|  |  |  |
| --- | --- | --- |
| |  | | --- | | 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 № 3** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Титов Владислав Андреевич |
|  |

Москва 2020

Оглавление

[Практическая работа №2 3](#_Toc54267065)

[Задание №1 3](#_Toc54267066)

[Задание №2 4](#_Toc54267067)

[Задание №3 5](#_Toc54267068)

[Задание №4 6](#_Toc54267069)

[Фильтр ip.src 9](#_Toc54267070)

[Фильтр ip.dst 10](#_Toc54267071)

[Фильтр ip.addr 10](#_Toc54267072)

[Фильтр udp.port 11](#_Toc54267073)

[Фильтр arp.src.hw\_mac 11](#_Toc54267074)

[Фильтр eth.dst 12](#_Toc54267075)

[Фильтр eth.src 12](#_Toc54267076)

# Практическая работа №2

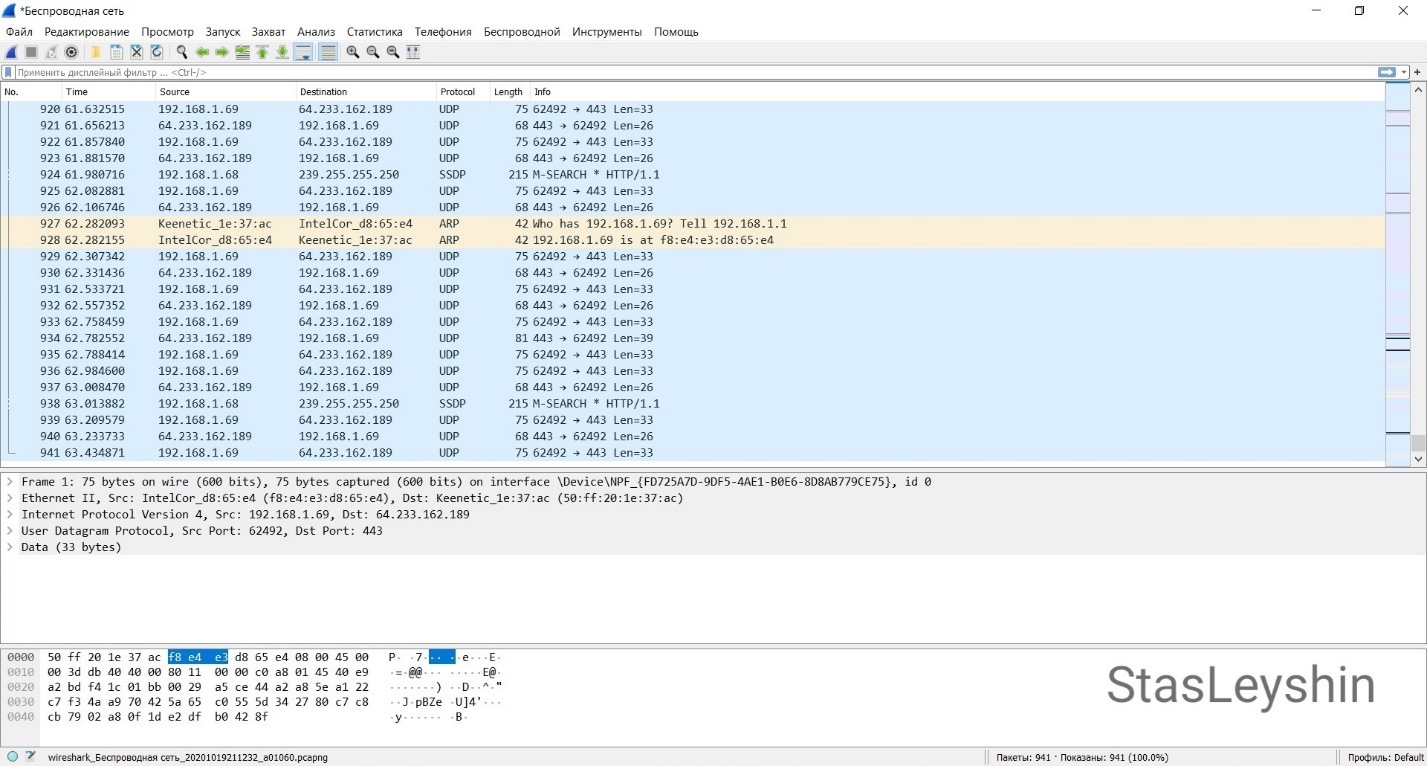
WIRESHARK

## Задание №1

Требуется проанализировать трафик протоколов, а именно:

1. Рассмотреть структуру пакета;

2. Указать назначение заголовков.

В данном окне представлены заголовки протоколов разных уровней:

Frame 1 – Frame протокол не является реальным протоколом, но используется Wireshark в качестве основы для всех других протоколов поверх него. Он показывает информацию из захвата, например точное время захвата определенного кадра. Кадр — это минимальная единица передаваемой информации в сети Ethernet. Вся информация передается только кадрами. Либо кадр прошел (информация дошла до получателя), либо по каким-то причинам получить его не удалось (коллизия, другое повреждение кадра, физические проблемы в сети и т.п.)

Ethernet II – Ethernet, протокол канального уровня;

Internet Protocol Version 4 – IPv4, протокол сетевого уровня;

User Datagram Protocol – UDP, протокол для передачи пользовательских (и многих служебных) данных (обращение к DHCP, DNS, WINS и т.п.). Используется для надежной передачи данных (без установки соединения). Самая важная информация протокола TCP - номер порта получателя и номер порта отправителя, то есть идентификаторы конечных приложений (служб) на компьютере, которым предназначен пакет.

Data – когда Wireshark не может определить, как часть пакета должна быть отформатирована, он помечает этот кусок как Data. Это может быть вызвано следующим:

* Data — это протокол, который Wireshark не поддерживает.
* Data — это протокол, который был отключен с помощью функции включенных протоколов Wireshark;
* Data — это протокол, который Wireshark поддерживает, но не распознает. Если это так, вы можете использовать функцию декодирования Wireshark, указанную пользователем, или ее настройки протокола, чтобы принудительно декодировать протокол;
* Data — это именно то, что является обычной полезной нагрузкой данных протокола.

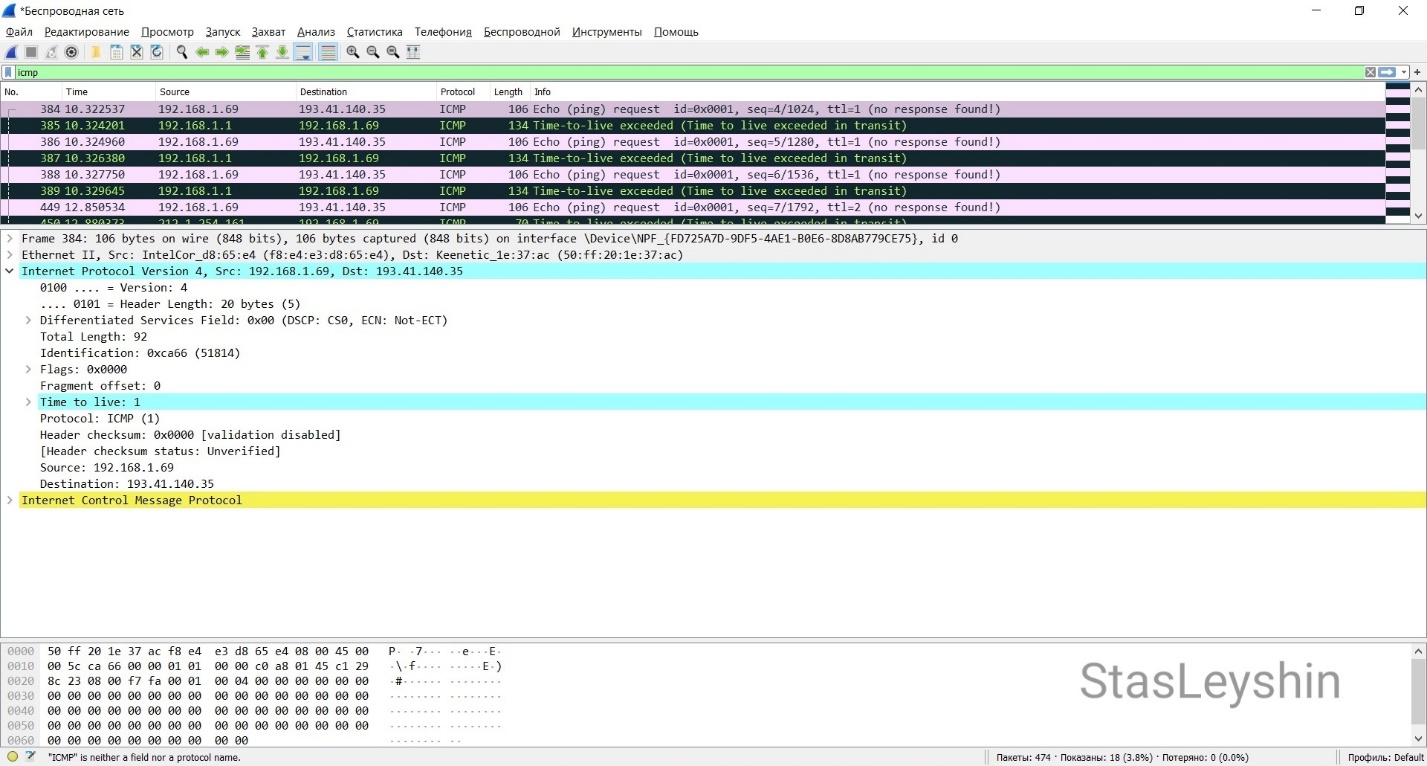
## Задание №2

1. Проанализируйте первый пакет ICMP Echo Request, отправленный вашим

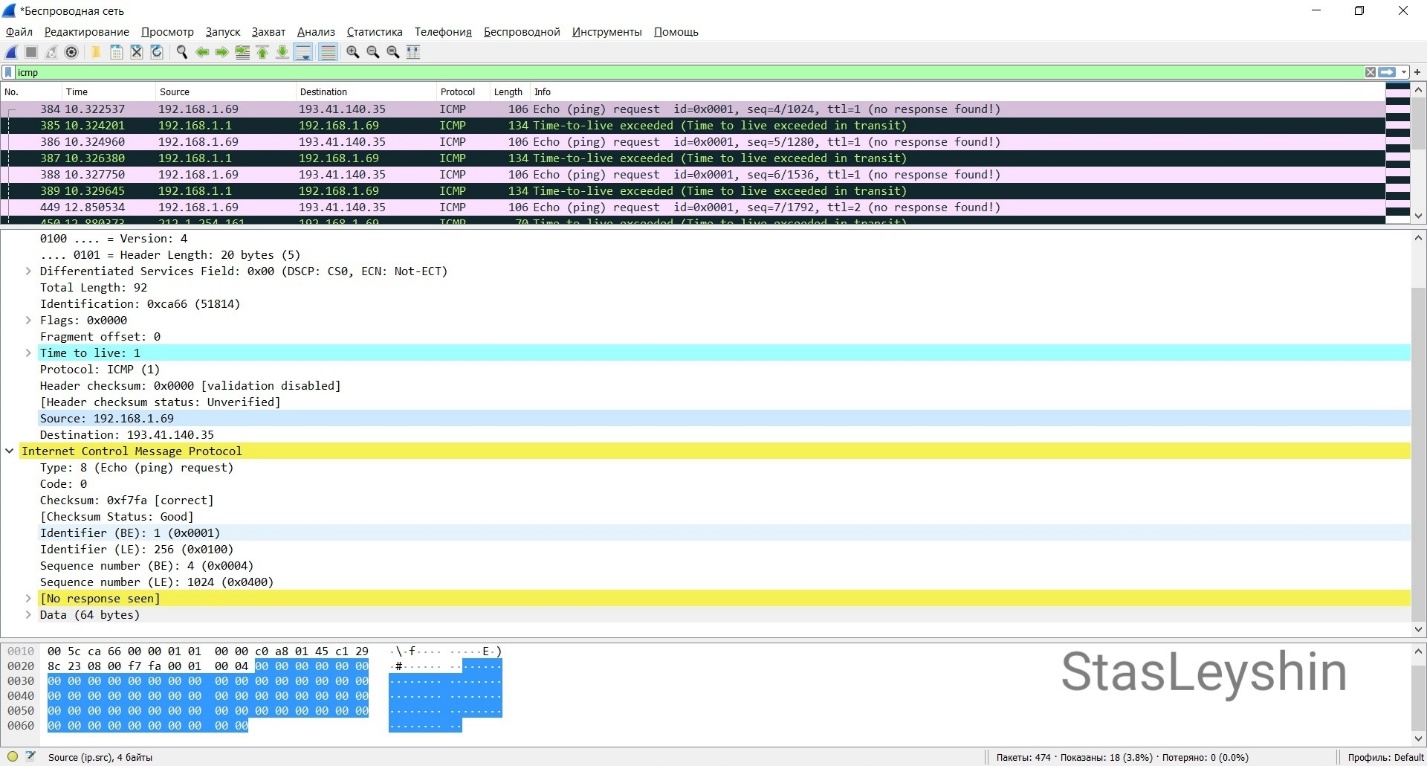
компьютером: укажите ваш IP-адрес.

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

3. Укажите значение TTL.



1. IP: 192.168.1.69
2. В заголовке 20 байтов, 64 байт в поле данных
3. TTL: 1

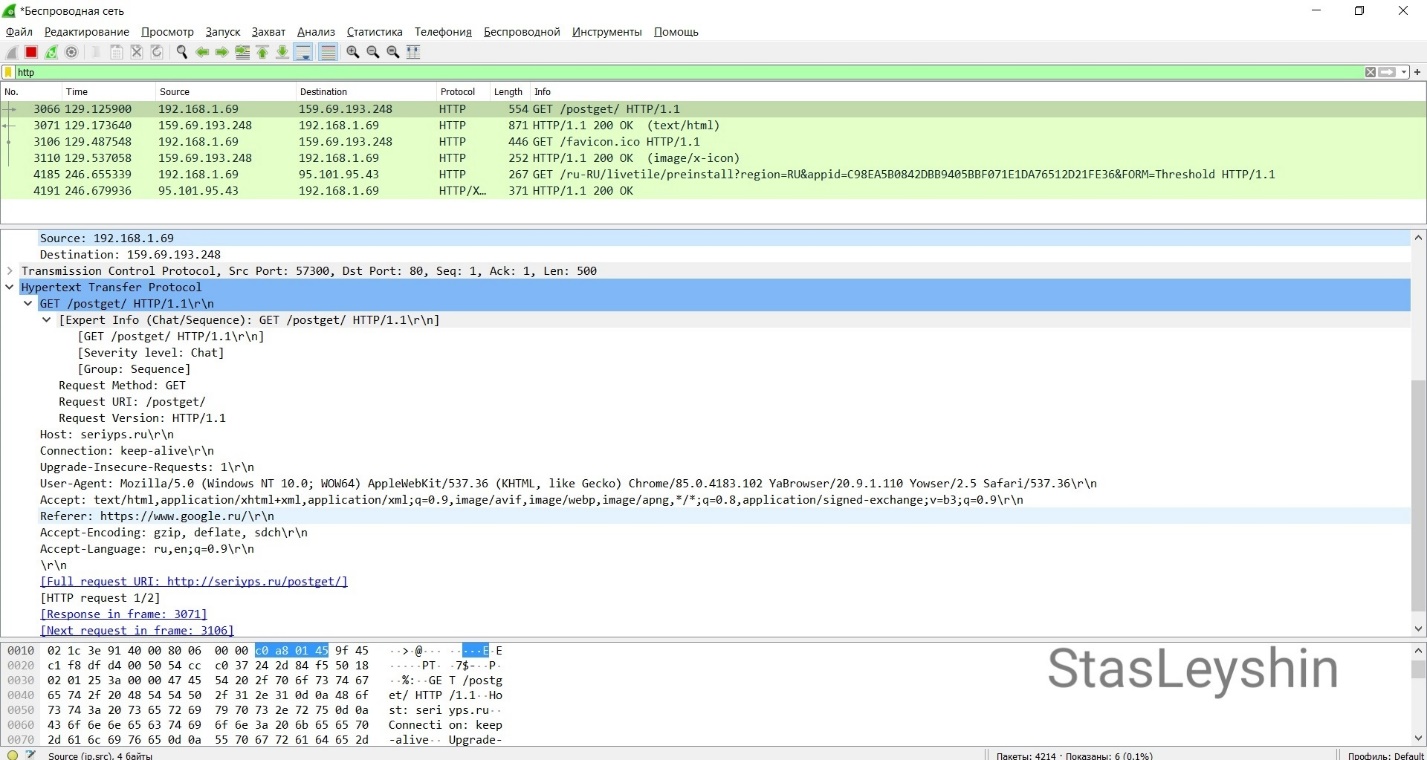


## Задание №3

В списке захваченных пакетов требуется найти пару HTTP сообщений (запросответ): 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).



1. Версия HTTP 1.1
2. IP компьютера: 192.168.1.69; IP адрес сервера: 159.69.193.248
3. Код состояния HTTP: 200
4. Длина тела сообщения: 554

## Задание №4

1. Произвести обнаружение узлов в ГИС «Интернет» узлов, использующ их

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;

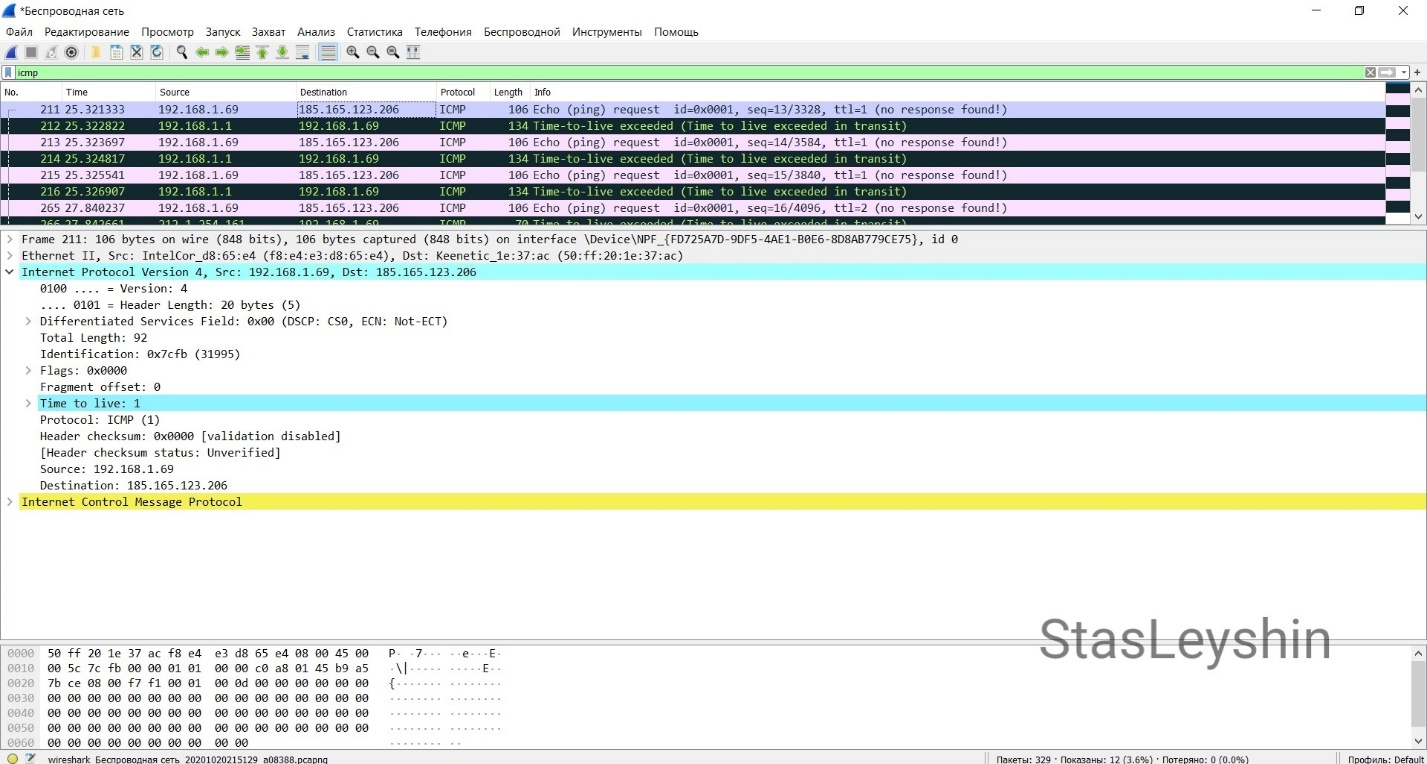
ip.addr, udp.port, arp.src.hw\_mac, eth.dst, eth.src.

6. Составить отчёт в электронном виде.

7. Загрузить отчёт в репозиторий на github.

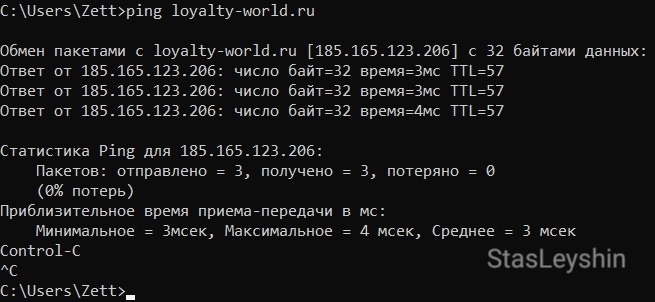
Ресурс: loyalty-world.ru

IP адрес: 185.165.123.206 команда: tracert loyalty-world.ru





IP адрес: 185.165.123.206 команда: ping loyalty-world.ru



IP адрес: 185.165.123.206 команда: nslookup loyalty-world.ru



1. Команда: nslookup -query=mx loyalty-world.ru

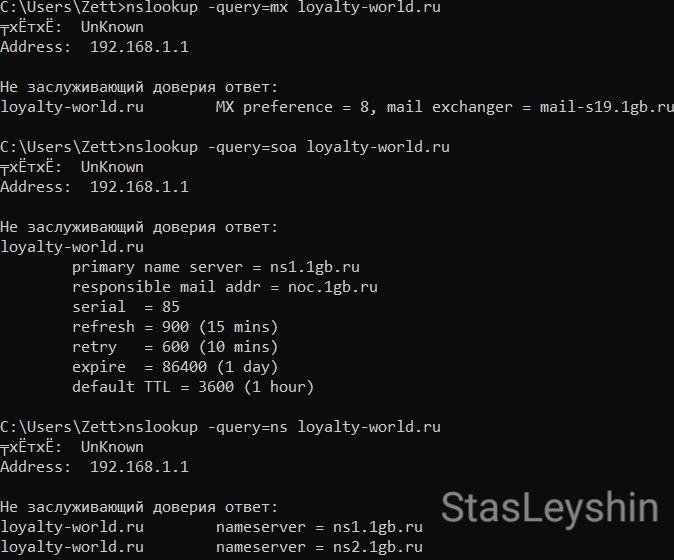
При вводе команды выводится соответственные доменному имени почтовые сервера. То есть, сервера, через которые должна отправляться вся почта на адреса «@loyalty-world.ru», в данном случае на «lw20@loyalty-world.ru». MX preference – приоритет. Чем ниже приоритет, тем больше вероятность (при нескольких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

2. Команда: nslookup -query=soa loyalty-world.ru

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.

3. Команда: nslookup -query=ns loyalty-world.ru

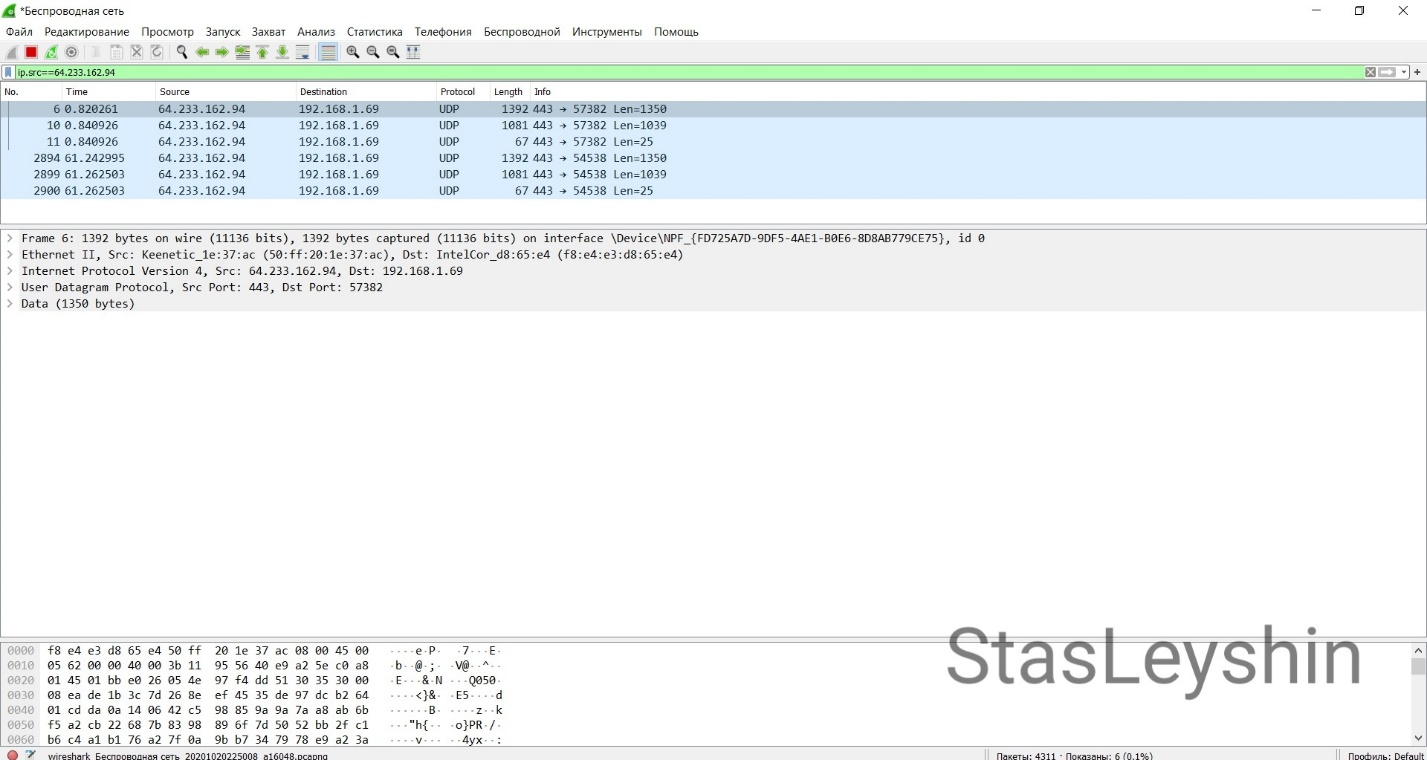
Выводит соответствие доменных имен DNS-серверам



### Фильтр ip.src

Пример: ip.src==64.233.162.94

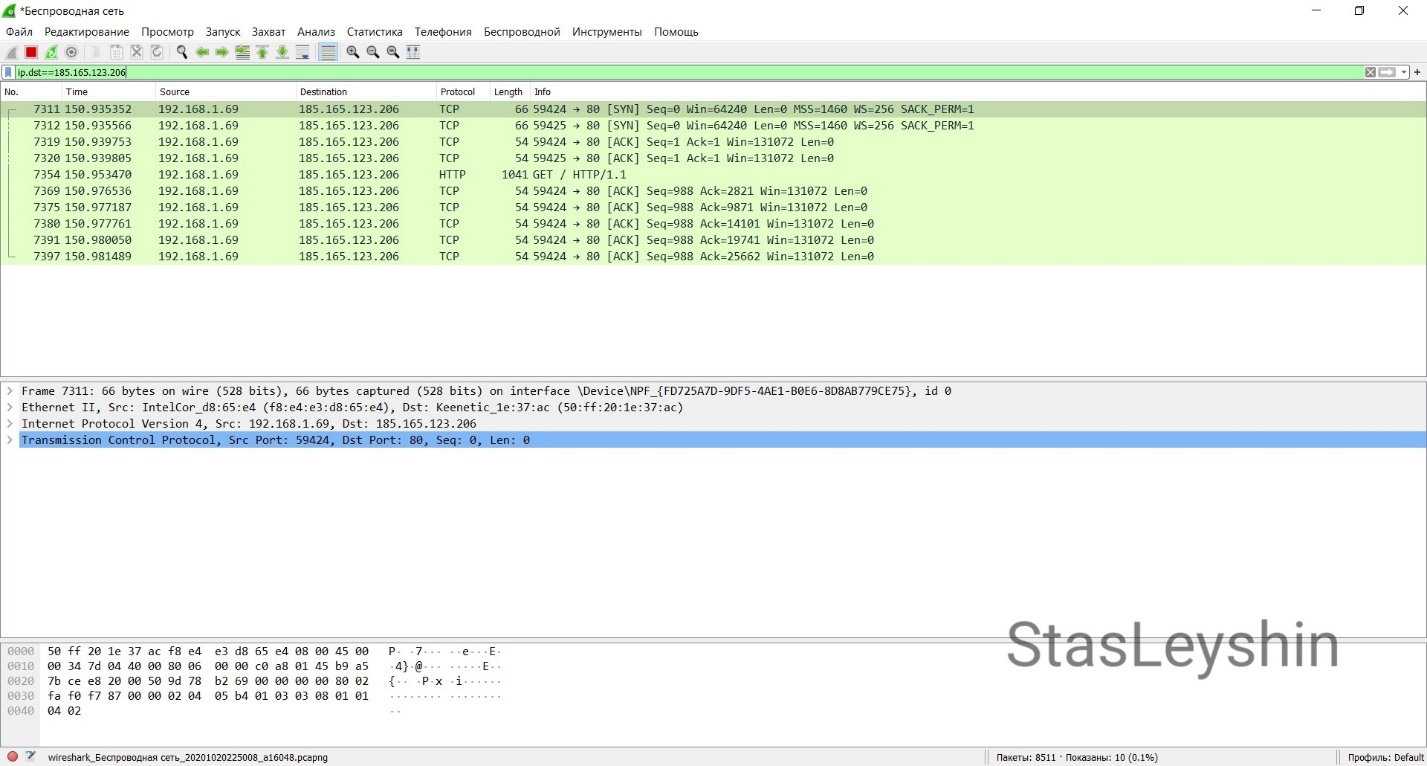
Покажет все захваченные пакеты с ip-адресом отправителя 64.233.162.94



### Фильтр ip.dst

Пример: ip.dst==185.165.123.206

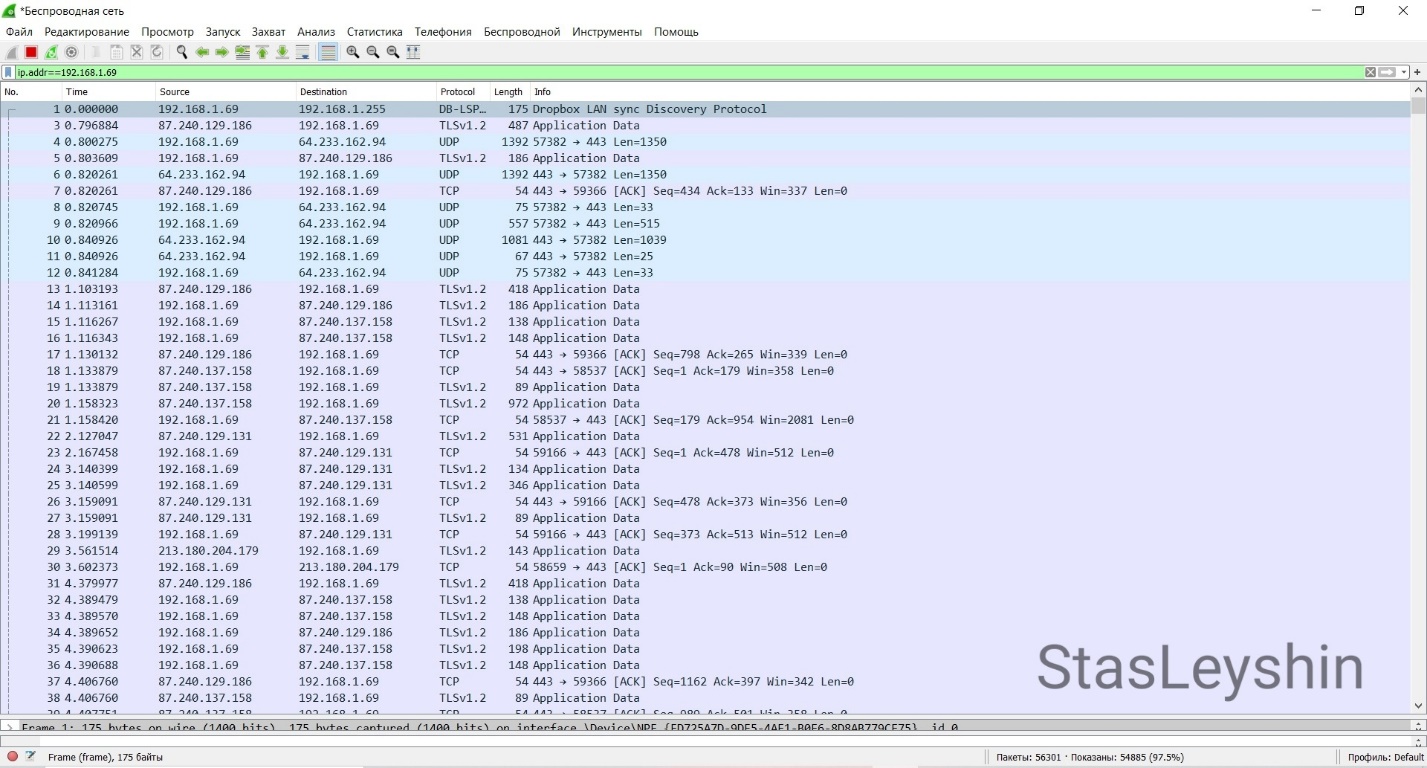
Покажет все захваченные пакеты с ip-адресом получателя 185.165.123.206



### Фильтр ip.addr

Пример: ip.addr==192.168.1.69

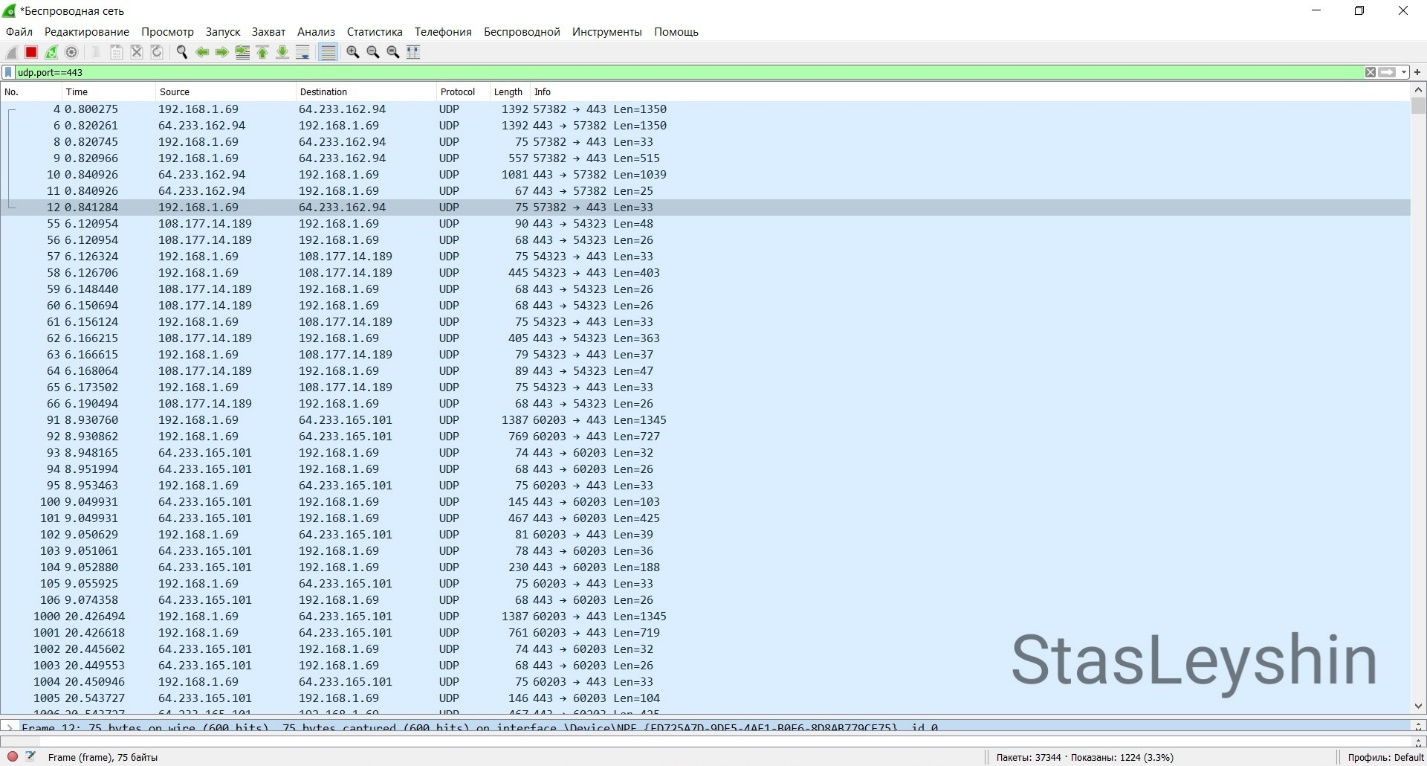
Покажет все захваченные пакеты с ip-адресом отправителя или получателя 192.168.1.69



### Фильтр udp.port

Пример: udp.port==443

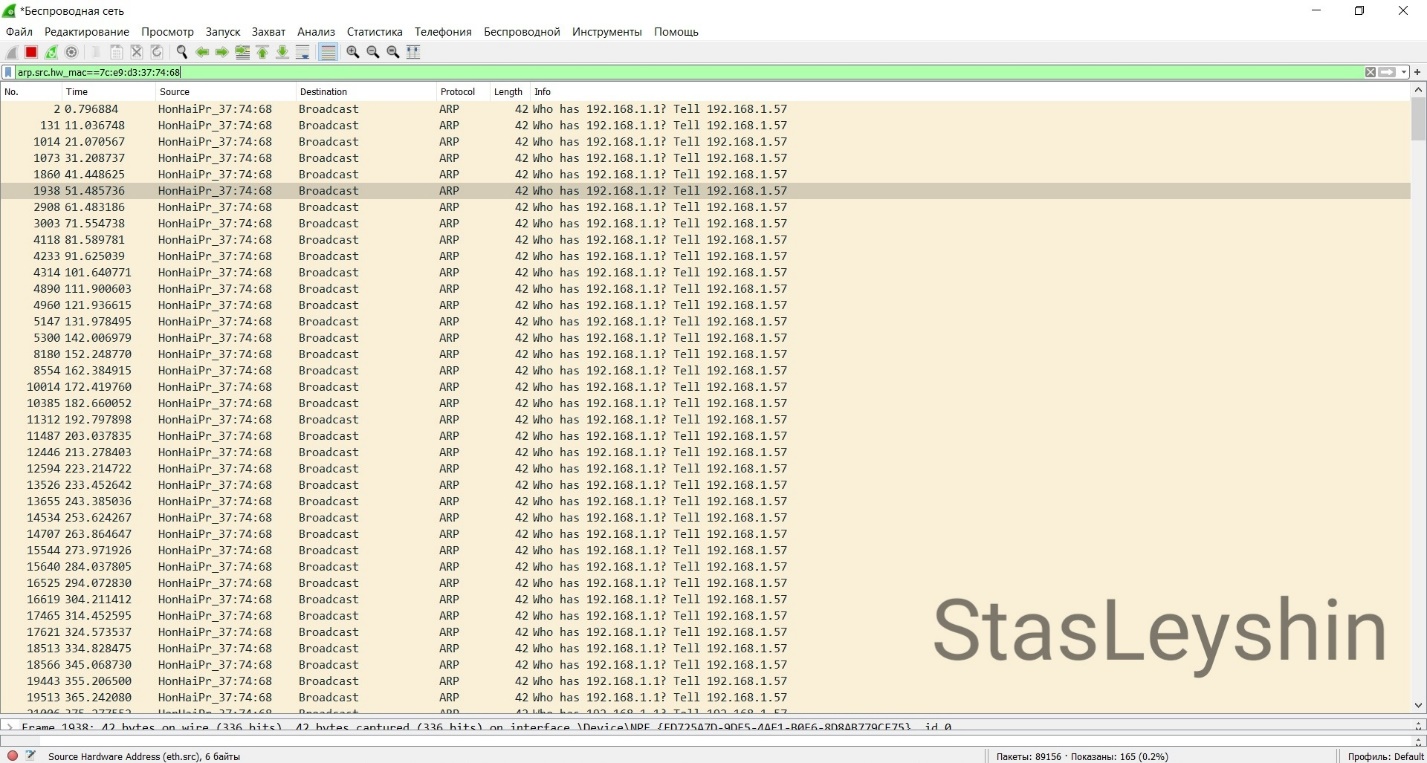
Выведет все захваченные пакеты с Udp портом 443 отправителя или получателя



### Фильтр arp.src.hw\_mac

Пример:arp.src.hw\_mac== 7c:e9:d3:37:74:68

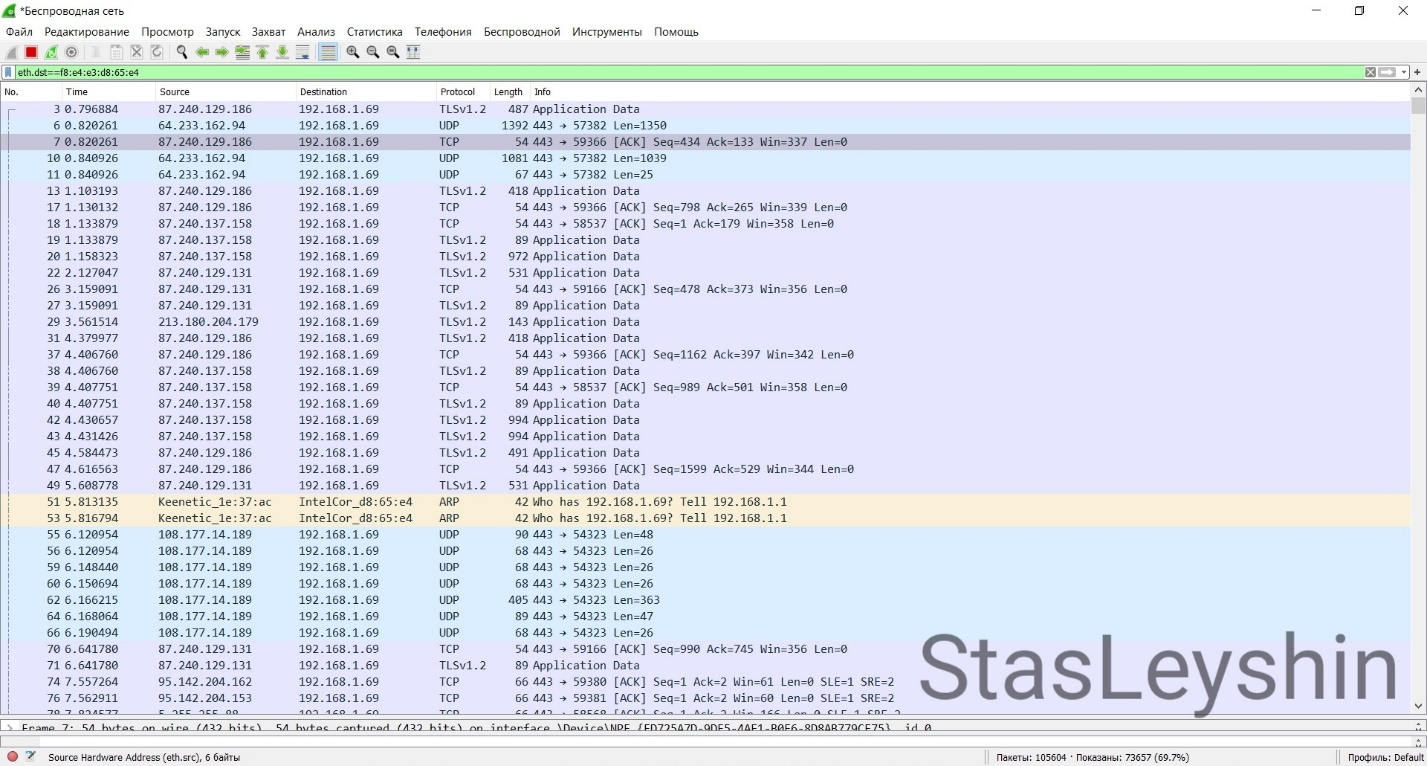
Покажет все захваченные пакеты протокола ARP с MAC-адресом отправителя



### Фильтр eth.dst

Пример:eth.dst== 7c:e9:d3:37:74:68

Покажет все захваченные пакеты с MAC-адресом получателя



### Фильтр eth.src

Пример: eth.src== 7c:e9:d3:37:74:68

Покажет все захваченные пакеты с MAC-адресом отправителя

