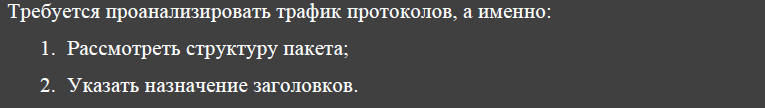
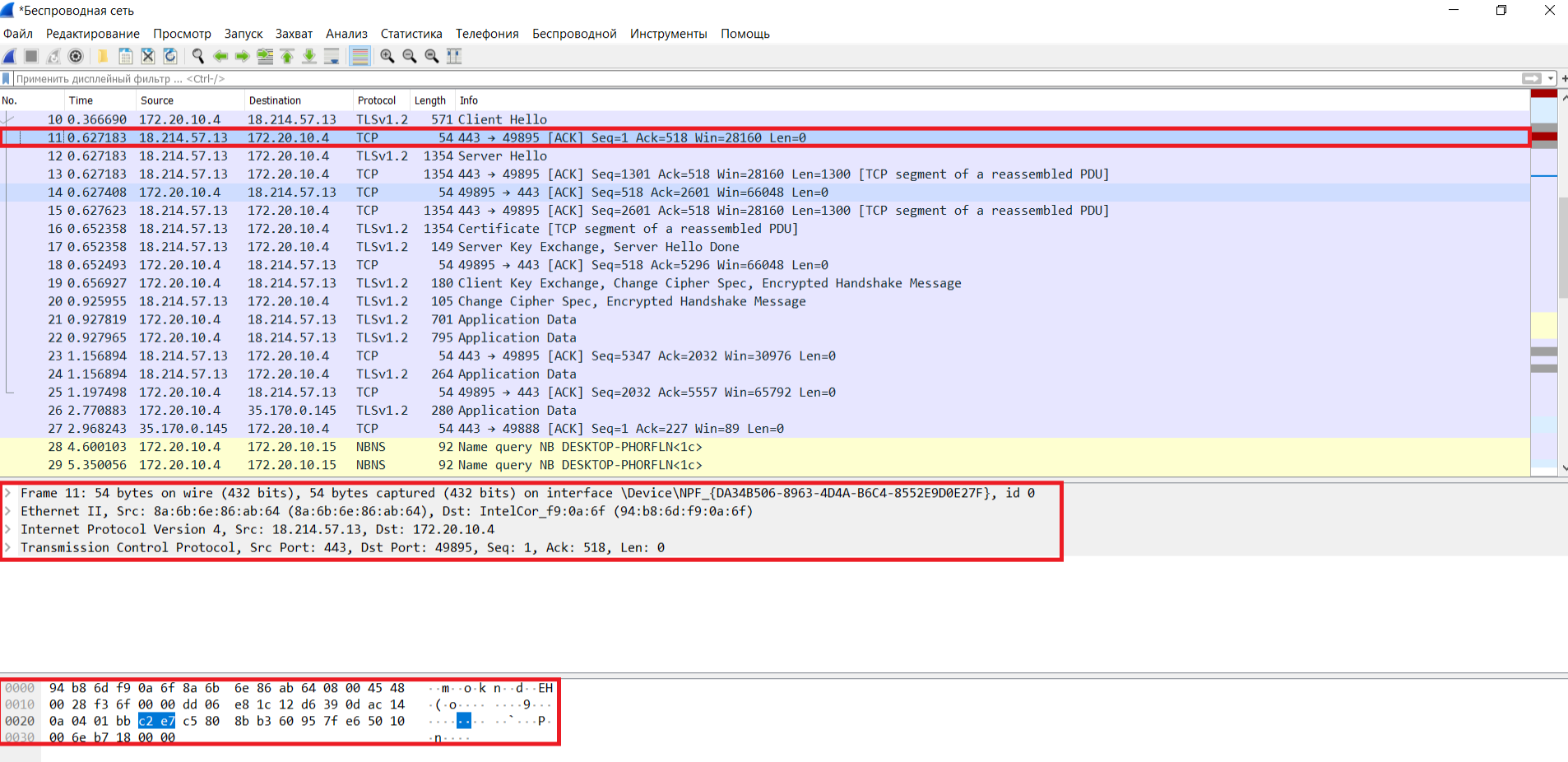
|  |
| --- |
|  |
| Отчёт по ОИБ |
| Практика №2 |

|  |
| --- |
| Кочалиев Расим Рустемович  09.10.2020 |

# Задание №1



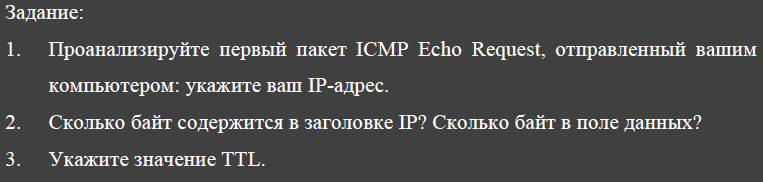
1. Для данного задания был взят 11 пакет.

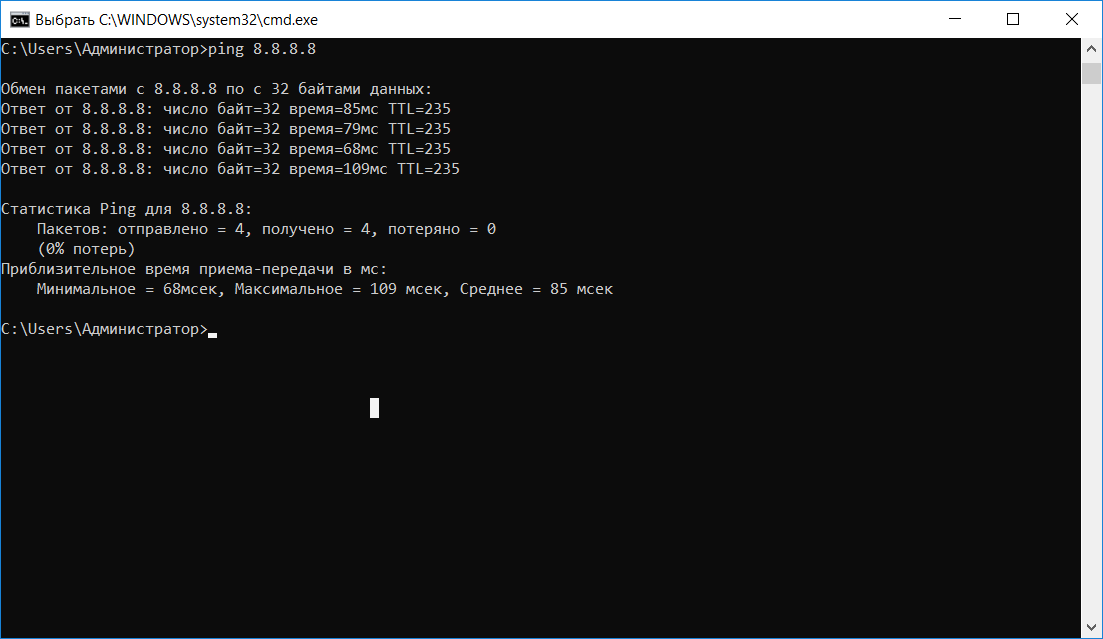
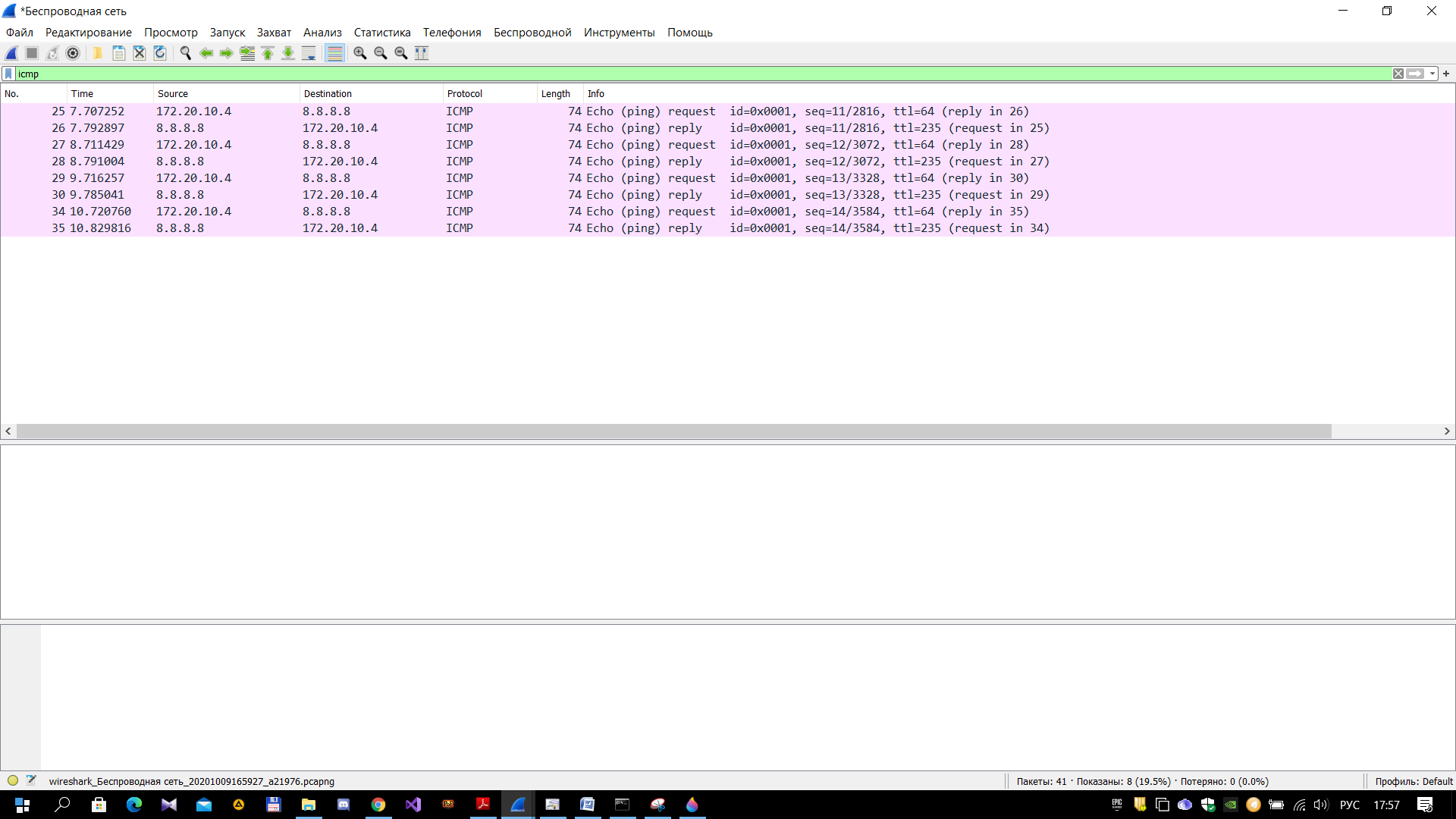


Кочалиев

1. Пакет состоит из 4 заголовков:
   1. Frame 11 (Протокол физического уровня)
   2. Ethernet 2 (Протокол канального уровня)
   3. Internet Protocol Version 4 (IPv4, Протокол сетевого уровня)
   4. Transmission Control Protocol (Протокол транспортного уровня)
2. Назначение заголовков:
   1. Frame (Физический уровень) — первый уровень сетевой модели OSI. Физический уровень описывает способы передачи бит (а не пакетов данных) через физические среды линий связи, соединяющие сетевые устройства.
   2. Ethernet – второй уровень сетевой модели OSI. Предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети.
   3. Internet Protocol Version – 3-й уровень сетевой модели OSI. Предназначается для определения пути передачи данных.
   4. Transmission Control Protocol – 4-й уровень сетевой модели OSI. Предназначен для доставки данных

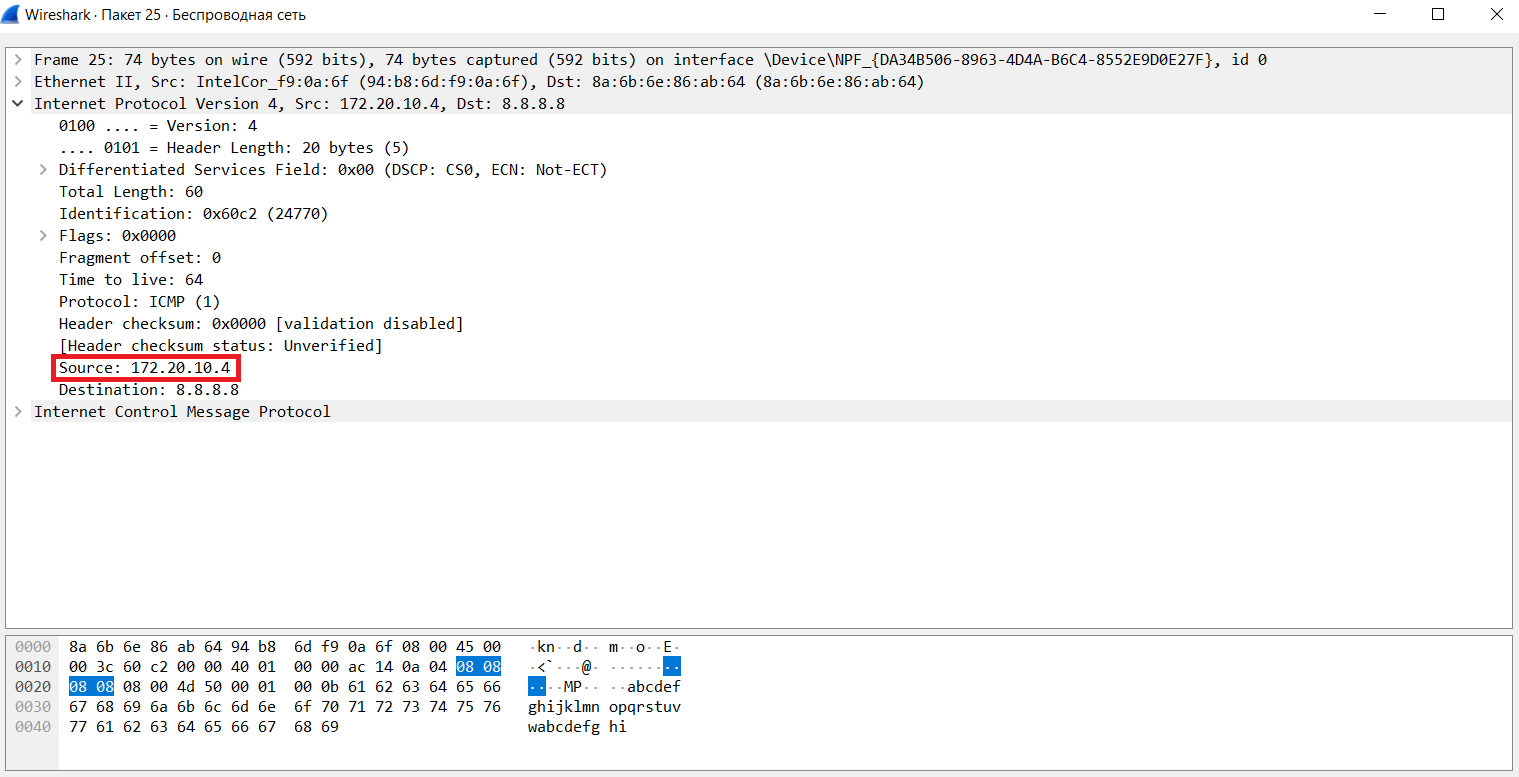
# Задание №2



1. Используя утилиту PING, я решил проверить доступность DNS-сервера Google, который имеет IP-адрес 8.8.8.8

Кочалиев

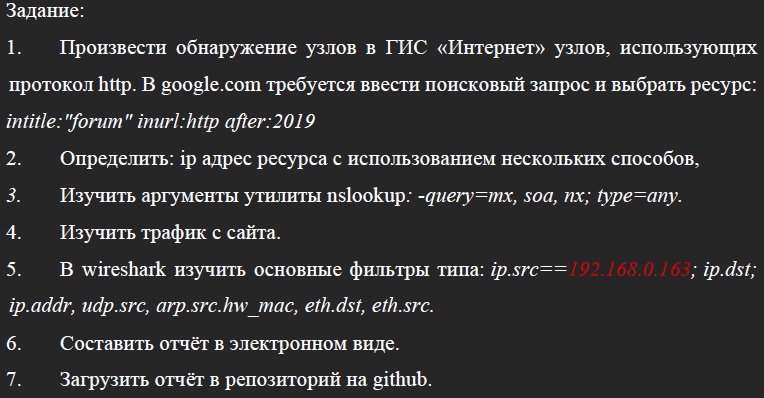
Кочалиев

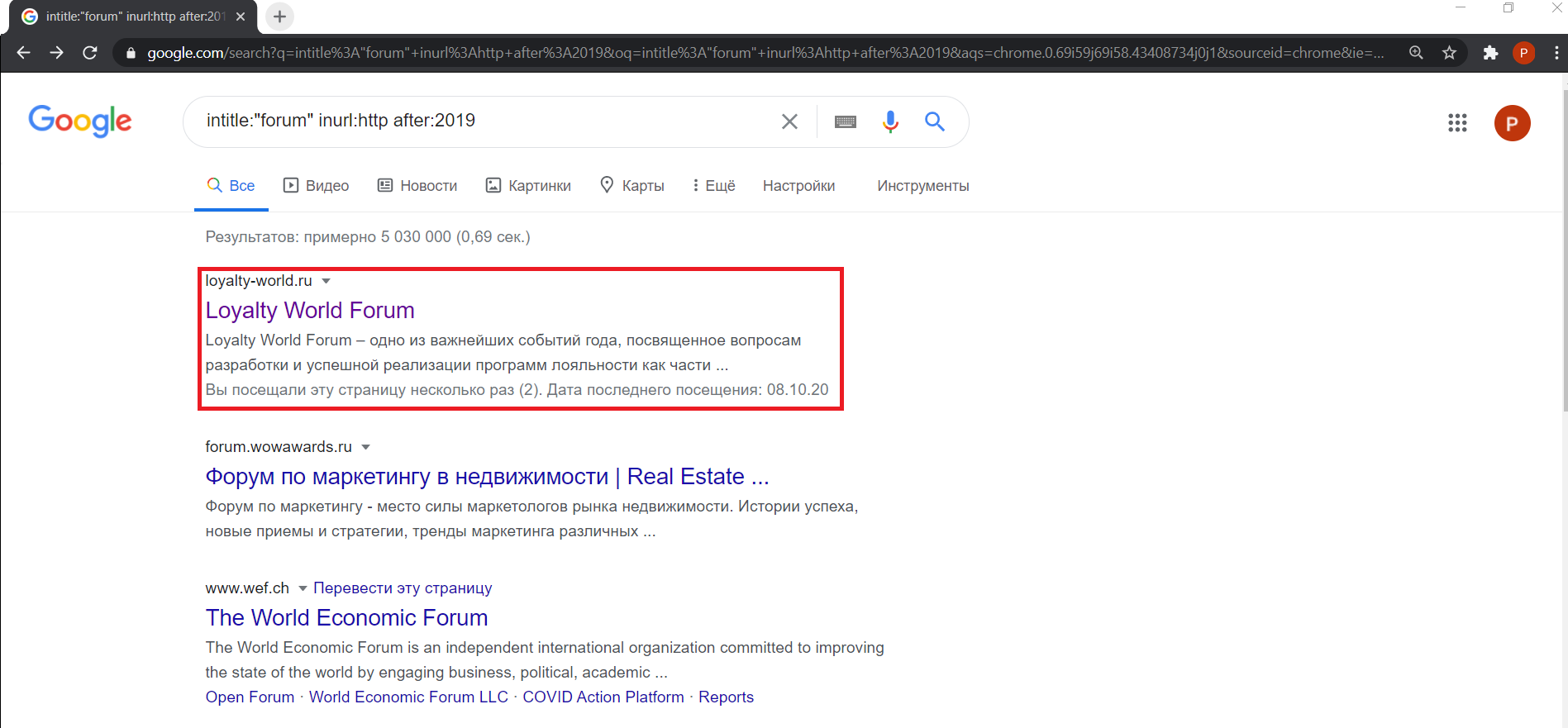


Кочалиев

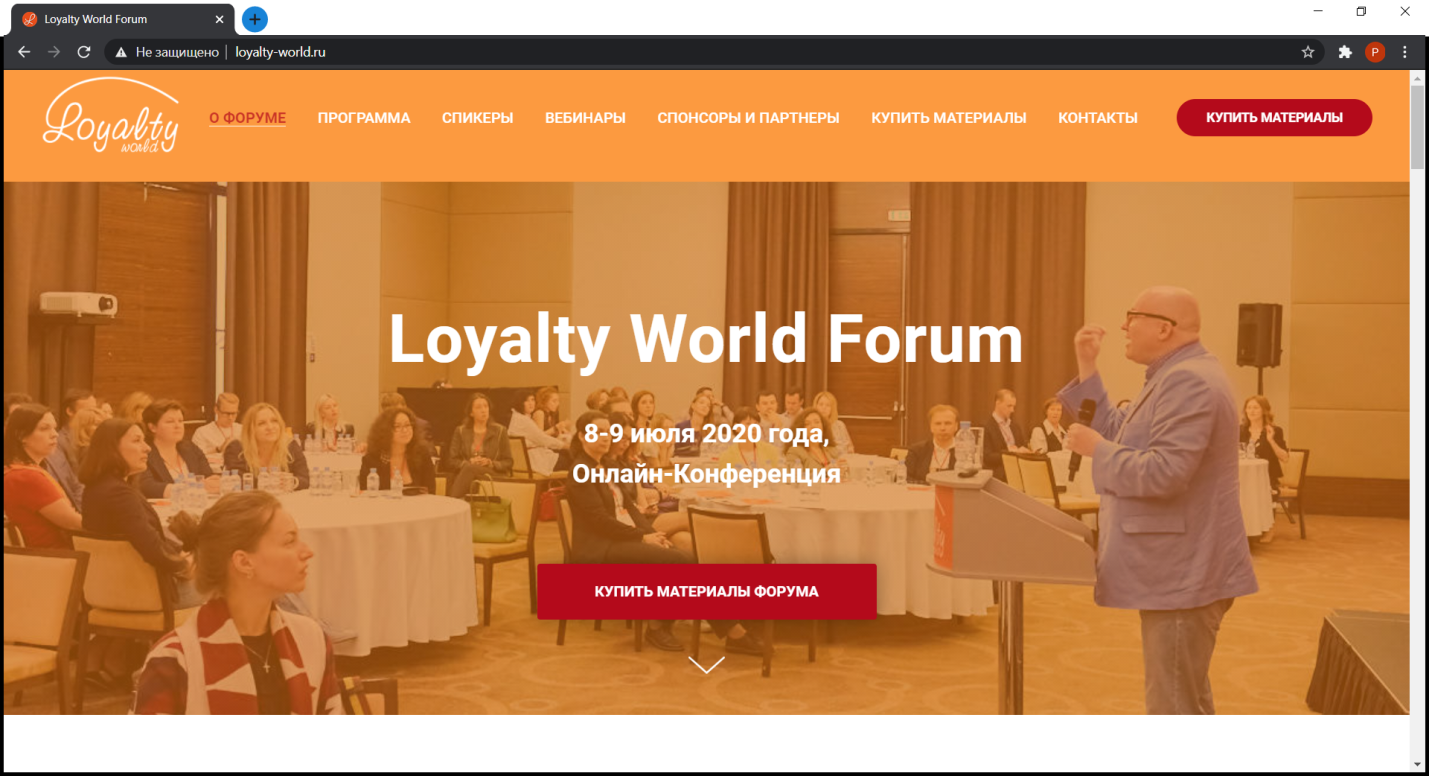
1. Проанализировав первый пакет ICMP, я понял, что мой IP-адрес: 172.20.10.4
2. 20 байт, 4 байта.
3. Time to live составляет 64

# Задание №3

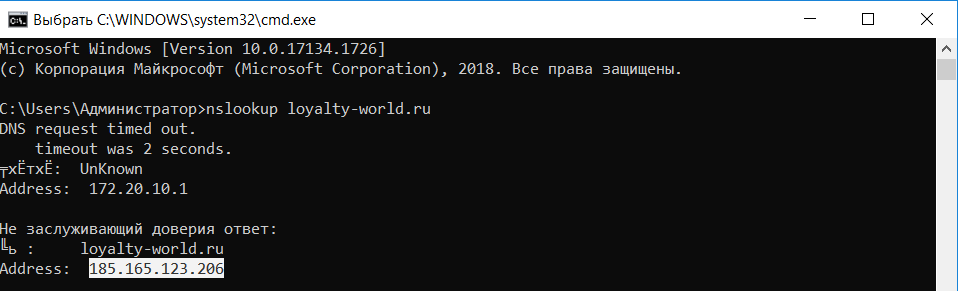


1. Введя в поисковый запрос intitle: “forum” in url: http after: 2019. Этот запрос является строгим, так как мы находим все сайты форумов с протоколом http, которые были проведены или будут проведены после 2019. Я выбираю самый первый Loyalty World Forum.

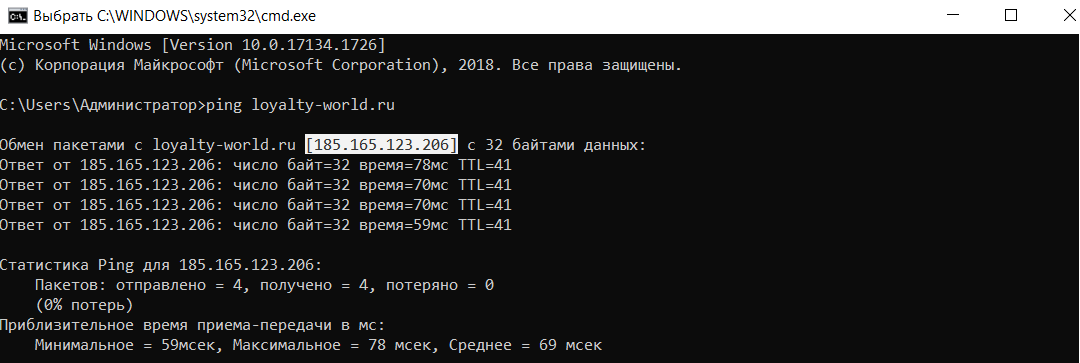
Кочалиев

1. Сайт выглядит следующим образом, теперь будем определять ip ресурса несколькими способами. 

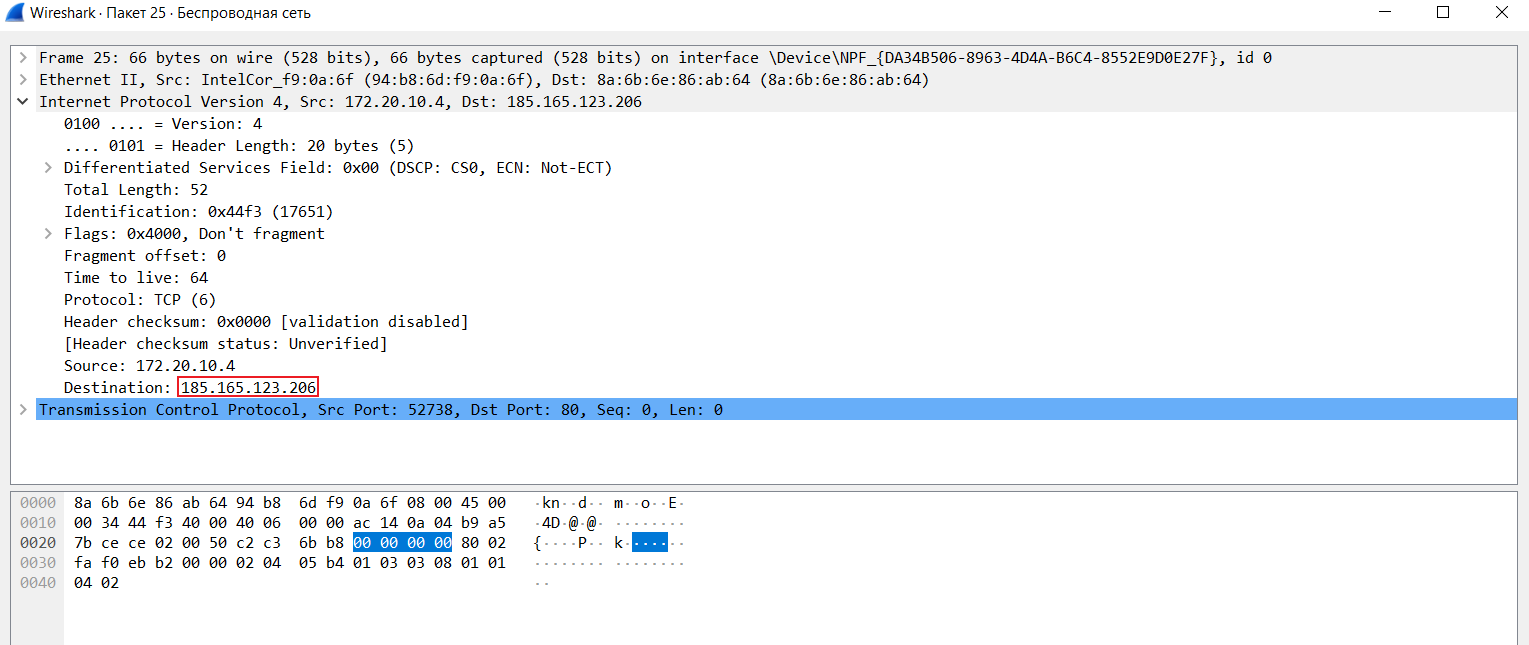
Кочалиев

1. Первый способ с помощью утилиты nslookup. Получили ip адрес 185.165.123.206

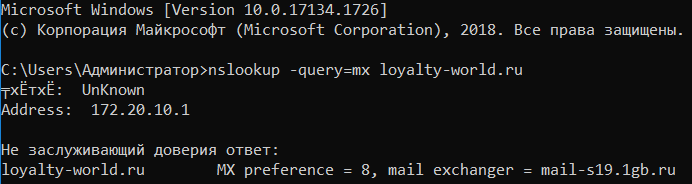
Кочалиев

1. Теперь попробуем определить ip адрес при помощи утилиты ping. Неудивителньо, что ip адрес мы получили такой же 185.165.123.206

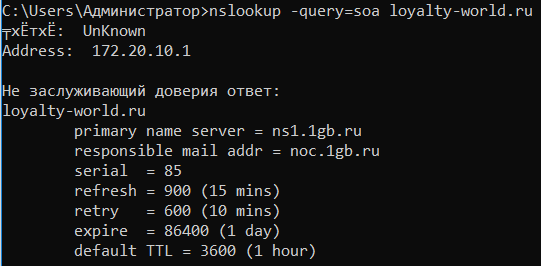
Кочалиев

1. И последней способ, это при помощи wireshark. Снова получаем ip адрес равный 185.165.123.206

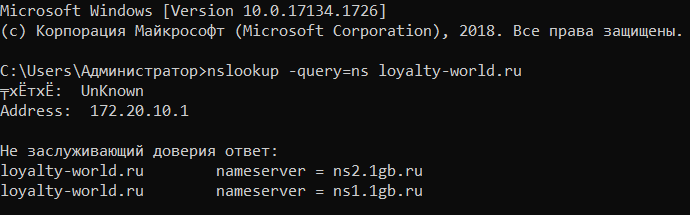
Кочалиев

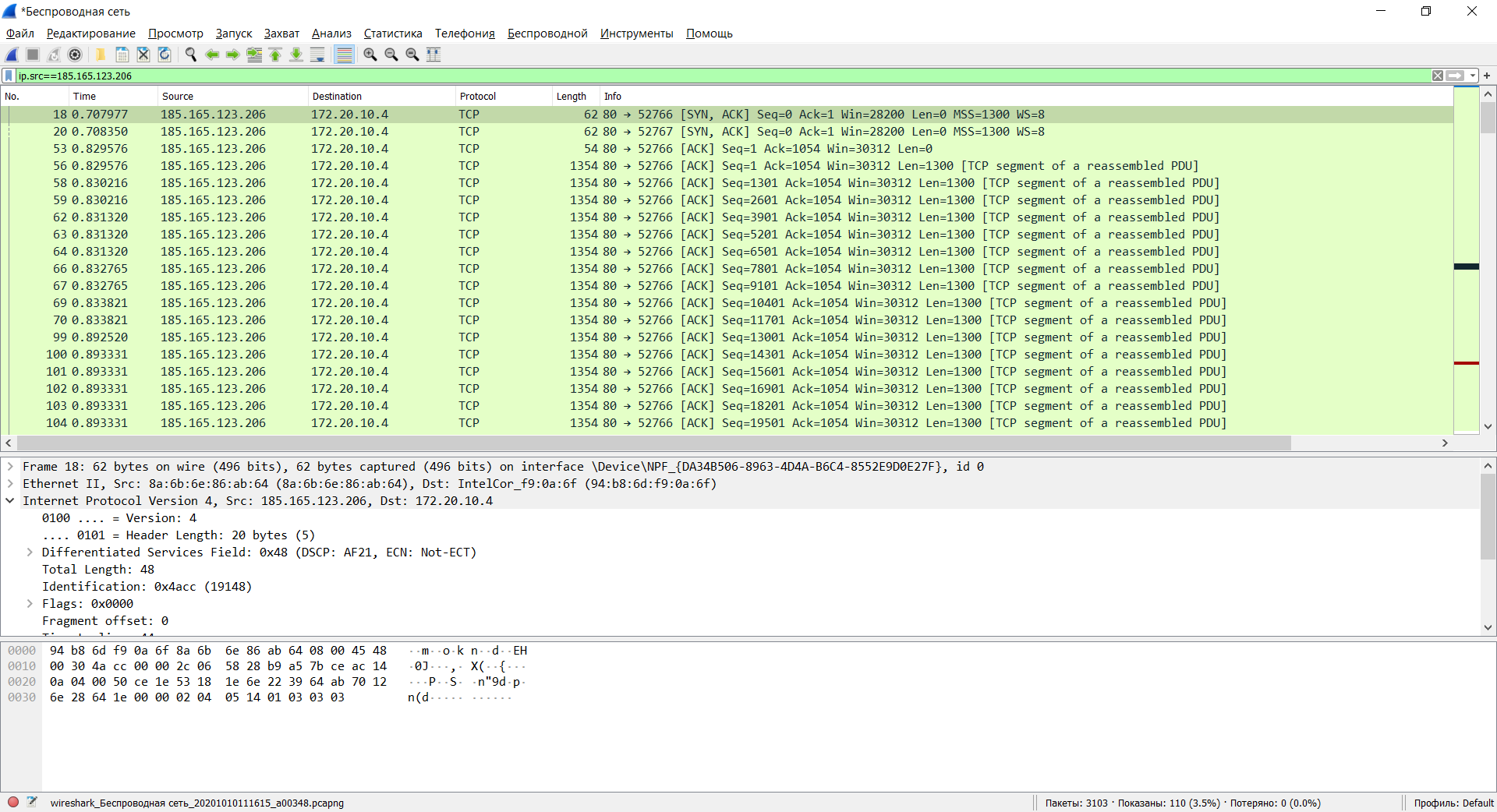
1. Изучение аргументов nslookup
   1. -query=mx. Хранит соответствие доменного имени почтовому серверу этого домена.

Кочалиев

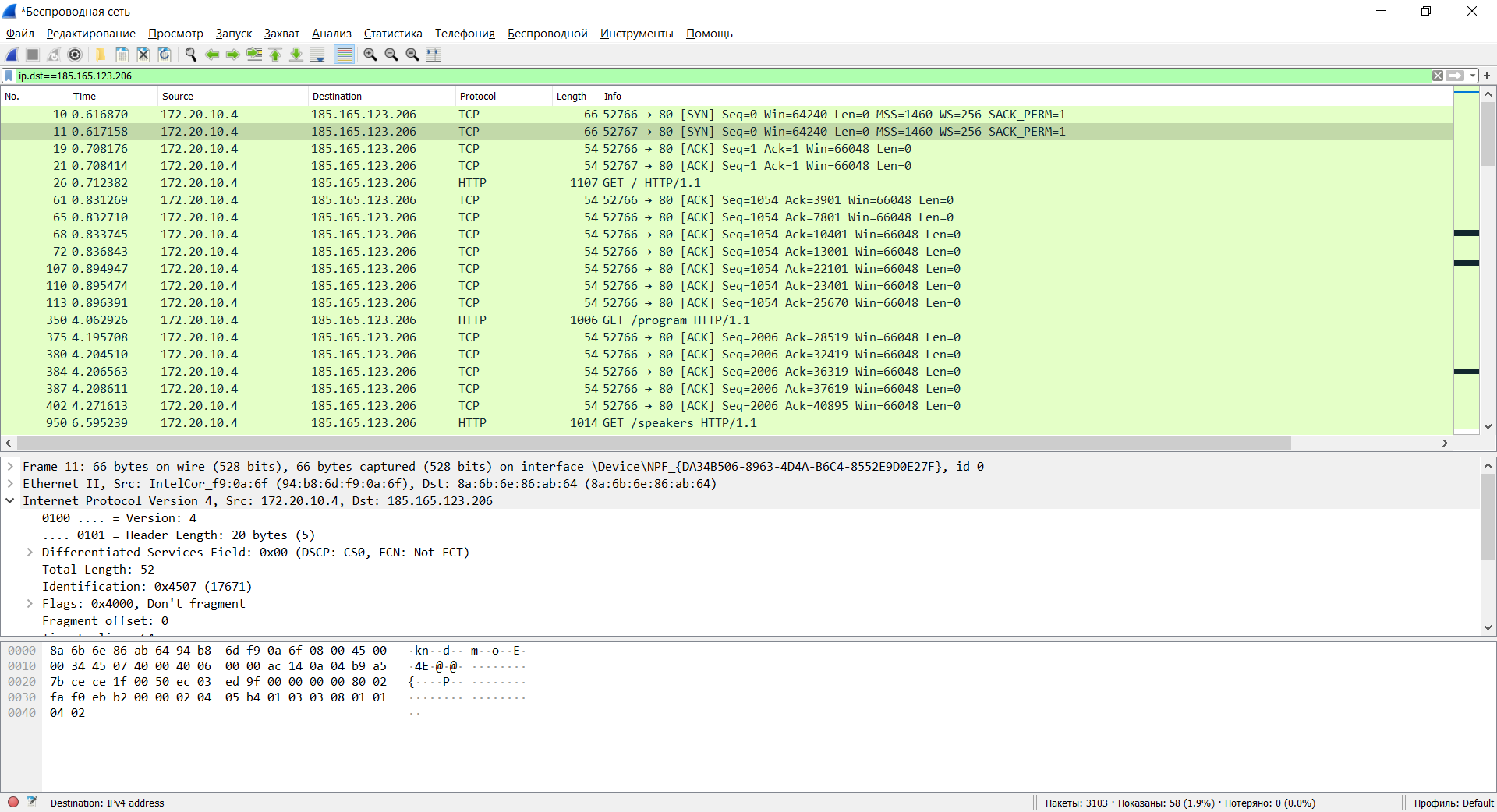
* 1. -query=soa. Cодержит информацию о зоне домена, адрес его администратора, серийный номер и т.д

Кочалиев

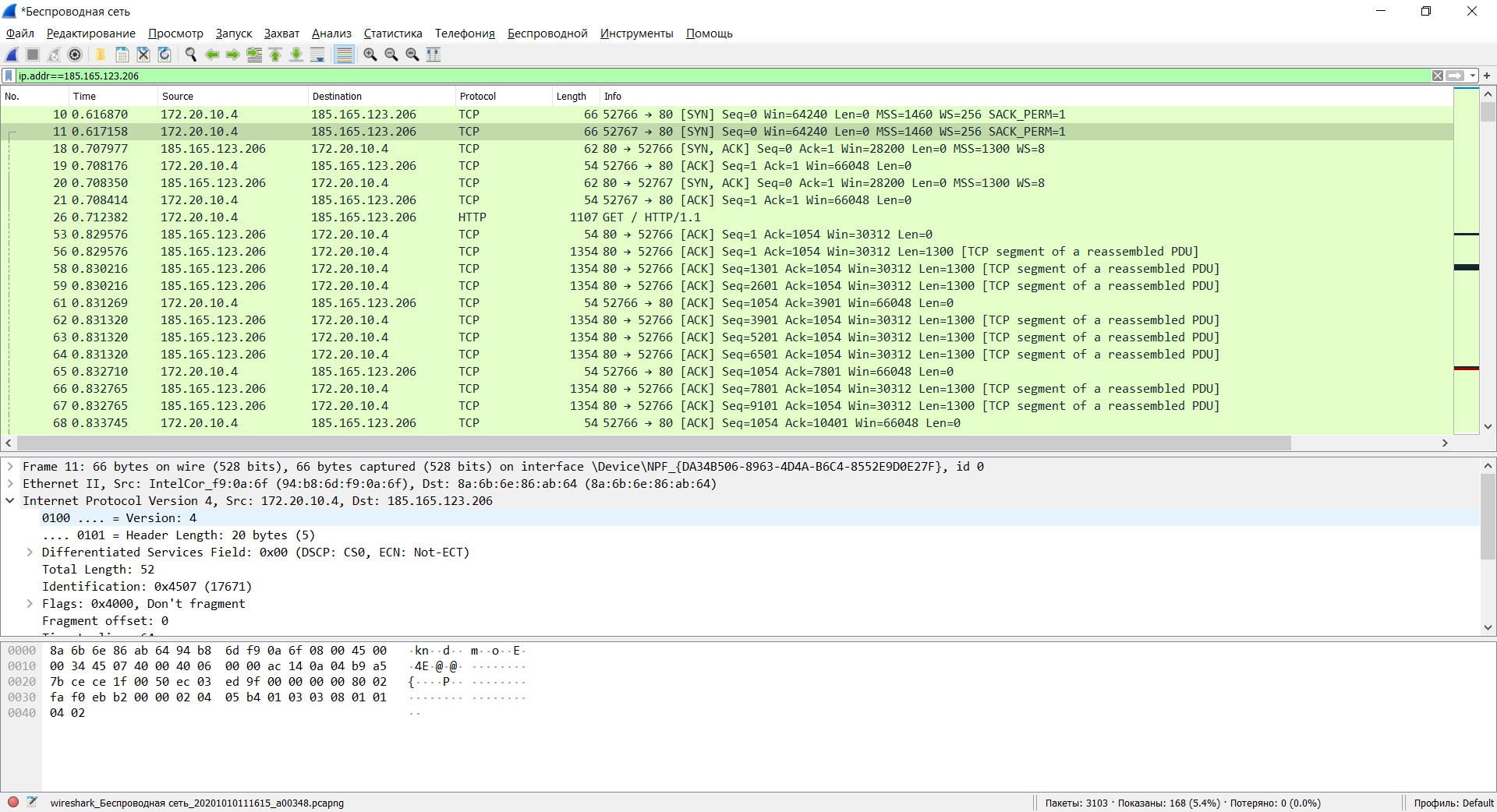
* 1. -query=ns. Cодержит соответствие доменного имени DNS-серверу, авторитативному для заданного домена.

1. Изучение основных фильтров
   1. ip.src==185.165.123.206. Фильтр по IP адресу отправителя

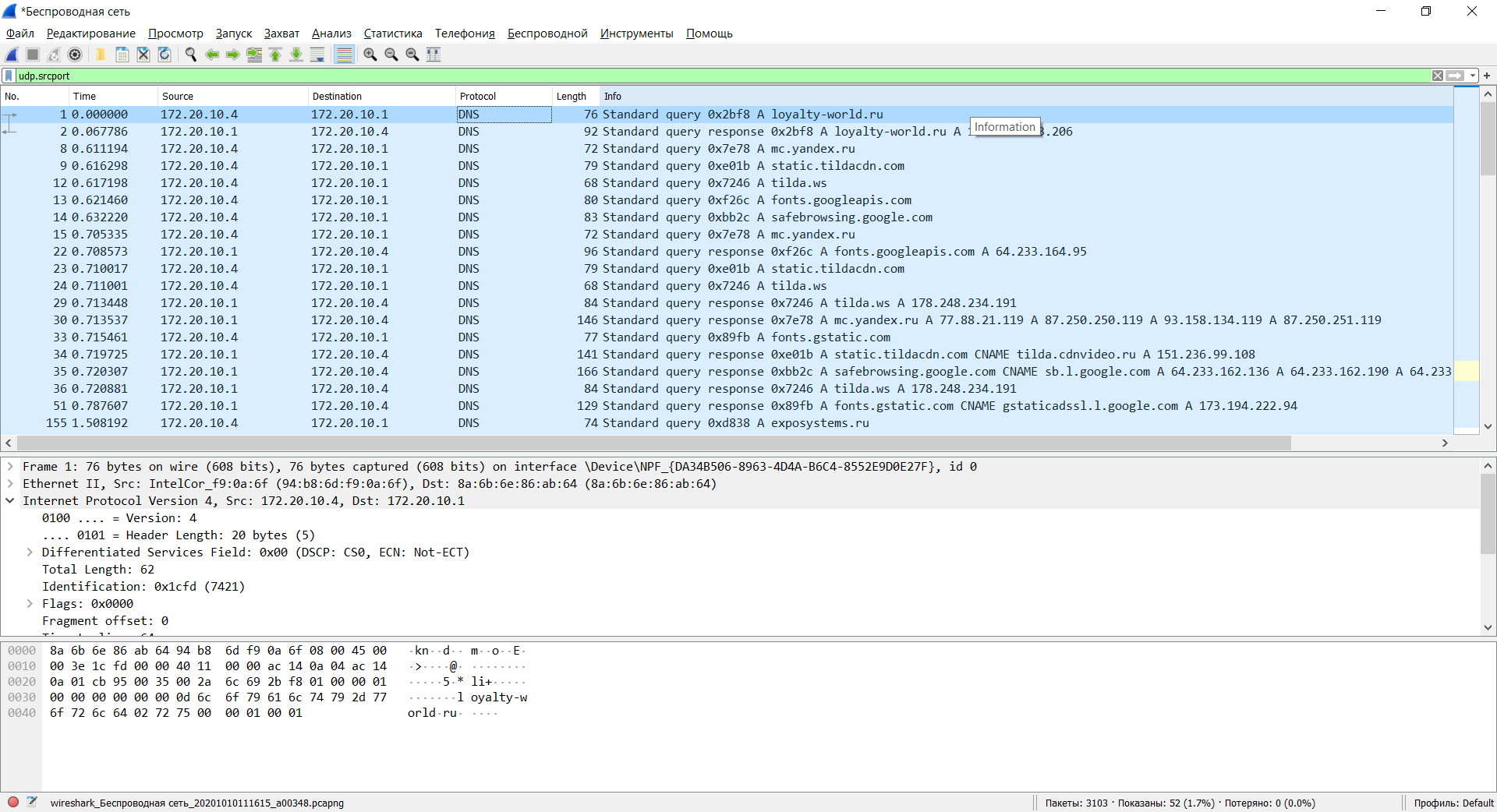
Кочалиев

* 1. ip.dst==185.165.123.206. Фильтр по IP адресу получателя

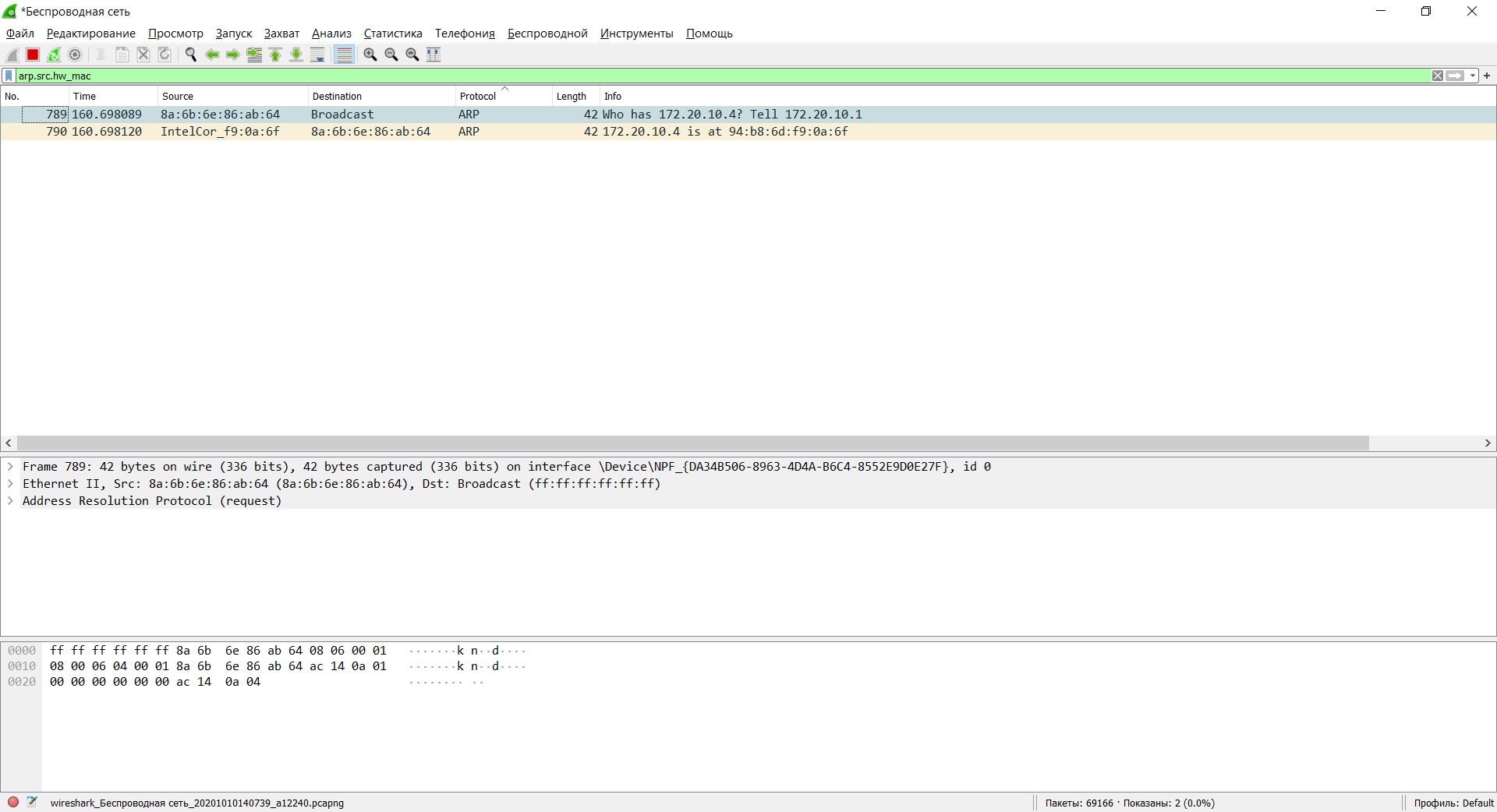
Кочалиев

* 1. ip.addr==185.165.123.206. Фильтр по IP адресу получателя и отправителя

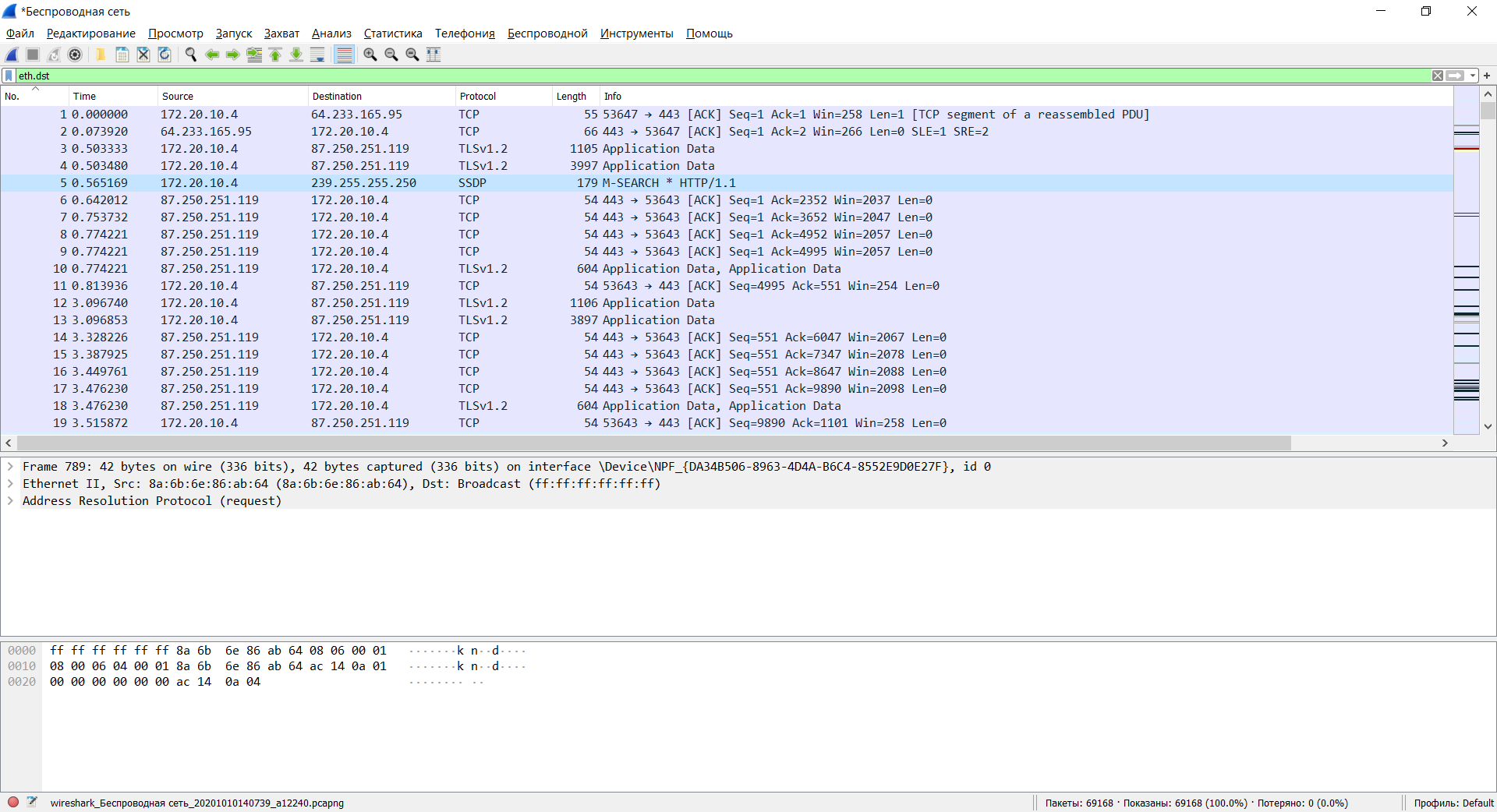
Кочалиев

* 1. udp.srcport. Фильтр по UDP порт отправителя

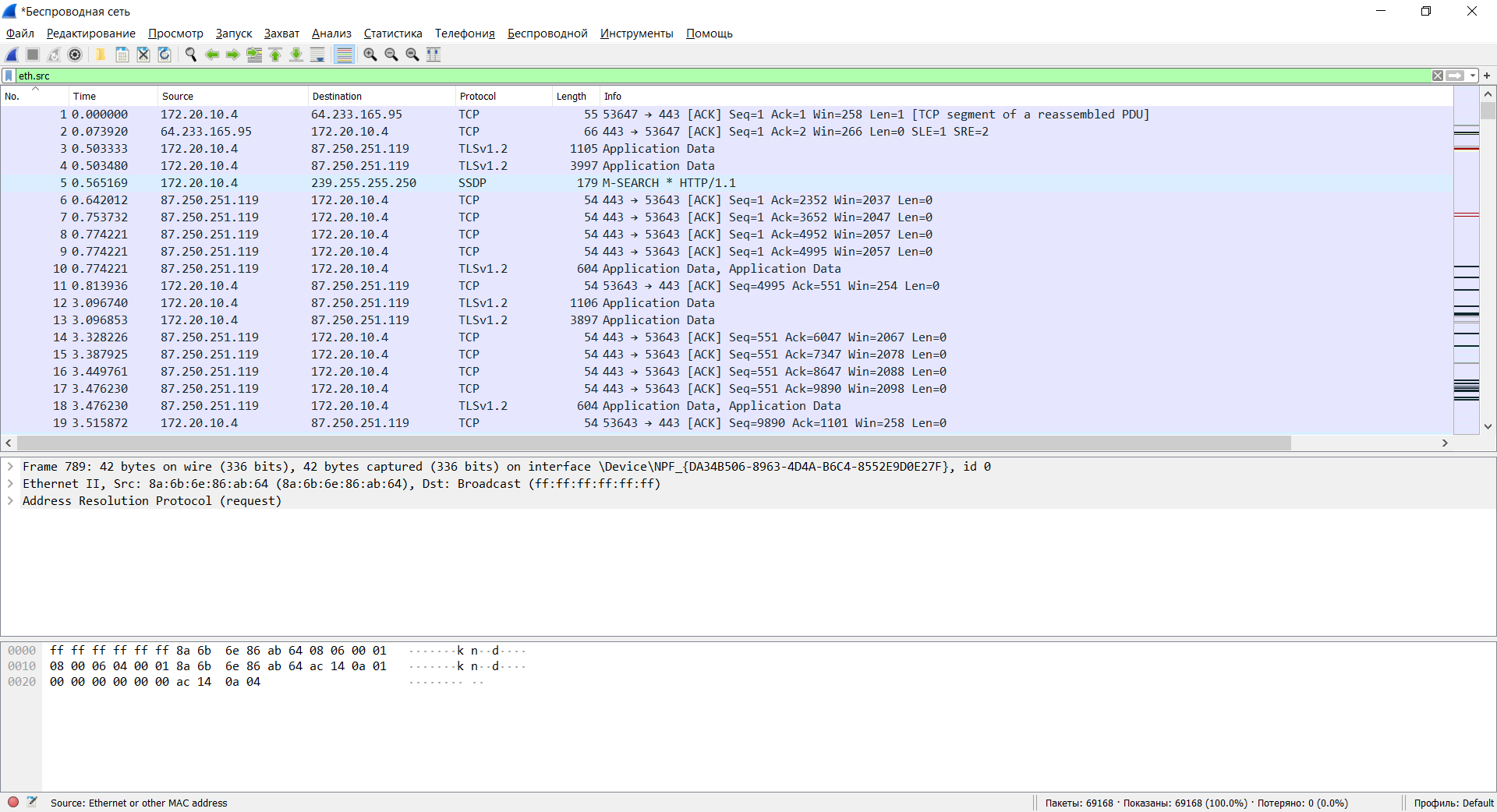
Кочалиев

* 1. arp.src.hw\_mac. Протокол ARP – MAC адрес получателя

Кочалиев

* 1. eth.dst. MAC-адрес получателя

Кочалиев

* 1. eth.src. MAC-адрес оправителя

Кочалиев