|  |  |  |
| --- | --- | --- |
| |  | | --- | | 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 | Шагалина Алина Денисовна  Аккаунт github: https://github.com/Evzdrafi |
|  |

Москва 2020

Wireshark

1.

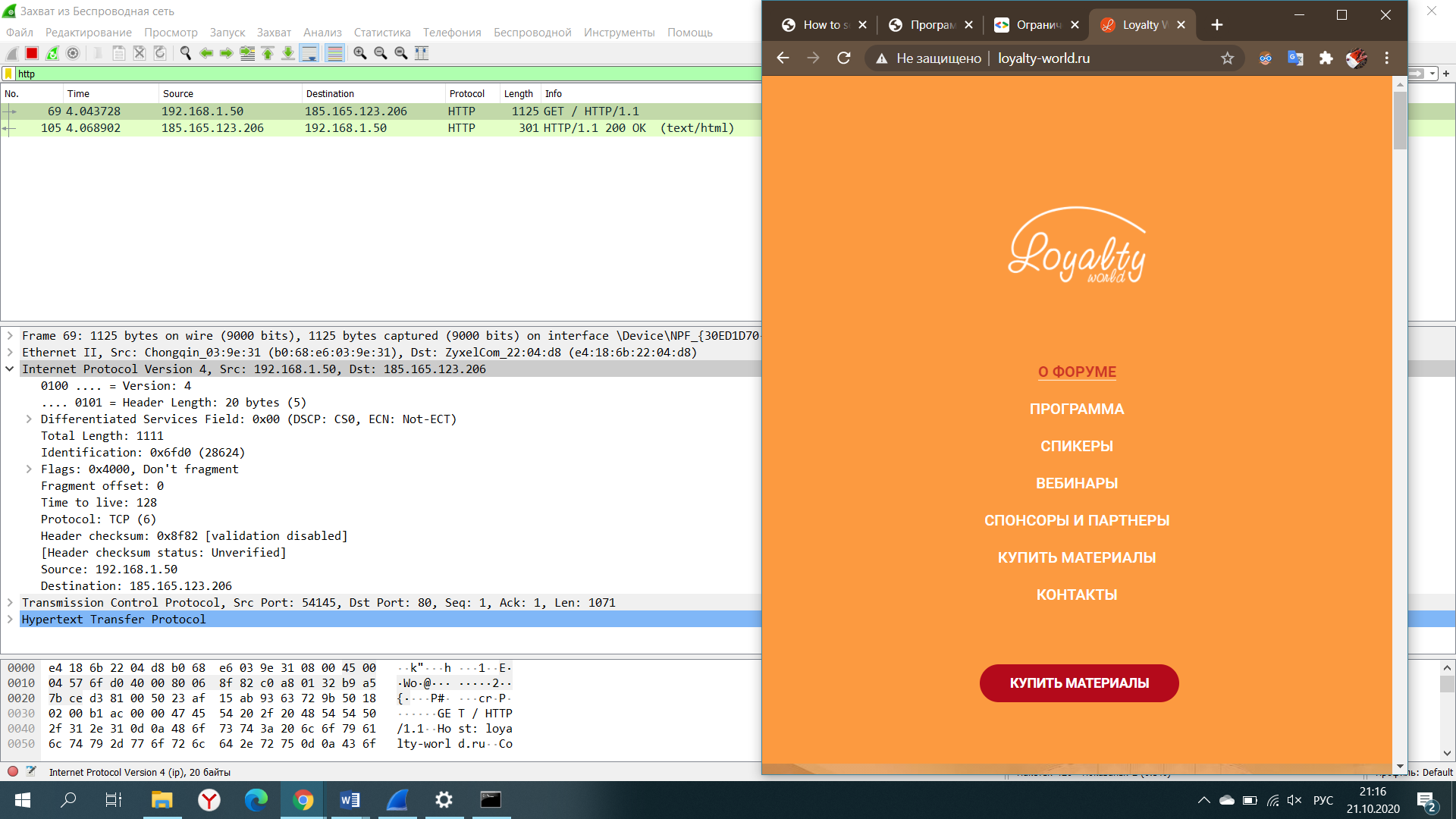


Мой IP-4: 192.168.1.50

В заголовке 20 байт, в поле данных 72 байта

TTL = 1.

2.



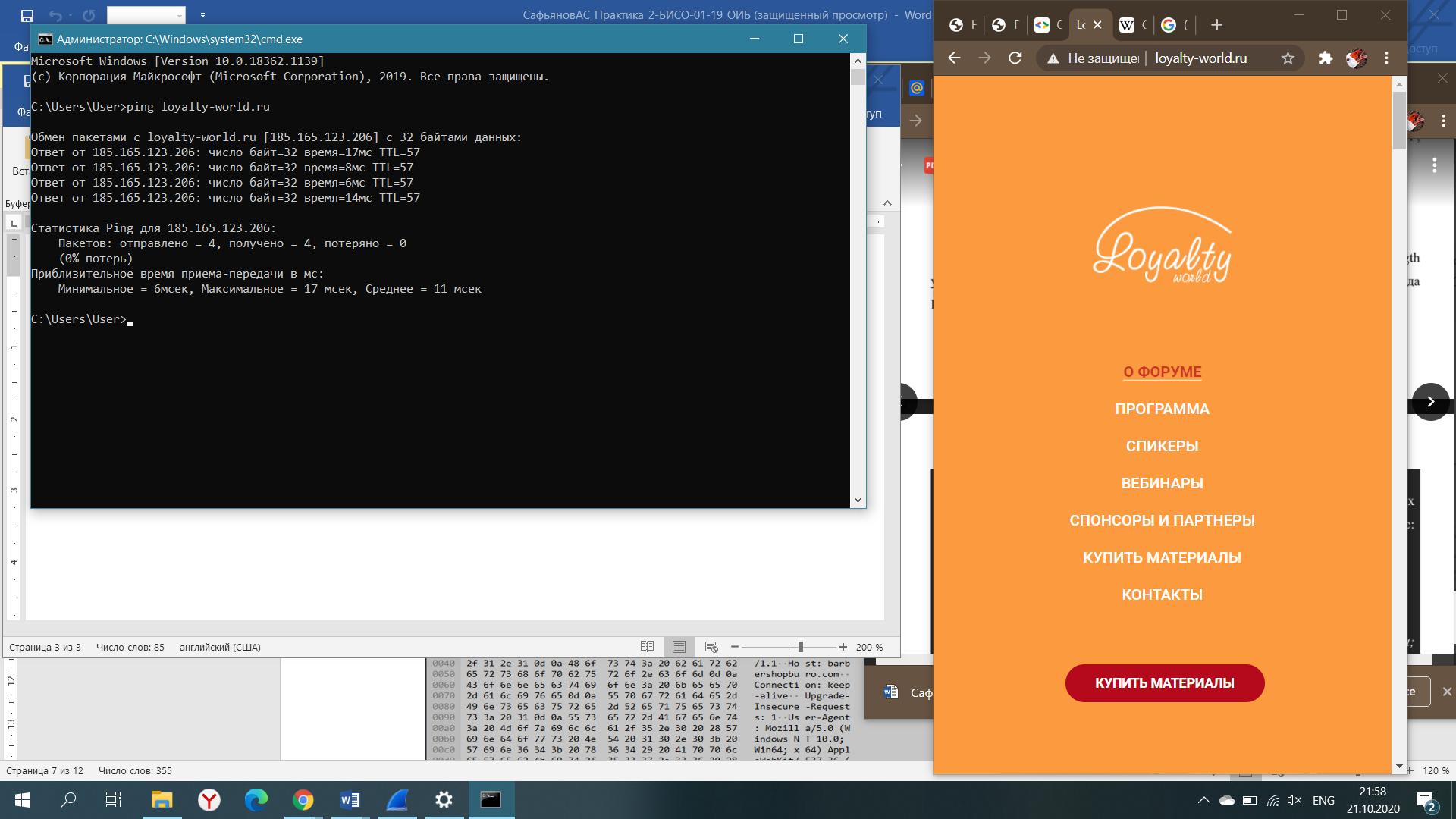
Версия HTTP 1.1

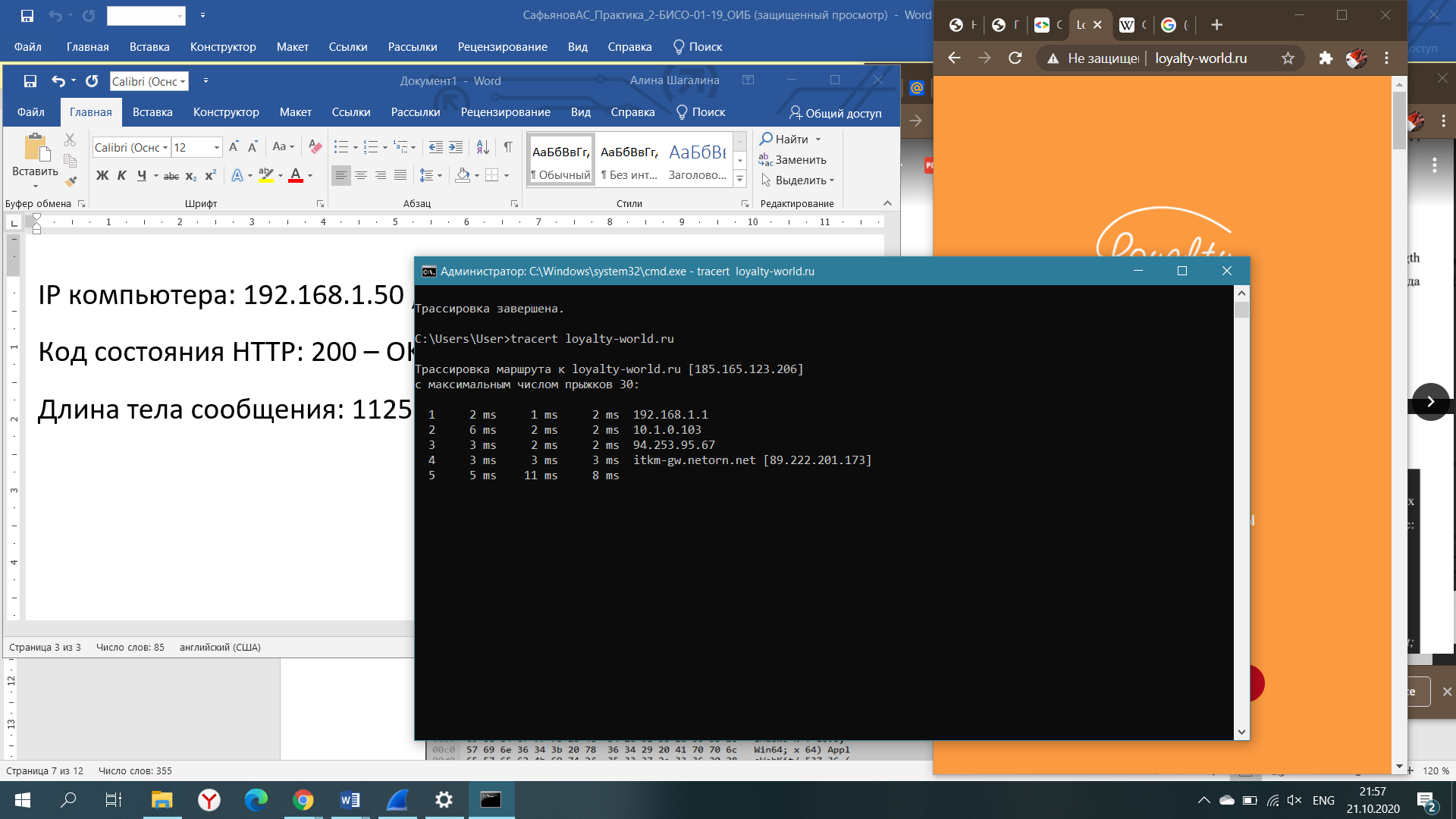
IP компьютера: 192.168.1.50 , IP адрес сервера: 185.165.123.206

Код состояния HTTP: 200 – OK

Длина тела сообщения: 1125

Определение IP адреса с помощью команд консоли:

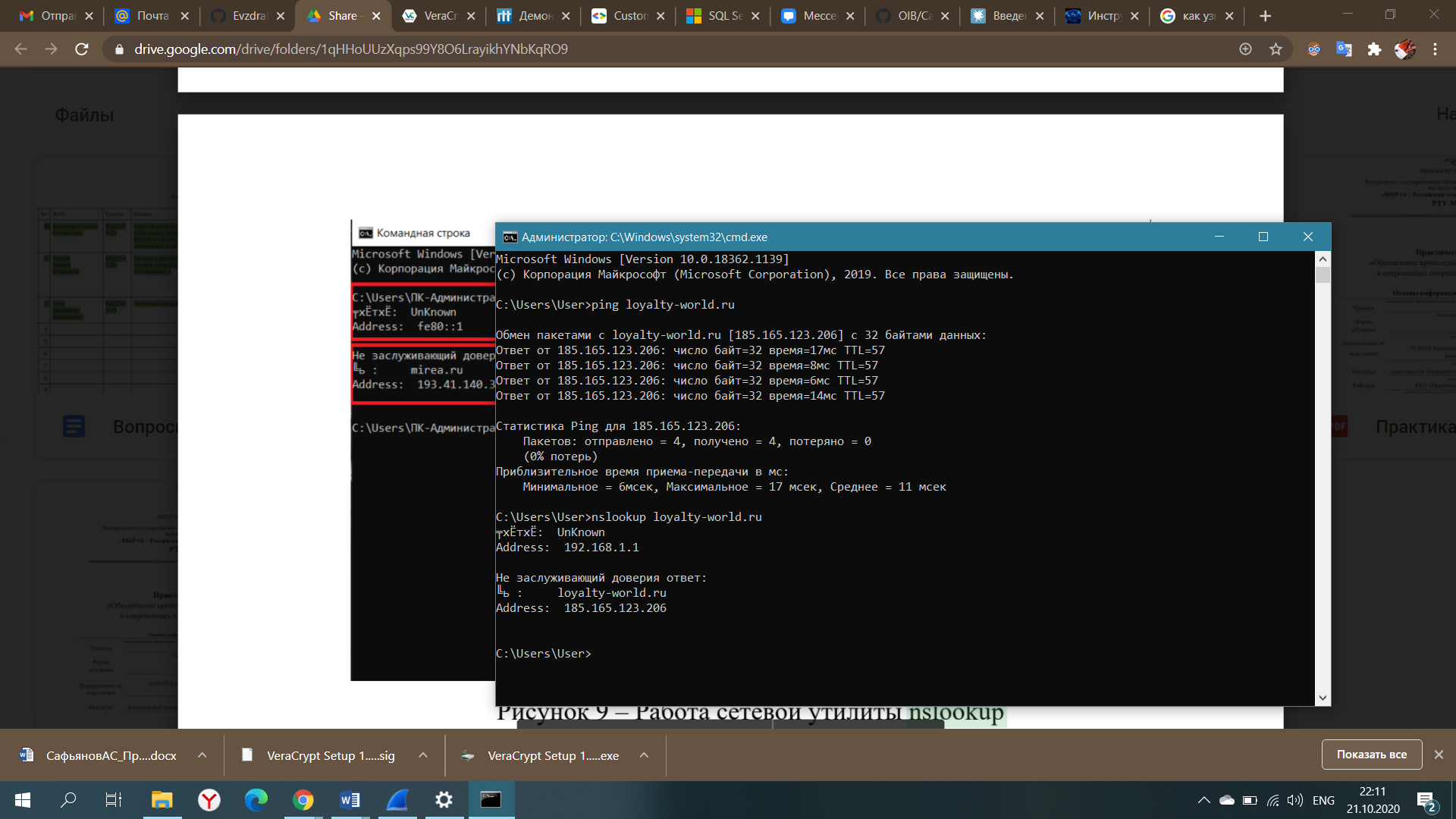




IP адрес ресурса: 185.165.123.206

3.

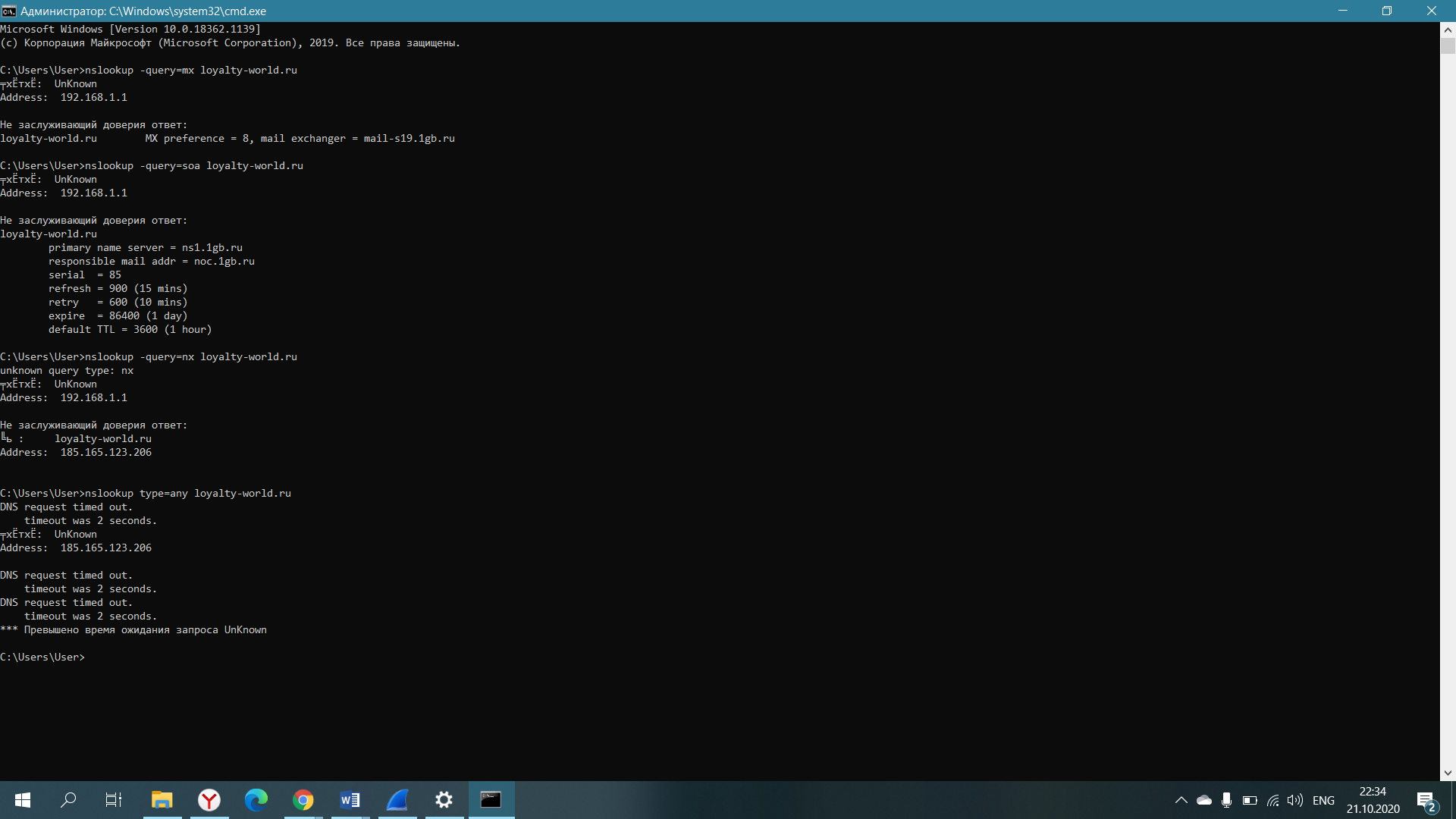
Nslookup – это сопоставление доменного имени IP-адресу ресурса:



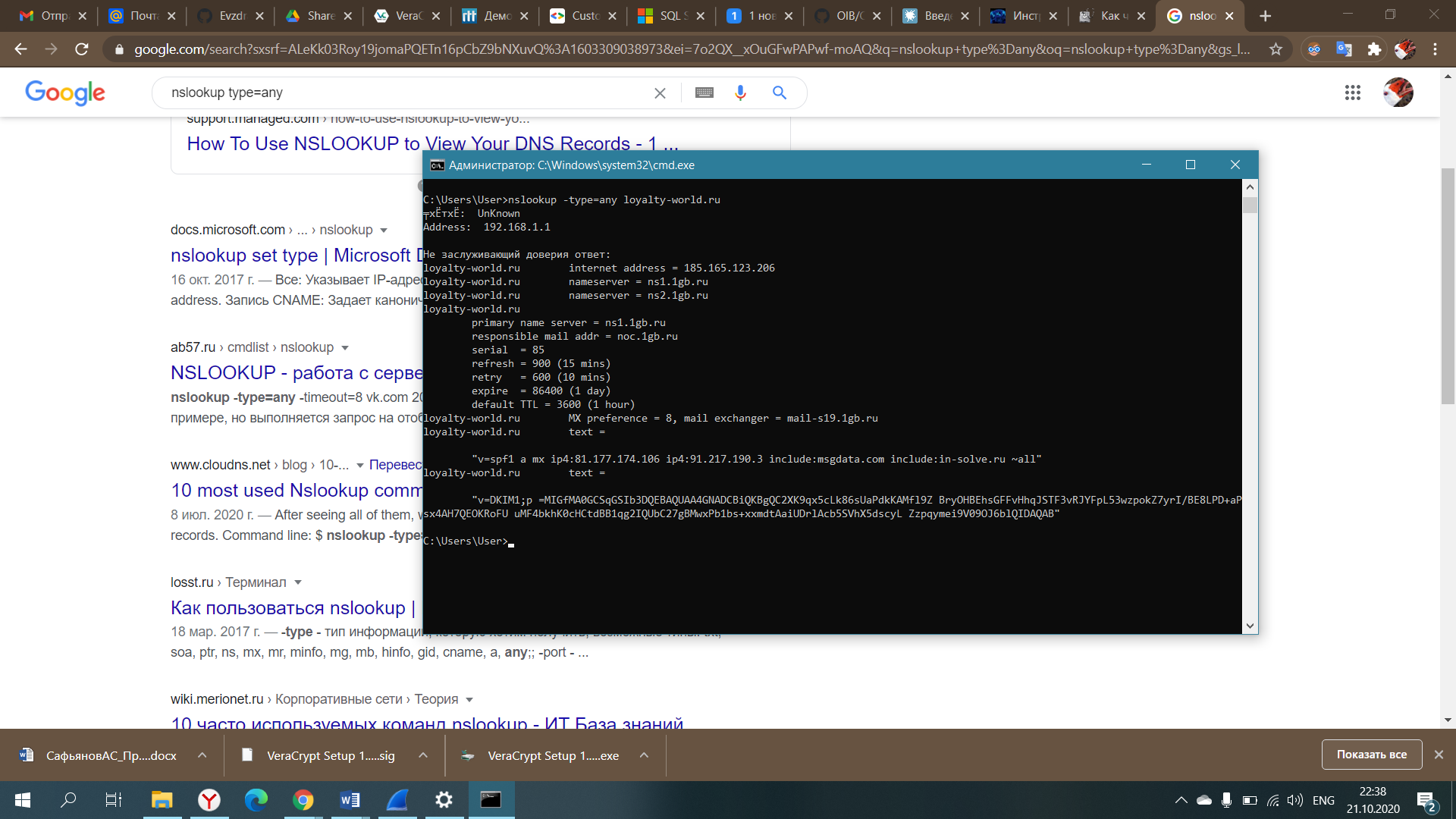
Nslookup -query=mx выводит записи о почтовых серверах

Nslookup -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.

Nslookup -query=ns выводит соответствие доменных имен DNS-серверам

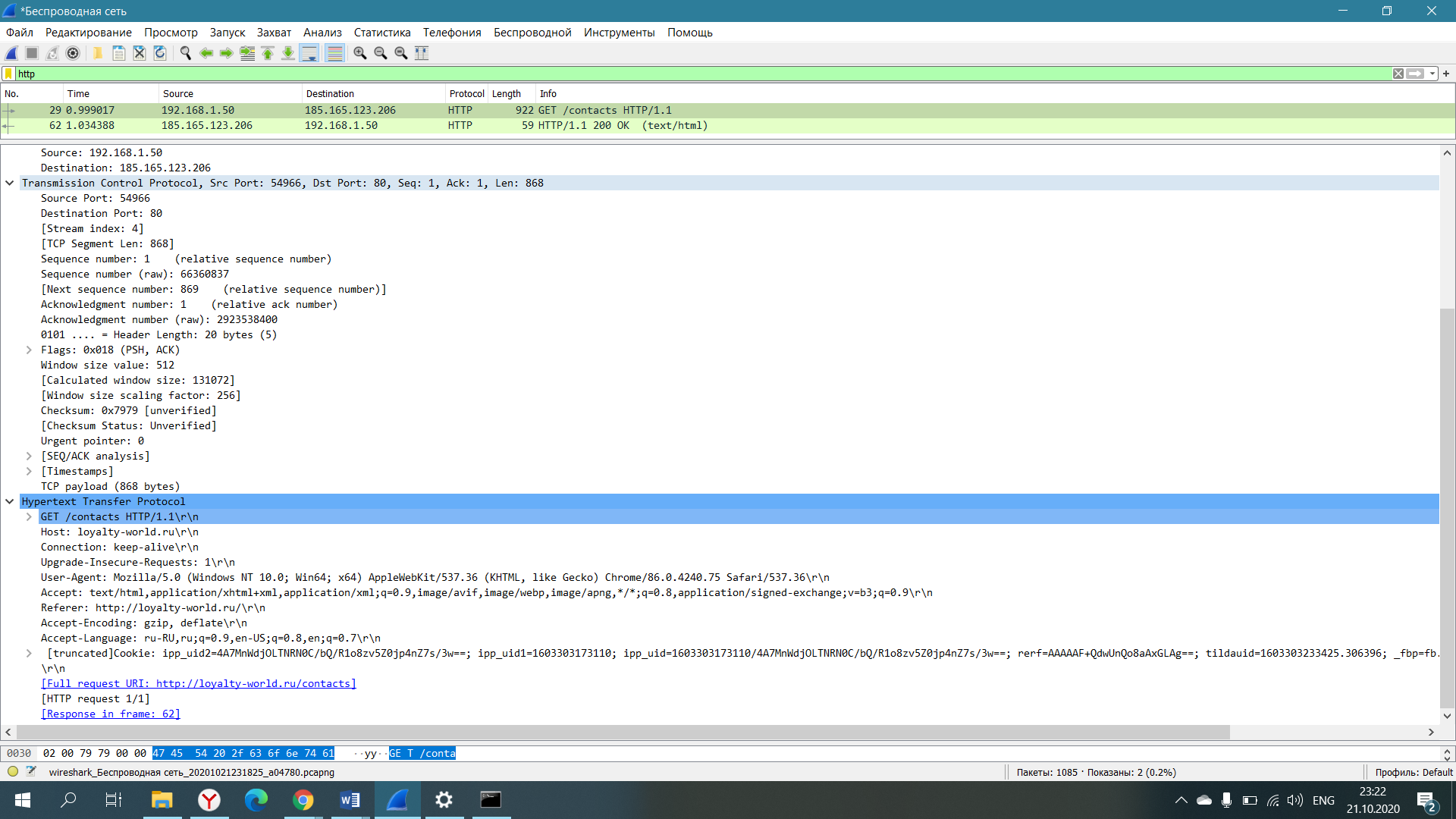


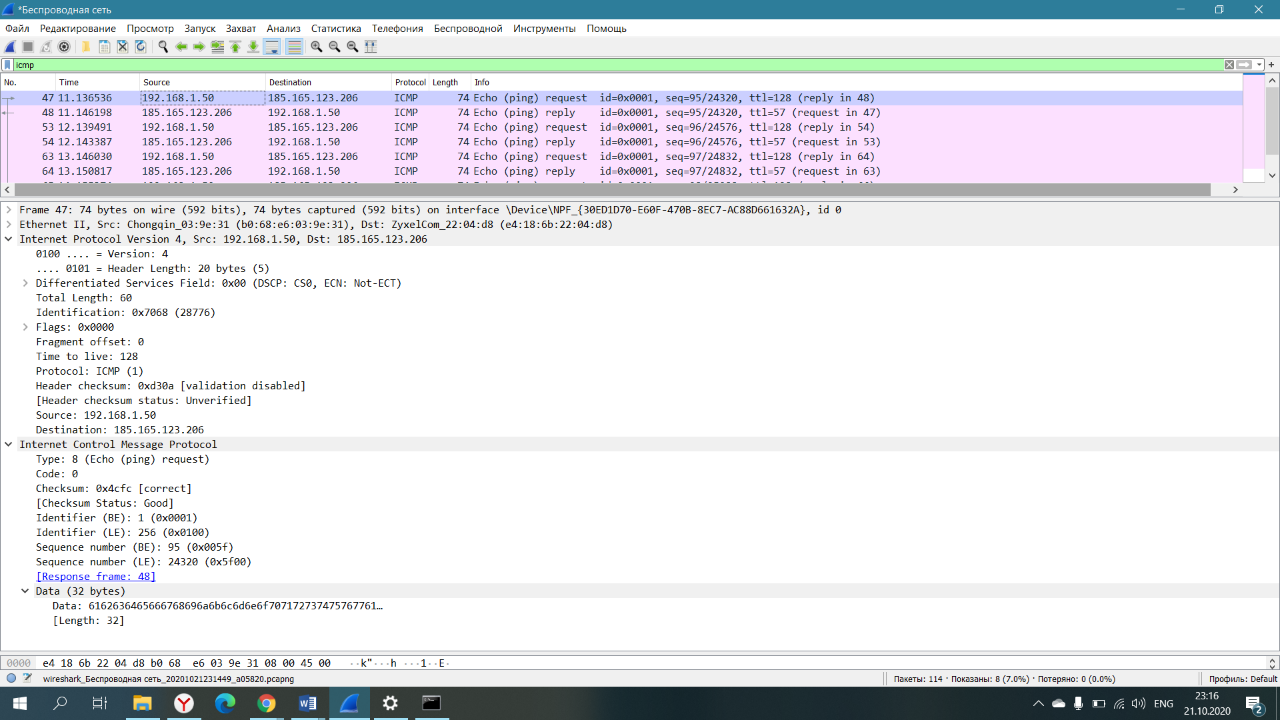
Nslookup –type=any: определение всех типов DNS-записей

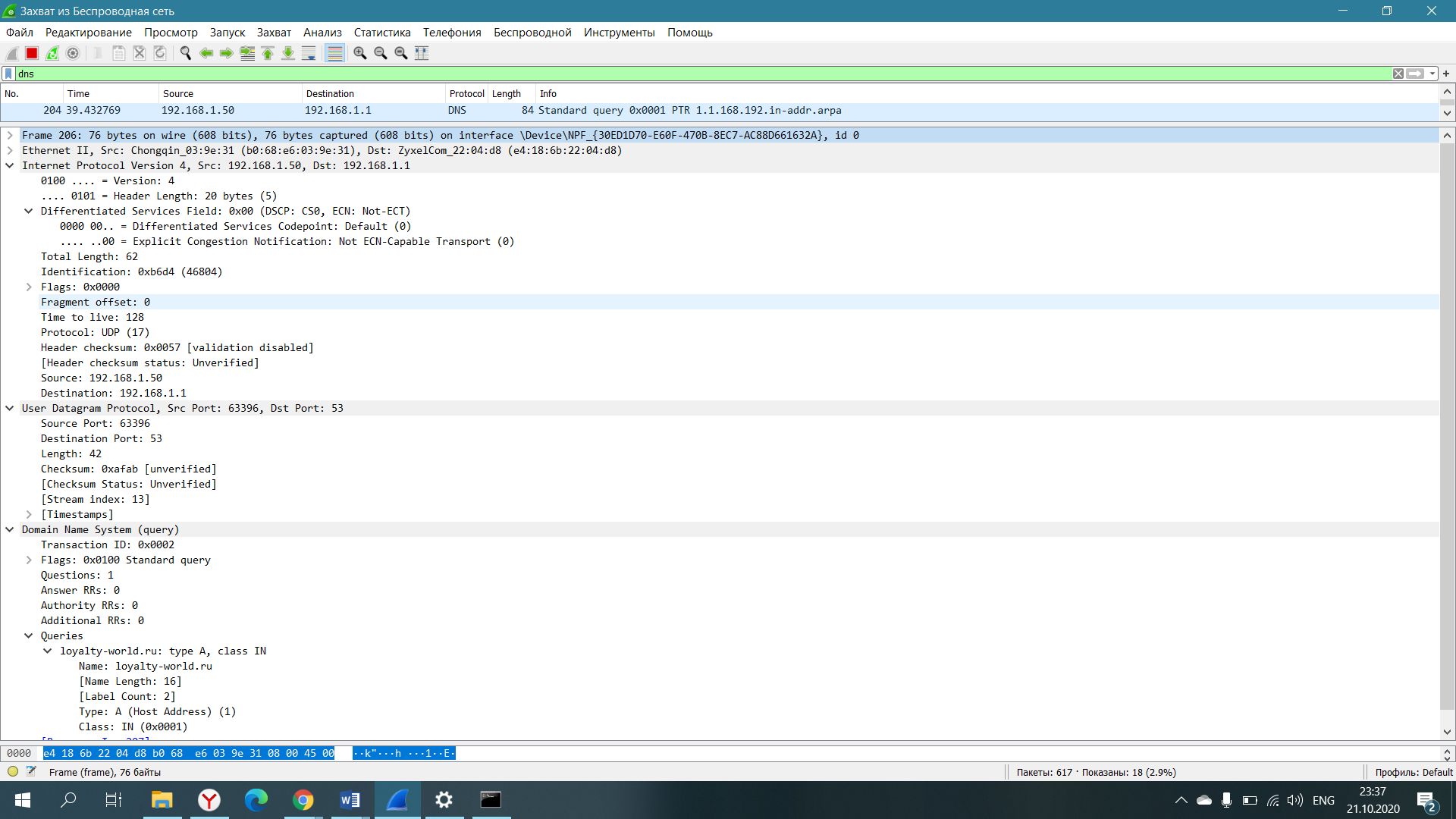


4.

трафик



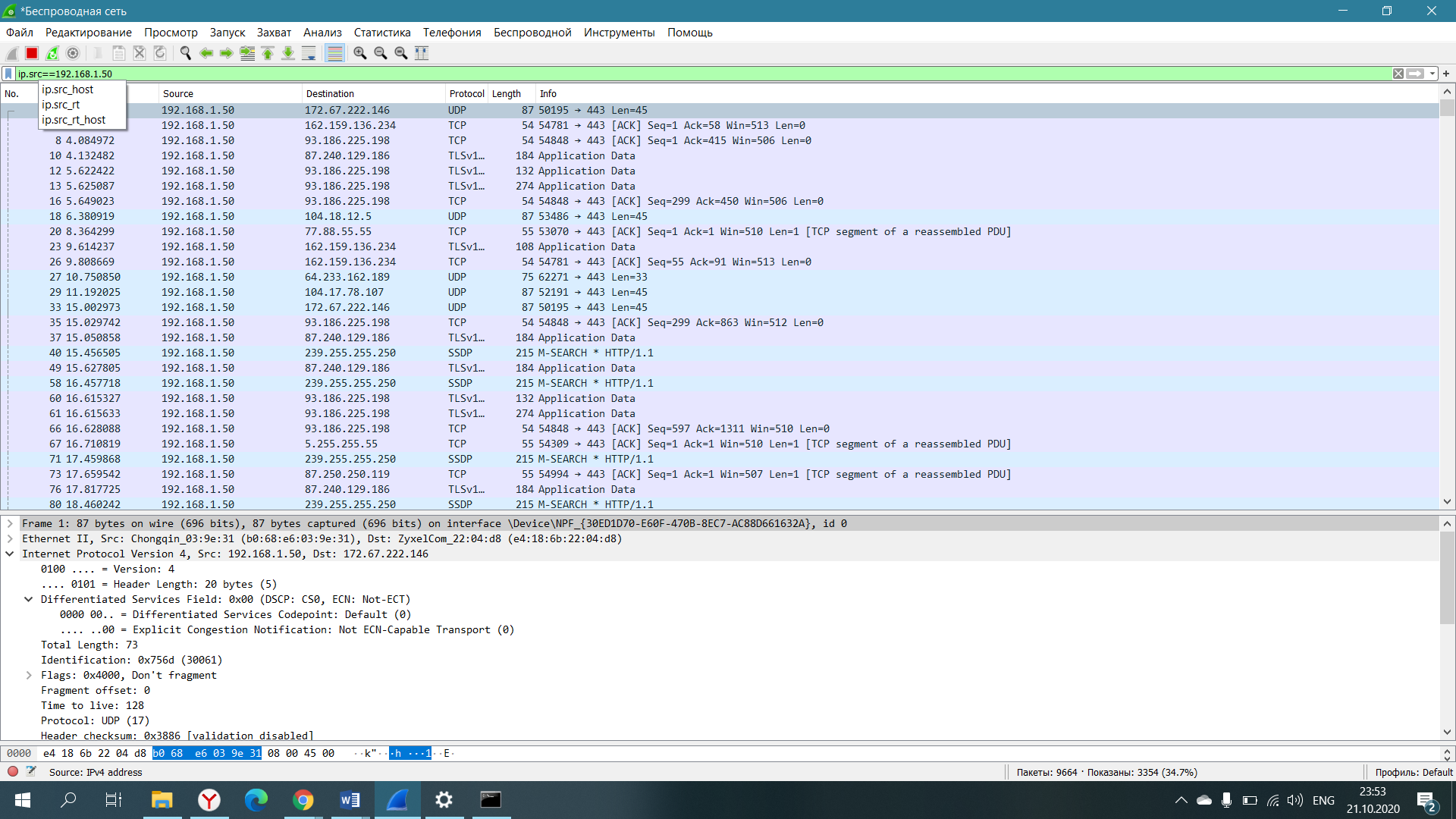




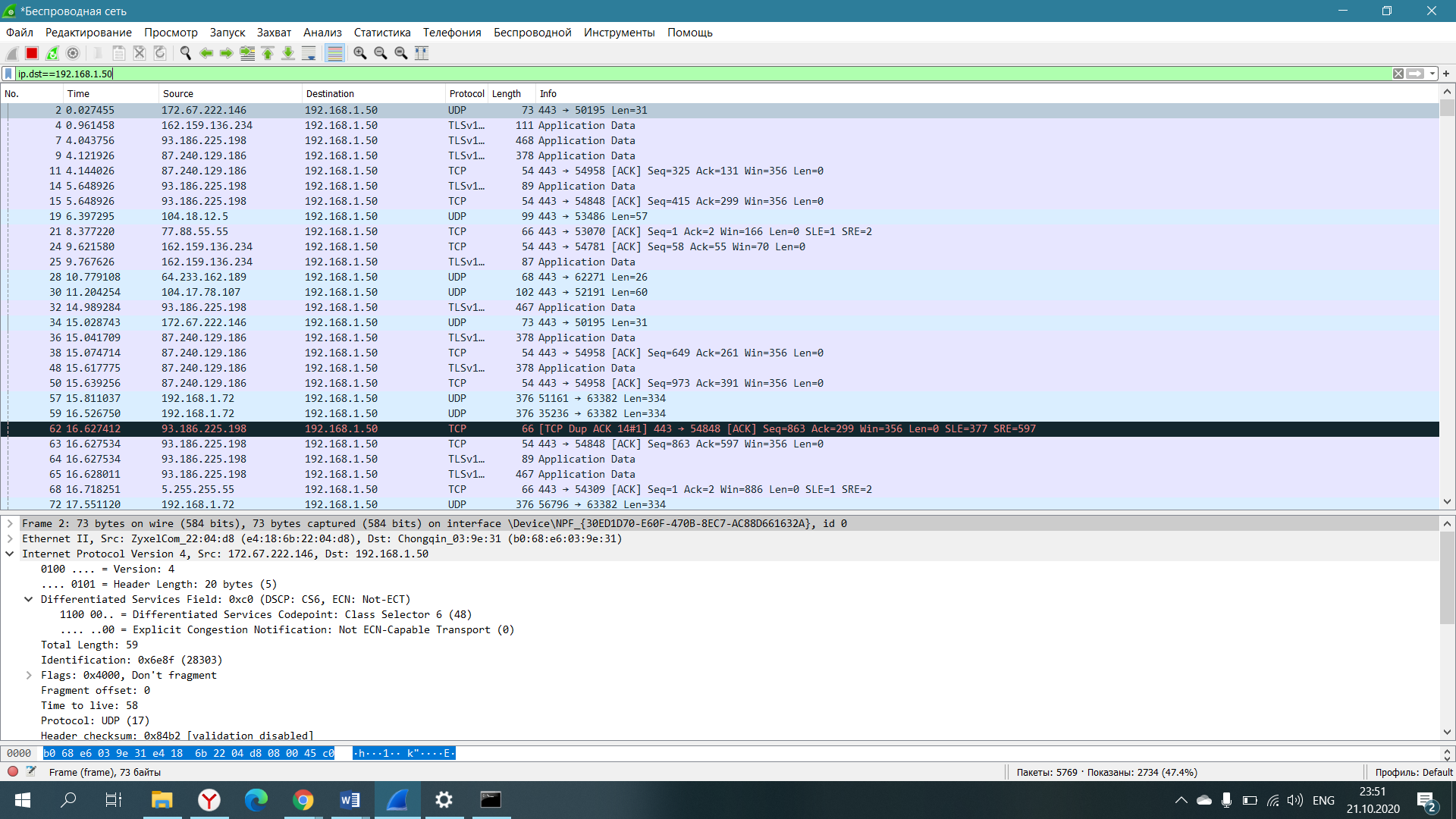
5.

Фильтры

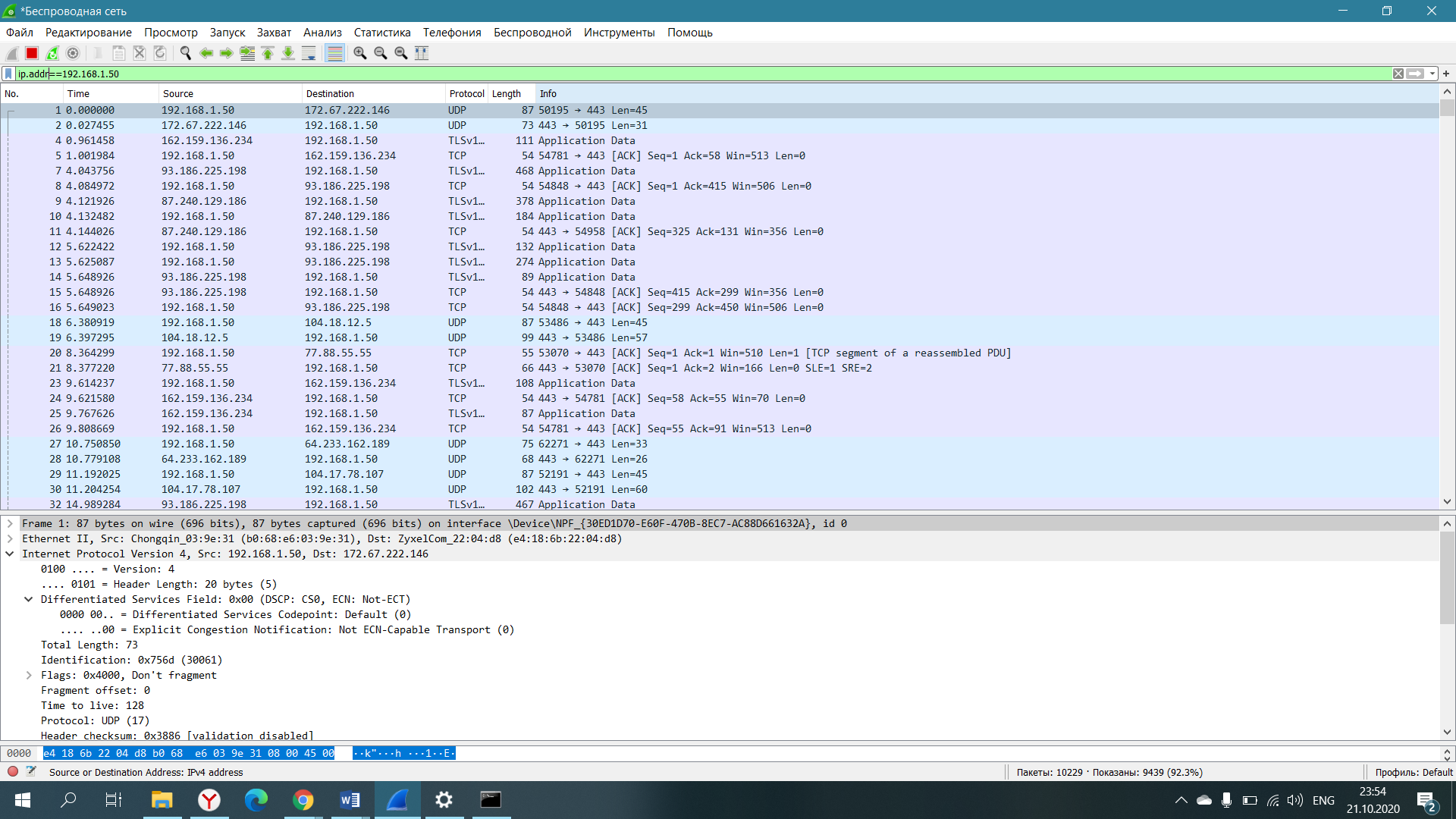
ip.src==192.168.1.50 покажет все захваченные пакеты с заданным ip-адресом отправителя



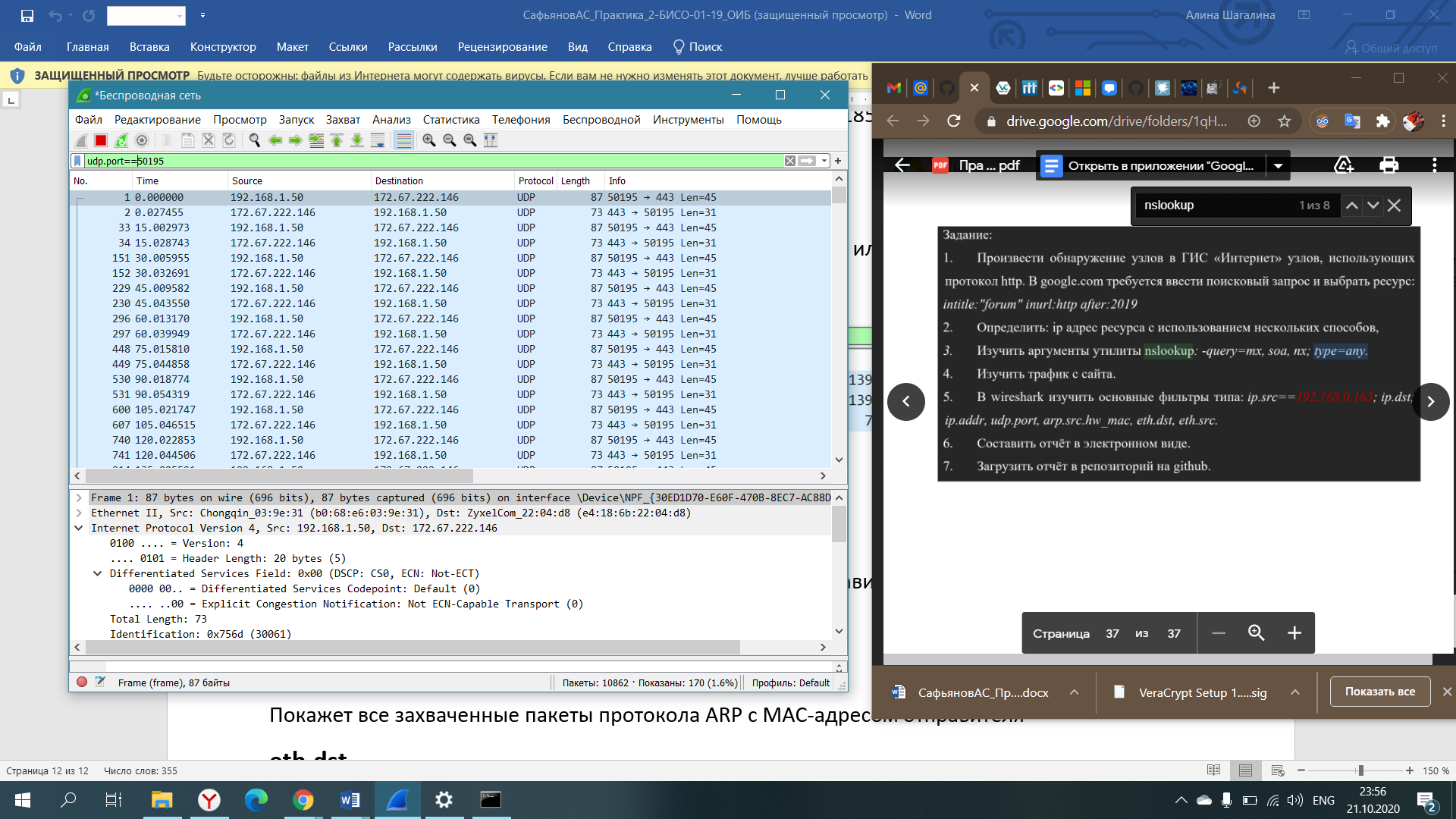
ip.dst==192.168.0.163 Покажет все захваченные пакеты с заданным ip-адресом получателя



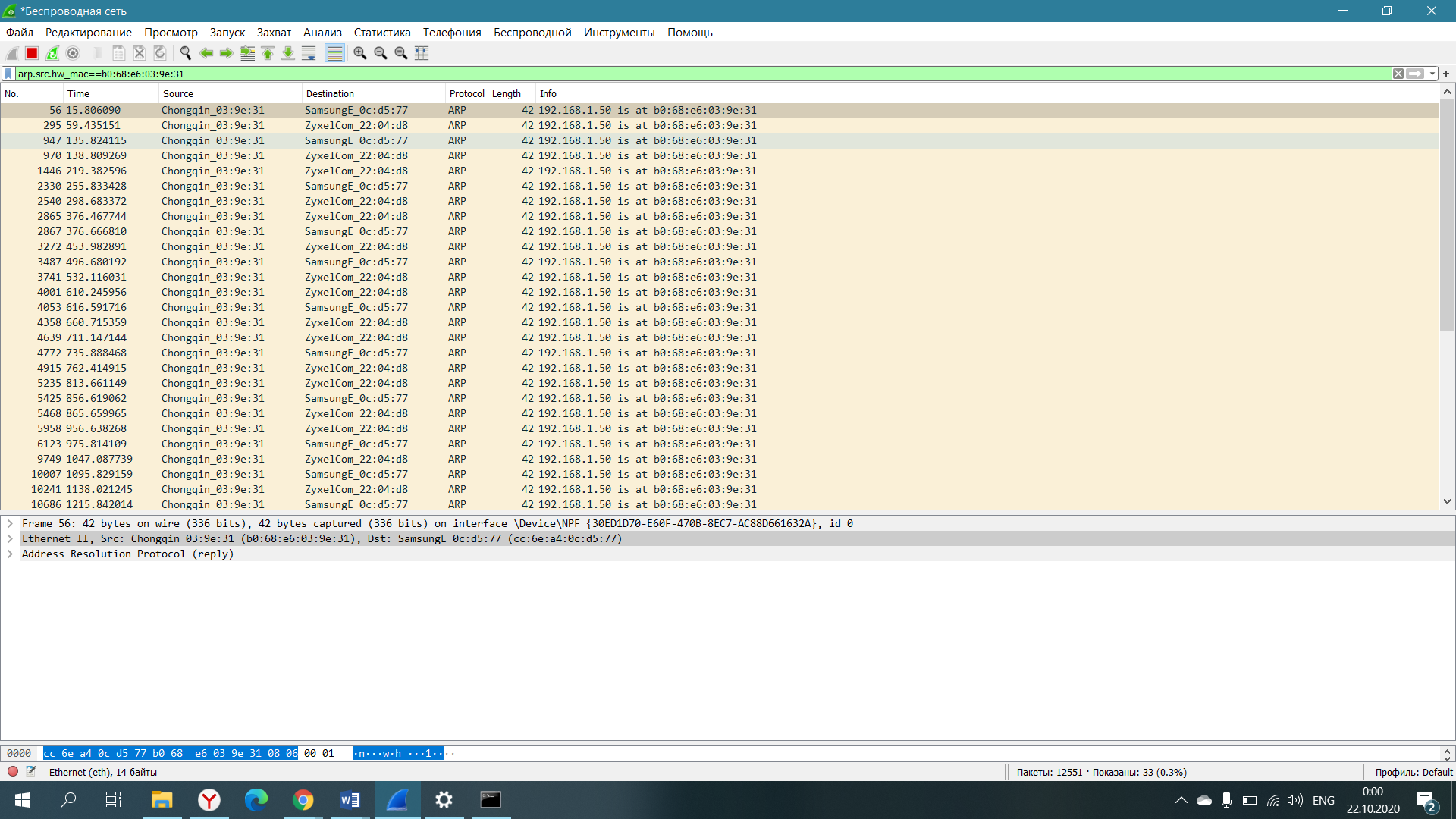
ip.addr==192.168.0.163 Покажет все захваченные пакеты с заданным ip-адресом отправителя или получателя



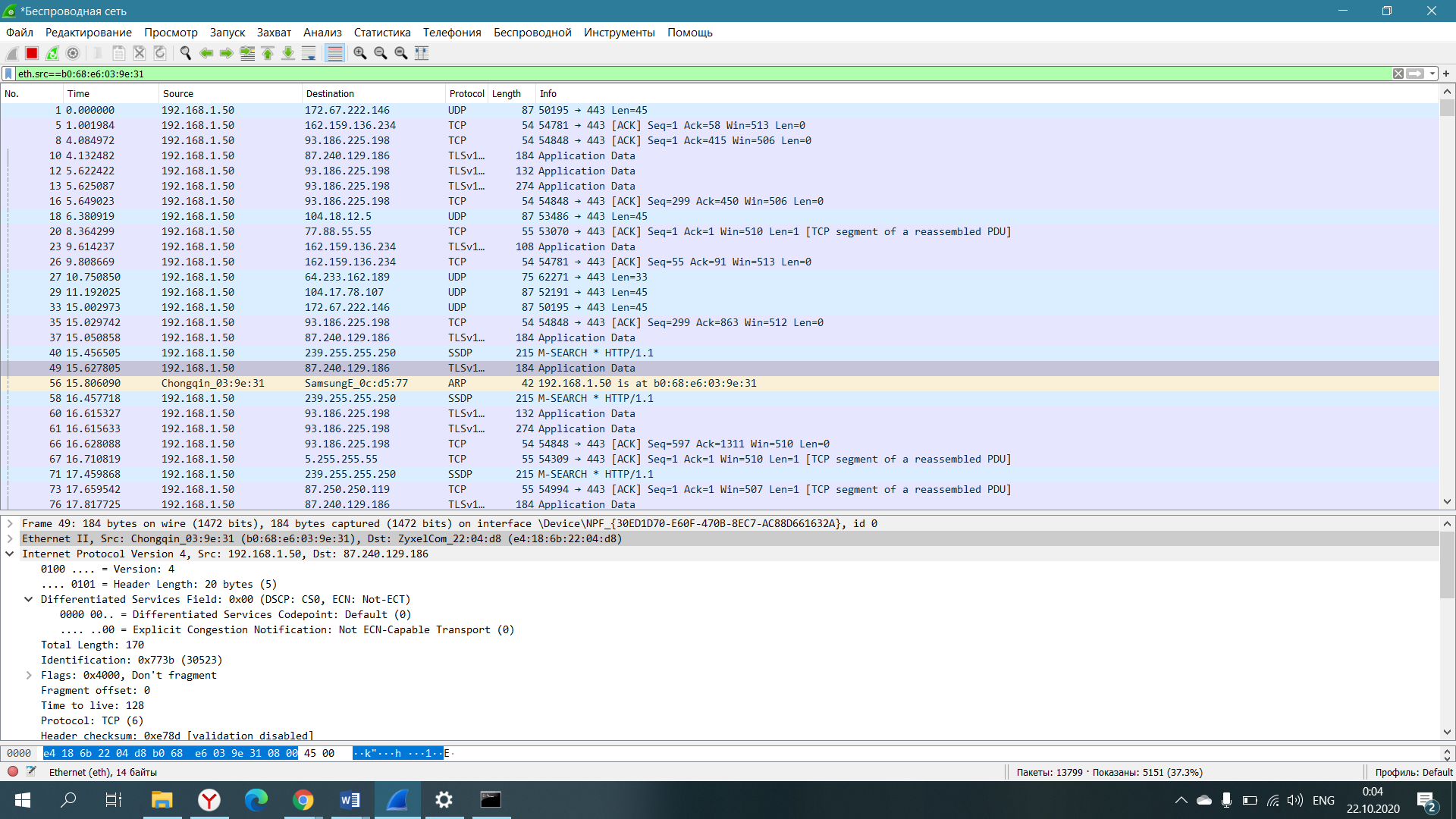
udp.port покажет все захваченные пакеты с заданным Udp портом отправителя или получателя



arp.src.hw\_mac==b0:68:e6:03:9e:31 покажет все захваченные пакеты протокола ARP с MAC-адресом отправителя



eth.dst==b0:68:e6:03:9e:31 покажет все захваченные пакеты с MAC-адресом получателя



eth.src==b0:68:e6:03:9e:31 Покажет все захваченные пакеты с MAC-адресом отправителя

