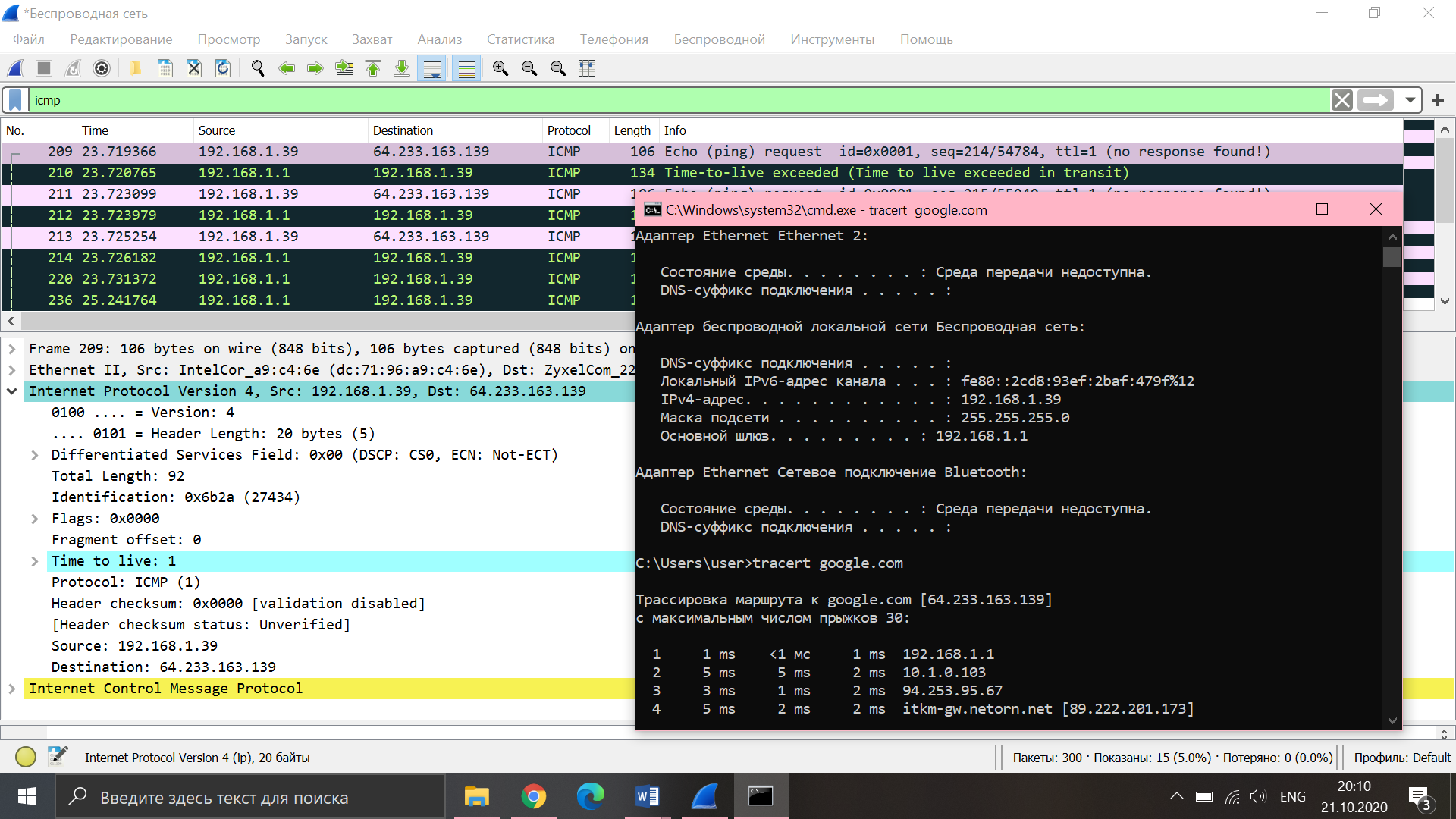
|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)**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

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 2** | |
| по дисциплине  «Основы информационной безопасности» | |
| Выполнил студент группы БИСО-01-19 | Попова Наталья Викторовна |
|  |

Аккаунт github: <https://github.com/Kometulus>

Москва 2020

Задание 1. Wireshark.

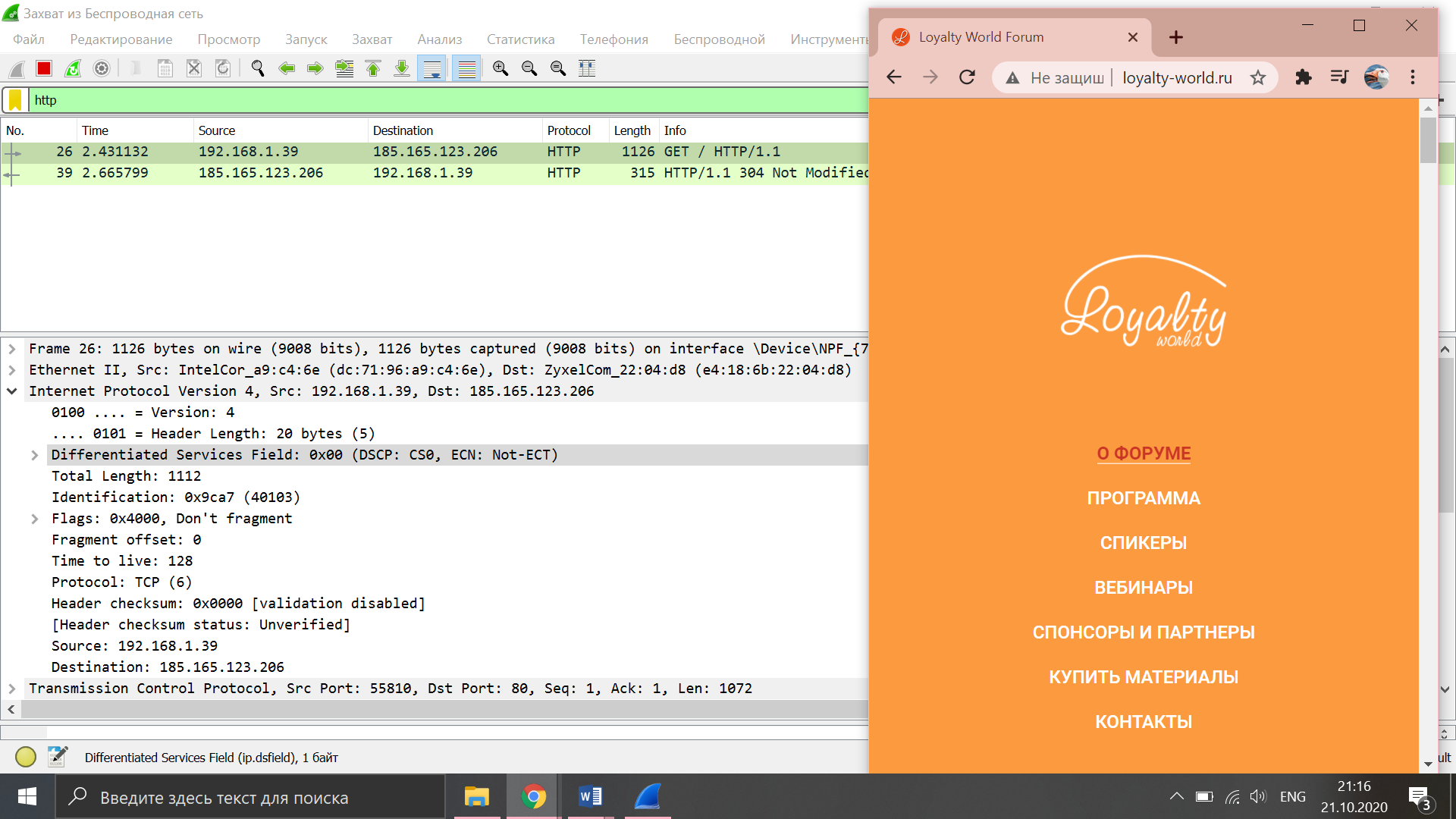


Мой IP-адрес: 192.168.1.39

В заголовке IP 20 байт, в поле данных 72 байта.

TTL( Time To Live) -1.

Задание 2.

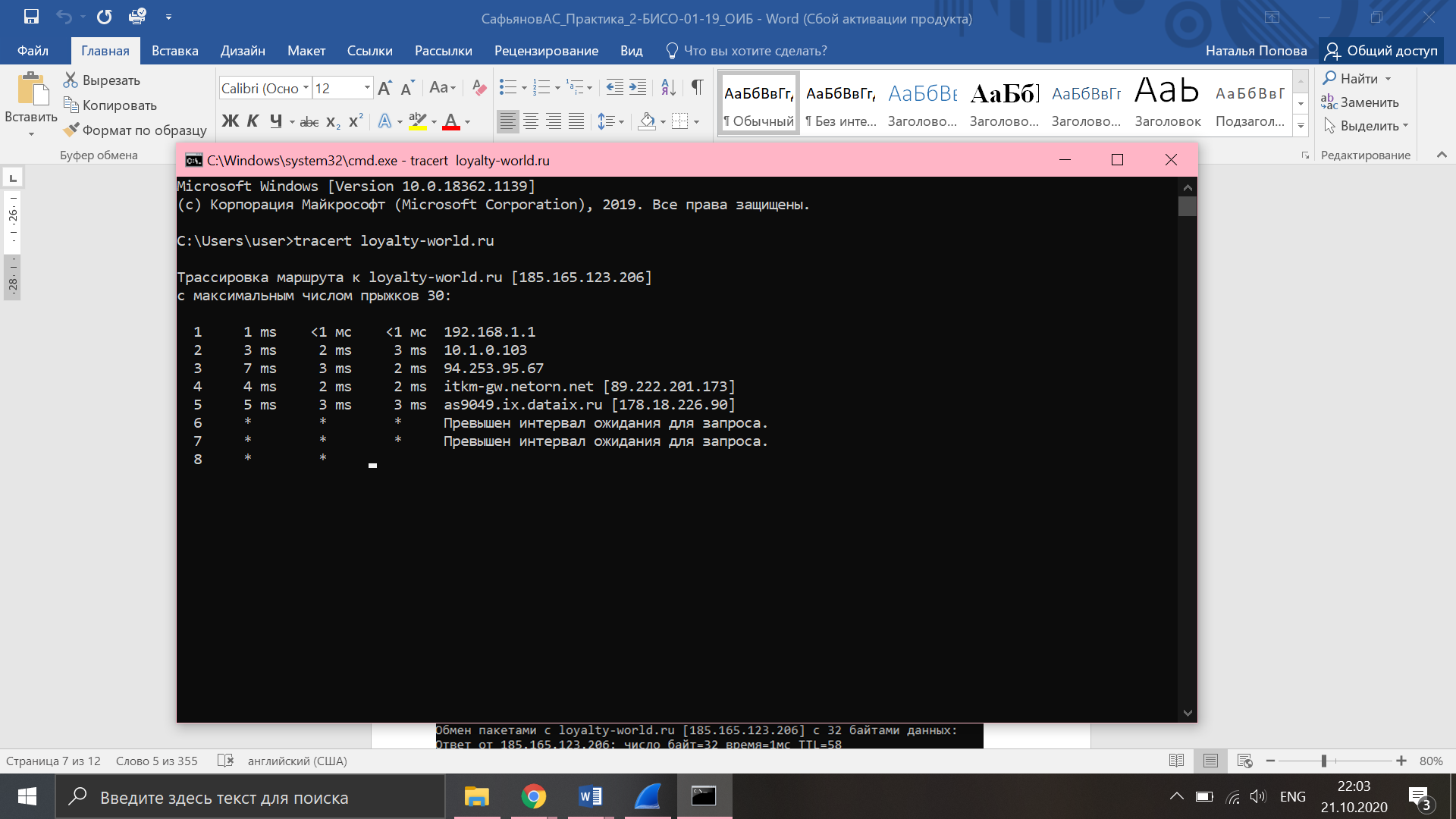


Версия HTTP 1.1

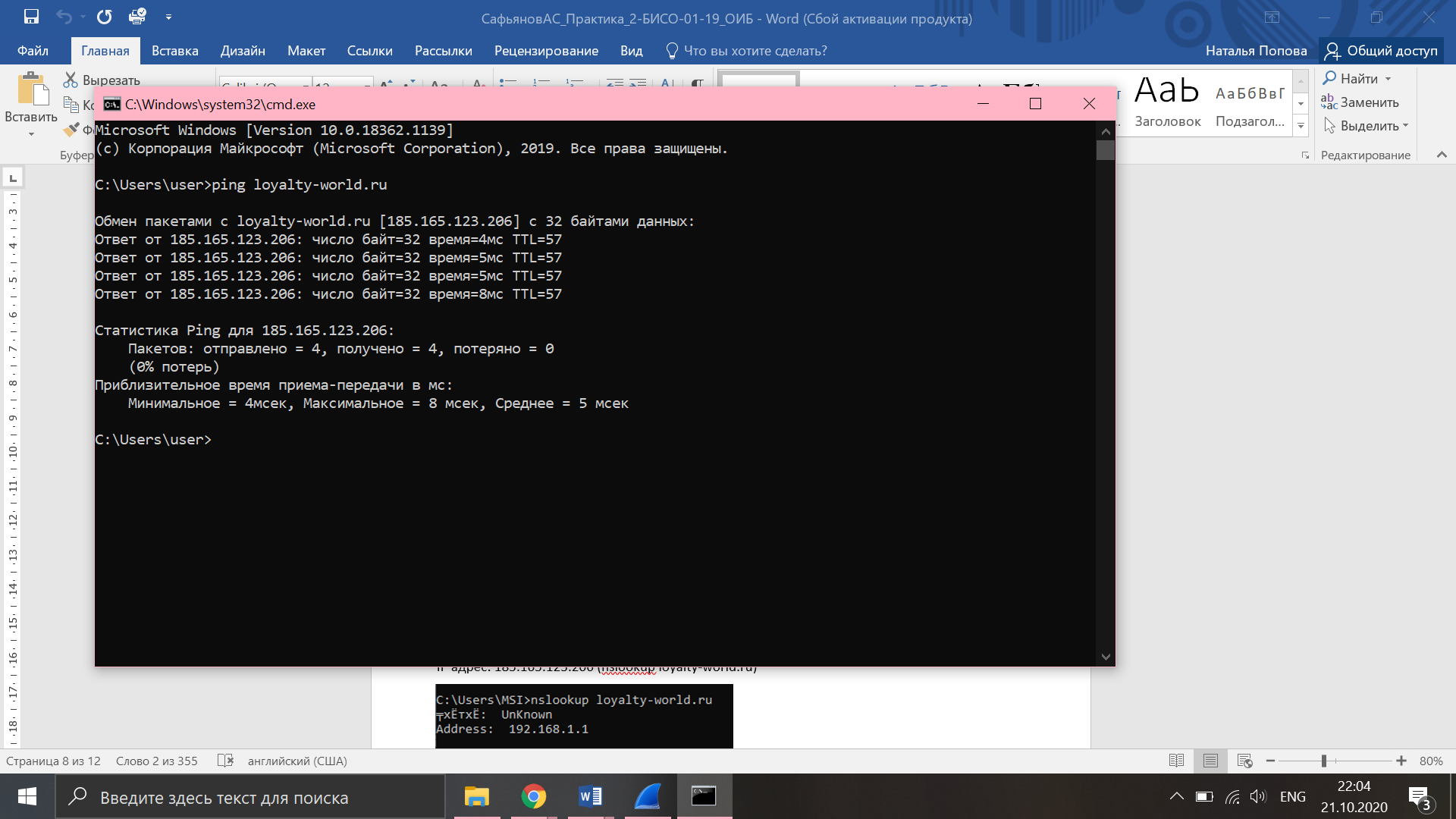
IP компьютера: 192.168.1.39 ; IP адрес сервера: 185.165.123.206

Код состояния HTTP: 304

Длина тела сообщения: 1126



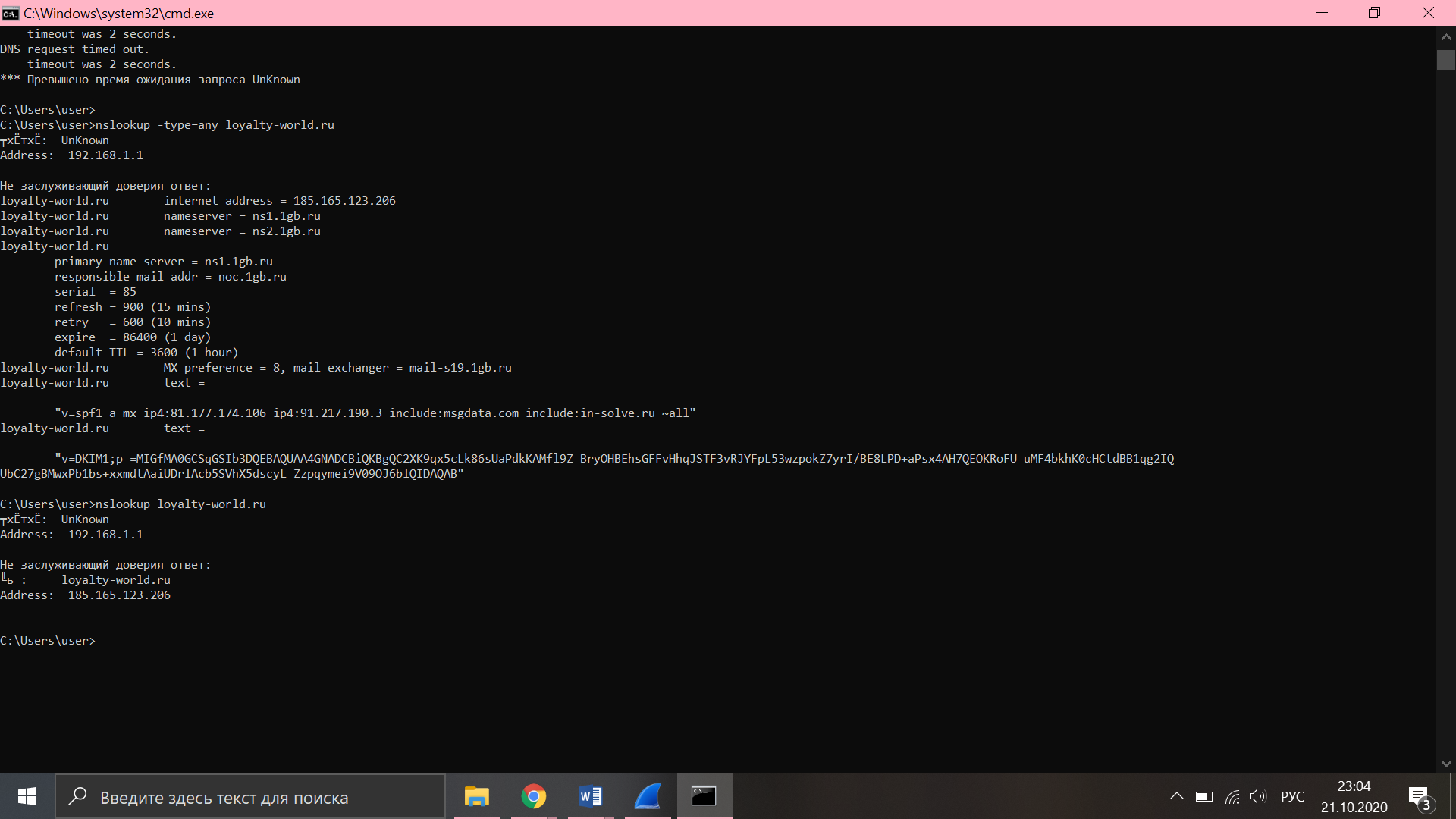
IP адрес: 185.165.123.206 (tracert loyalty-world.ru)



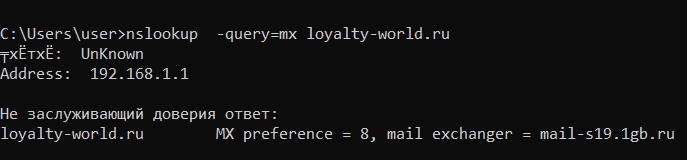
IP адрес: 185.165.123.206 (ping loyalty-world.ru)

Задание 3.

Nslookup-сопоставление доменного имени IP-адресу ресурса



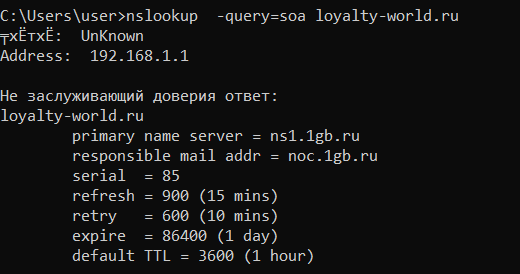
-query=mx



Выводит соответствующие доменному имени почтовые сервера.

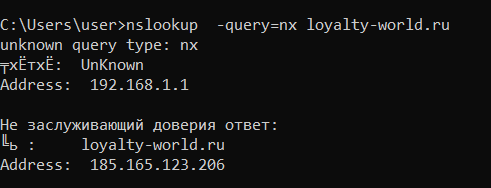
Приоритет MX preference- меньше приоритет -> больше вероятность отправки через этот сервер.

-query=soa



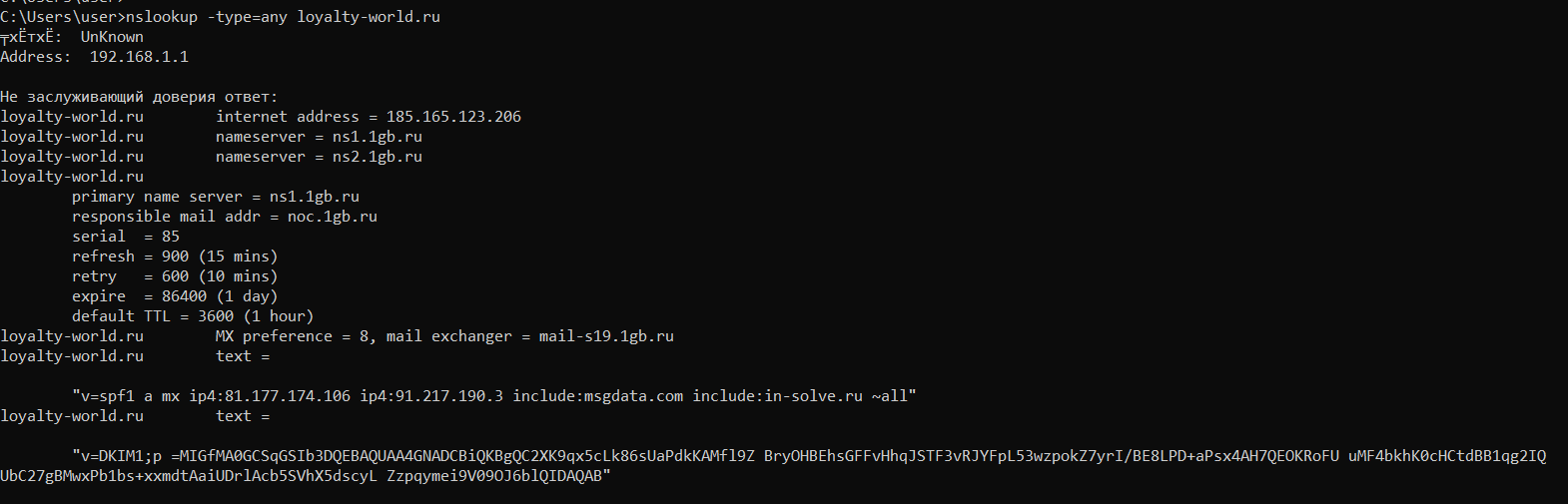
Выводит информацию о зоне домена, адресе его администратора, серийном номере файла зоны и о интервалах: через которое проверится серийный номер, для повторного соединения, хранения кэша и минимального времени хранения.

-query=ns



Показывает соответствие доменных имен DNS-серверам.

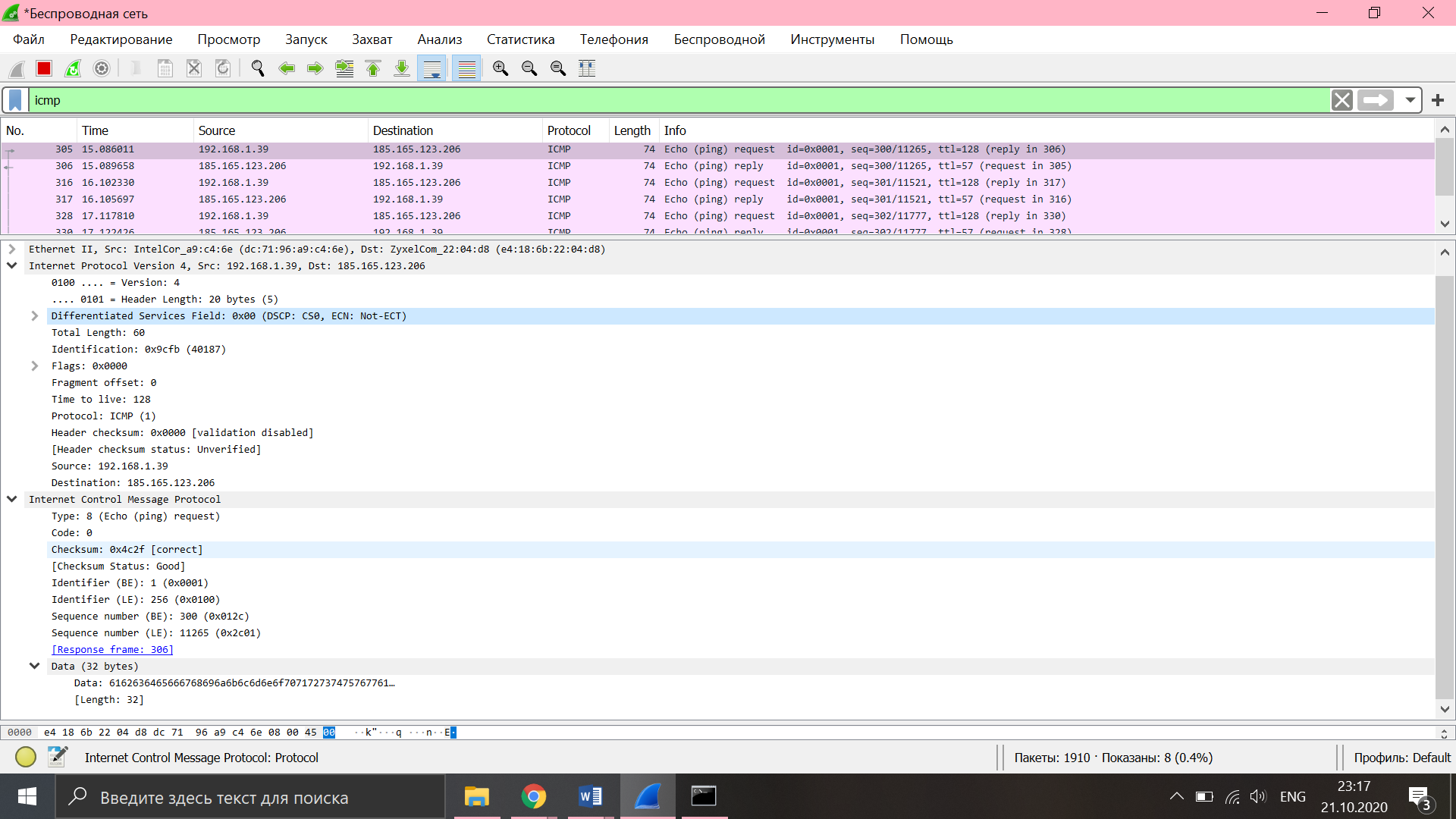
-type=any

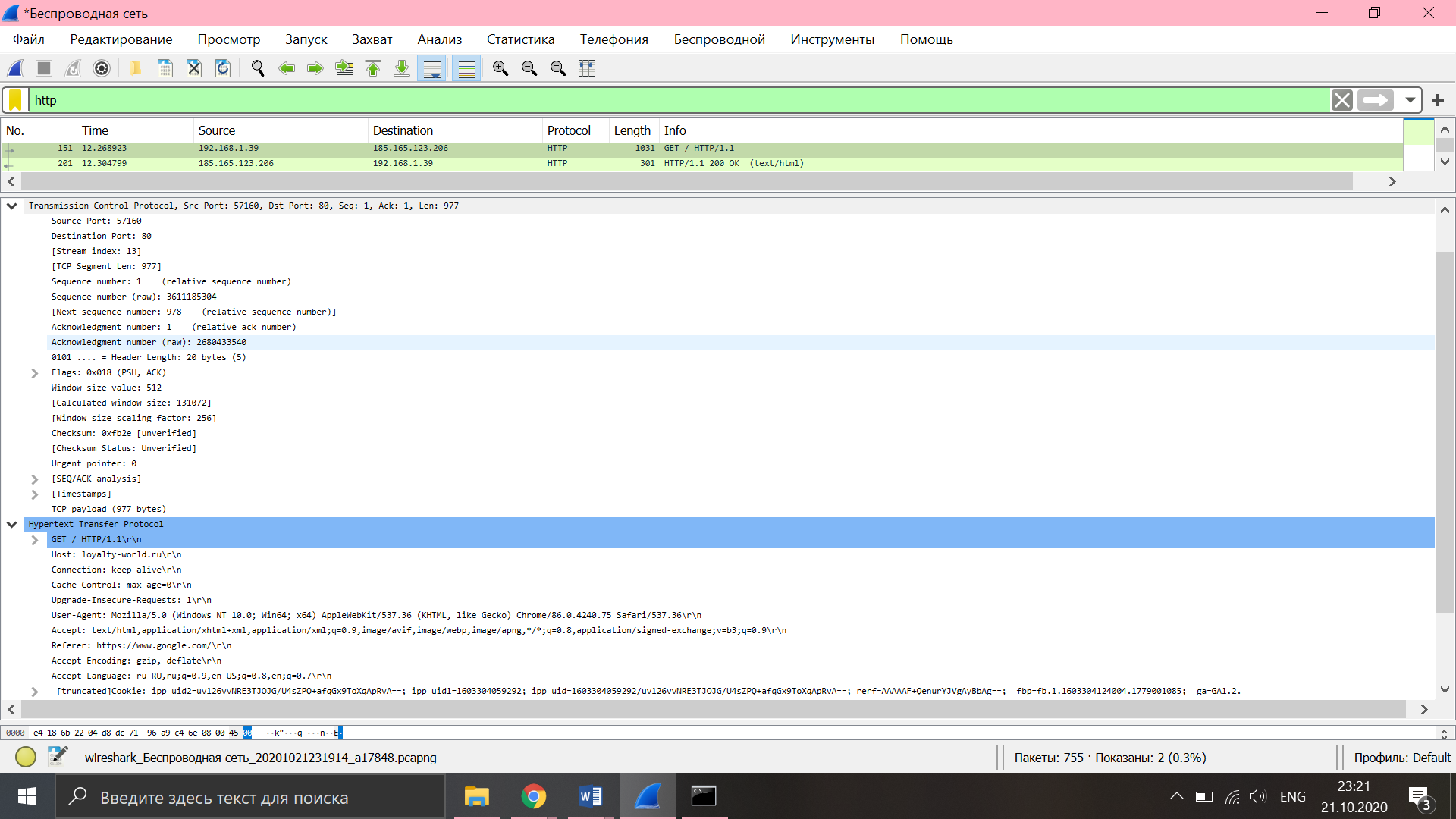


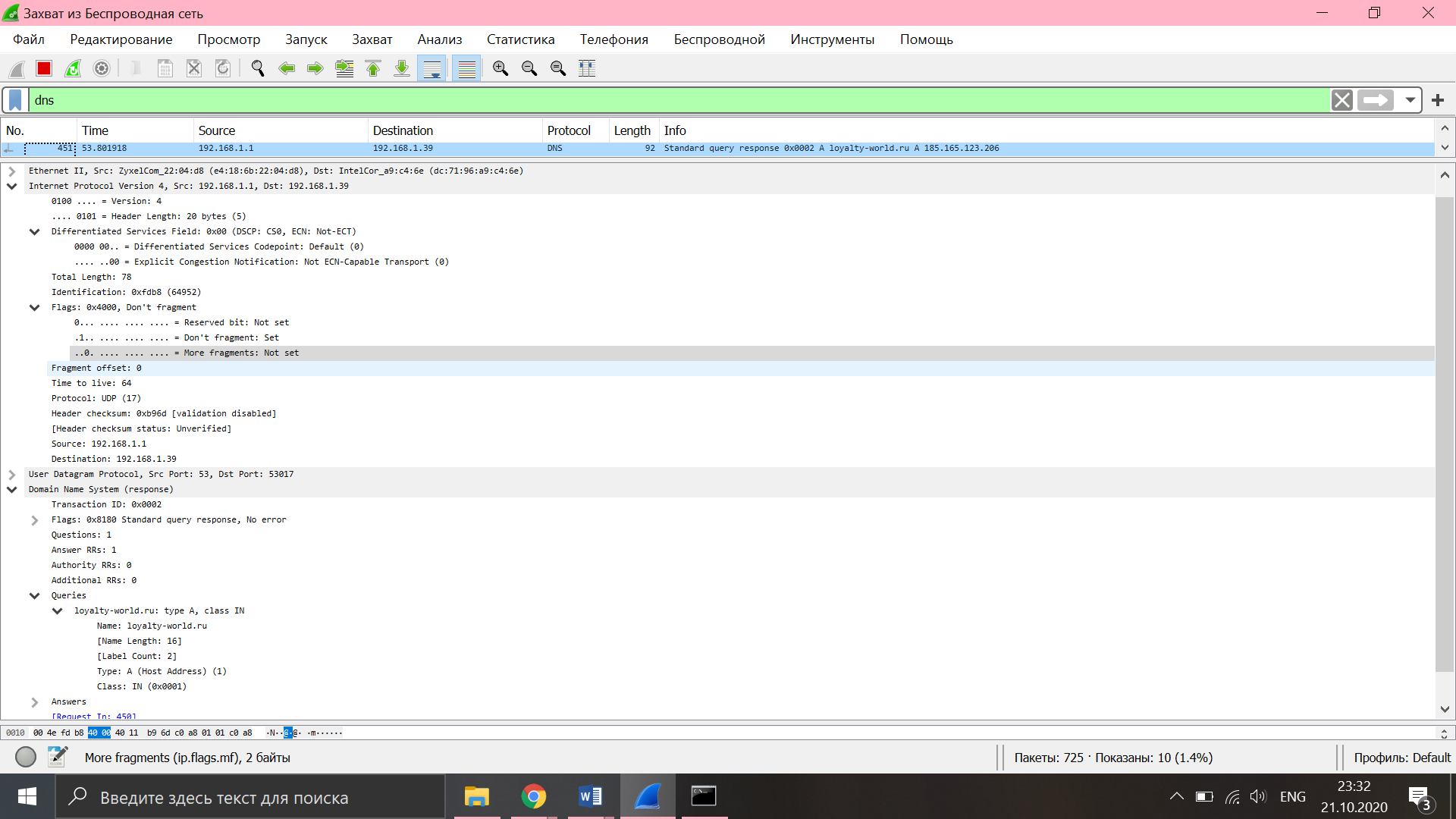
Определение всех типов DNS-записей

Задание 4.

Трафик сайта







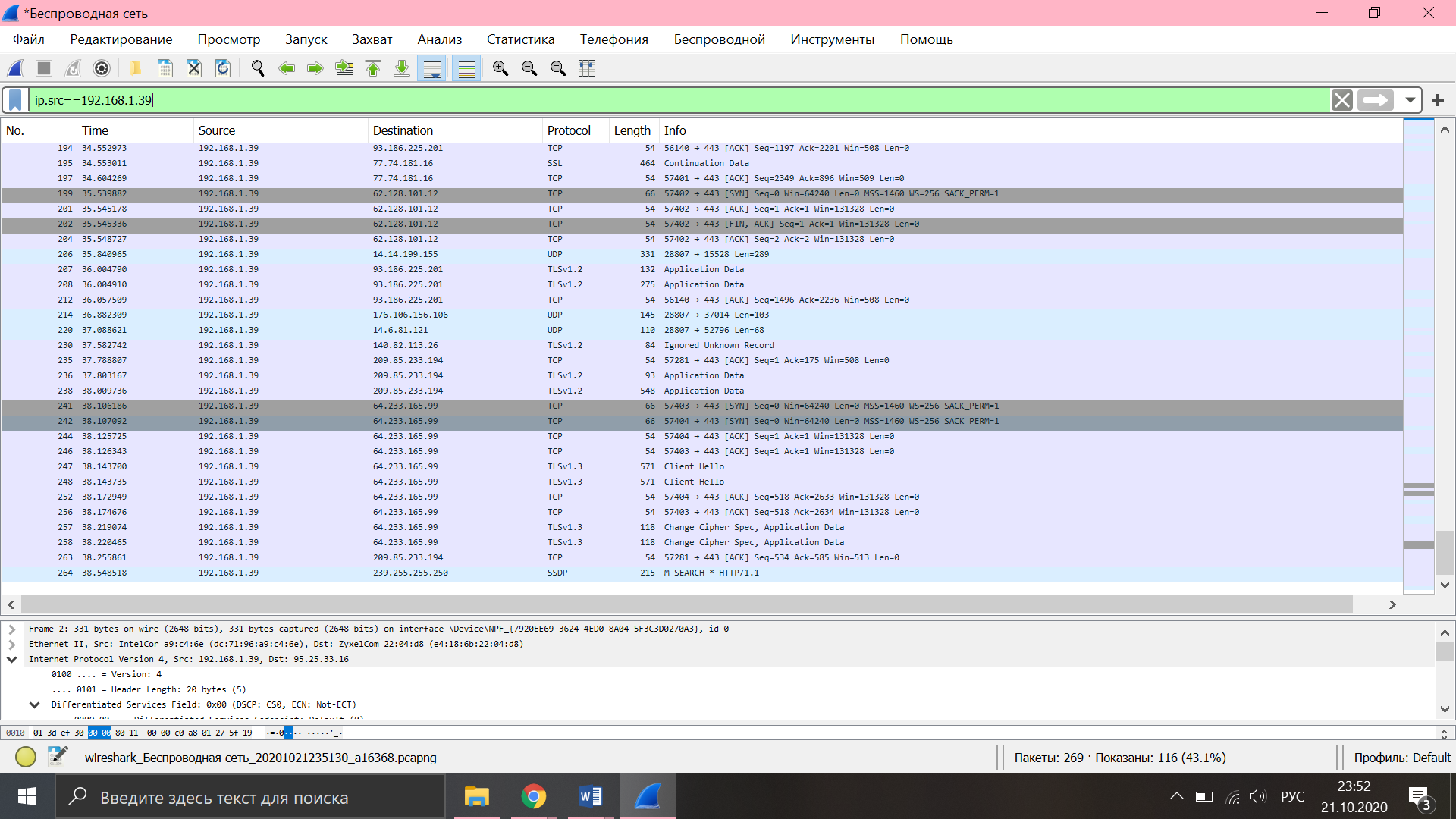
Задание 5.

Фильтры

**ip.src**

Показывает перехваченные пакеты отправителя, отсортированные по его IP.

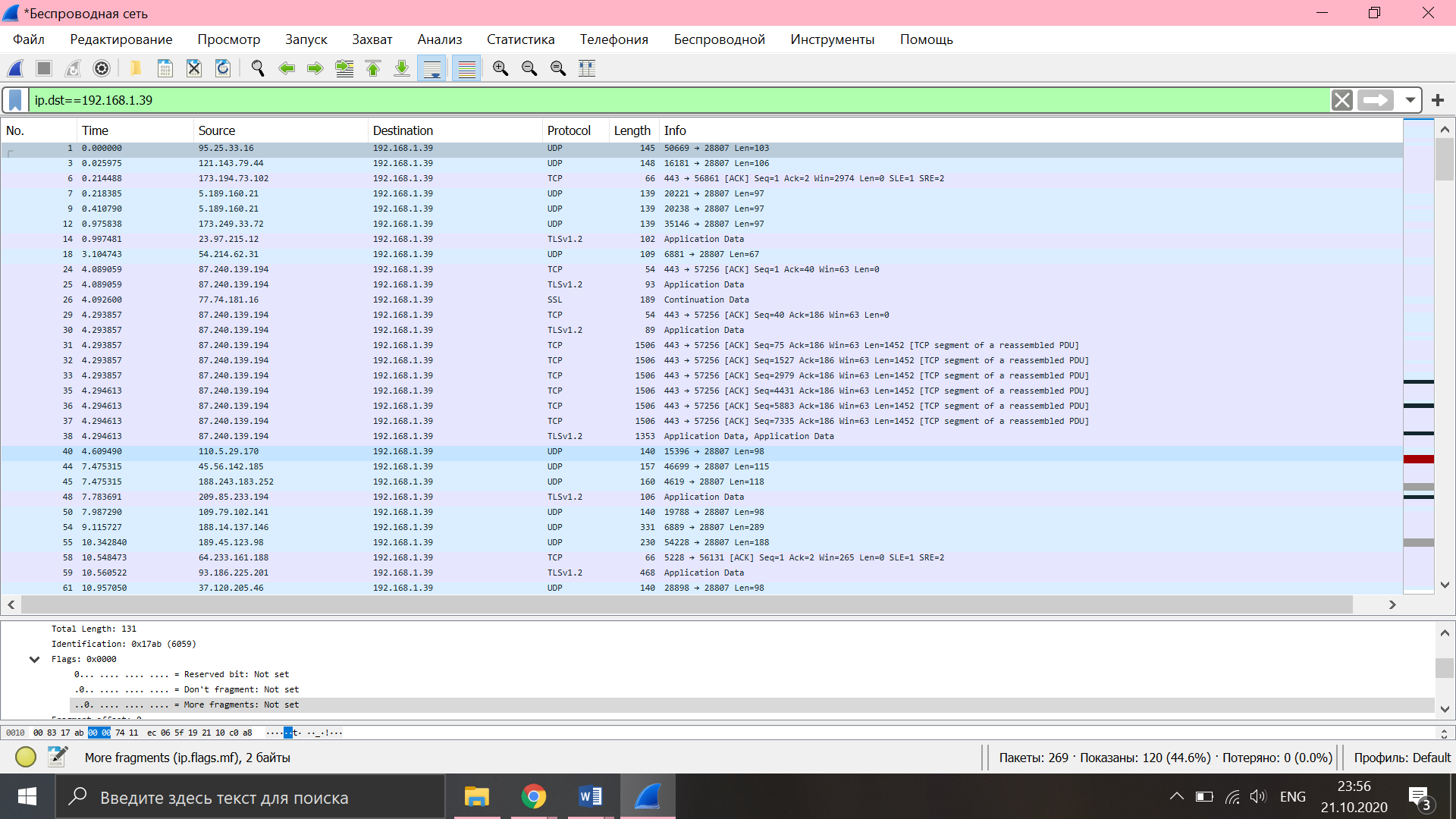
ip.src==192.168.1.39



**ip.dst**

Показывает перехваченные пакеты получателя, отсортированные по его IP.

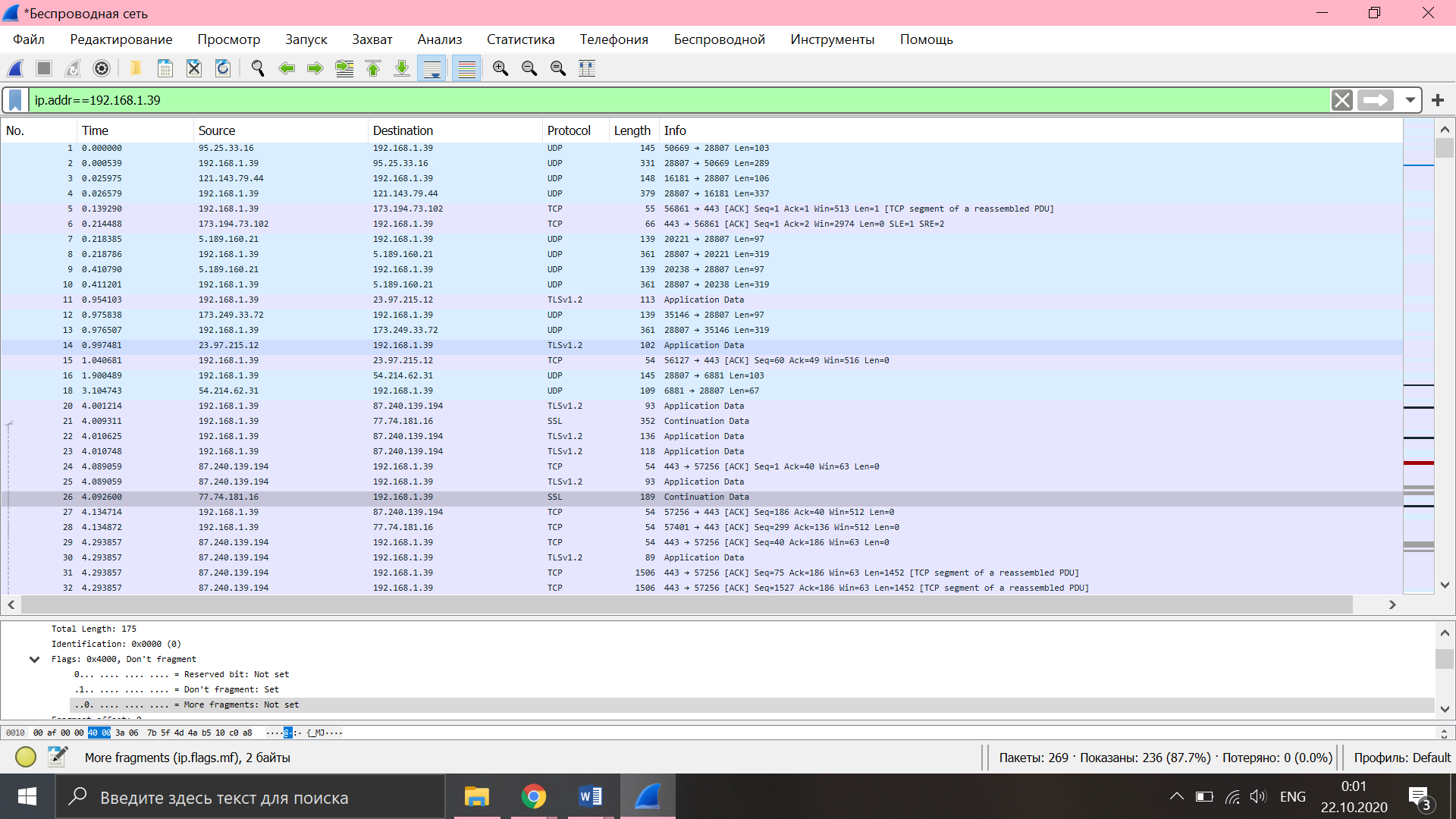
ip.dst==192.168.1.39



**ip.addr**

Показывает перехваченные пакеты отправителя или получателя по его IP.

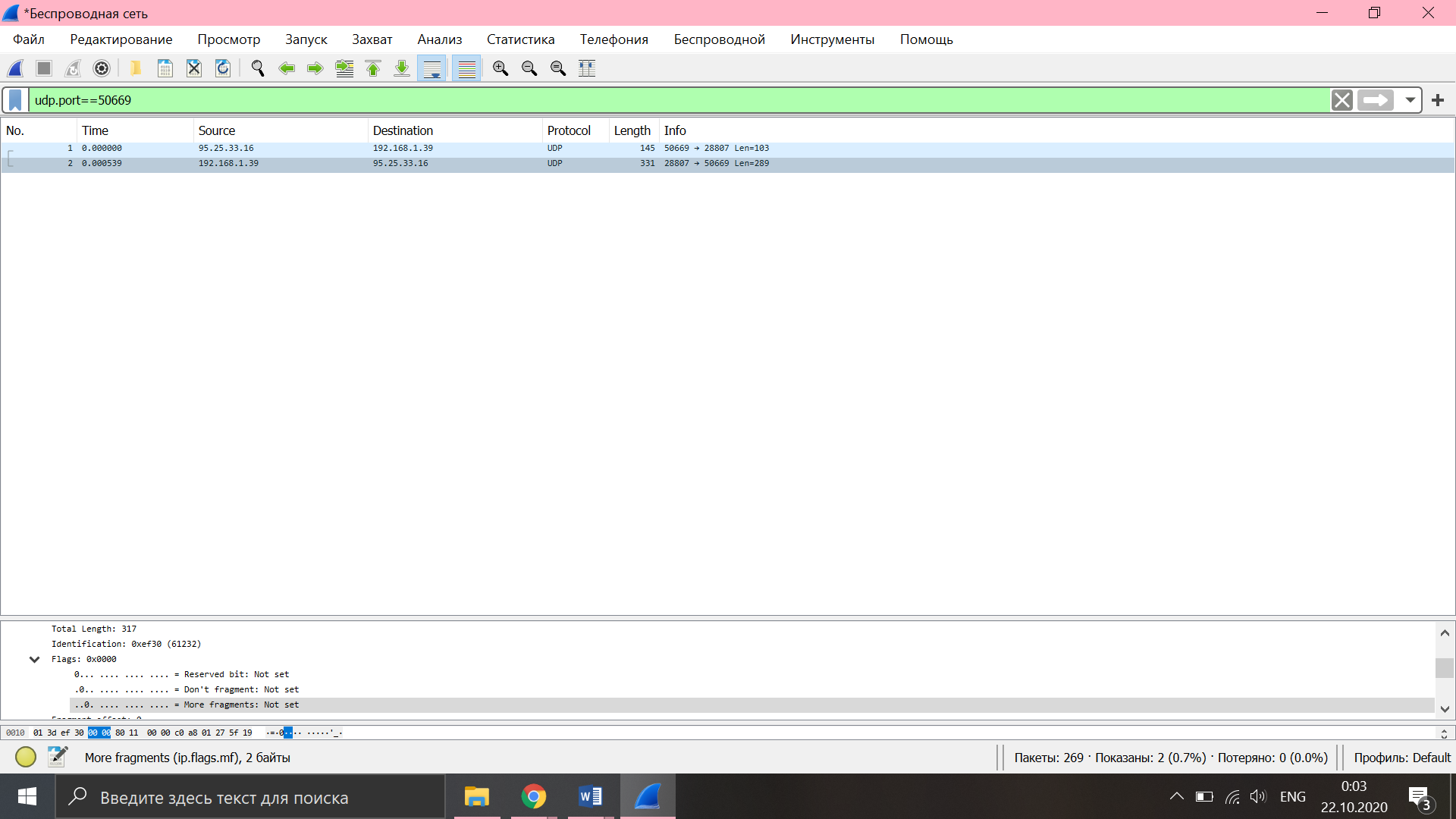
ip.addr==192.168.1.39



**udp.port**

Показывает перехваченные пакеты с udp портом получателя или отправителя.

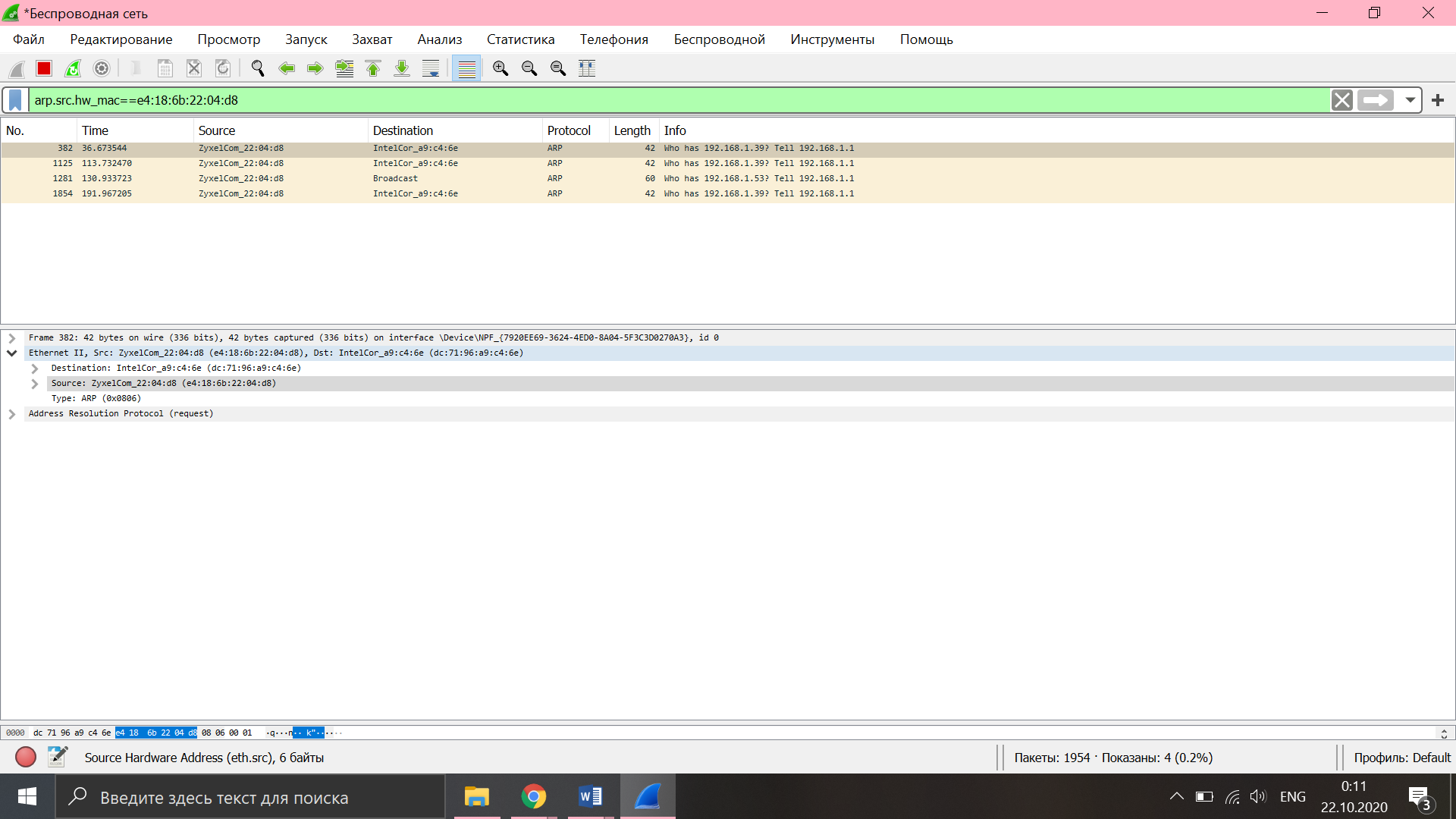
udp.port==50669



**arp.src.hw\_mac**

Показывает перехваченные пакеты протокола ARP c MAC-адресом отправителя.

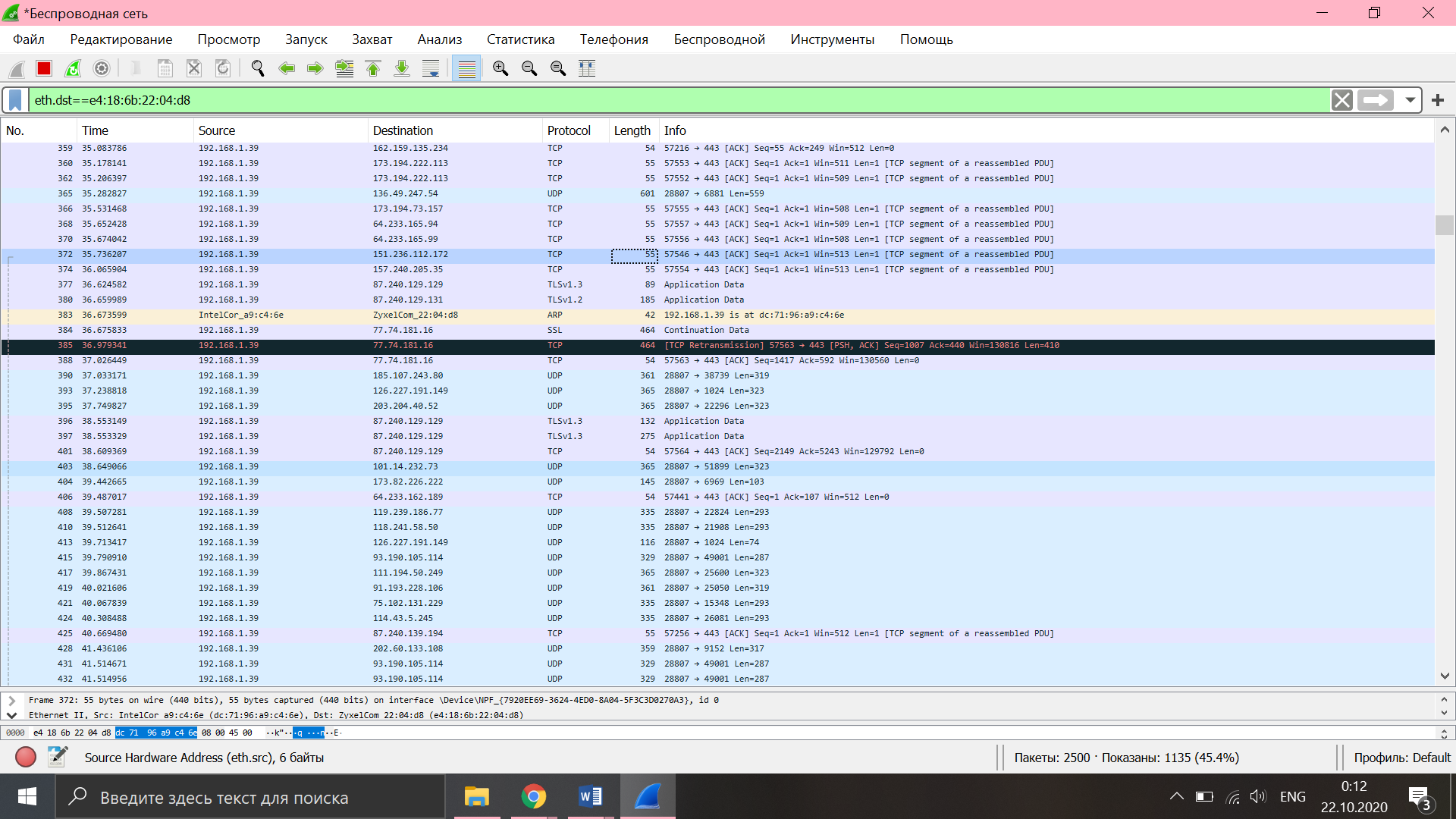
arp.src.hw\_mac==e4:18:6b:22:04:d8



**eth.dst**

Показывает перехваченные пакеты с MAC-адресом получателя.

eth.dst==e4:18:6b:22:04:d8



**eth.src**

Показывает перехваченные пакеты с MAC-адресом отправителя.

eth.src==e4:18:6b:22:04:d8

