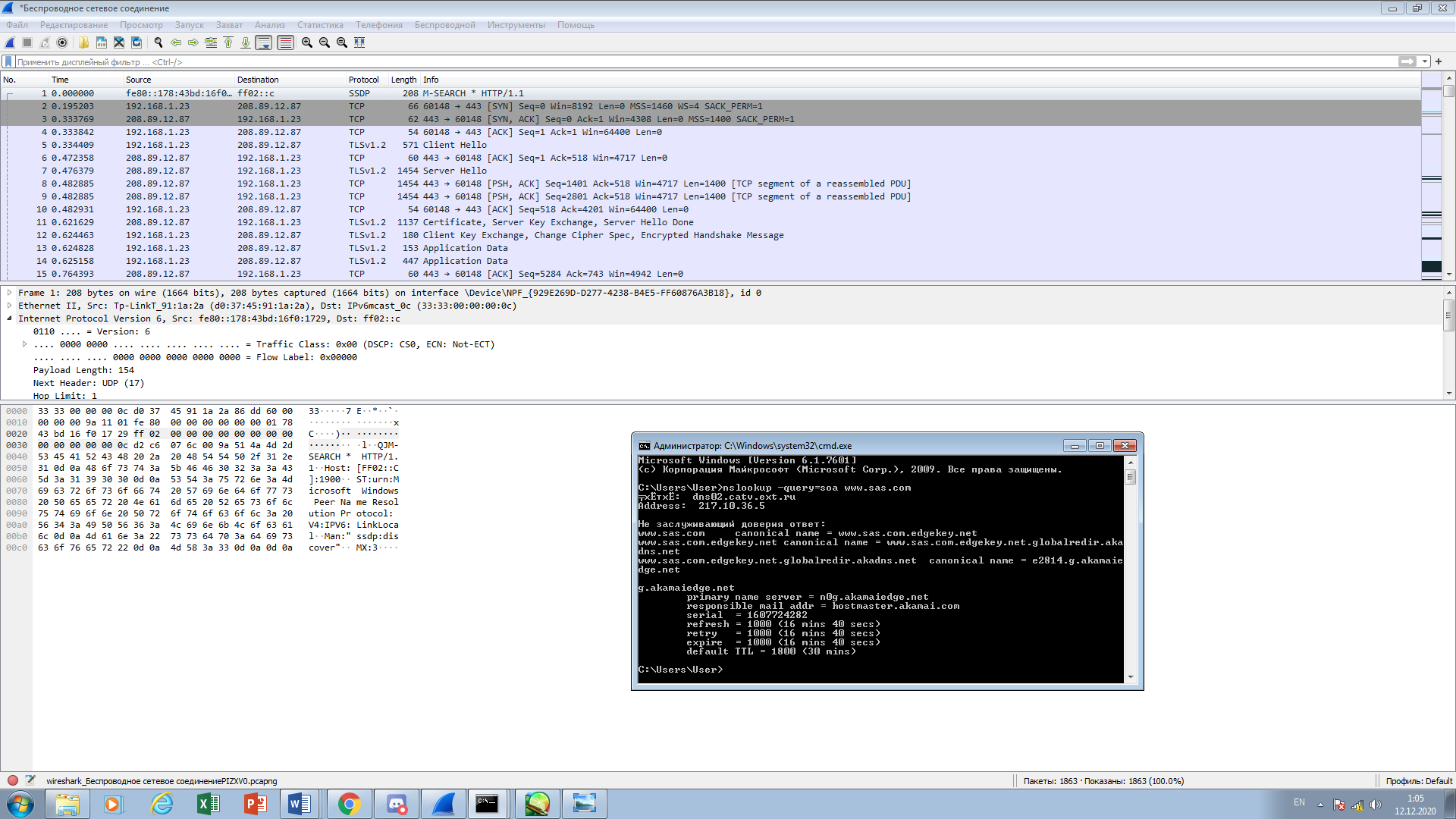
1. И последней способ, это при помощи wireshark. Снова получаем ip адрес равный 104.109.67.87



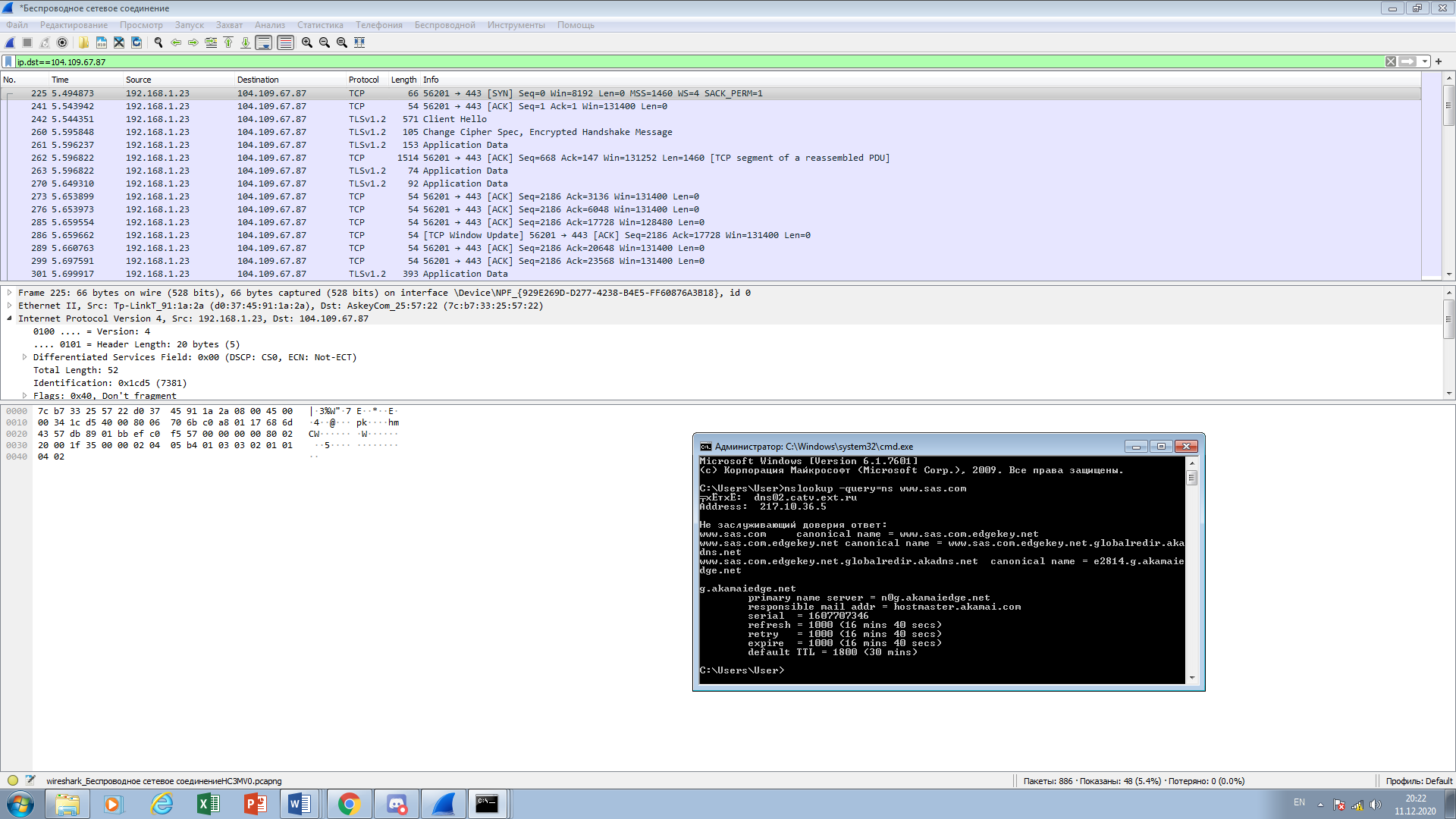
1. Изучение аргументов nslookup
   1. -query=mx. Хранит соответствие доменного имени почтовому серверу этого домена.



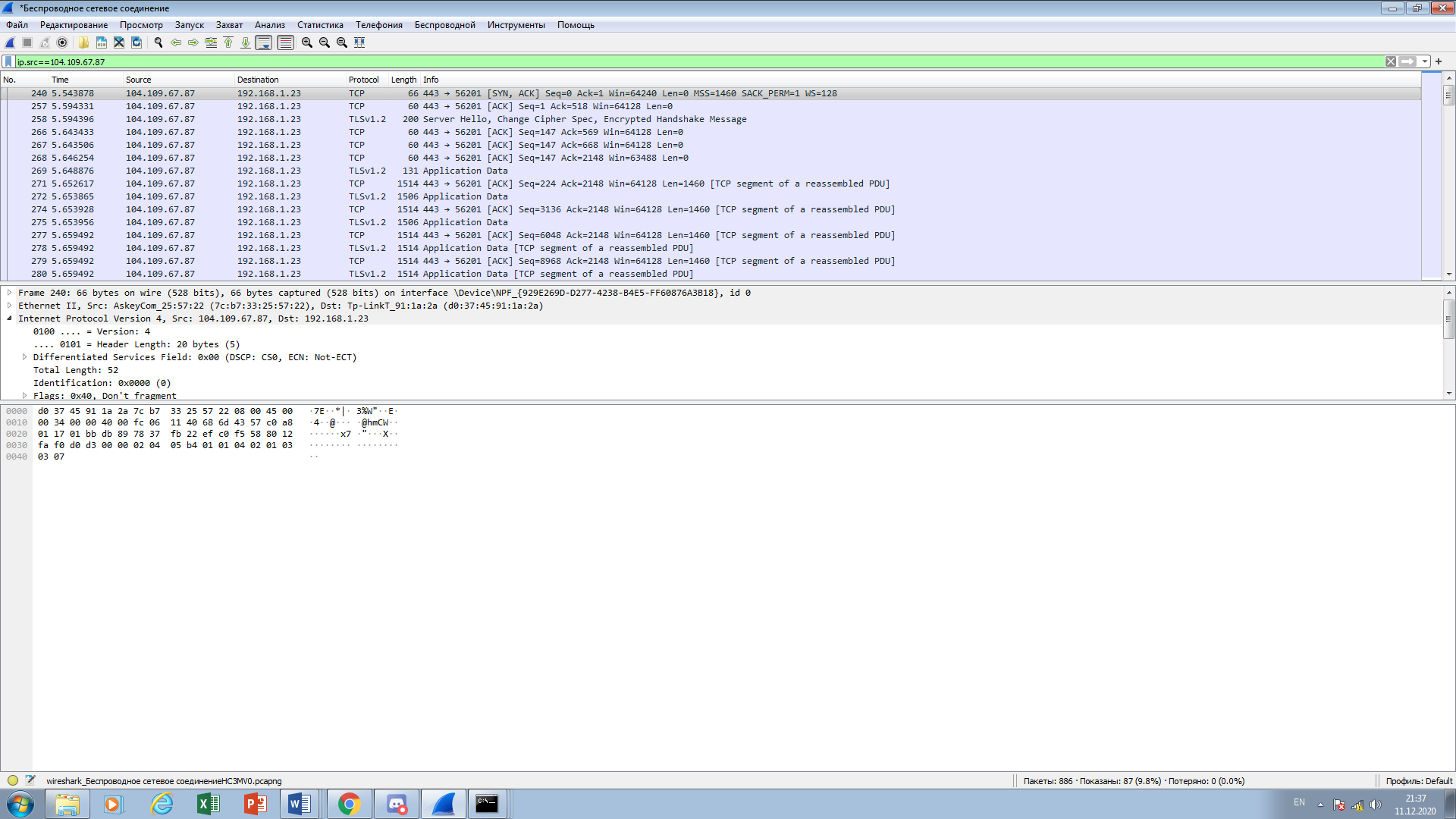
* 1. -query=soa. Cодержит информацию о зоне домена, адрес его администратора, серийный номер и т.д



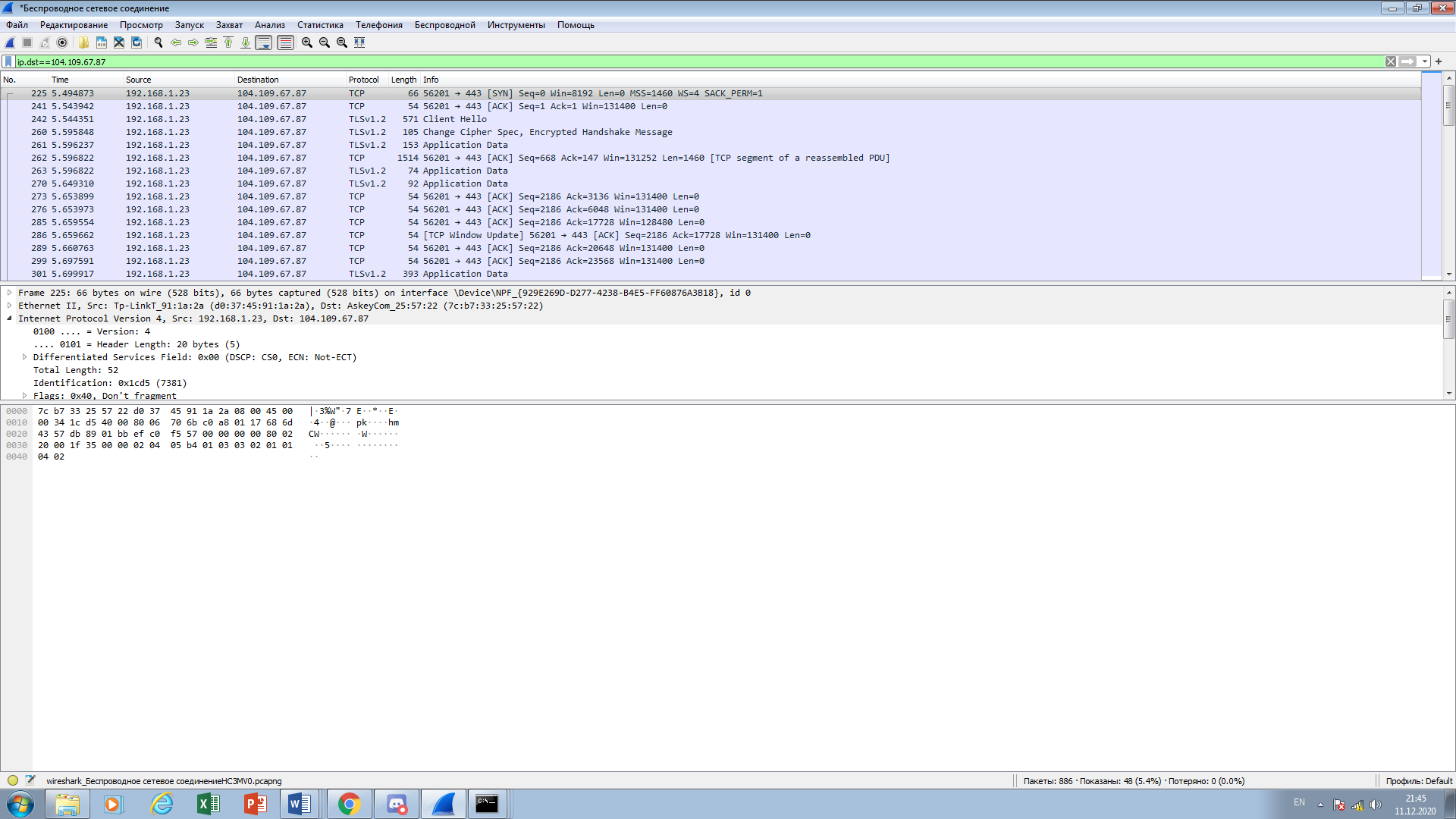
* 1. -query=ns. Cодержит соответствие доменного имени DNS-серверу, авторитативному для заданного домена.



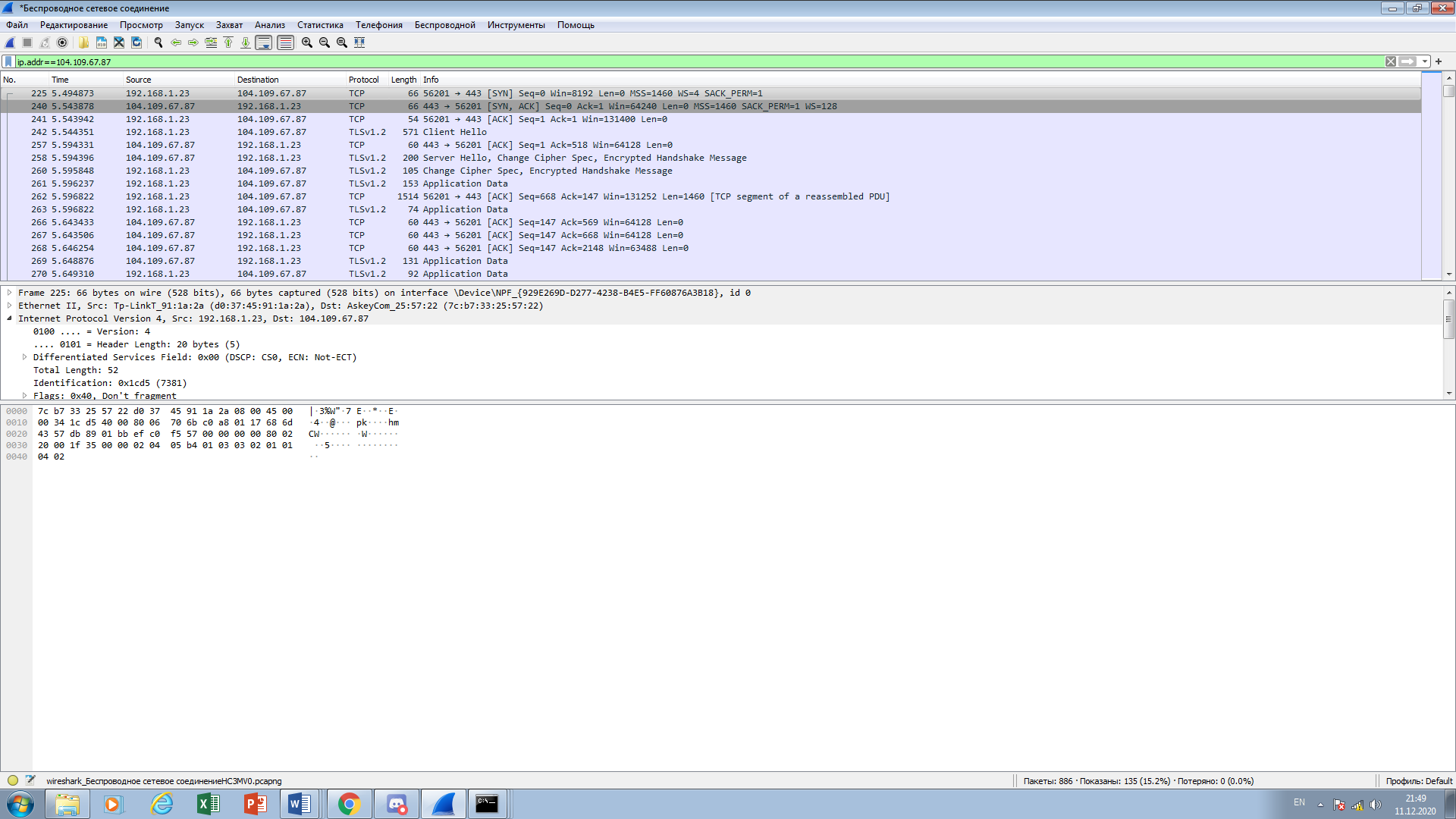
1. Изучение основных фильтров
   1. ip.src==104.109.67.87. Фильтр по IP адресу отправителя



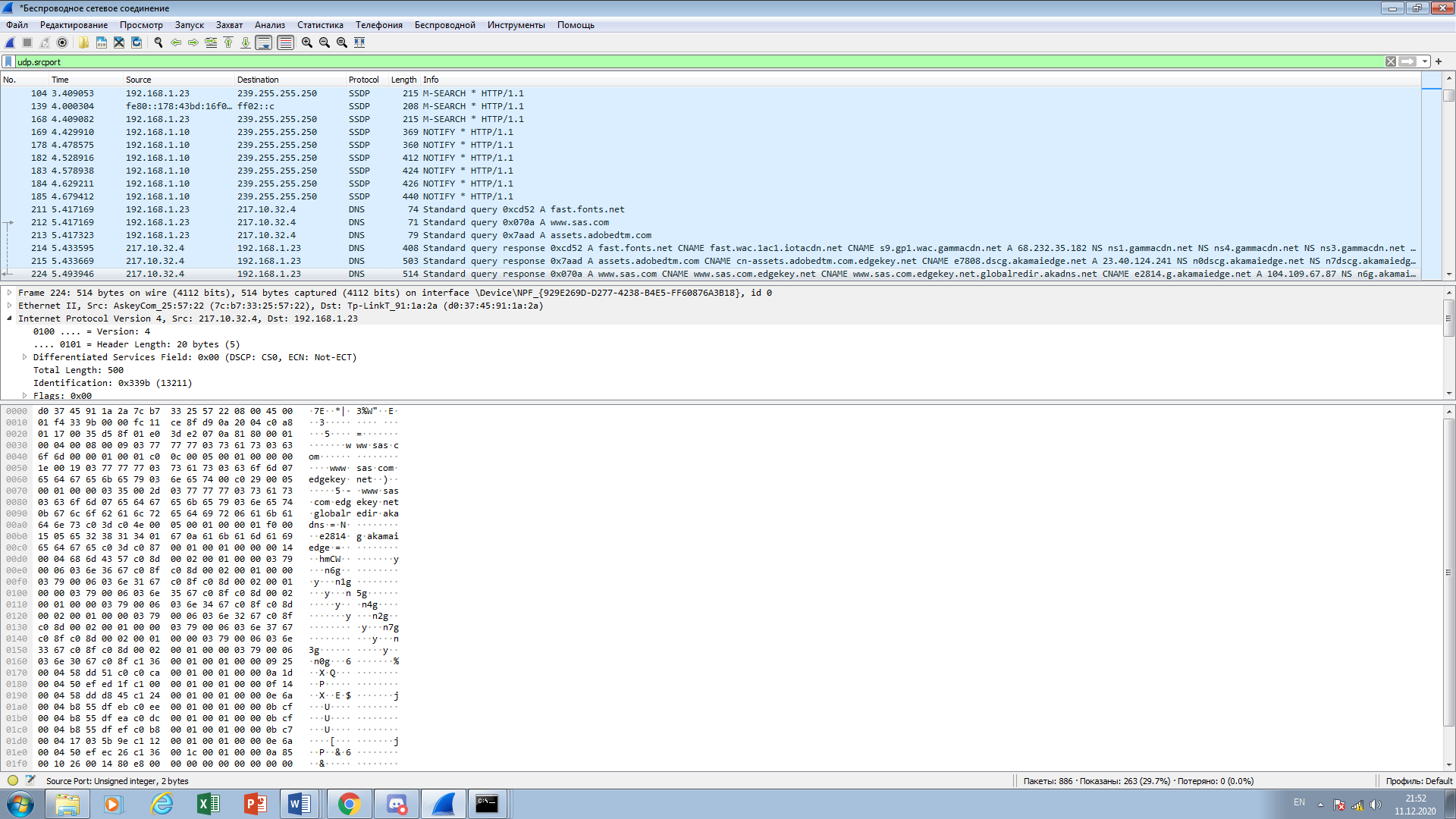
* 1. ip.dst==104.109.67.87. Фильтр по IP адресу получателя



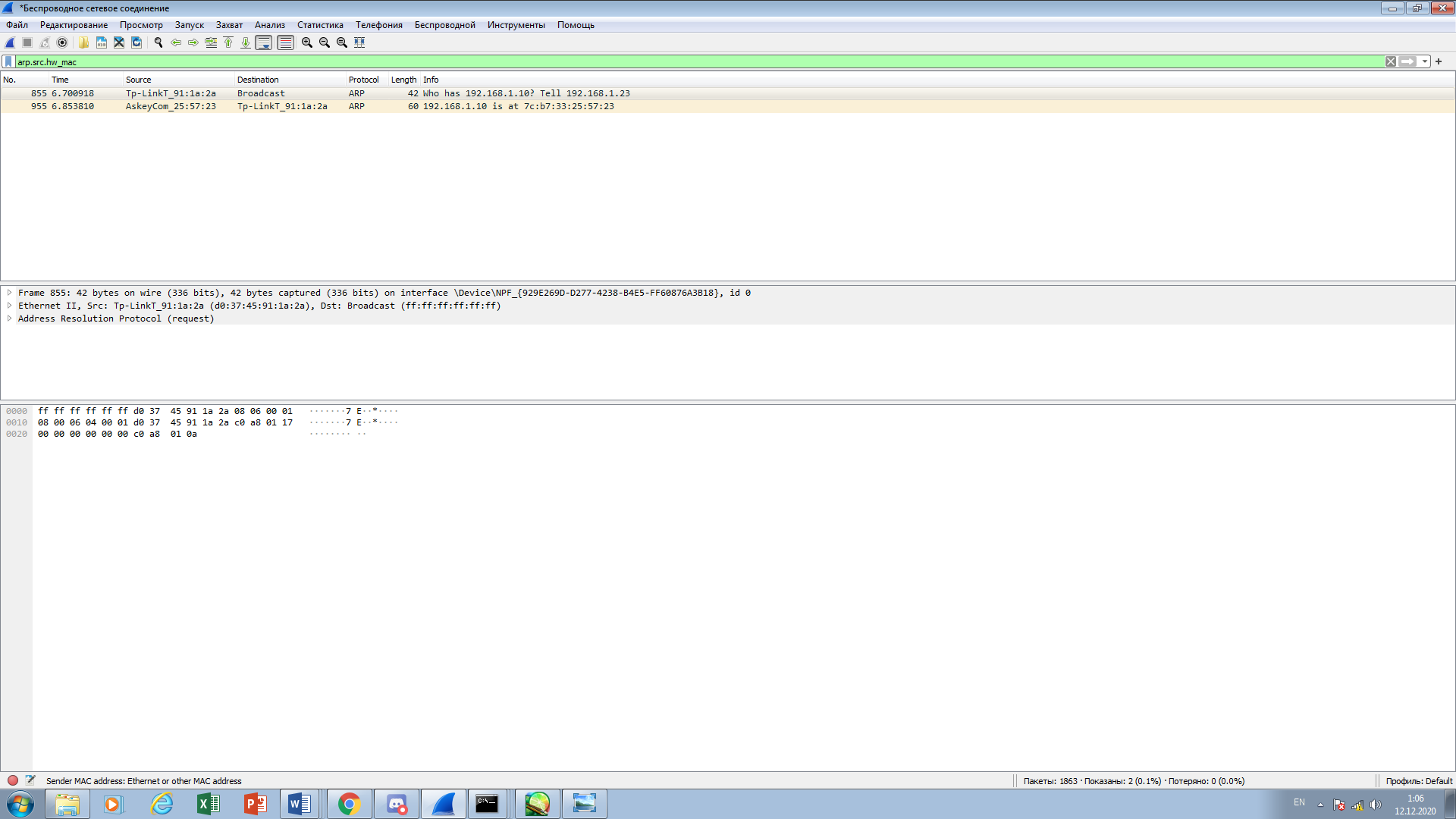
* 1. ip.addr==104.109.67.87. Фильтр по IP адресу получателя и отправителя



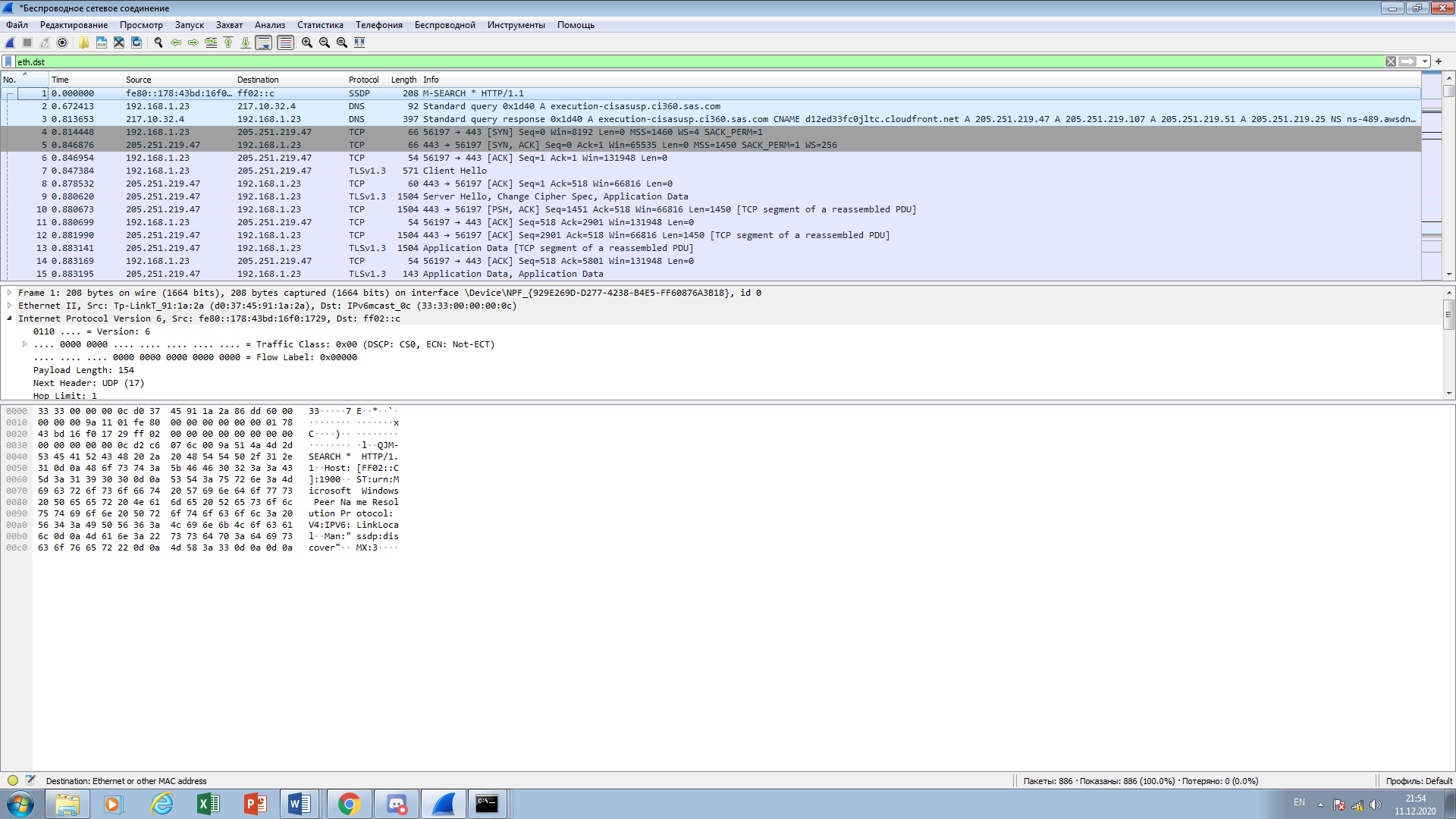
* 1. udp.srcport. Фильтр по UDP порт отправителя



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



* 1. eth.dst. MAC-адрес получателя



* 1. eth.src. MAC-адрес отправителя

