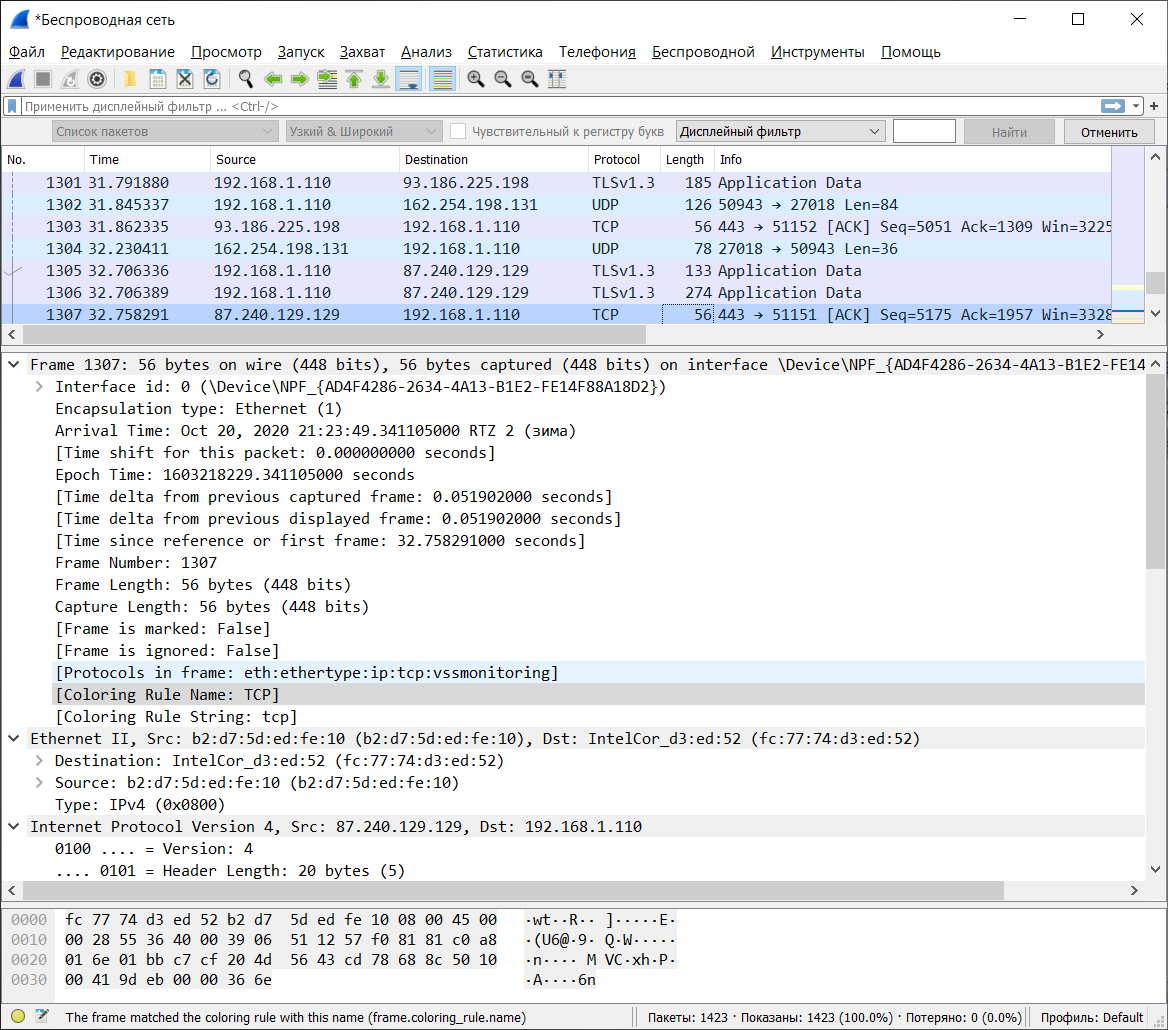
**1) Wireshark**

Требуется проанализировать трафик протоколов, а именно:

1. Рассмотреть структуру пакета;

2. Указать назначение заголовков.



**Содержимое пакета в 16-чной и текстовой формах**

**Информационное поле с детальной информацией по выбранному пакету**

**Список захваченных пакетов**

**Фильтр**

**Меню, панель инструментов**

**2) Ip**

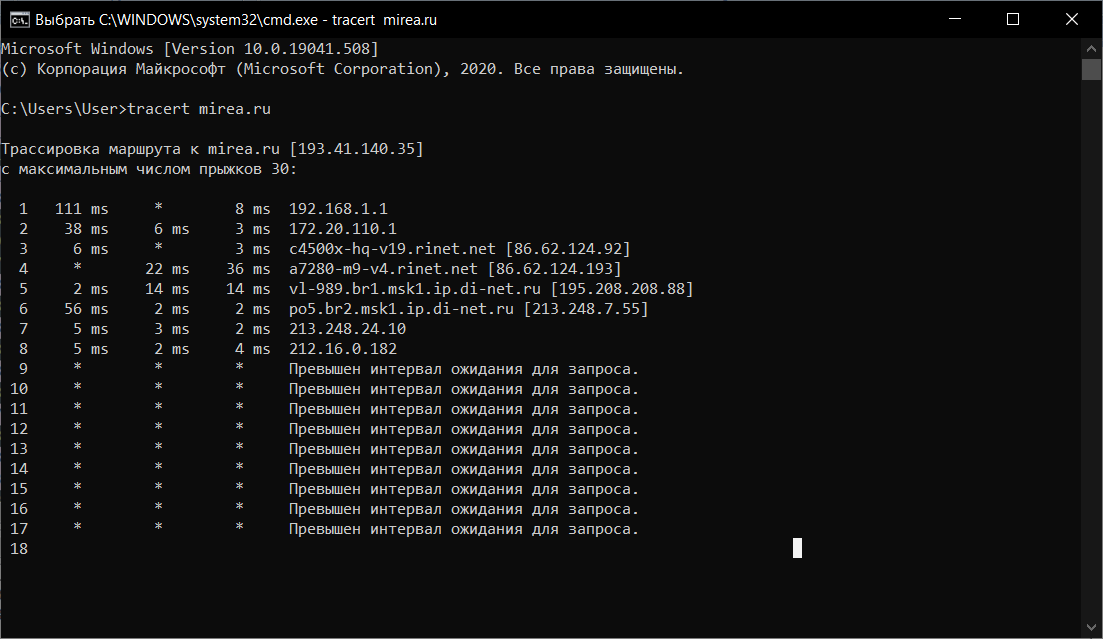
Задание:

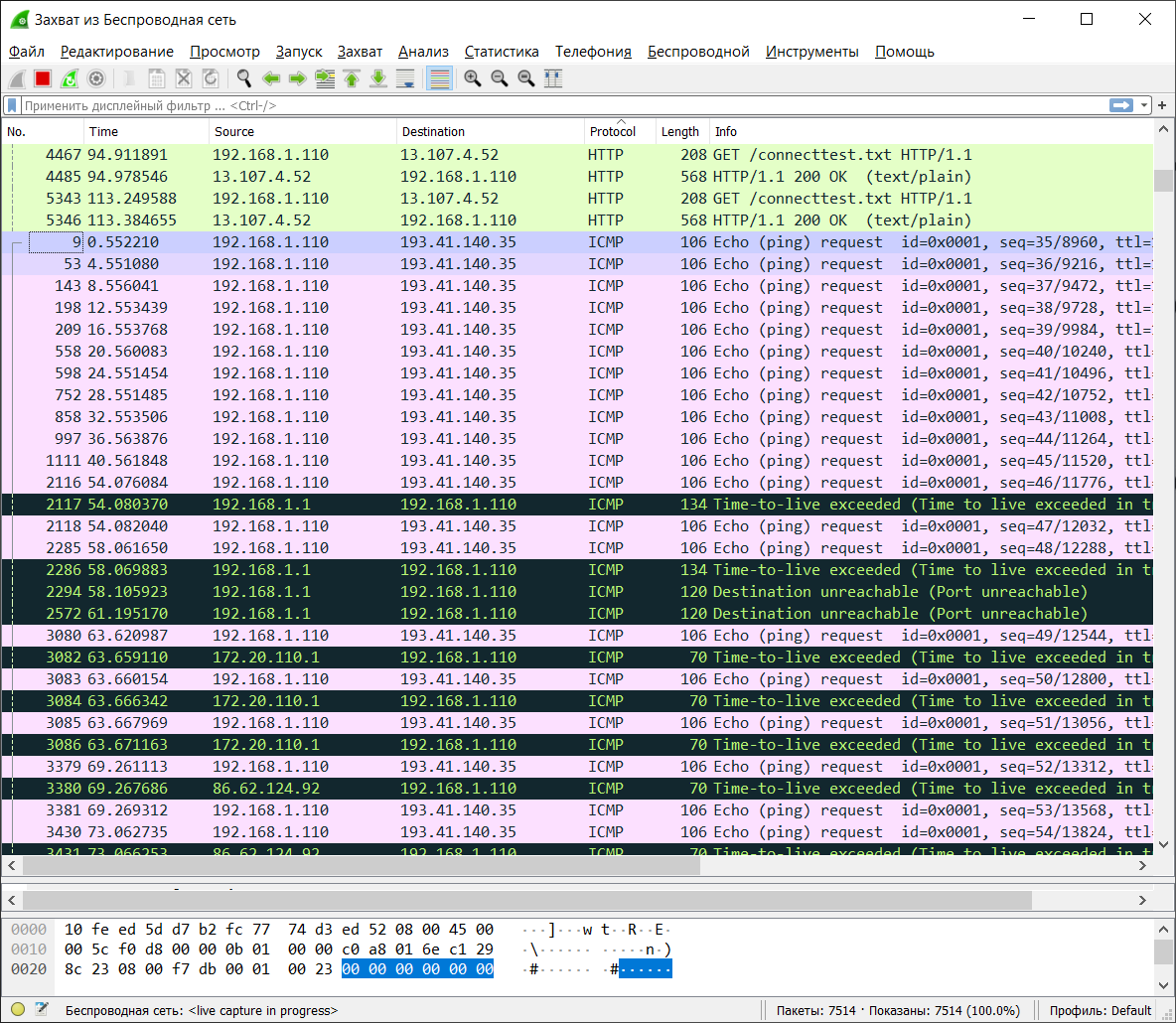
1. Проанализируйте первый пакет ICMP Echo Request, отправленный вашим

компьютером: укажите ваш IP-адрес.

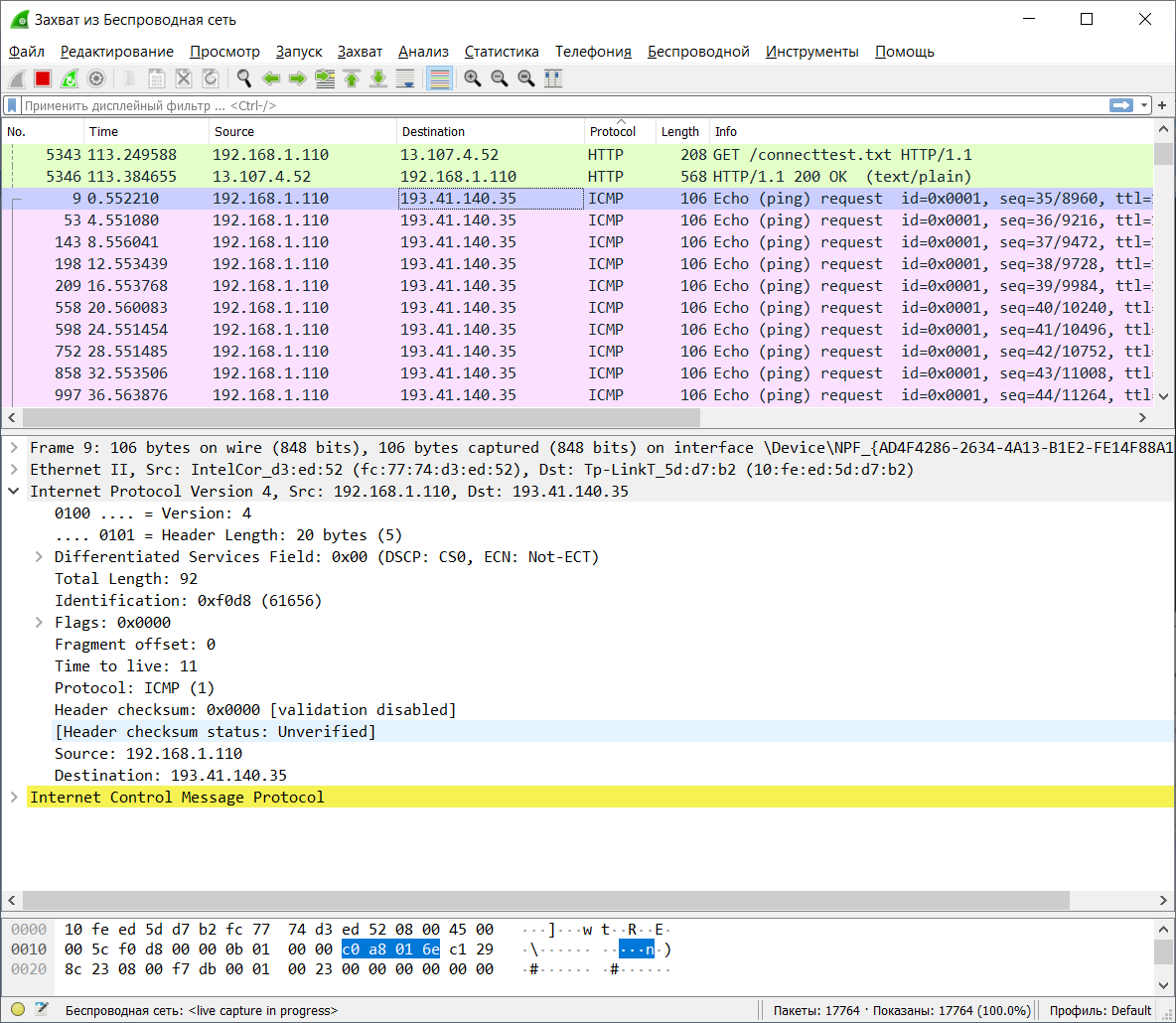
2. Сколько байт содержится в заголовке IP? Сколько байт в поле данных?

3. Укажите значение TTL.



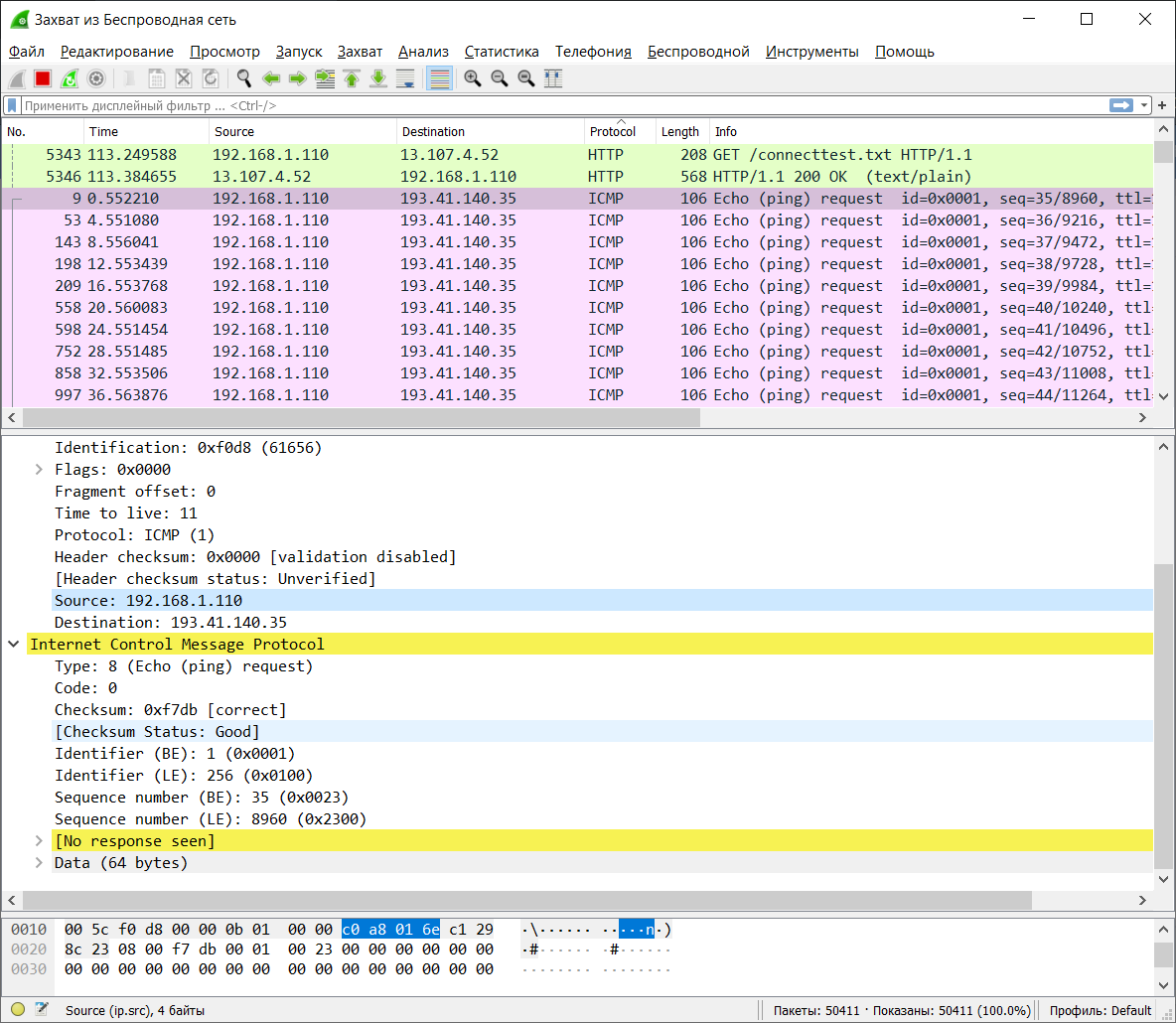


**Первый пакет**



**TTL=11**

**IP устройства**



**В заголовке IP -4 байта**

**В поле данных -64 байта**

**3) Протокол http**

Задание:

1. Произвести обнаружение узлов в ГИС «Интернет» узлов, использующих

протокол http. В google.com требуется ввести поисковый запрос и выбрать ресурс:

intitle:"forum" inurl:http after:2019

2. Определить: ip адрес ресурса с использованием нескольких способов,

3. Изучить аргументы утилиты nslookup: -query=mx, soa, nx; type=any.

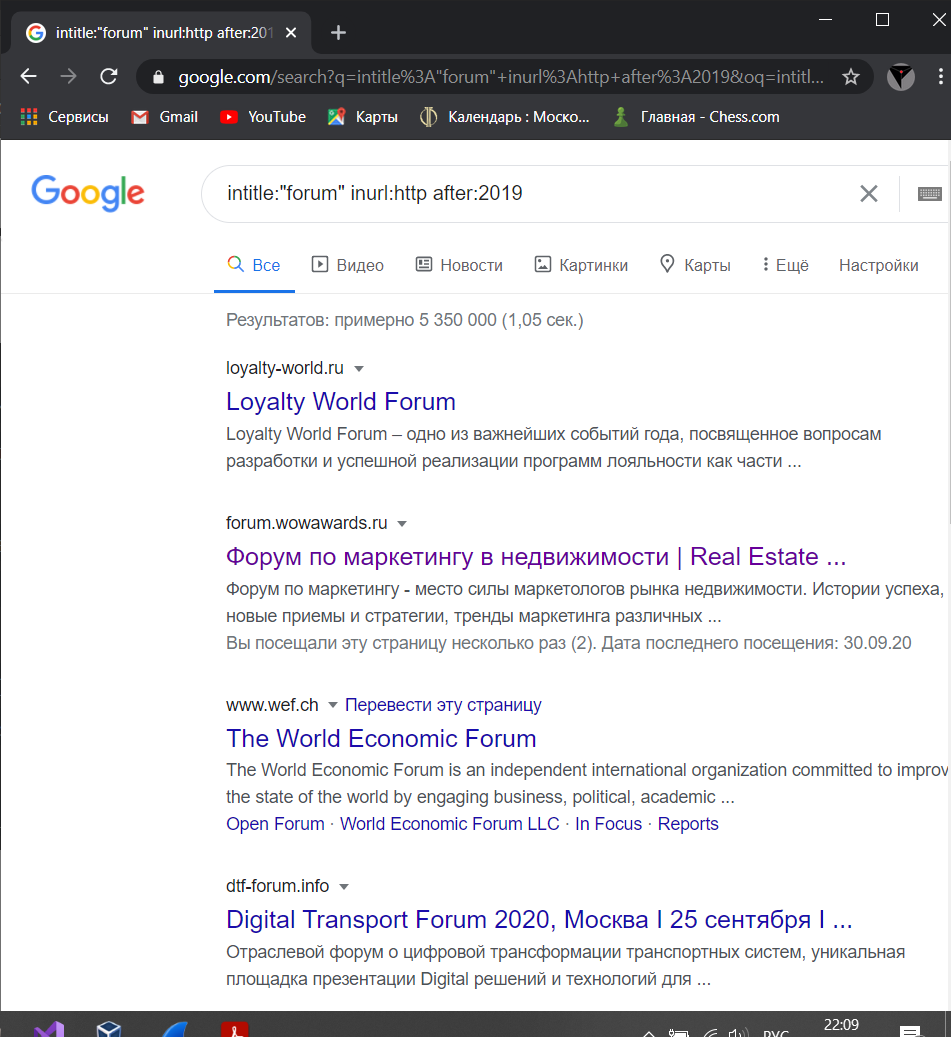
4. Изучить трафик с сайта.

5. В wireshark изучить основные фильтры типа: ip.src==192.168.0.163; ip.dst;

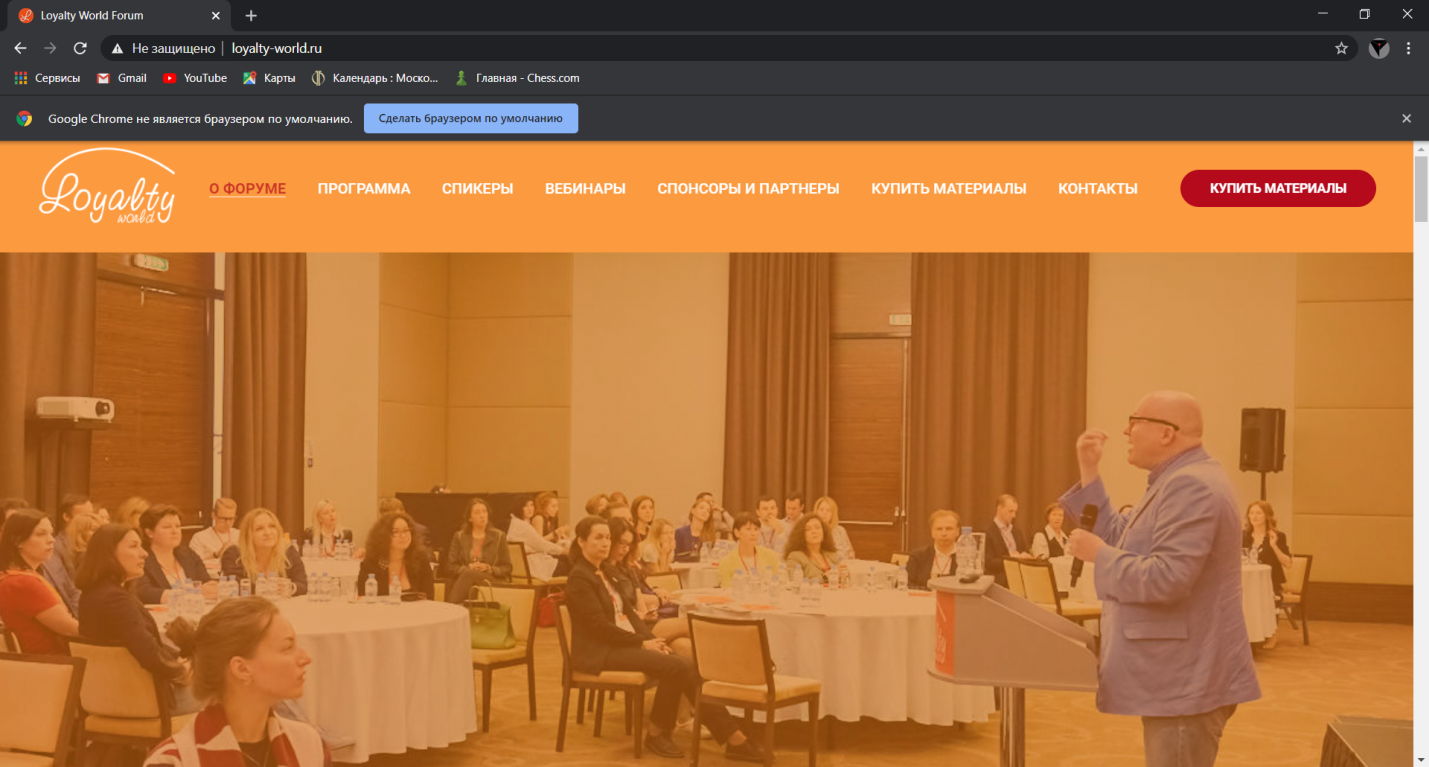
ip.addr, udp.src, arp.src.hw\_mac, eth.dst, eth.src.

6. Составить отчёт в электронном виде.

7. Загрузить отчёт в репозиторий на github.

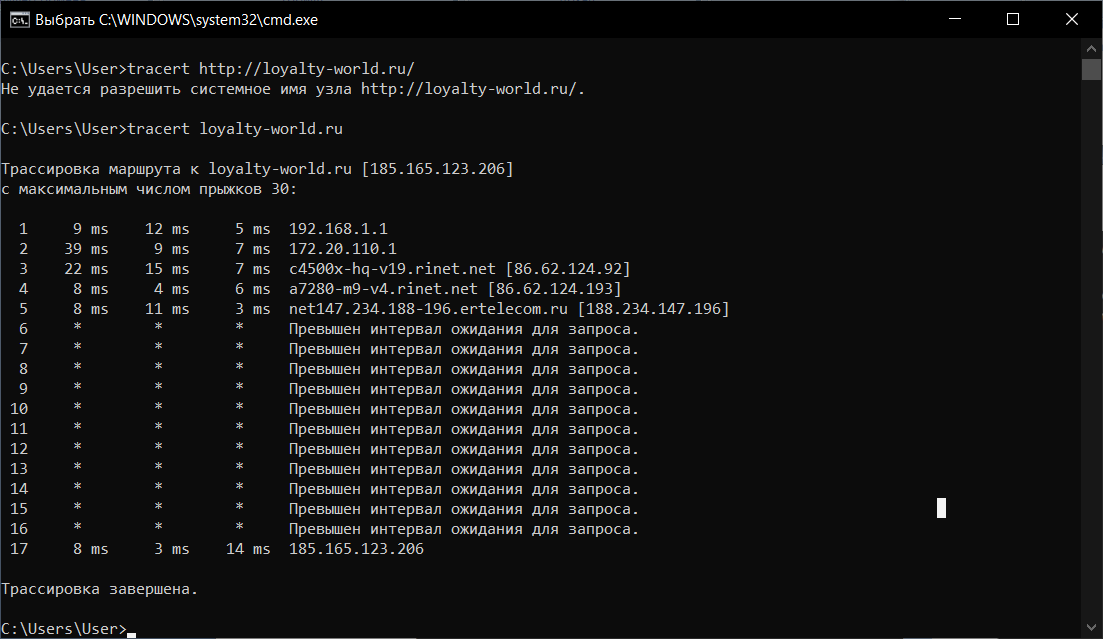


**1**

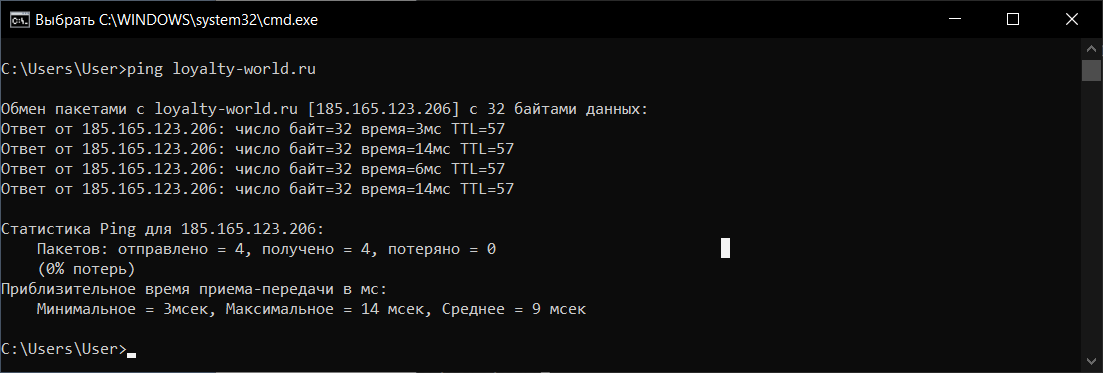


**2**

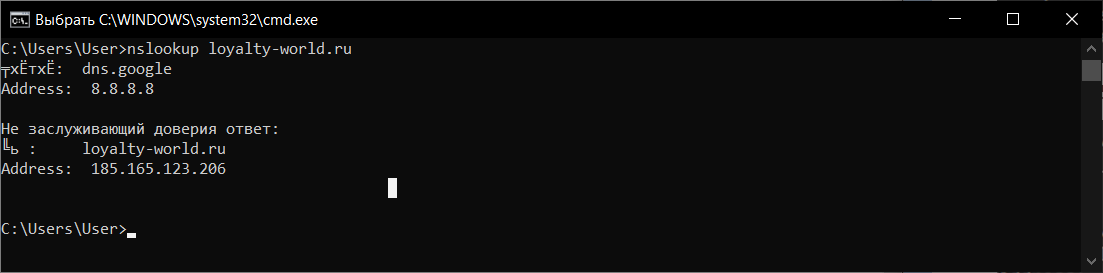
**адрес**



**Ip- 185.165.123.206**

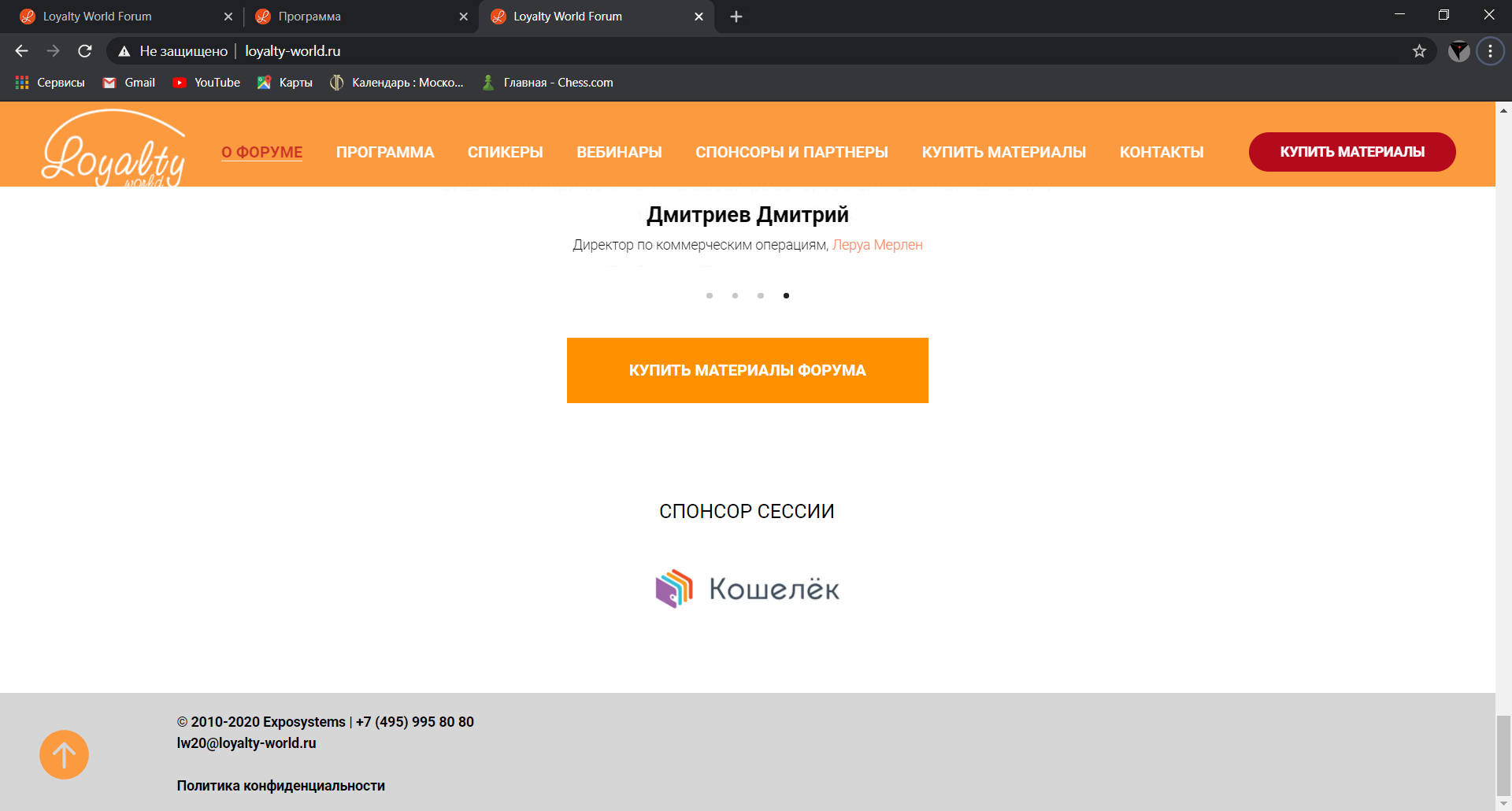
****

**Ip-185.165.123.206**

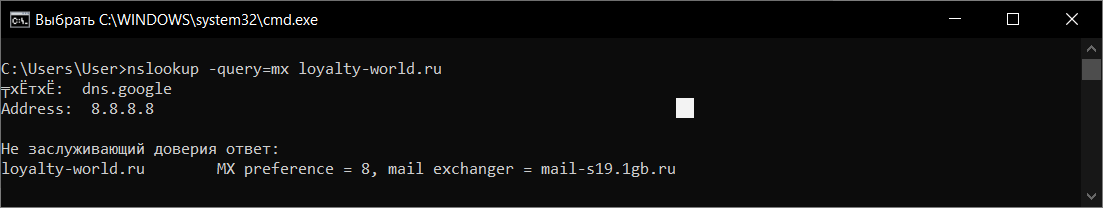
****

**Ip-185.165.123.206**

Проверив Ip тремя способами можно уверенно сказать, что Ip адресом loyalty-world.ru является **185.165.123.206.**

****

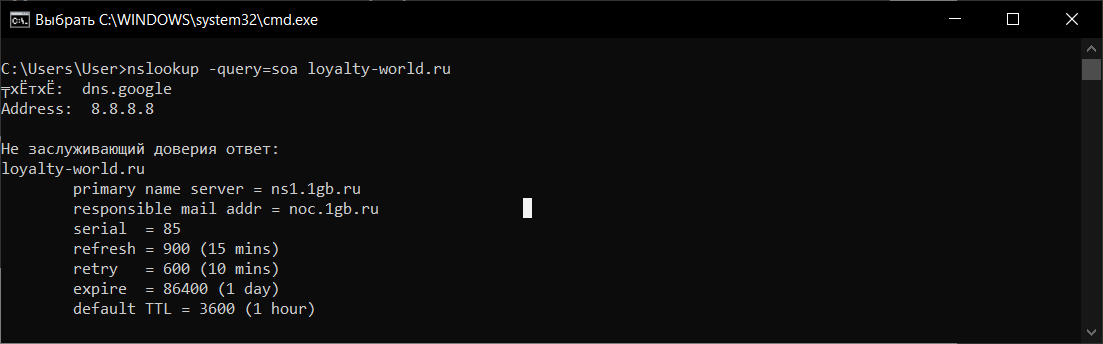
**3**

****

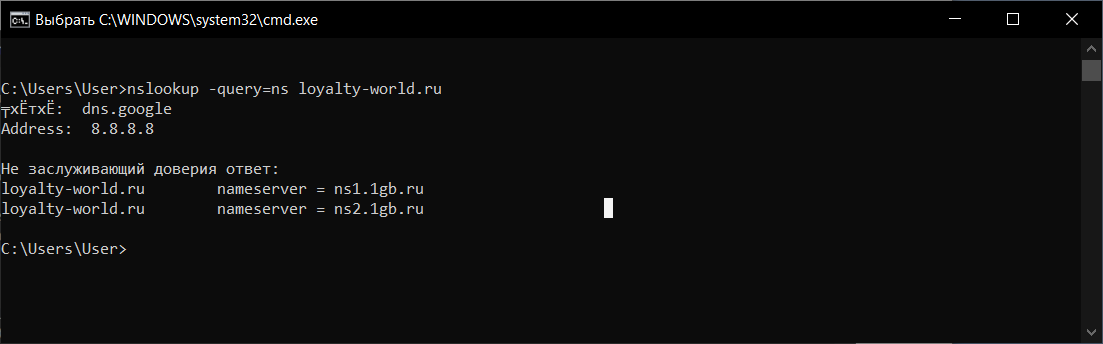
**Приоритет**

**почтовый сервер**

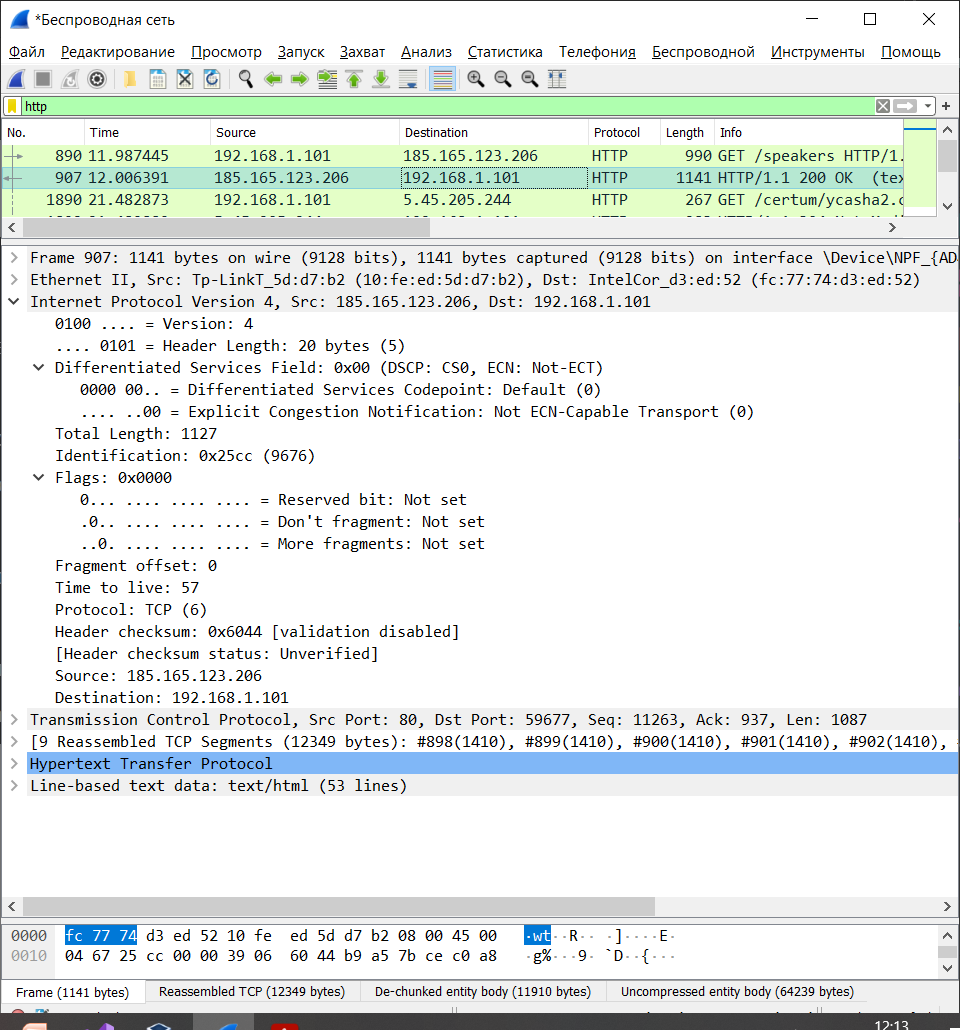
С помощью команды **nslookup –query=mx** на экран выводятся все почтовые сервера, через которые отправляется вся почта на lw20@loyalty-world.ru. MX preference- приоритет. Чем он ниже, тем больше шанс отправления почты через этот сервер.



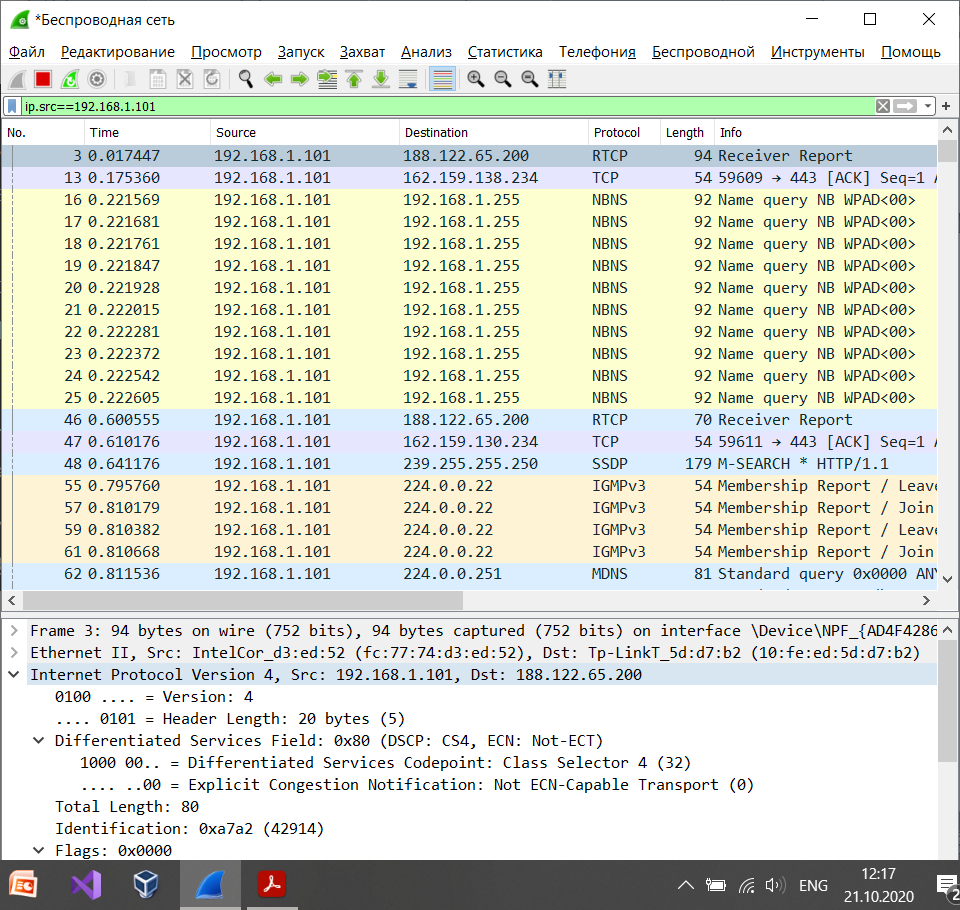
С помощью команды **nslookup -query=soa** можно получить информацию о зоне домена, адресе его администратора, серийном номере файла зоны и о интервалах: через которое проверится серийный номер, для повторного соединения, хранения кэша и минимального времени хранения.(Сверху вниз по списку)



С помощью команды **nslookup -query=ns** можно вывести соответствие доменных имен DNS-серверам.

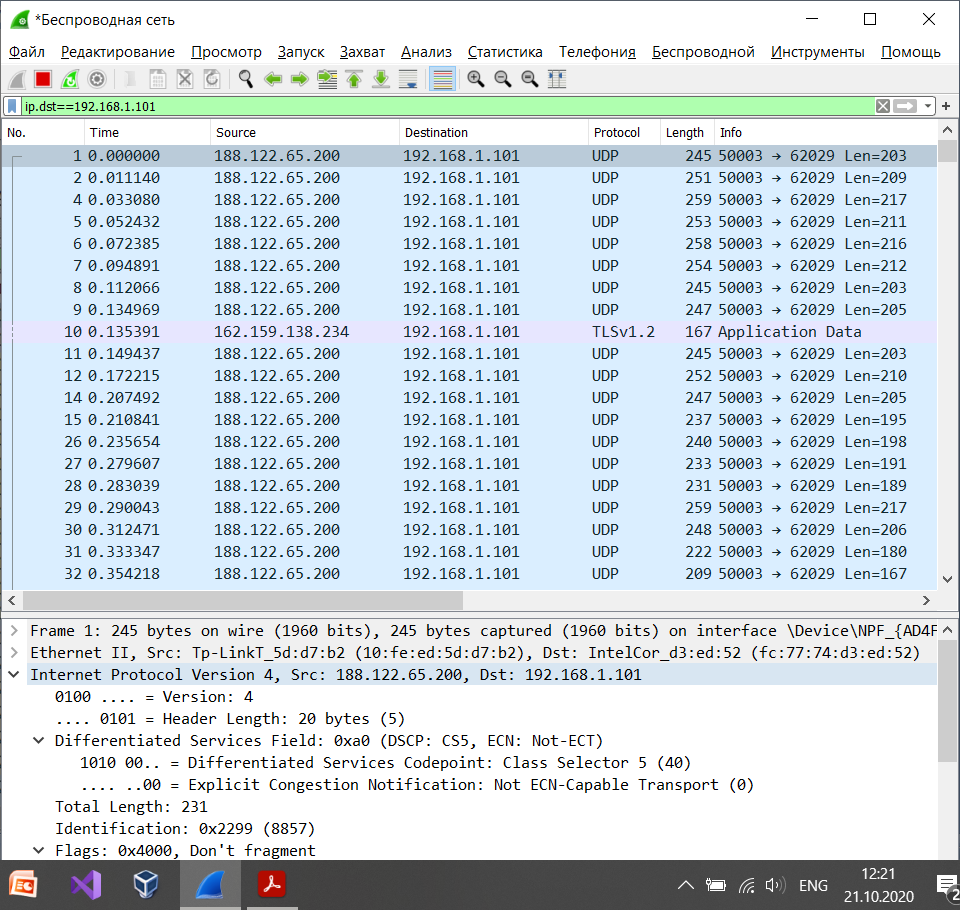


**4**

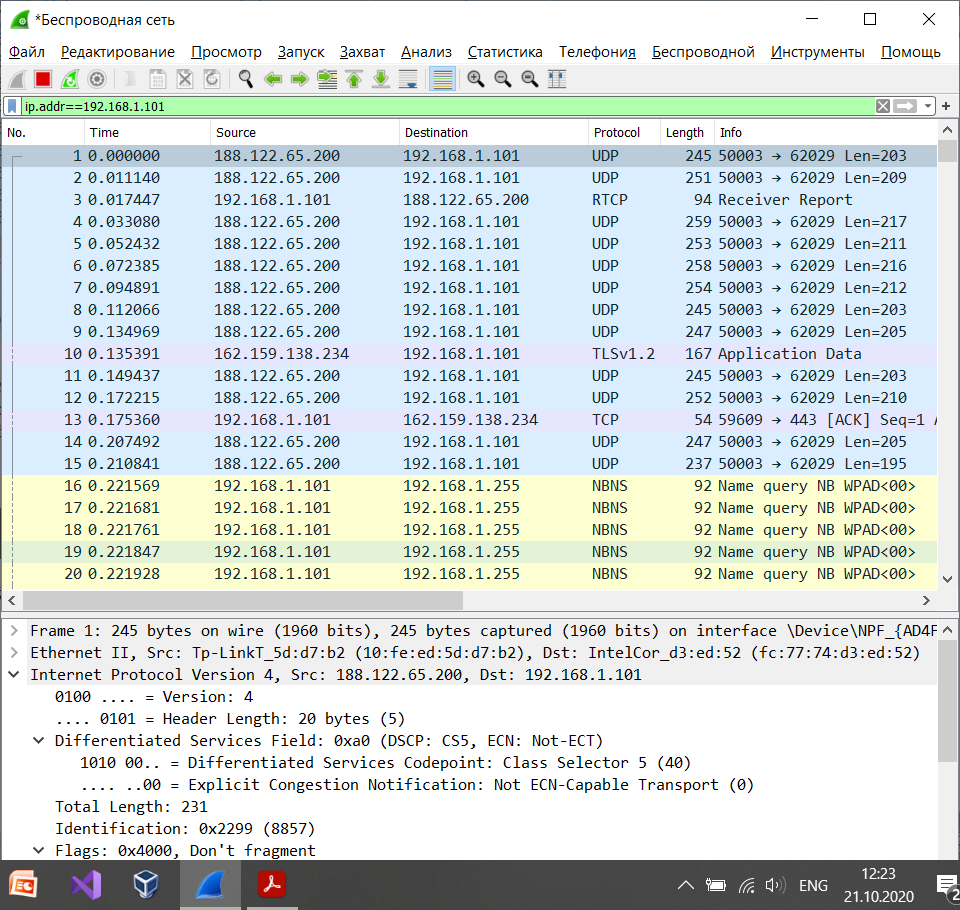


**5**

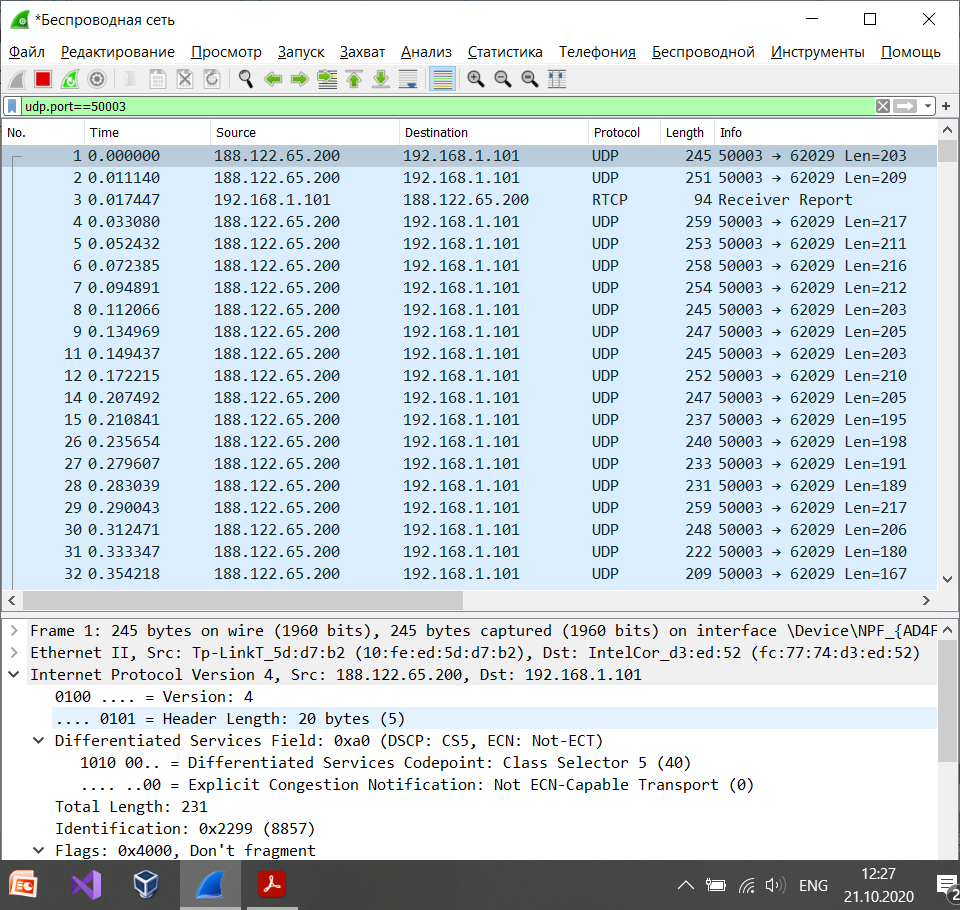
**ip.src == <** нужный ip **>** будет перехватывать пакеты ip-адресом этого отправителя.



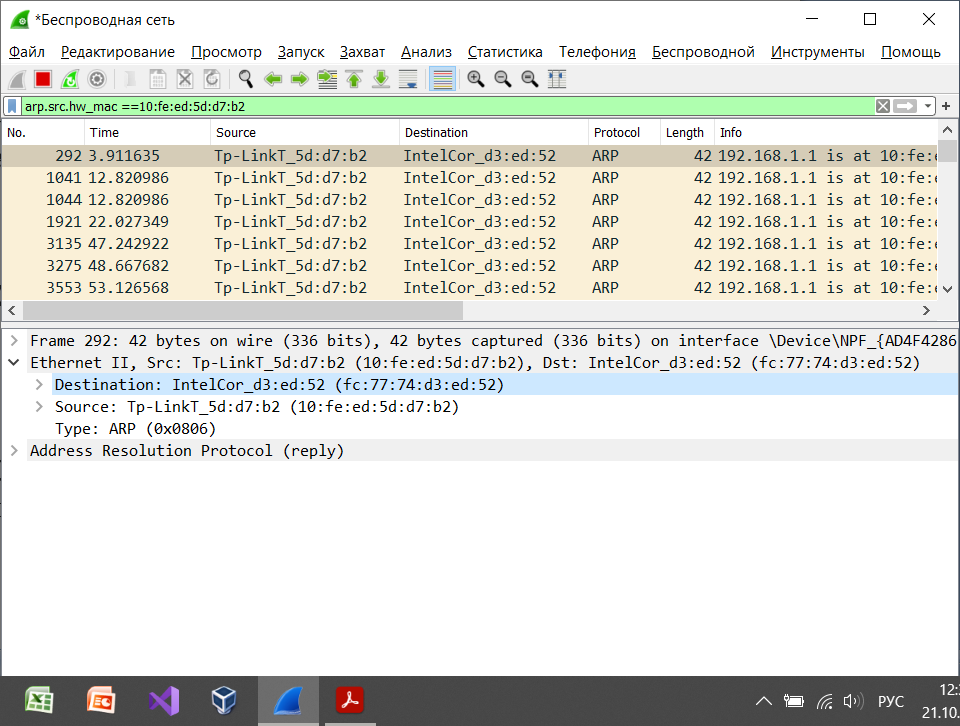
**ip.src == <** нужный ip **>** будет перехватывать пакеты отправленные нужному нам получателю с выбранным ip.



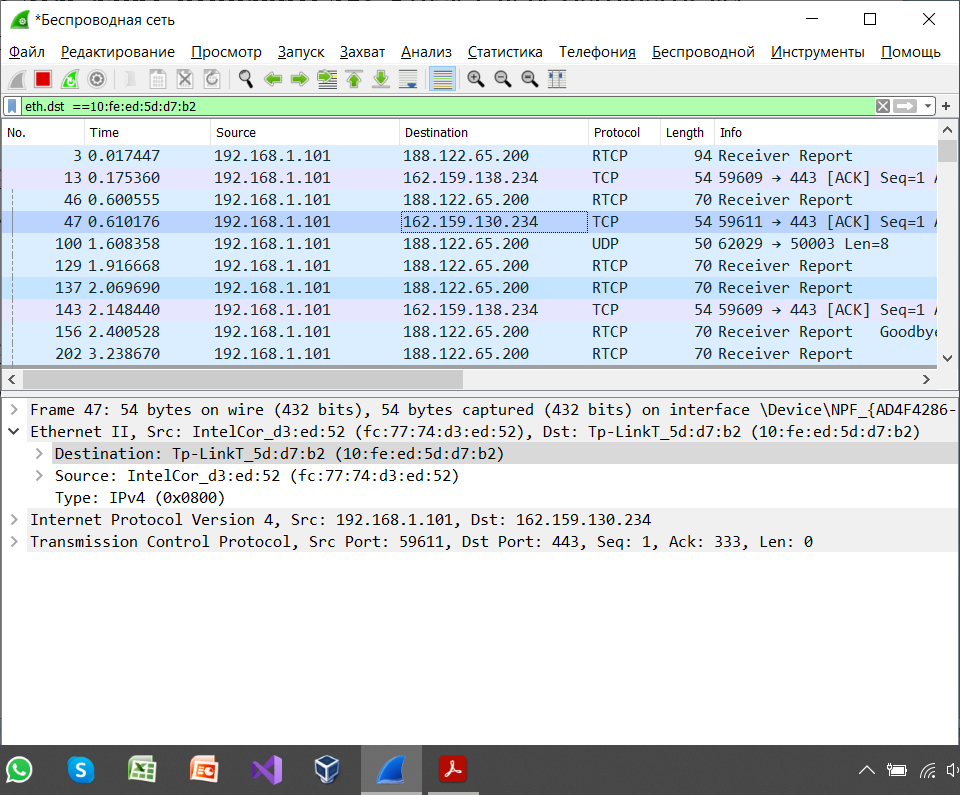
**ip.addr == <** нужный ip **>** будет перехватывать все пакеты отправленные или полученные устройством с этим ip.



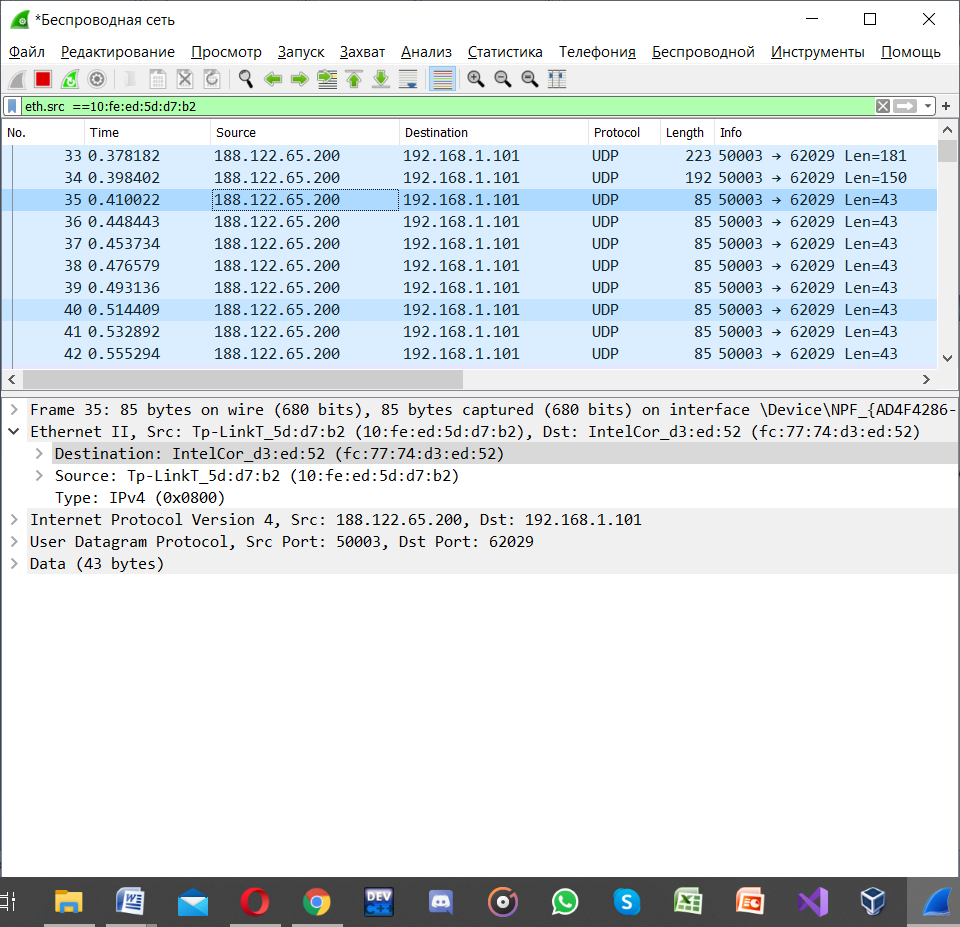
**udp.port == <** нужный порт **>** будет перехватывать все пакеты отправленные или полученные с использованием определённого udp порта.



**arp.src.hw\_mac == < Mac адрес отправителя> -** будет перехватывать все пакеты протокола ARP отправленные пользователем с этим Mac адресом.



**eth.dst** **== < Mac адрес получателя> -** будет перехватывать все пакеты полученные пользователем с этим Mac адресом.

****

**eth.src == < Mac адрес> -** будет перехватывать все пакеты отправленные пользователем с этим Mac адресом.

**4) Http**

В списке захваченных пакетов требуется найти пару HTTP сообщений (запрос-ответ): GET сообщение и ответ сервера.

В информационном поле необходимо развернуть строку, содержащую HTTP,

и отметите указанную ниже информацию:

- версия HTTP;

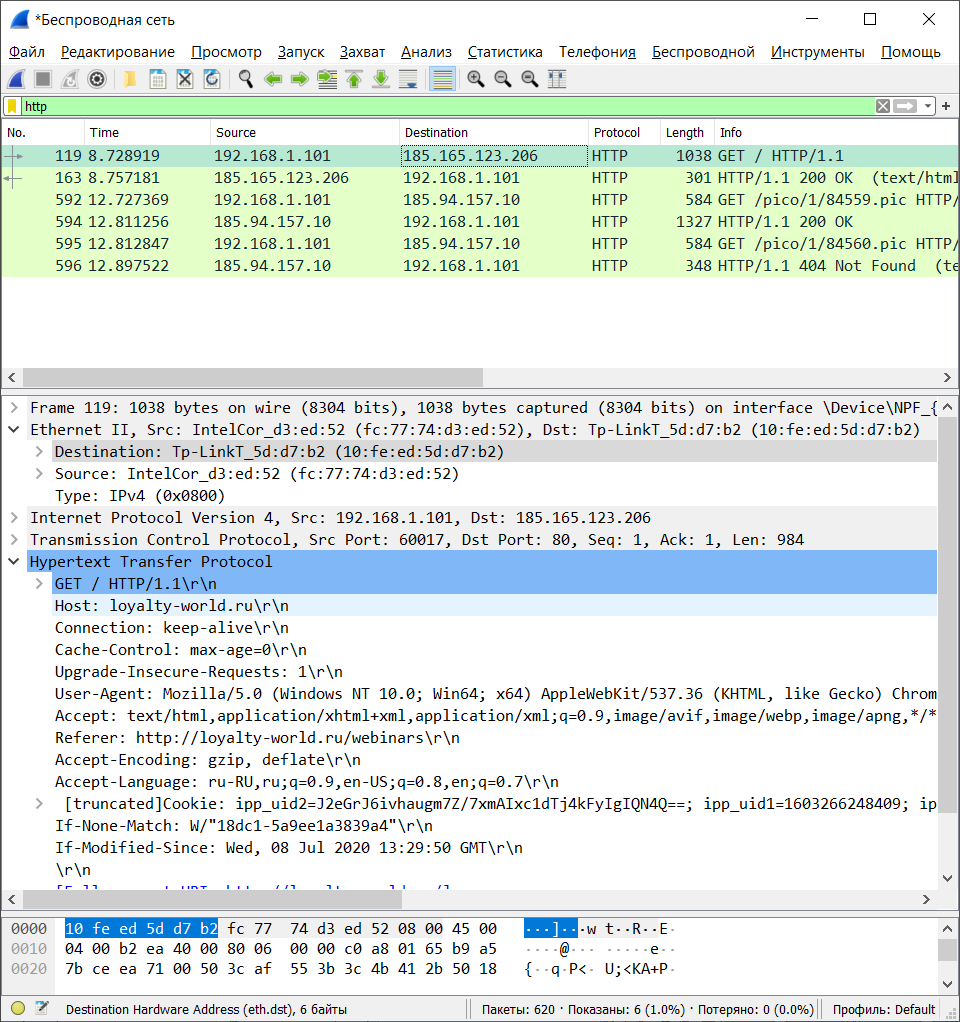
- IP-адреса компьютера и сервера;

- код состояния HTTP;

- длина тела сообщения (содержимое поля заголовка объекта Content Length

указывает длину тела сообщения в октетах (десятичное число), или в случае метода

HEAD, размер тела объекта, который мог бы быть послан при запросе GET).



**Версия – HTTP 1.1**

**IP компьютера – 192.168.1.101**

**IP адрес сервера – 185.165.123.206**

**Код состояния HTTP – 200**

**Длина тела сообщения – 1038 byte**