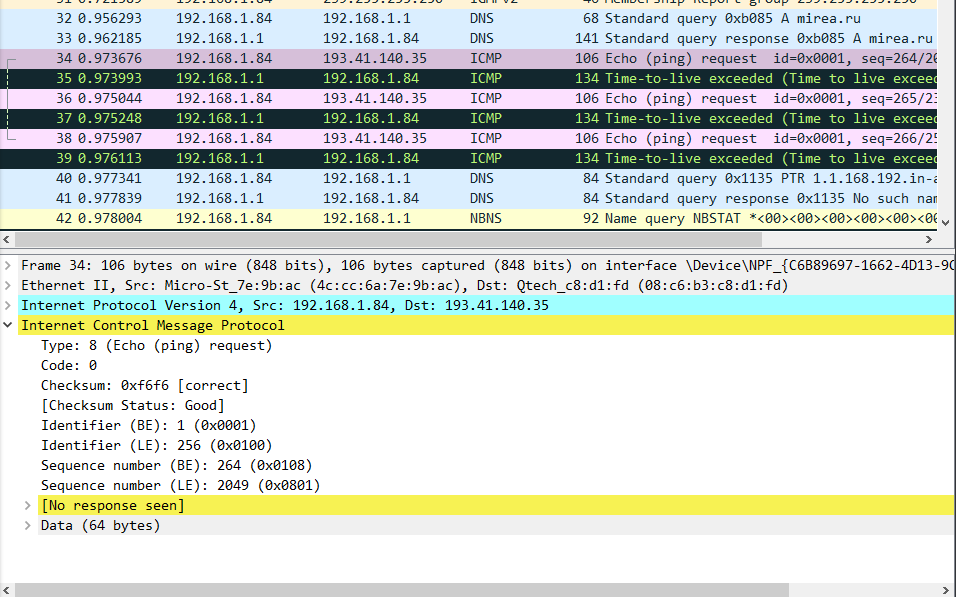
|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)**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

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 2** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Сафьянов Александр Сергеевич |
|  |

Москва 2020

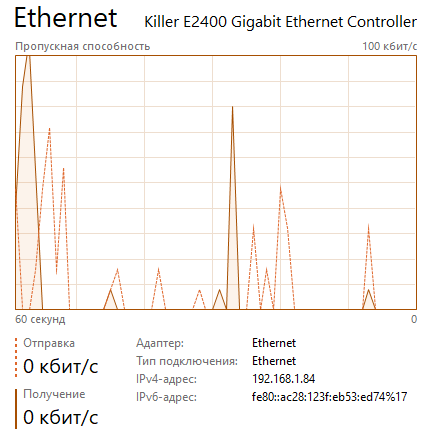
1. **WireShark**



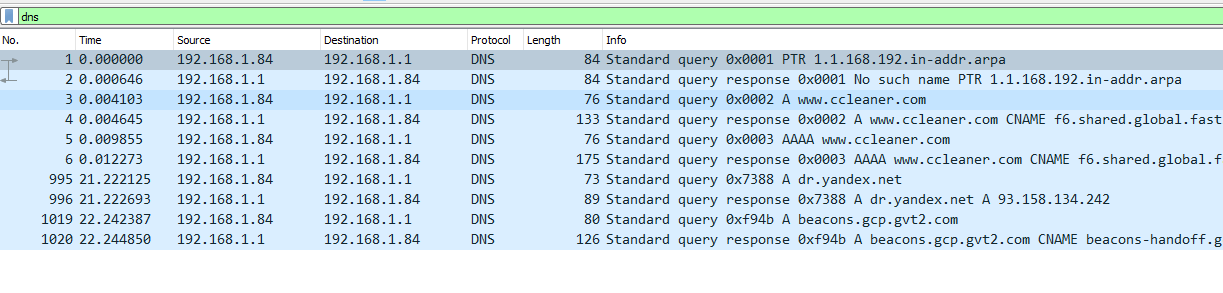
Отправлен Эхо запрос;

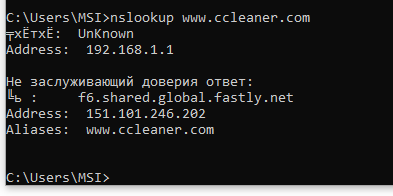
Big Endian (BE), так и Little Endian (LE) – порядковые поля, служат для облегчения подсчета эхо запросов ICMP;

И ответ был не получен.

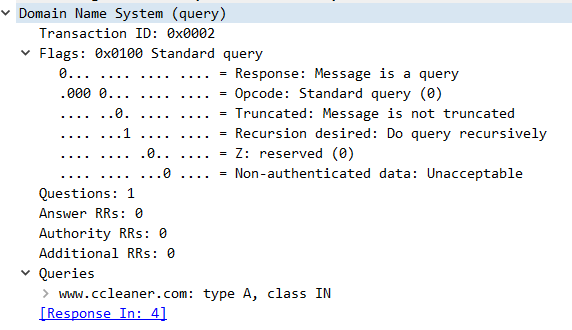
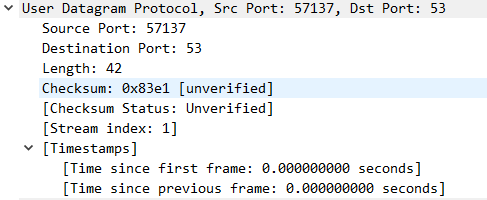


1. Мой IPv4: 192.168.1.84
2. В заголовке 20 байтов, 64 байт в поле данных
3. TTL: 128
4. **DNS**

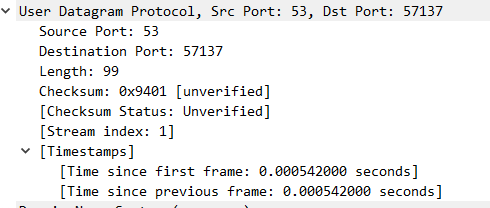


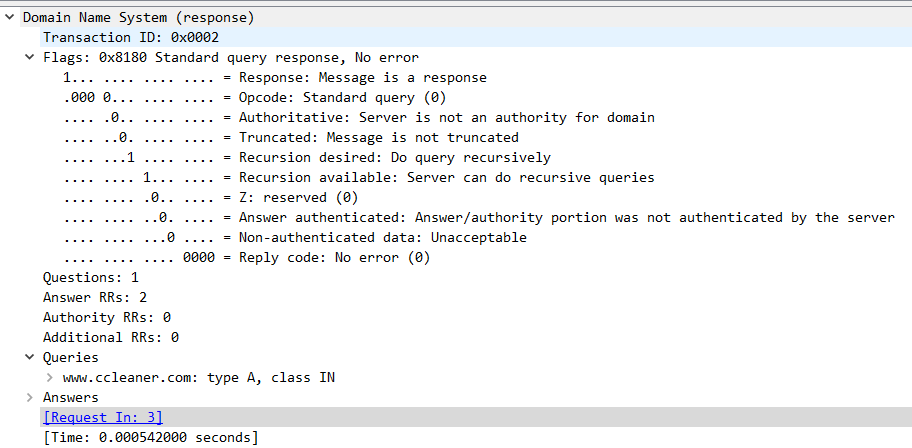


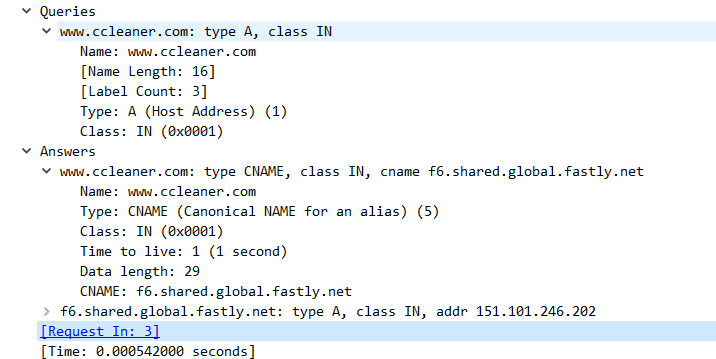
**Запрос**

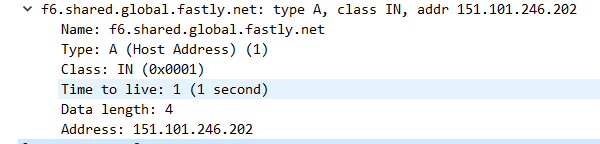


**Ответ**

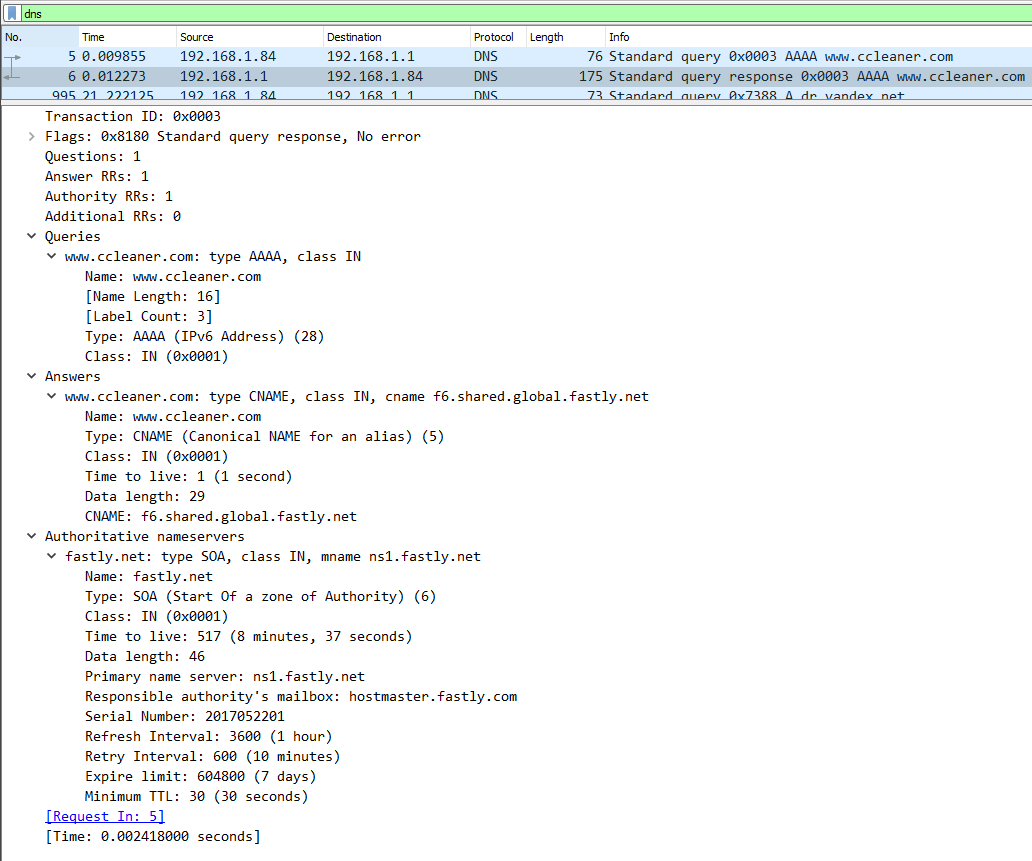






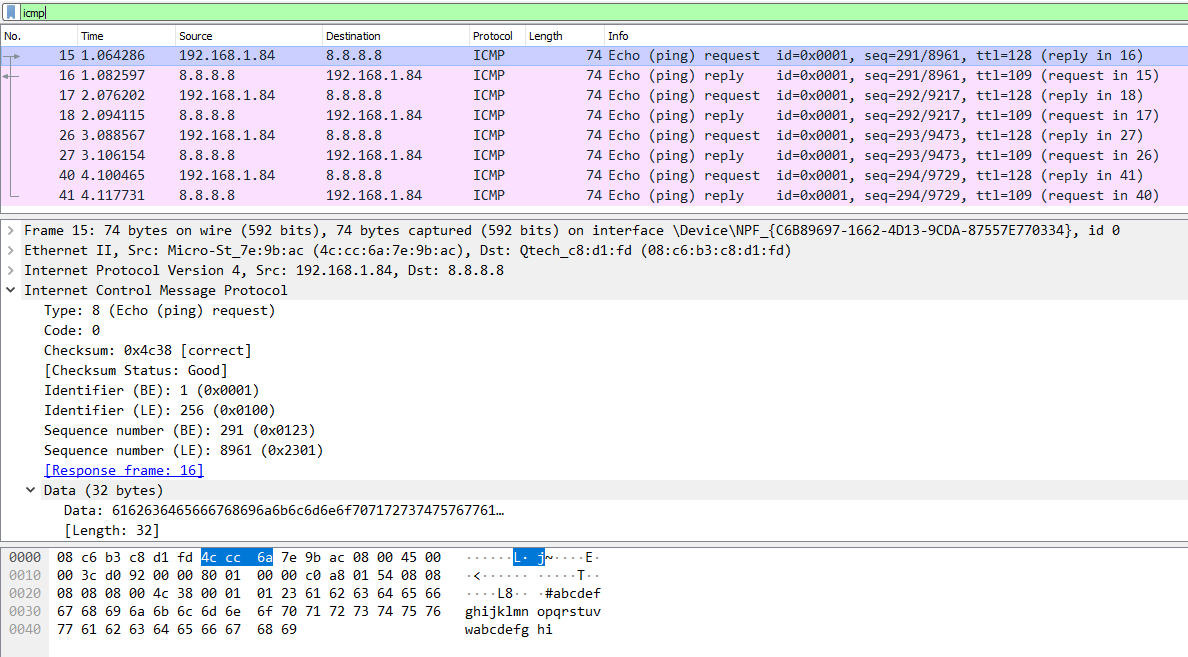


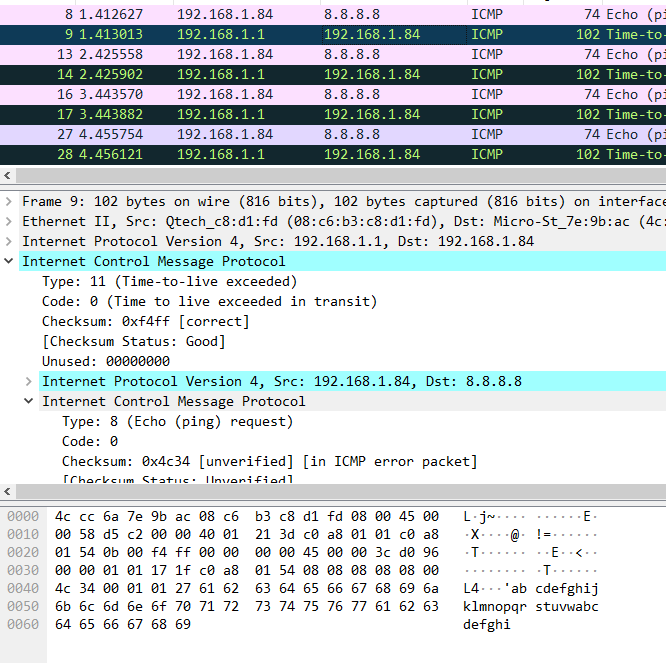
Запись типа CNAME позволяет иметь и использовать на сервере более одного имени домена (хоста).



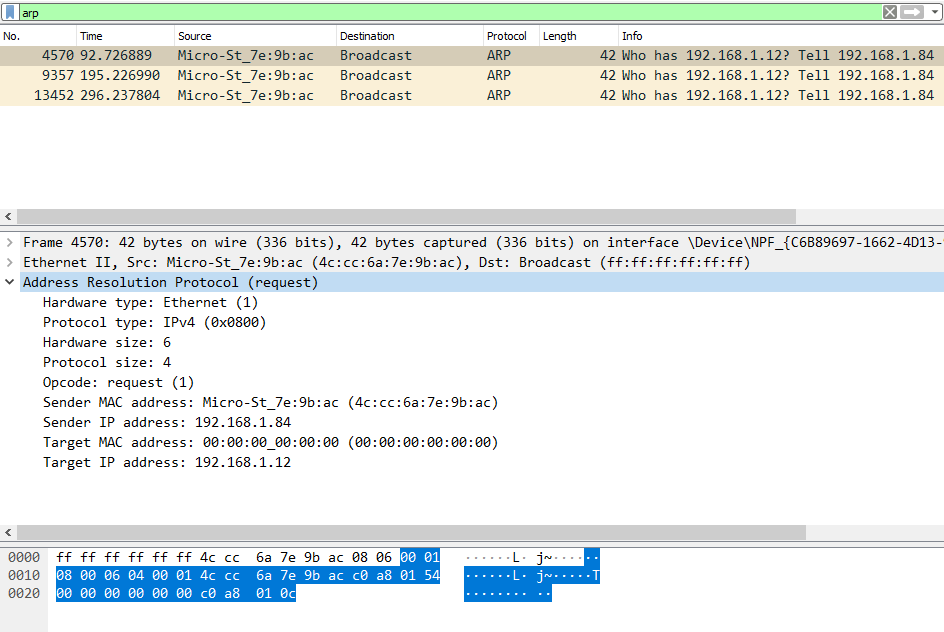
**Запись типа SOA** показывает, где храниться на каком сервере лежит основная информация об этом домене. В записи типа SOA указывается полное, уточненное доменное имя зоны.

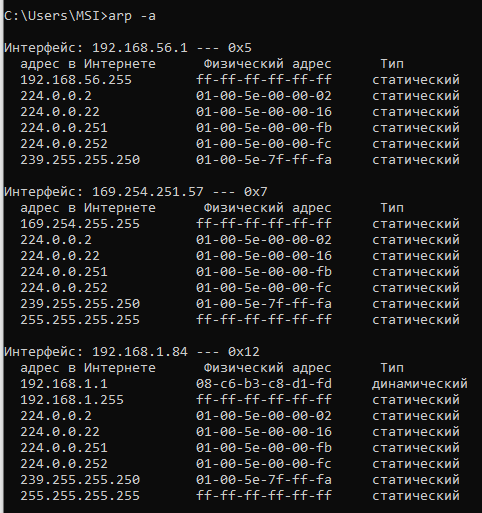
1. **ICMP**



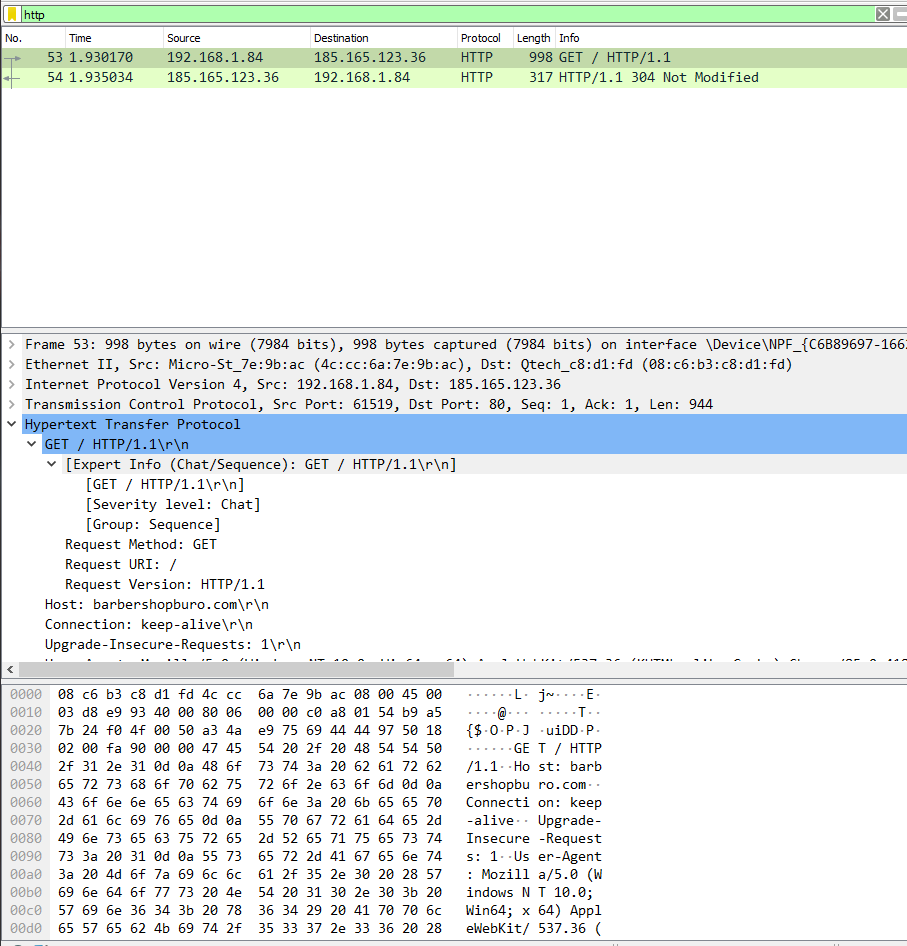


1. **ARP**



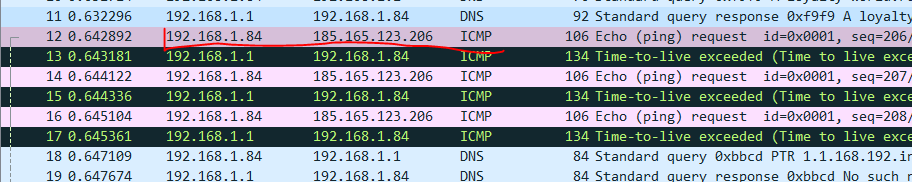


1. **HTTP**

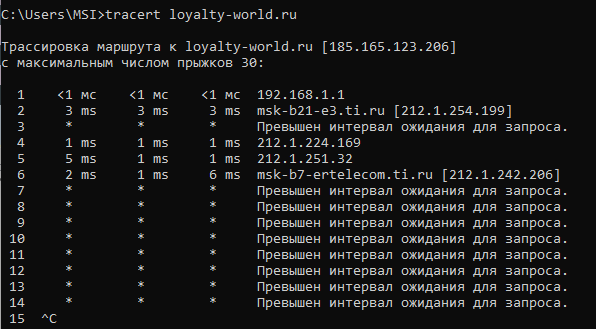


1. Версия HTTP 1.1
2. IP компьютера: 192.168.1.84 - IP адрес сервера: 185.165.123.36
3. Код состояния HTTP: 304
4. Длина тела сообщения: 998
5. **2. Задание**

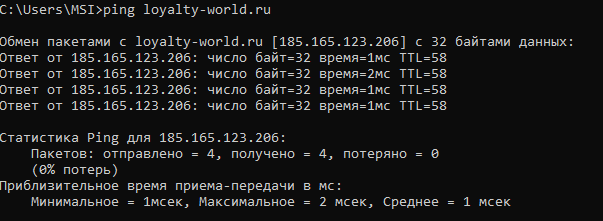
Ресурс: loyalty-world.ru

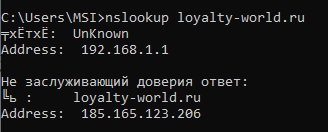


IP адрес: 185.165.123.206 (tracert loyalty-world.ru)

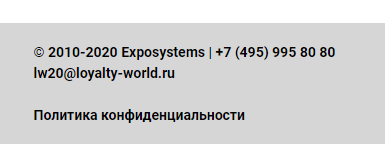


IP адрес: 185.165.123.206 (ping loyalty-world.ru)

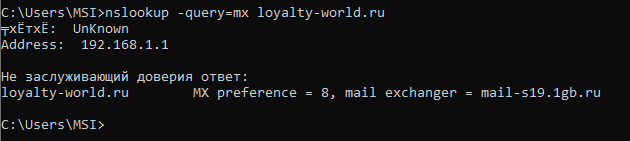


IP адрес: 185.165.123.206 (nslookup loyalty-world.ru)

**3. 3. NSLOOKUP и ее опции**

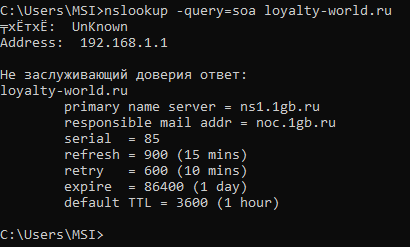


**-query=mx**



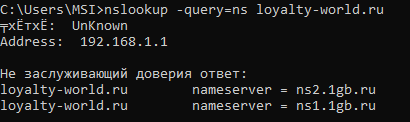
При вводе команды выводится соответственные доменному имени почтовые сервера. То есть, сервера, через которые должна отправляться вся почта на адреса «@loyalty-world.ru», в данном случае на «lw20@loyalty-world.ru». MX preference – приоритет. Чем ниже приоритет, тем больше вероятность (при нескольких почтовых серверов), что почта отправиться через это 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.

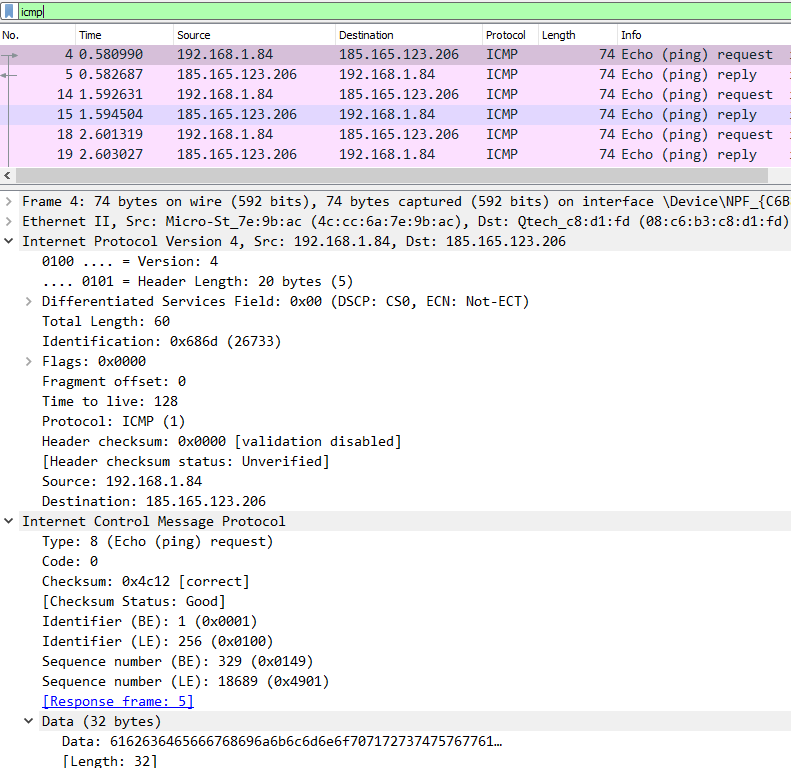
**-query=ns**

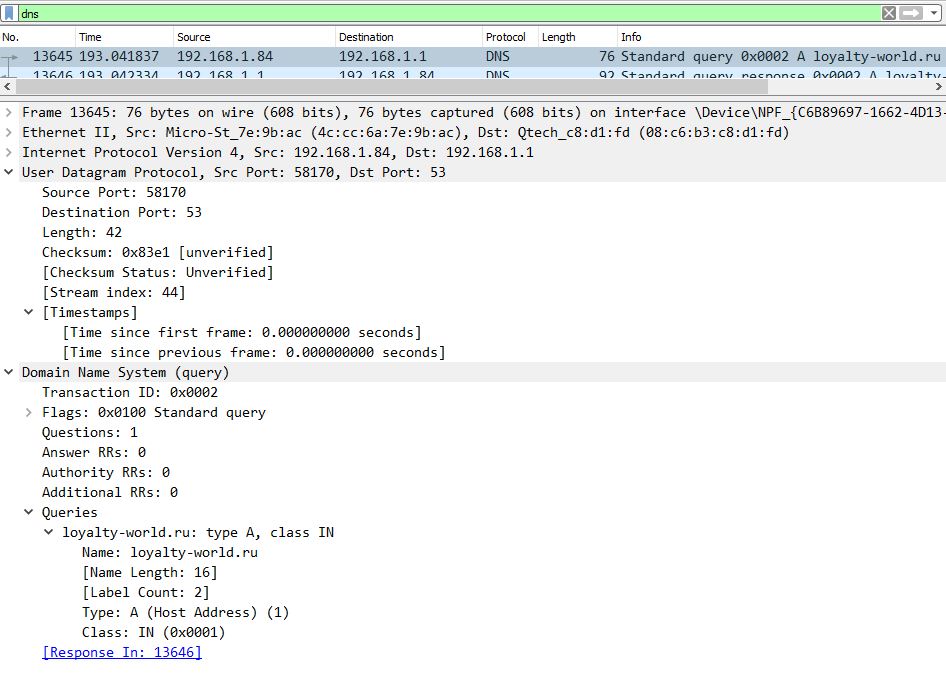


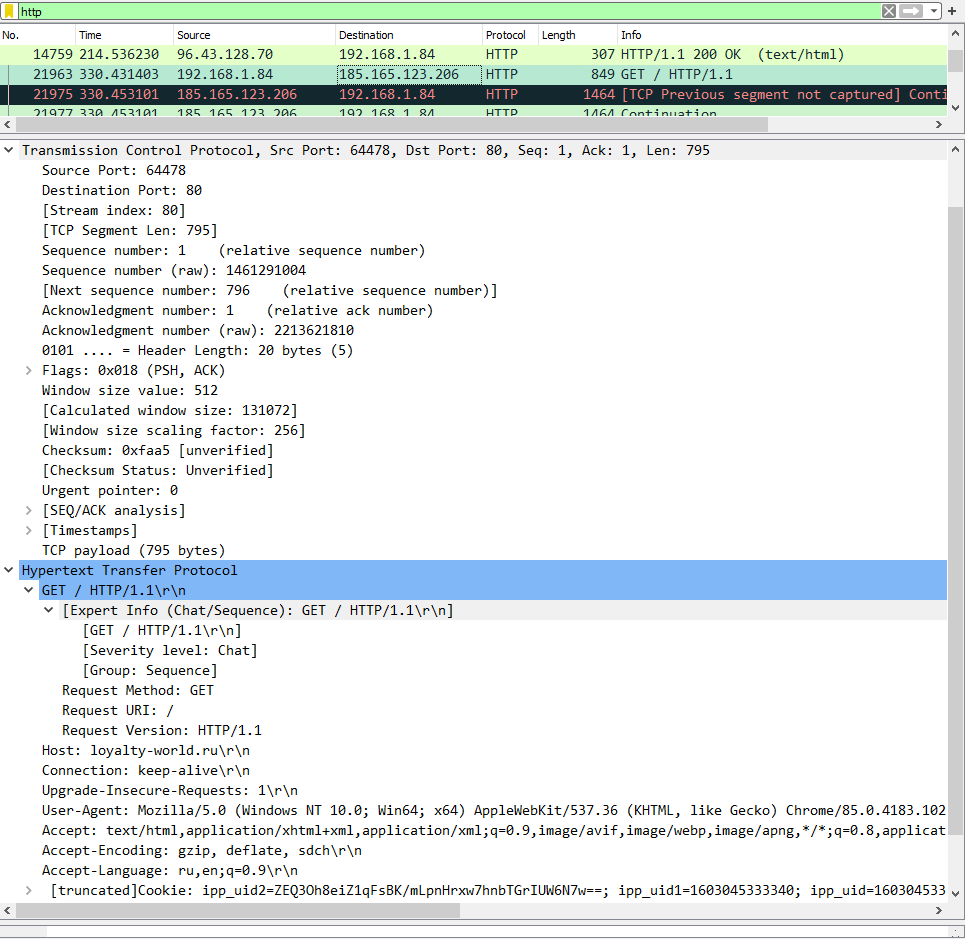
Выводит соответствие доменных имен DNS-серверам

**3. 4. Трафик с сайта**

IP ресурса 185.165.123.206

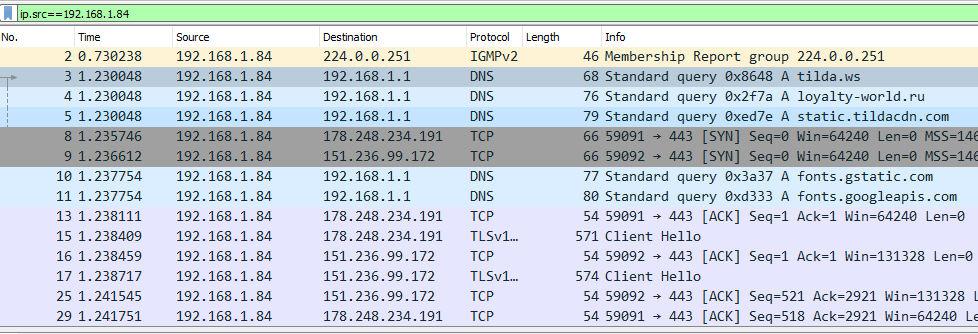






**3. 5. Фильтры**

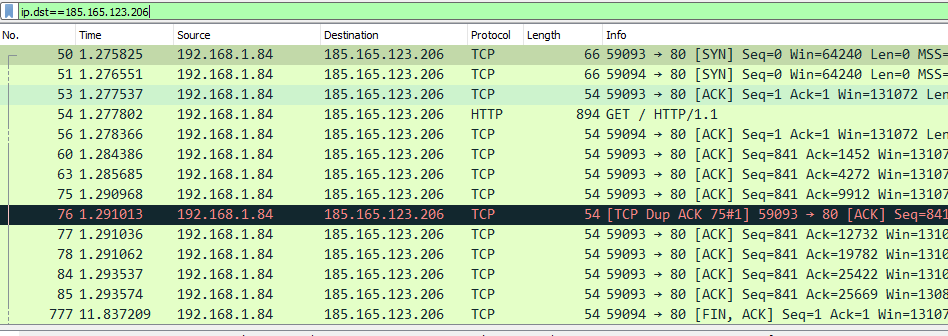
**ip.src**



Пример: i*p.src==192.168.1.84*

Покажет все захваченные пакеты с ip-адресом отправителя 192.168.1.84

**ip.dst**



Пример: i*p.dst==185.165.123.206*

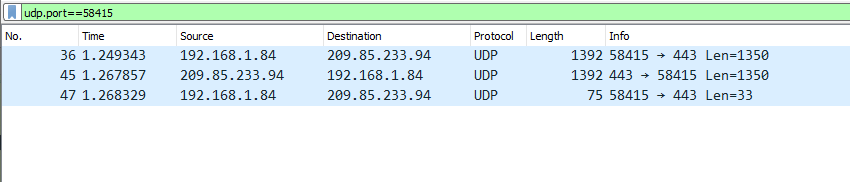
Покажет все захваченные пакеты с ip-адресом получателя 185.165.123.206

**ip.addr**

Пример: *ip.addr==192.168.1.84*

Покажет все захваченные пакеты с ip-адресом отправителя или получателя 192.168.1.84

**udp.port**



Пример: *udp.port==58415*

Выведет все захваченные пакеты с Udp портом *58415* отправителя или получателя

**arp.src.hw\_mac**

Пример:arp.src.hw\_mac==08:c6:b3:c8:d1:fe

Покажет все захваченные пакеты протокола ARP с MAC-адресом отправителя

**eth.dst**

Пример:eth.dst==08:c6:b3:c8:d1:fe

Покажет все захваченные пакеты с MAC-адресом получателя

**eth.src**

Пример: eth.src==08:c6:b3:c8:d1:fe

Покажет все захваченные пакеты с MAC-адресом отправителя