|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| **Институт комплексной безопасности и специального приборостроения** | | |
|  |  |  |

Кафедра КБ-1 «Защиты информации»

**Отчет**

по выполнению лабораторной работы № 2

««АНАЛИЗ СТРУКТУРЫ СЕТЕВОГО ТРАФИКА

С ПОМОЩЬЮ ПРОГРАММЫ WIRESHARK»»

по дисциплине «Основы Информационной Безопасности»

Выполнил:

Студент 2 курса

Группа :БИСО-02-19

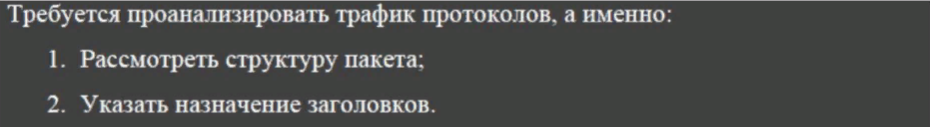
ФИО: Борисенко П.Е

Проверил:

Изергин Д.А.

Москва, 2020

**Задание №1**



1. Для данного задания был взят 3 пакет.

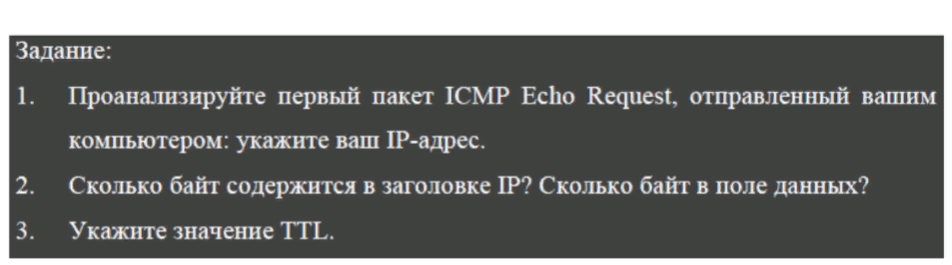


2. Пакет состоит из 4 заголовков:

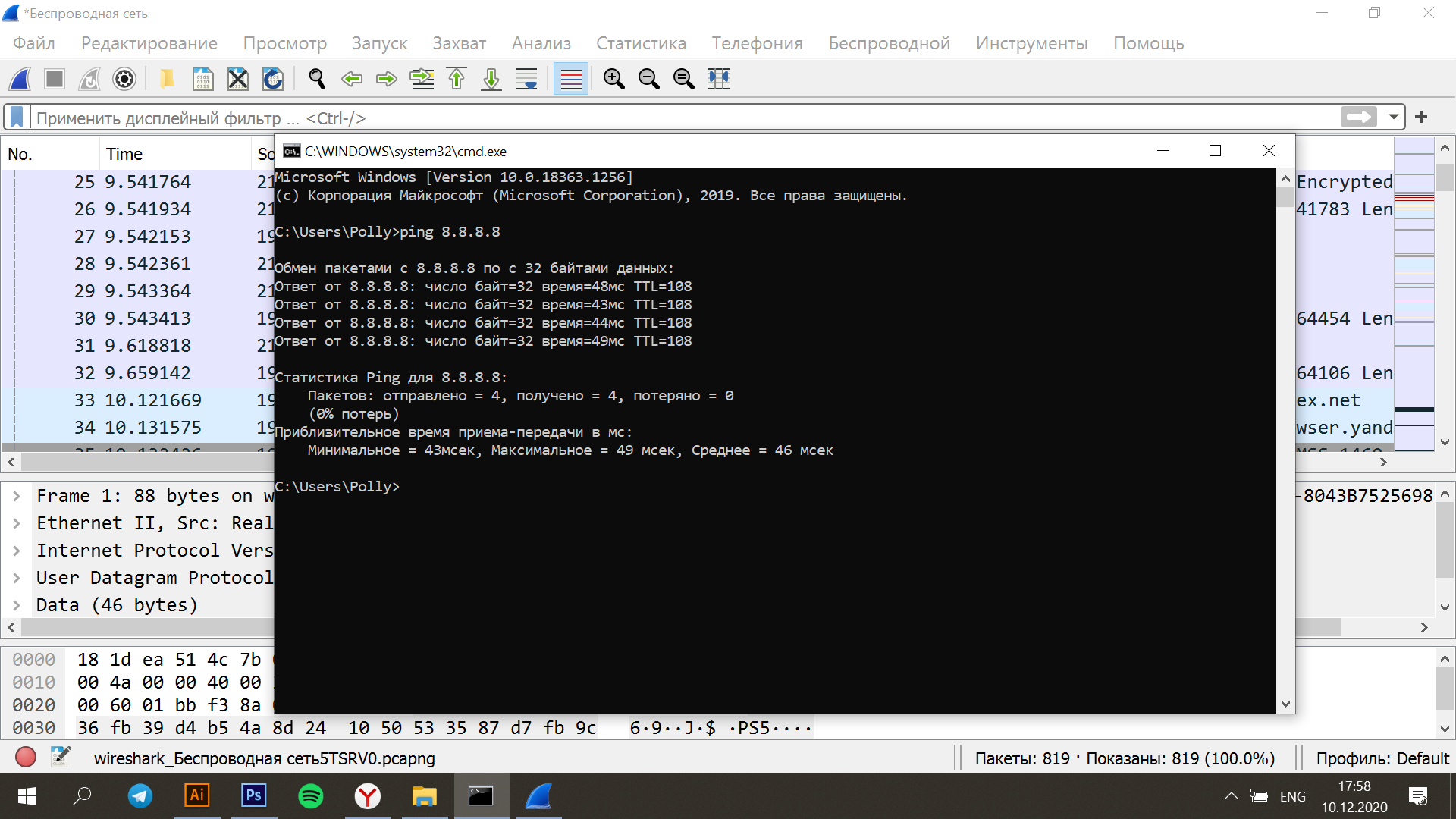
a. Frame 3 (Протокол физического уровня)  
b. Ethernet 2 (Протокол канального уровня)  
c. Internet Protocol Version 4 (IPv4, Протокол сетевого уровня)  
d. Transmission Control Protocol (Протокол транспортного уровня)

3. Назначение заголовков:

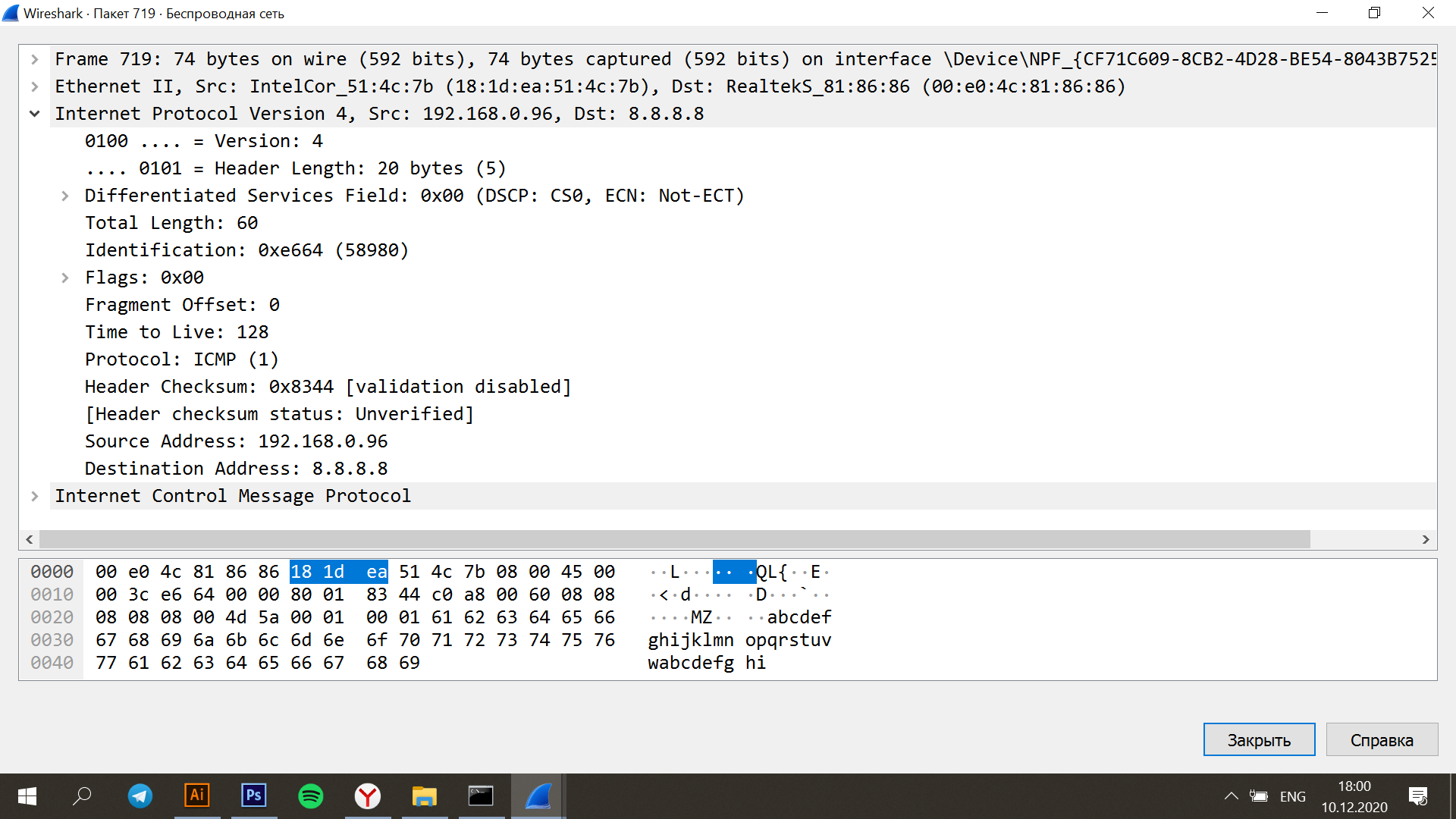
a. Frame (Физический уровень) — первый уровень сетевой модели OSI. Физический уровень описывает способы передачи бит (а не пакетов данных) через физические среды линий связи, соединяющие сетевые устройства.  
b. Ethernet – второй уровень сетевой модели OSI. Предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети.  
c. Internet Protocol Version – 3-й уровень сетевой модели OSI. Предназначается для определения пути передачи данных  
d. Transmission Control Protocol – 4-й уровень сетевой модели OSI. Предназначен для доставки данных

**Задание №2  
**

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

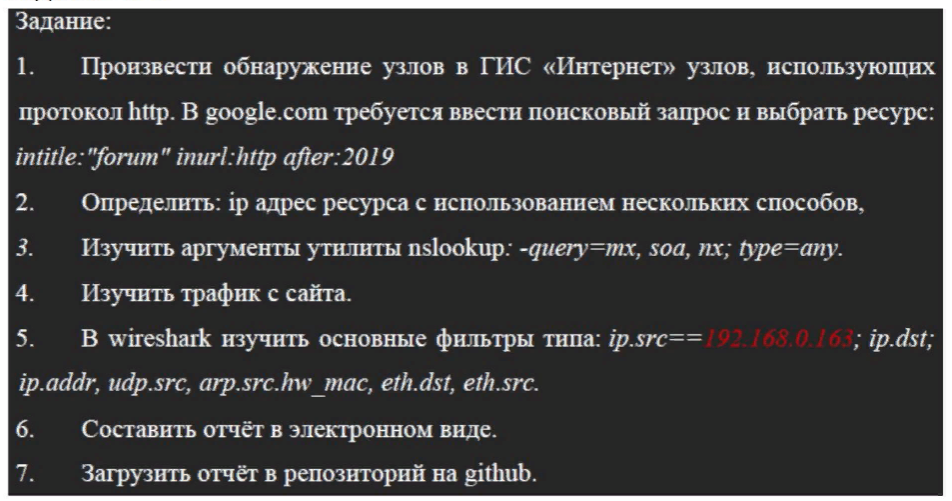




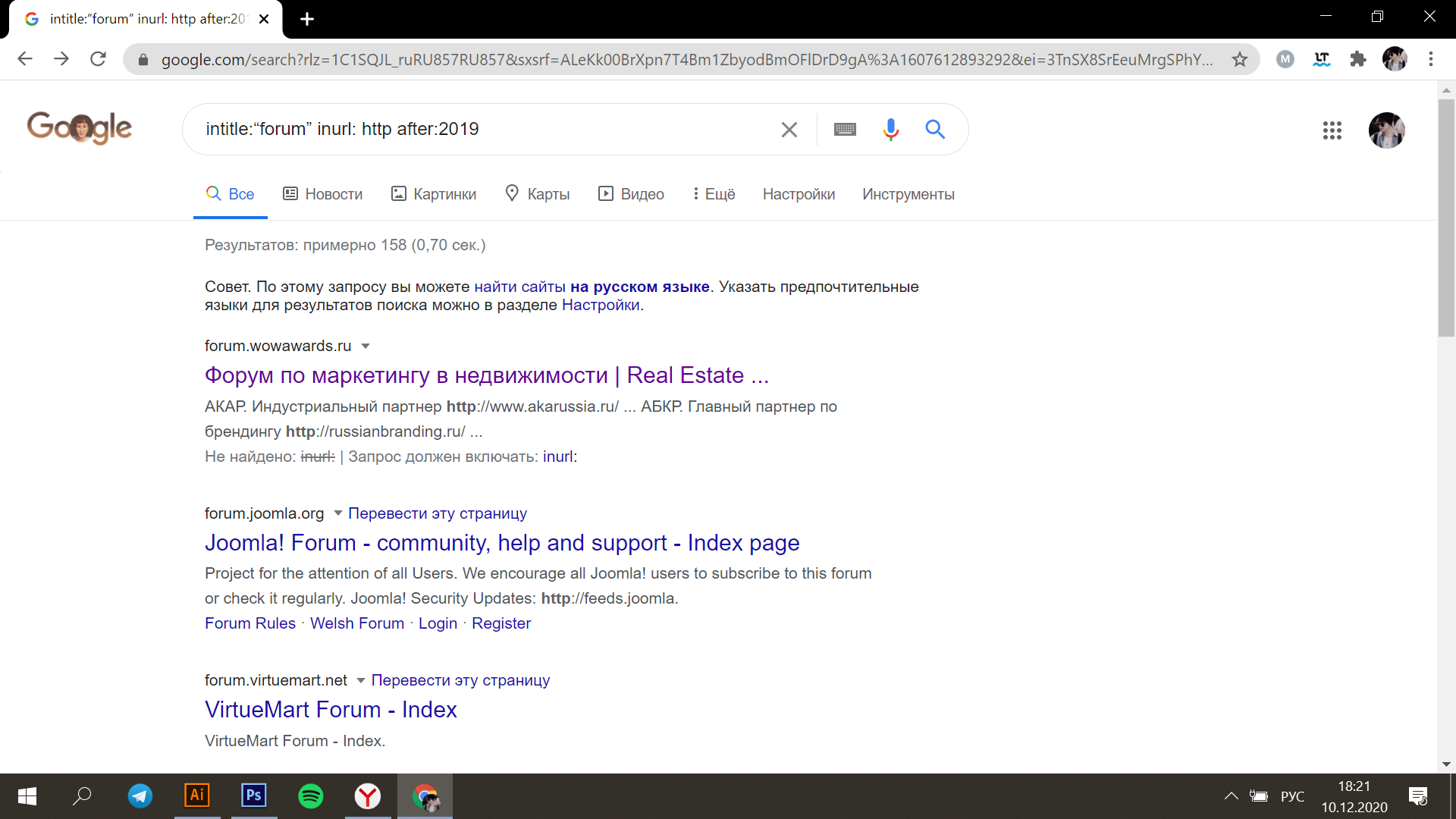


2. Проанализировав первый пакет ICMP, я поняла, что мой IP-адрес: 192.168.0.96  
3. 20 байт, 4 байта  
4. Time to live составляет: 128

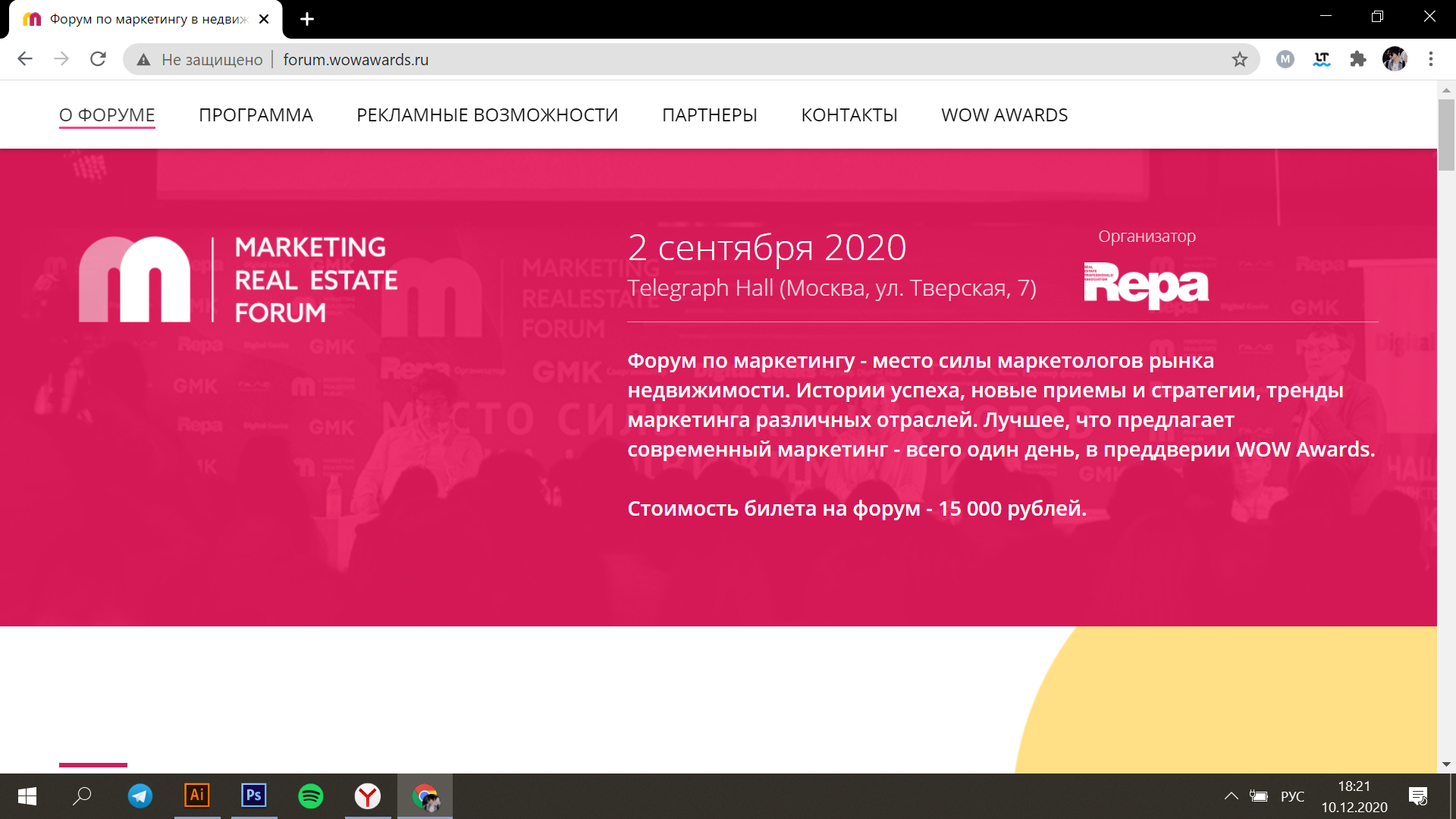
**Задание № 3**

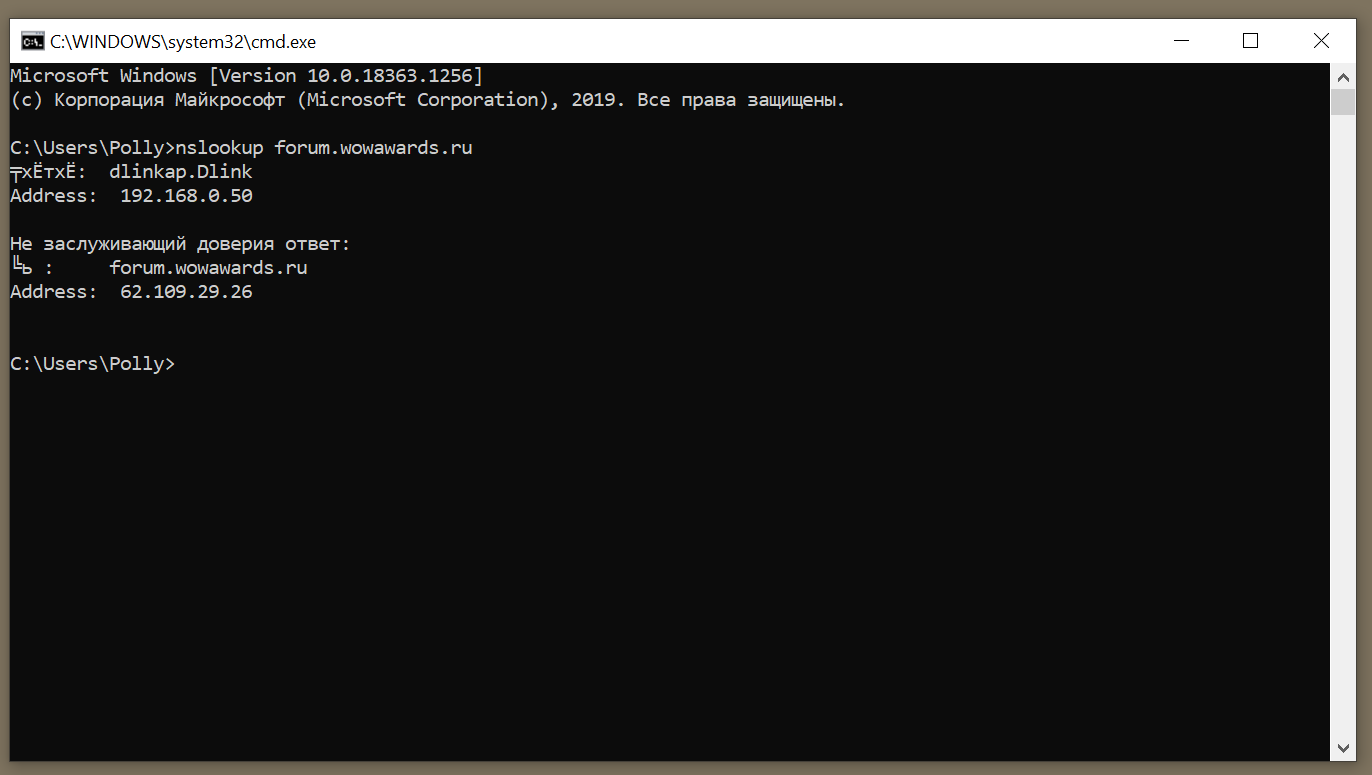
****

1. Введя в поисковый запрос intitle: “forum” inurl: 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 Loyalty World Forum.

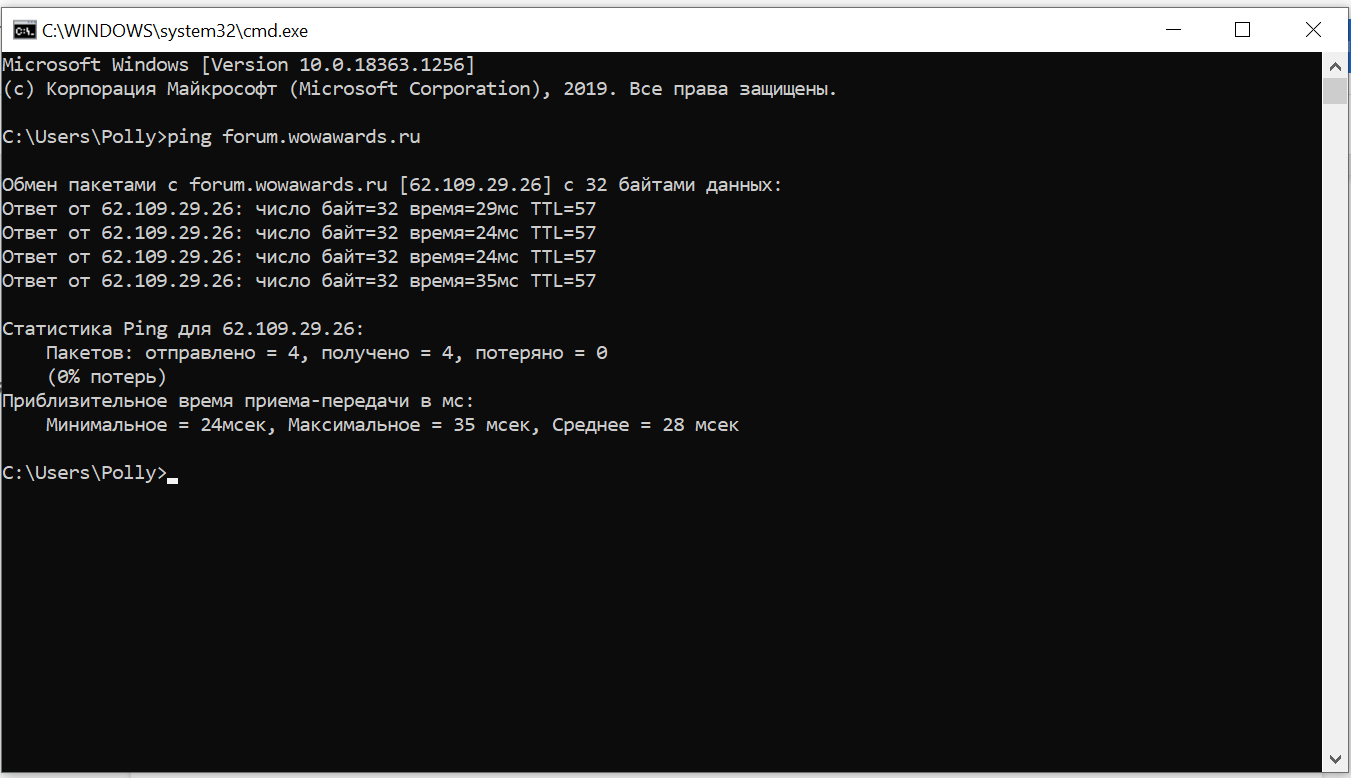


2. Сайт выглядит следующим образом, теперь будем определять ip ресурса несколькими способами.

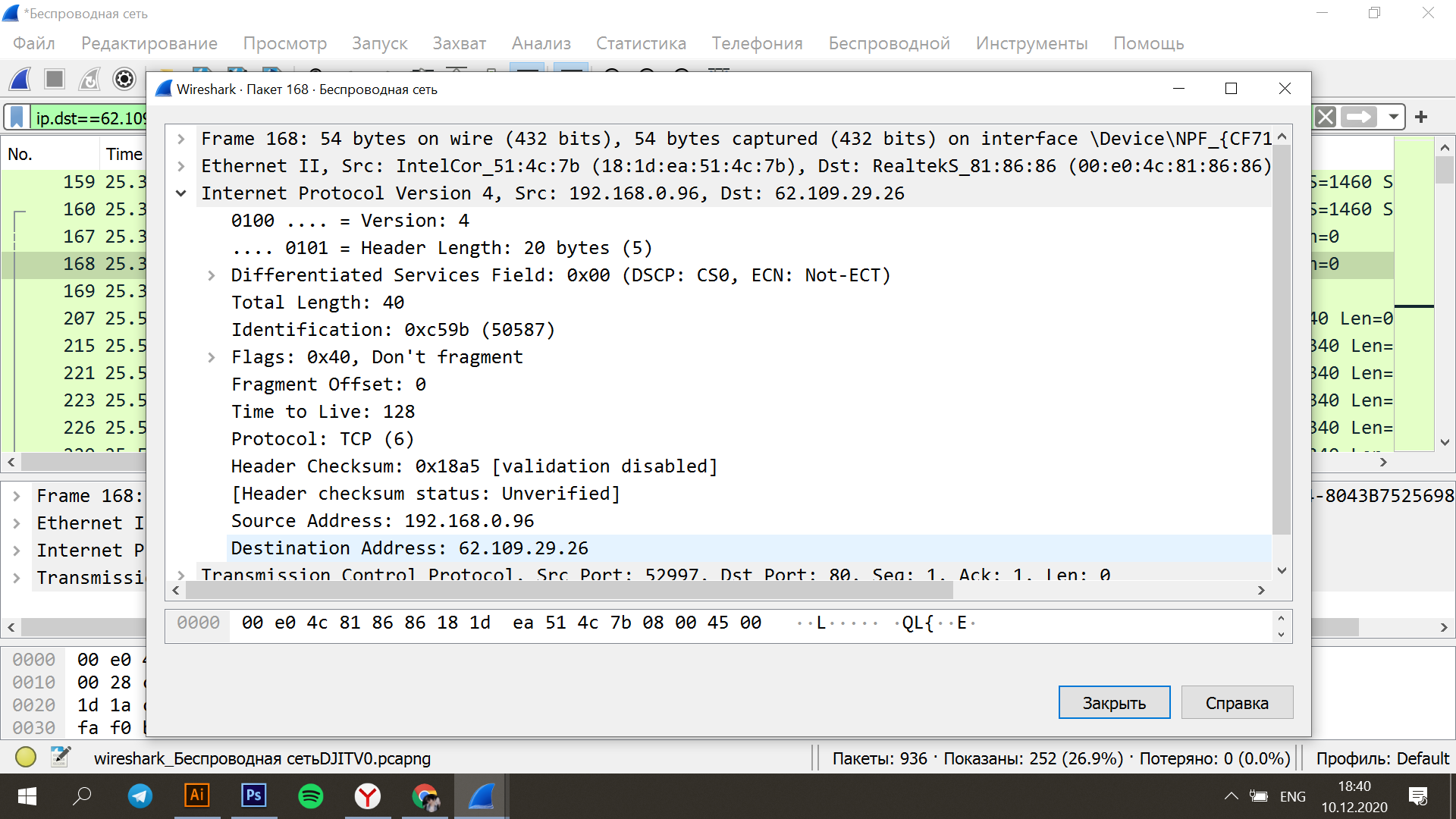


a) Первый способ с помощью утилиты nslookup. Получили ip адреc: 62.109.29.26  


b) Теперь попробуем определить ip адрес при помощи утилиты ping. Получаем такой же адрес: 62.109.29.26

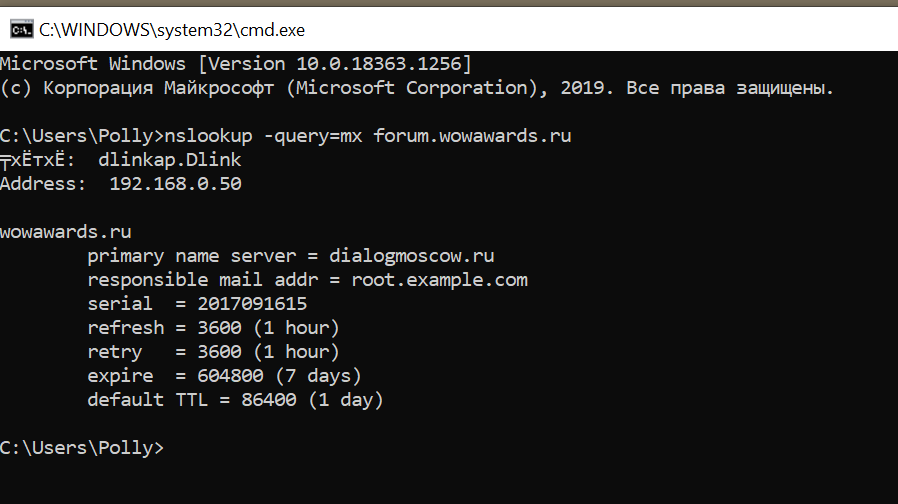


c) И последней способ, это при помощи wireshark. Снова получаем ip адрес равный: 62.109.29.26

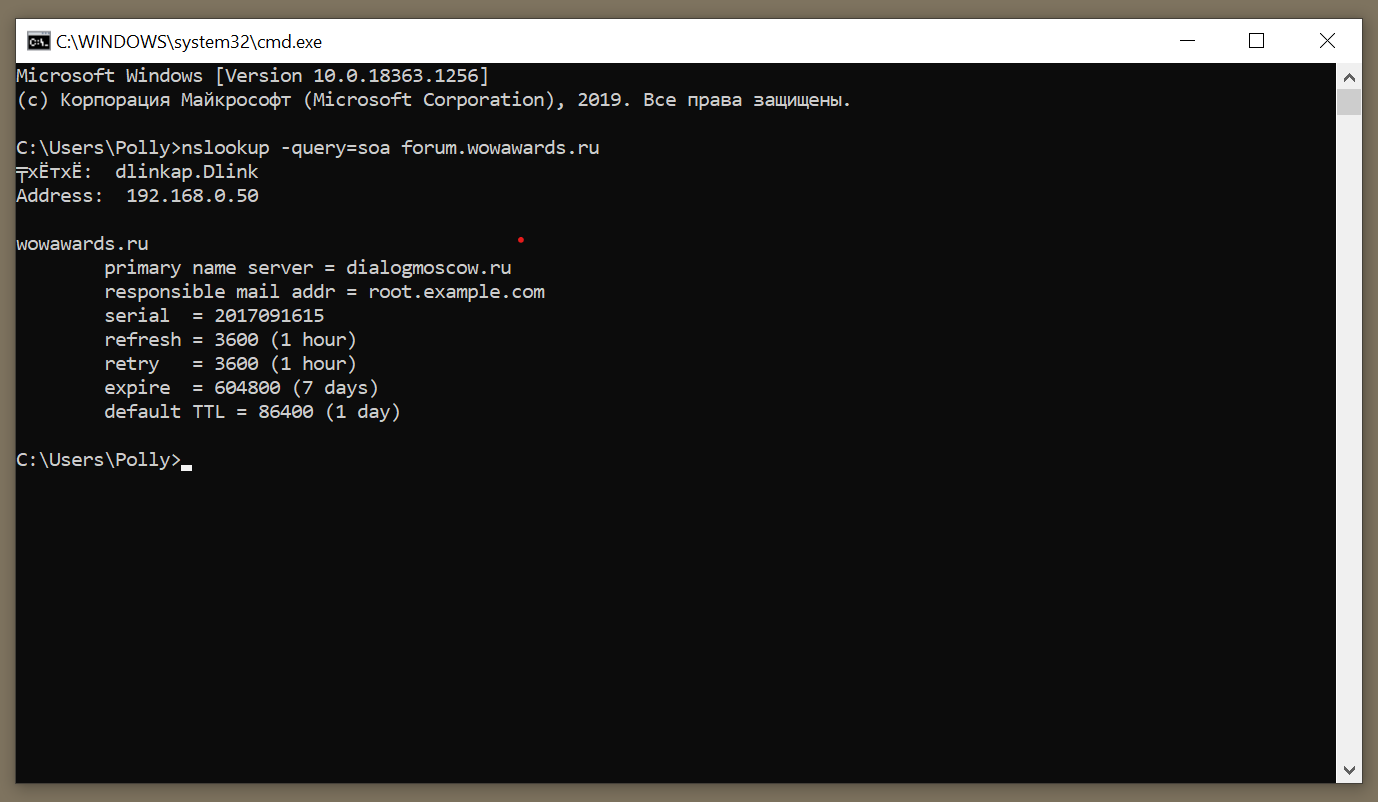


3. Изучение аргументов nslookup

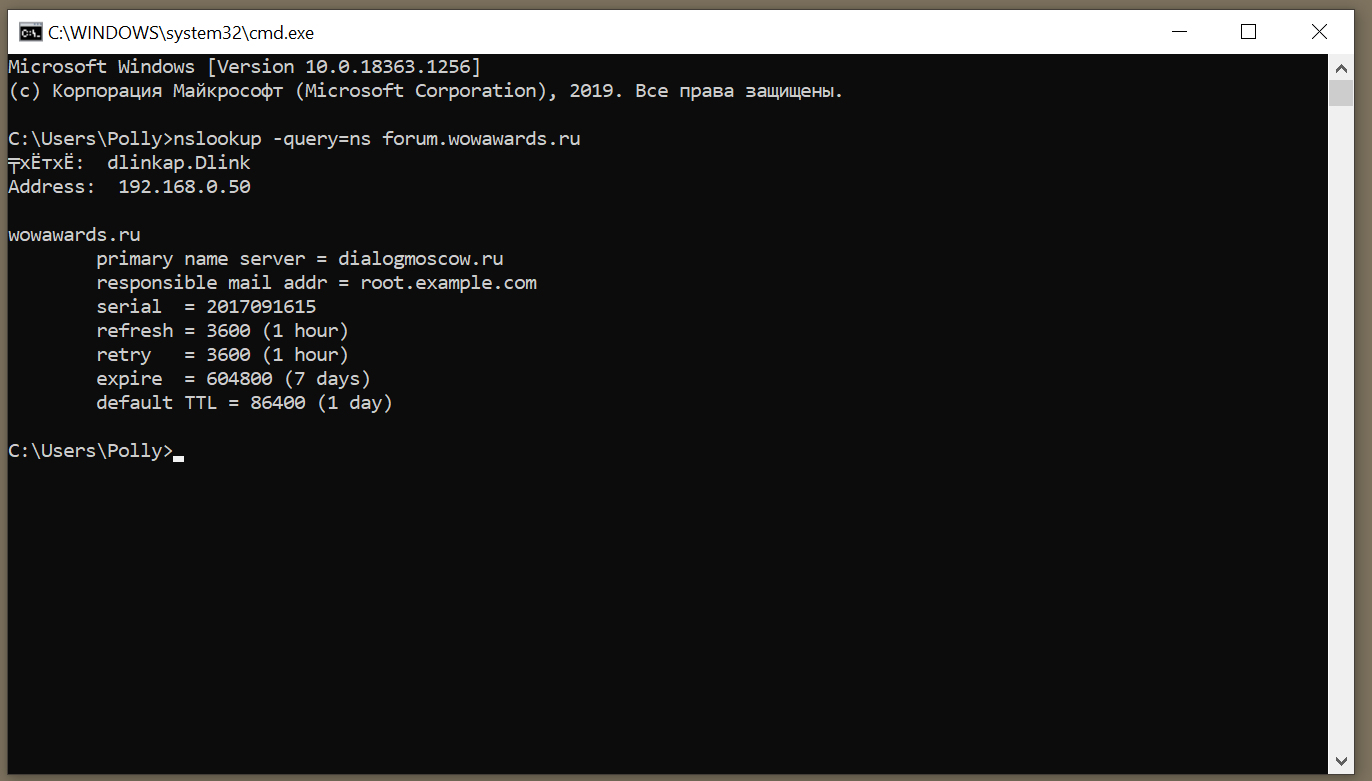
* -query=mx. Хранит соответствие доменного имени почтовому серверу этого домена.



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

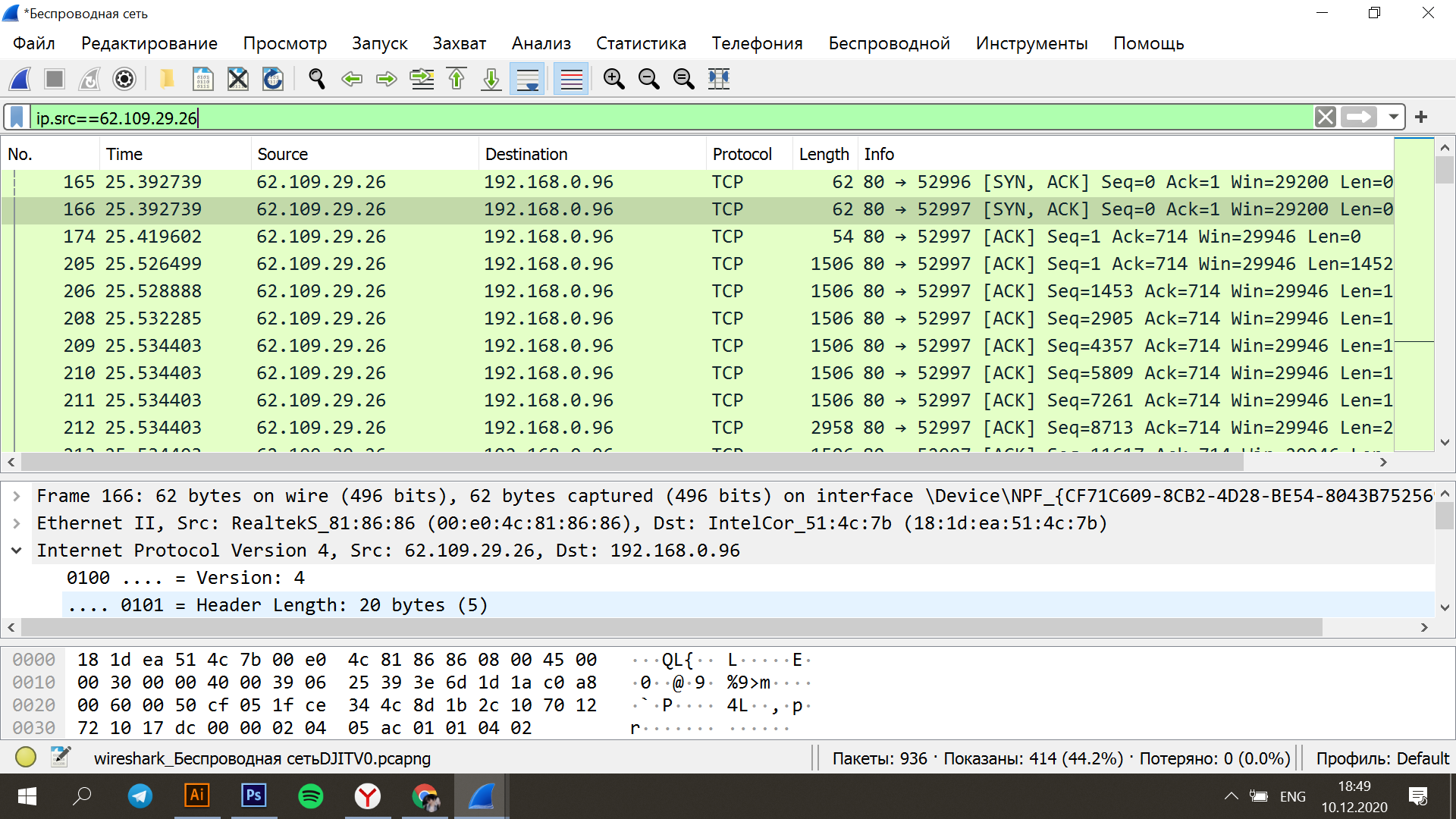


* -query=ns. Cодержит соответствие доменного имени DNS-серверу, авторитативному для заданного домена

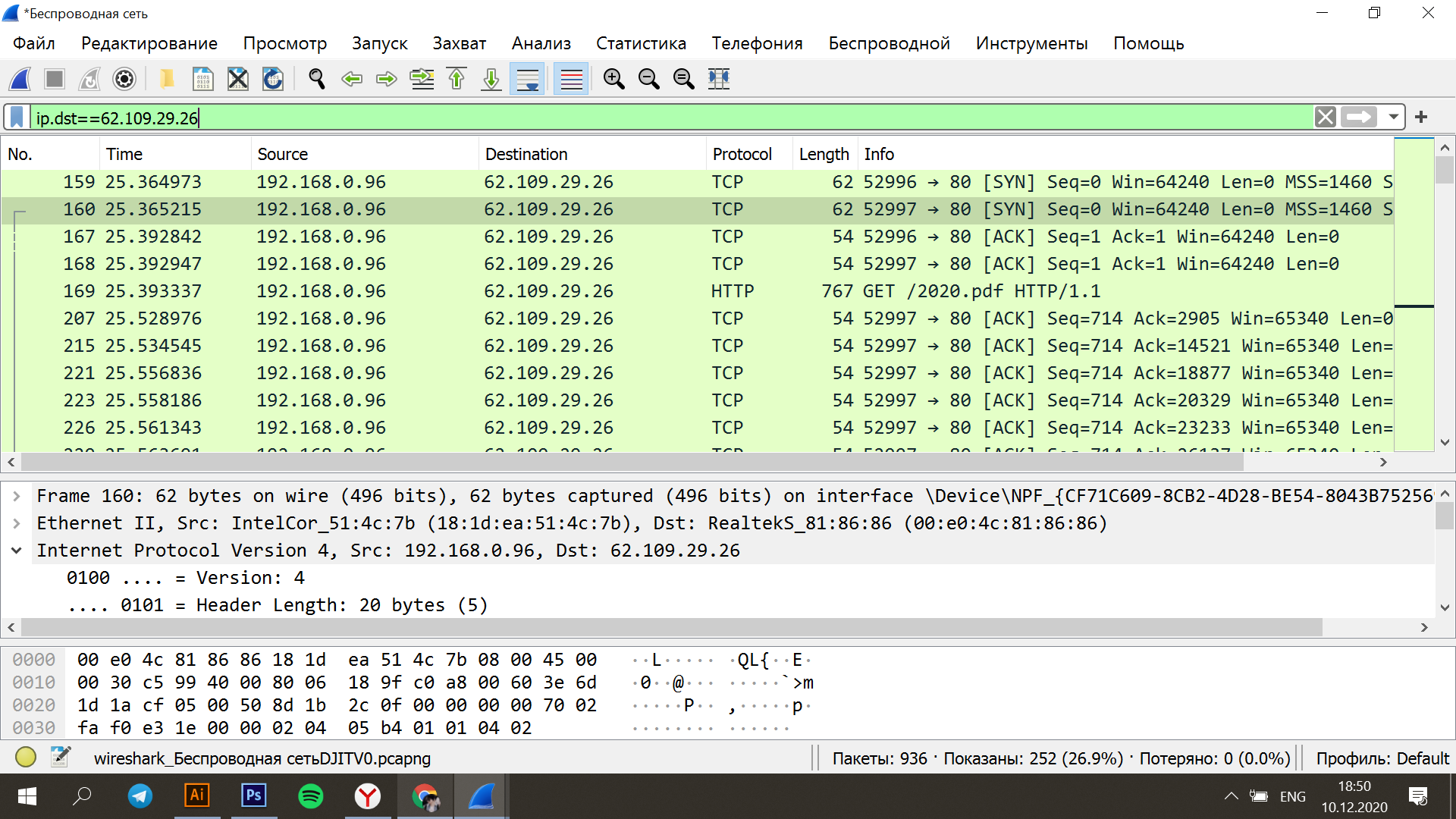


4. Изучение основных фильтров

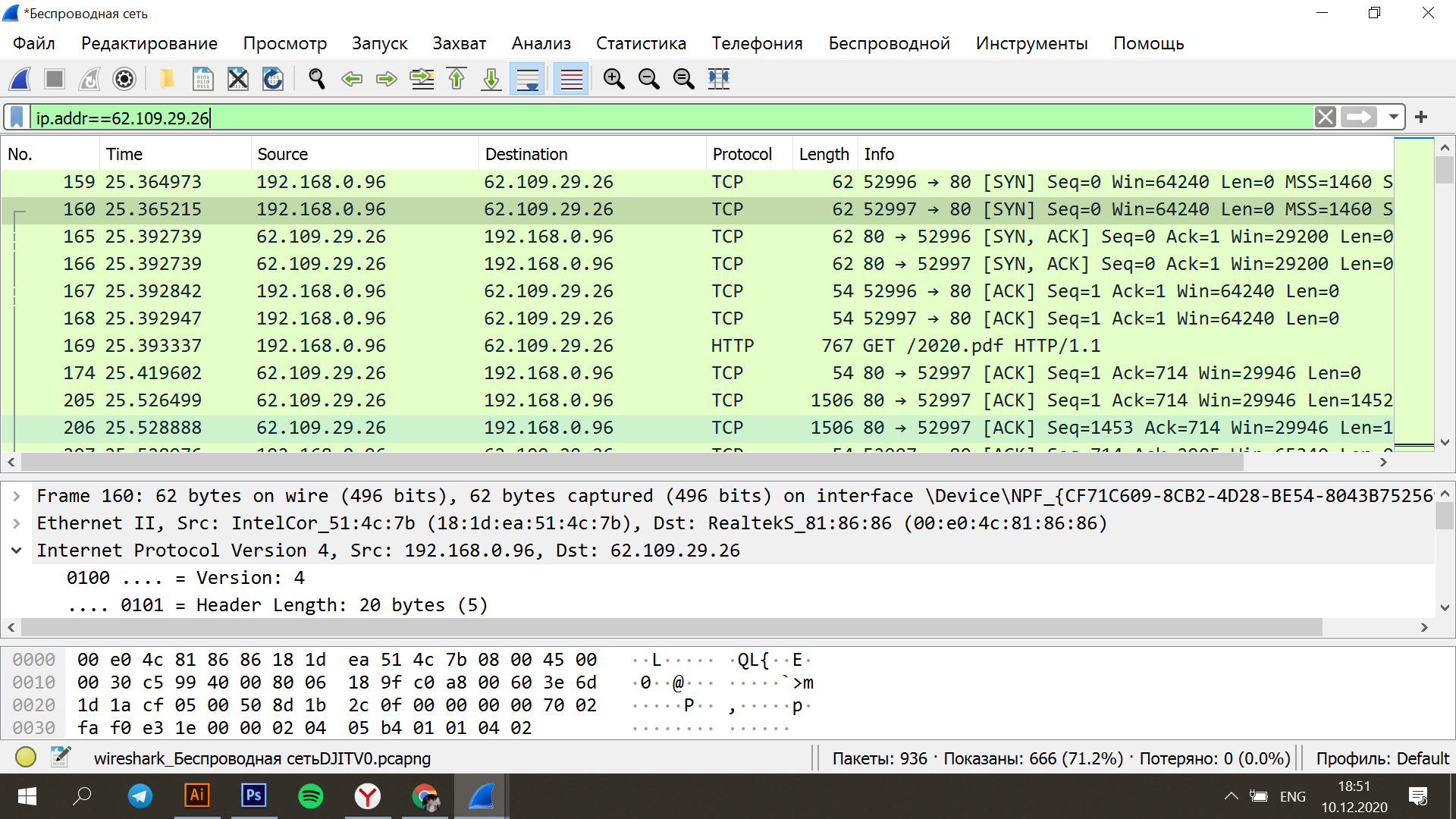
* ip.src==62.109.29.26. Фильтр по IP адресу отправителя



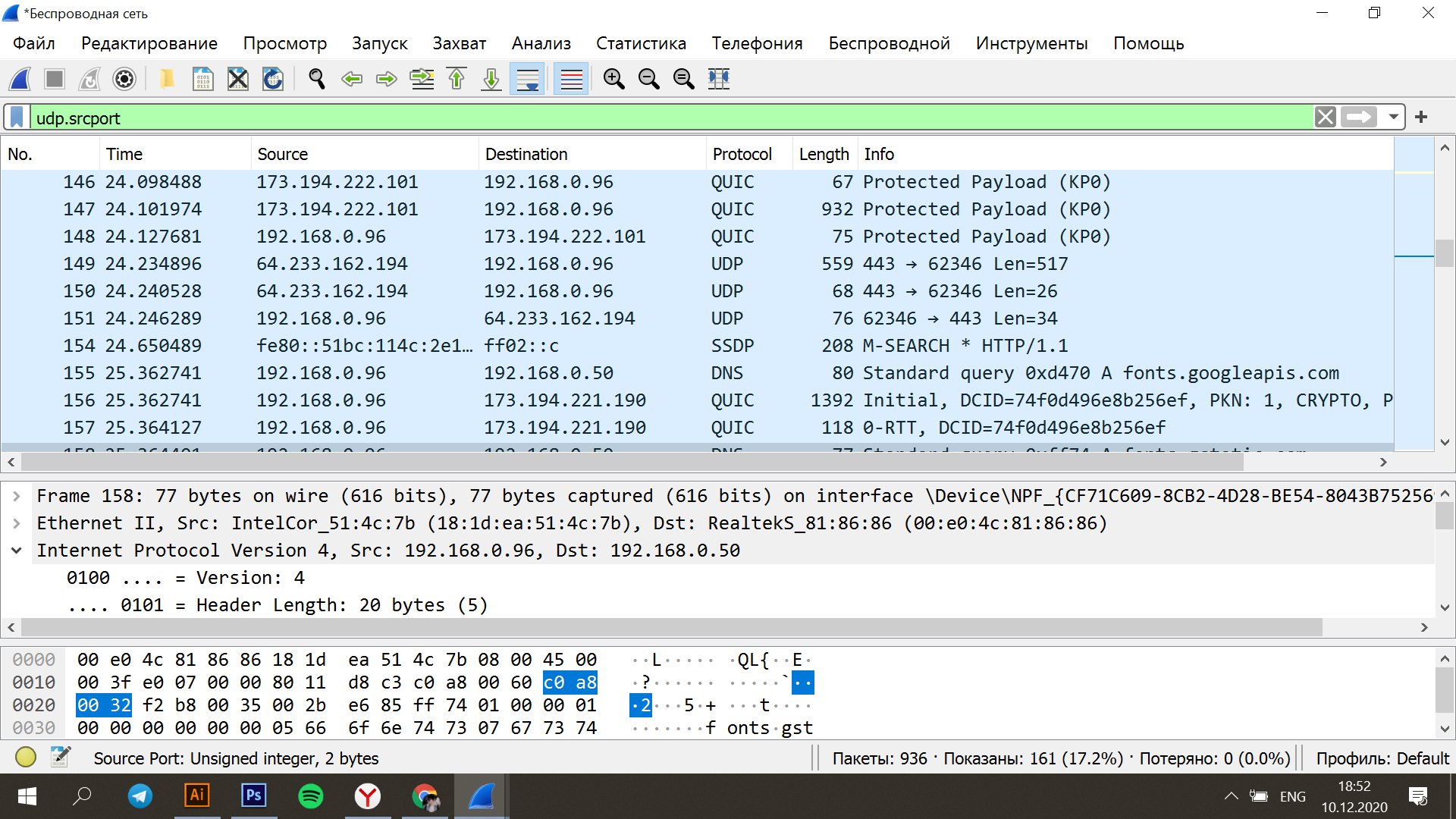
* ip.dst==62.109.29.26. Фильтр по IP адресу получателя



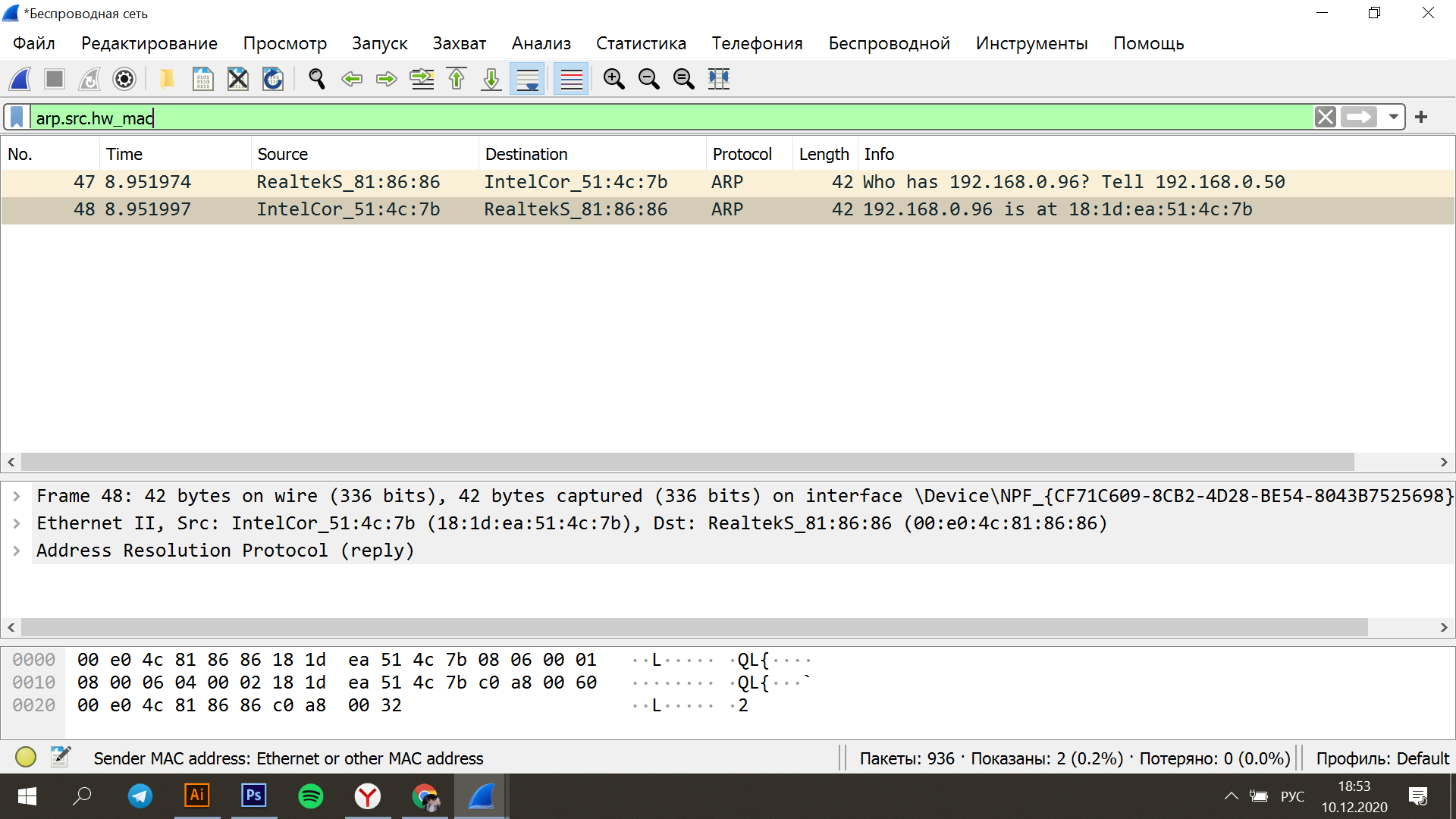
* ip.addr==62.109.29.26. Фильтр по IP адресу получателя и отправителя



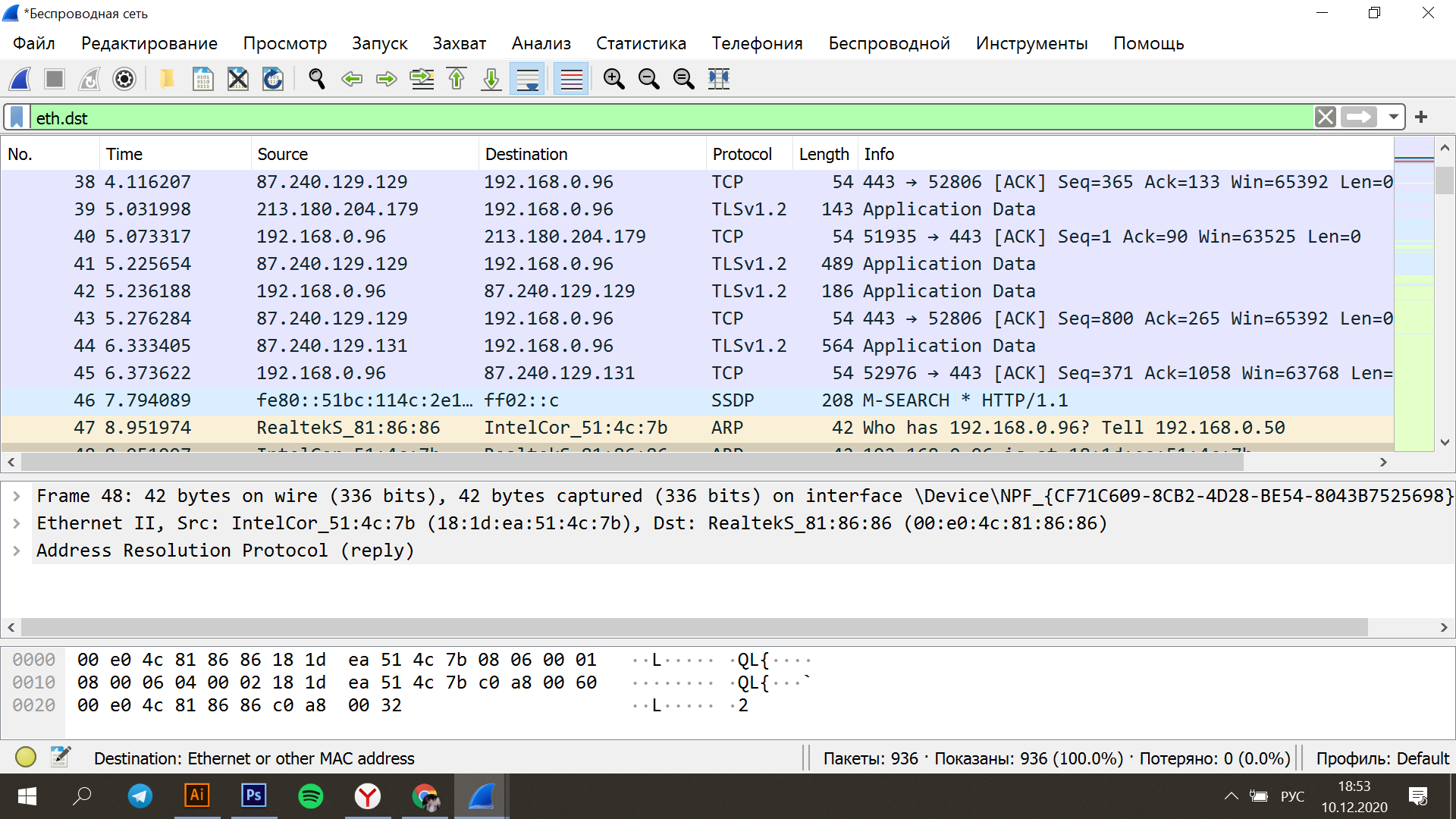
* udp.srcport. Фильтр по UDP порт отправителя



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



* eth.dst. MAC-адрес получателя



* eth.src. MAC-адрес отправителя

