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

Кафедра КБ-1 «Защита информации»

**Отчет**

по выполнению лабораторной работы № 2

««АНАЛИЗ СТРУКТУРЫ СЕТЕВОГО ТРАФИКА

С ПОМОЩЬЮ ПРОГРАММЫ WIRESHARK»»

по дисциплине «Основы Информационной Безопасности»

Выполнил:

Студент 2 курса

Группа БИСО-02-19

Шифр 19Б1160

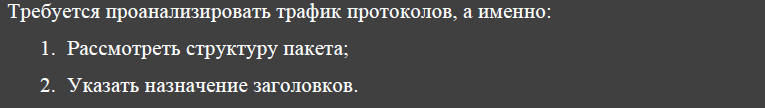
Страхов Алексей Леонидович

Проверил:

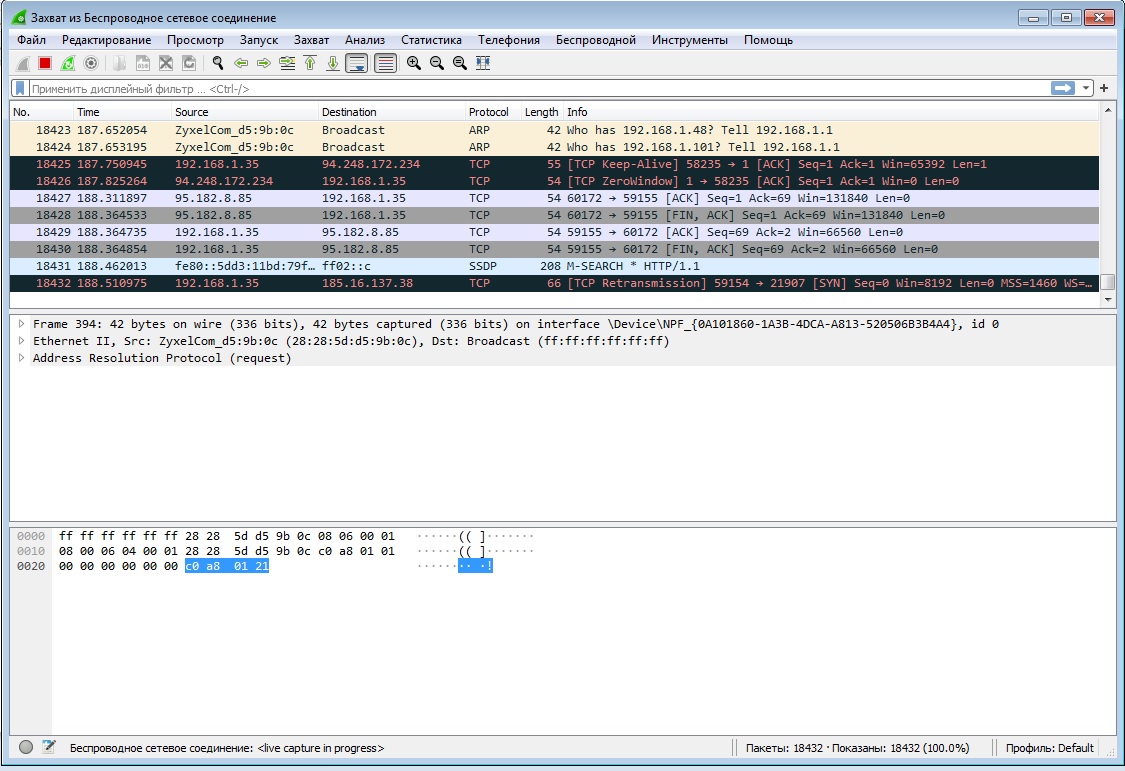
Изергин Д.А.

Москва, 2020

**Задание №1**

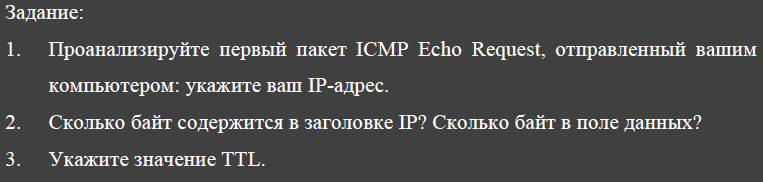


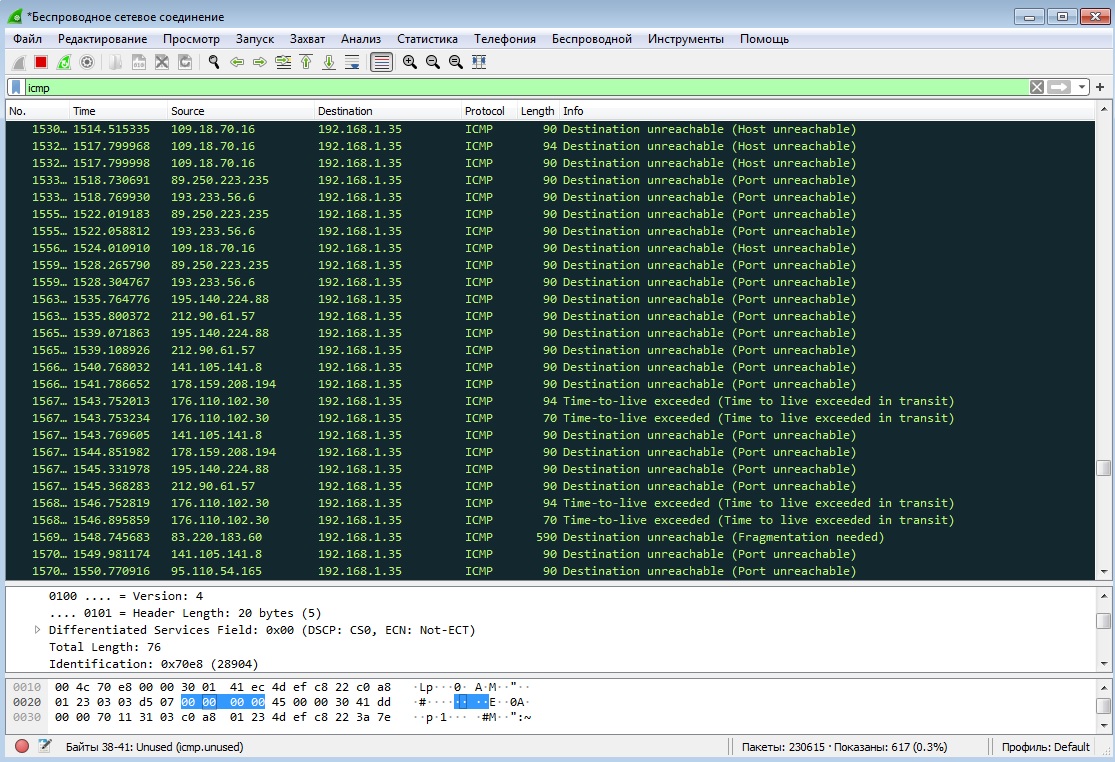
1. Для данного задания был взят 11 пакет.

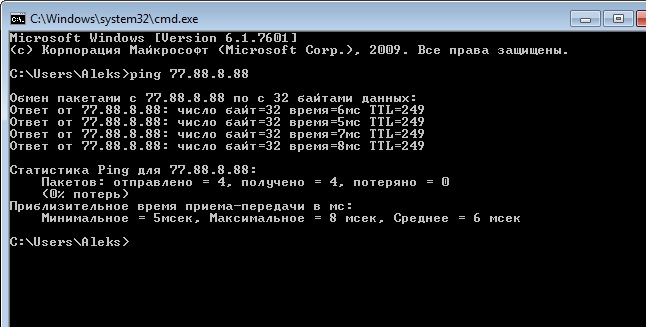


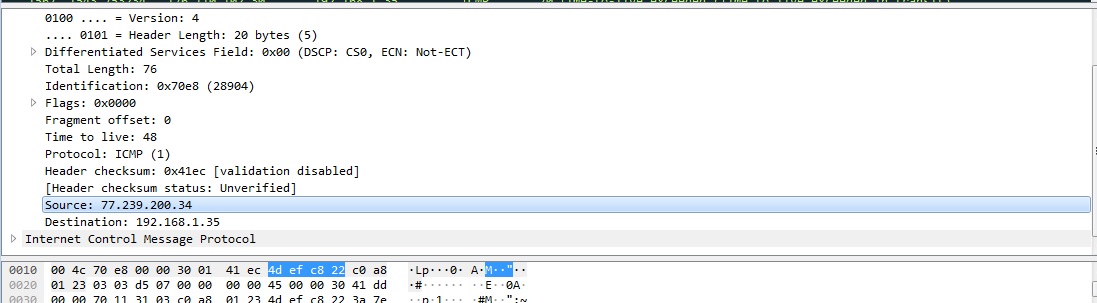
1. Пакет состоит из 4 заголовков:
   1. Frame 394 (Протокол физического уровня)
   2. Ethernet 2 (Протокол канального уровня)
   3. Address Resolution Protocol\ARP (Протокол сетевого уровня)
2. Назначение заголовков:
   1. Frame (Физический уровень) — первый уровень сетевой модели OSI. Физический уровень 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. ARP – третий уровень сетевой модели OSI. предназначенный для определения *MAC-адреса* по IP-адресу другого компьютера.

**Задание №2**







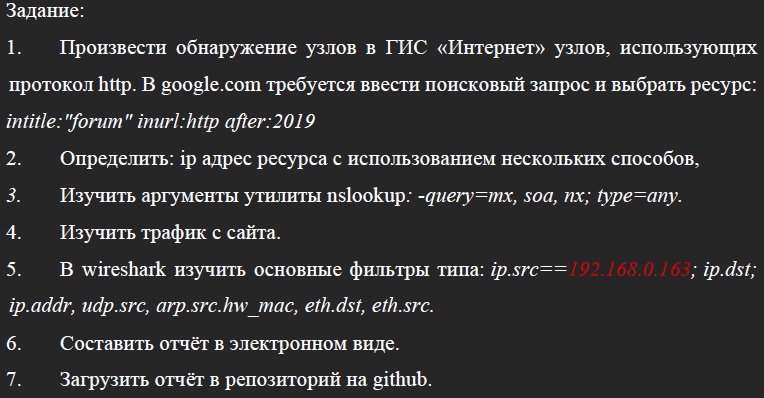


1. Проанализировав первый пакет ICMP, я понял, что мой IP-адрес: 77.239.200.34

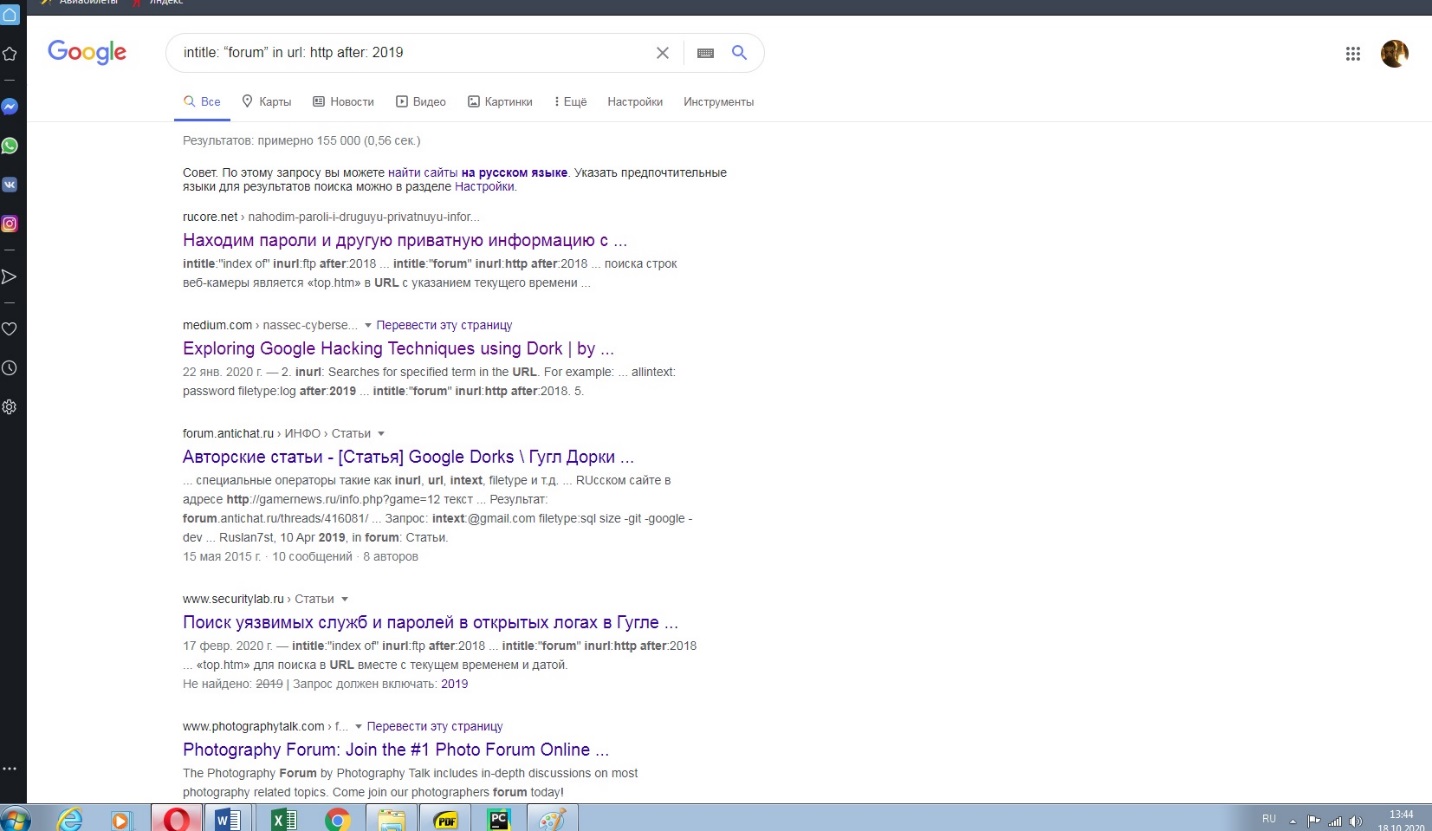
2. 20 байт, 4 байта

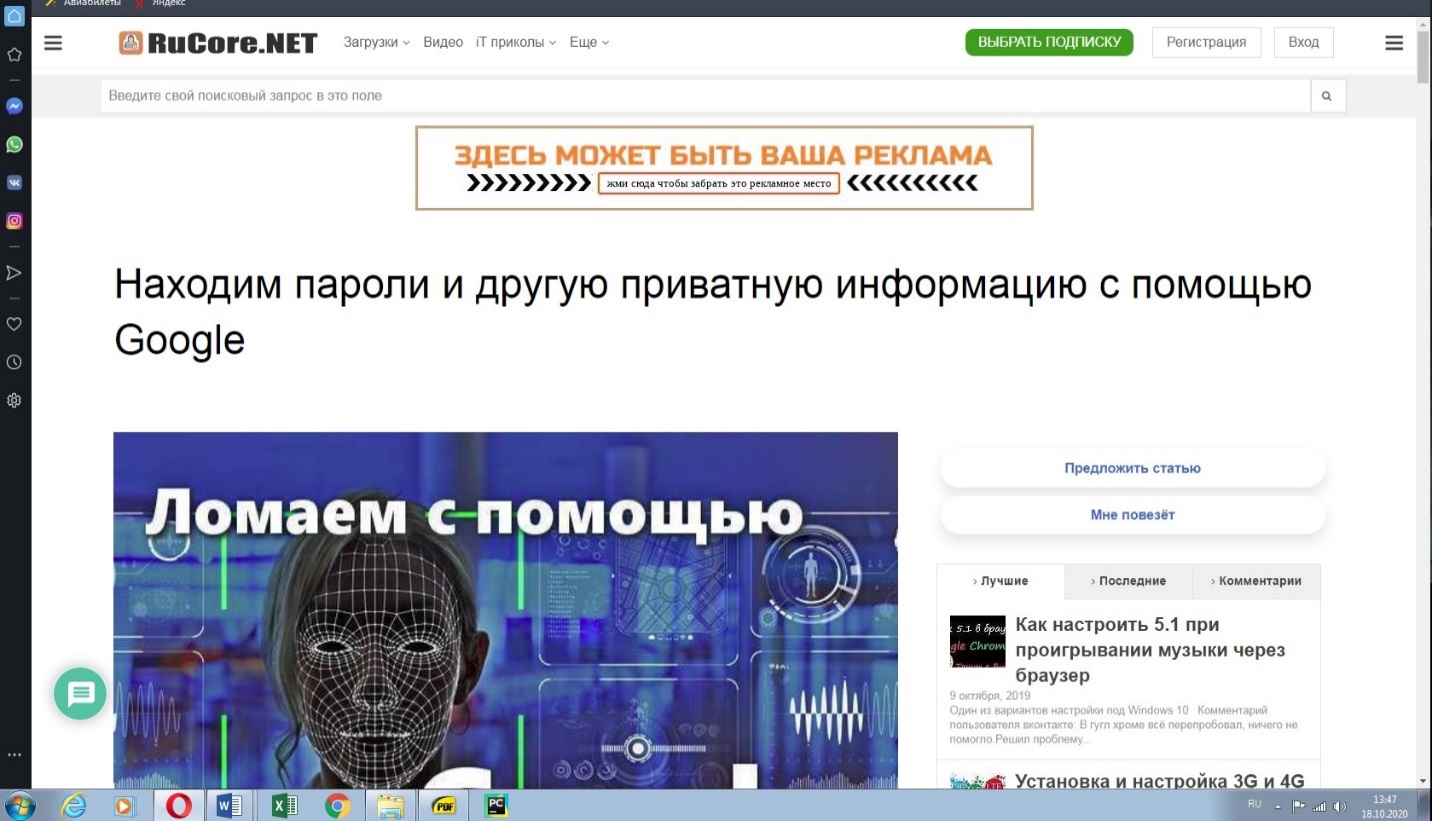
3. Time to live составляет 48

# Задание №3

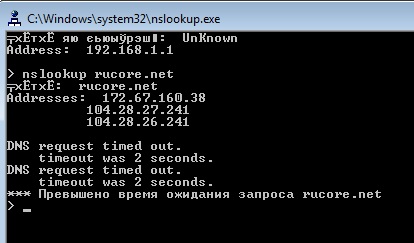


1. Введя в поисковый запрос intitle: “forum” in url: http after: 2019. Этот запрос является строгим, так как мы находим все сайты форумов с протоколом http, которые были проведены или будут проведены после 2019. Я выбираю самый первый Находим пароли и другую приватную информацию с помощью Google.

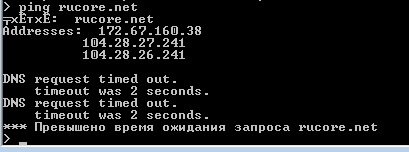


2. Сайт выглядит следующим образом, теперь будем определять ip ресурса несколькими способами. 

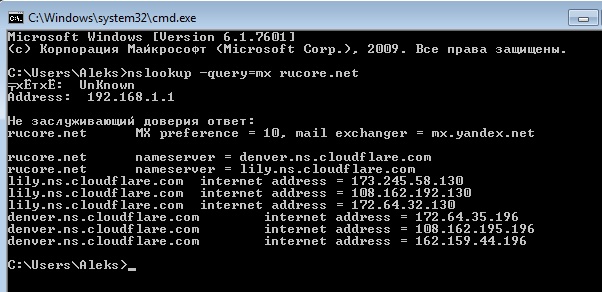
2.1) Первый способ с помощью утилиты nslookup. Получили ip адрес 172.67.160.38



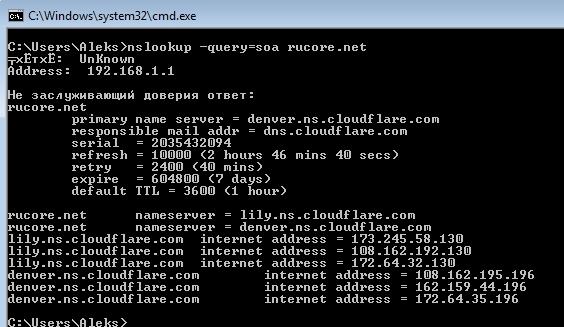
2.2) Теперь попробуем определить ip адрес при помощи утилиты ping. Неудивителньо, что ip адрес мы получили такой же 172.67.160.38



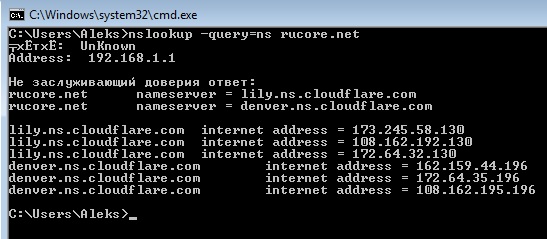
3. Изучение аргументов nslookup

3.1) -query=mx. Хранит соответствие доменного имени почтовому серверу этого домена 

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

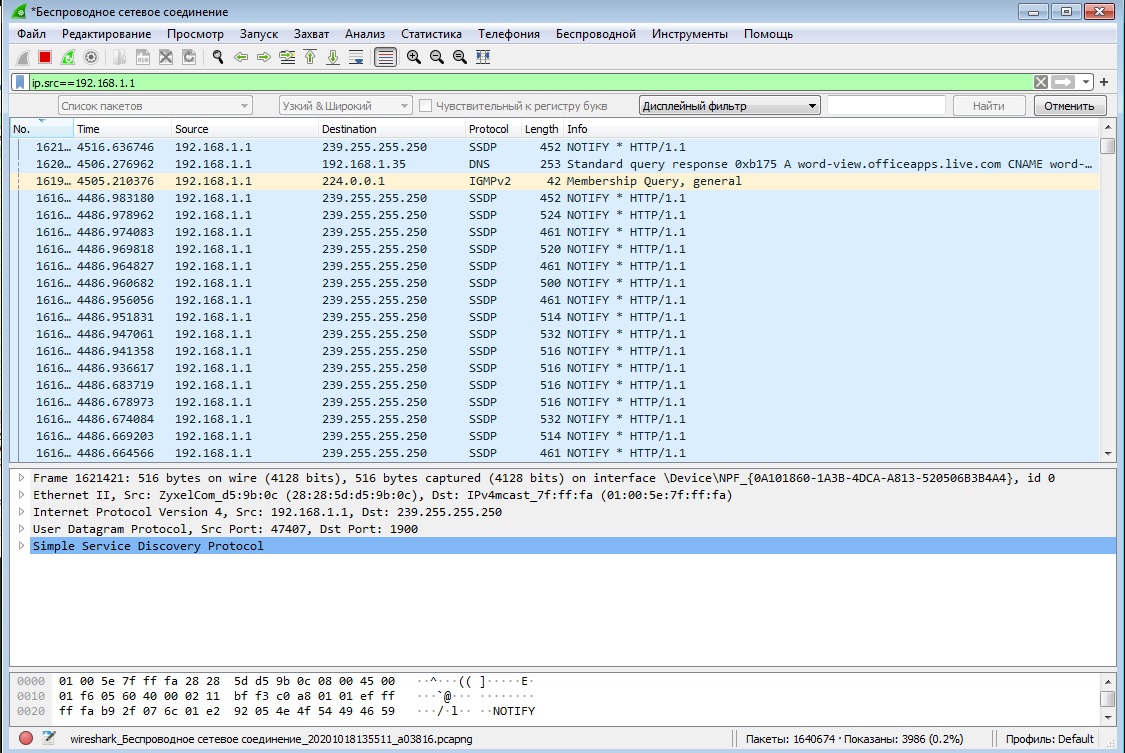


3.3) -query=ns. Cодержит соответствие доменного имени DNS-серверу, авторитативному для заданного домена.

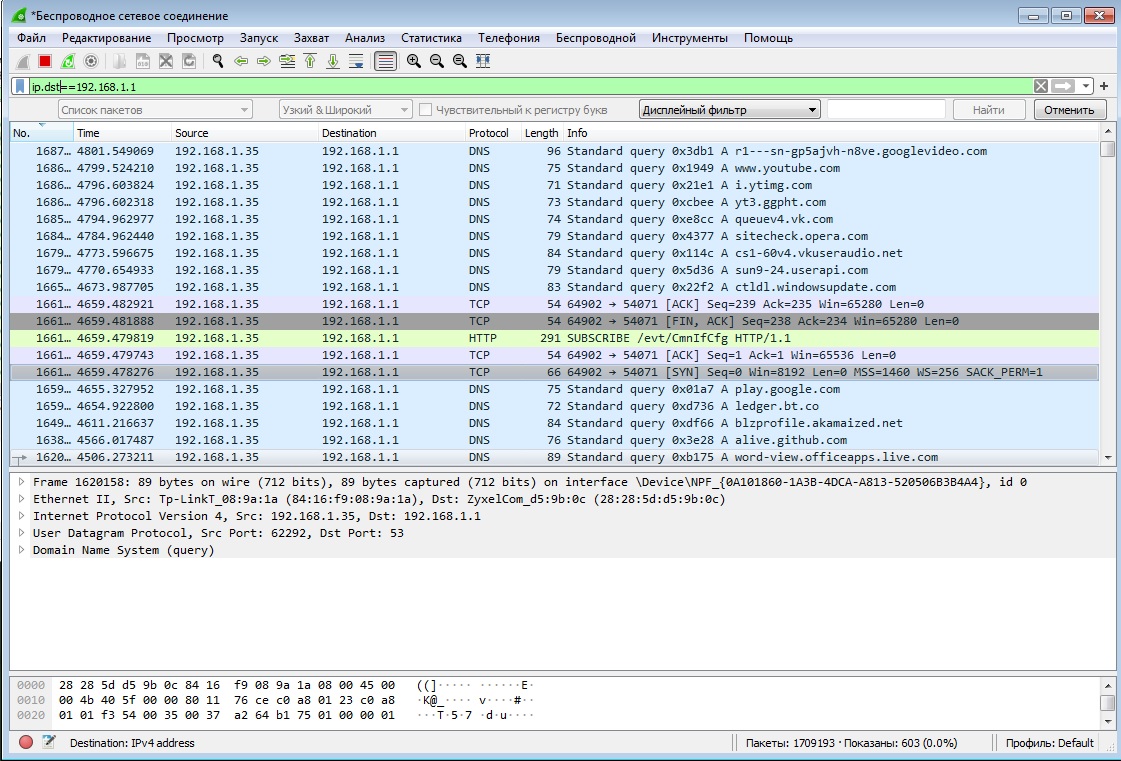


4. Изучение основных фильтров

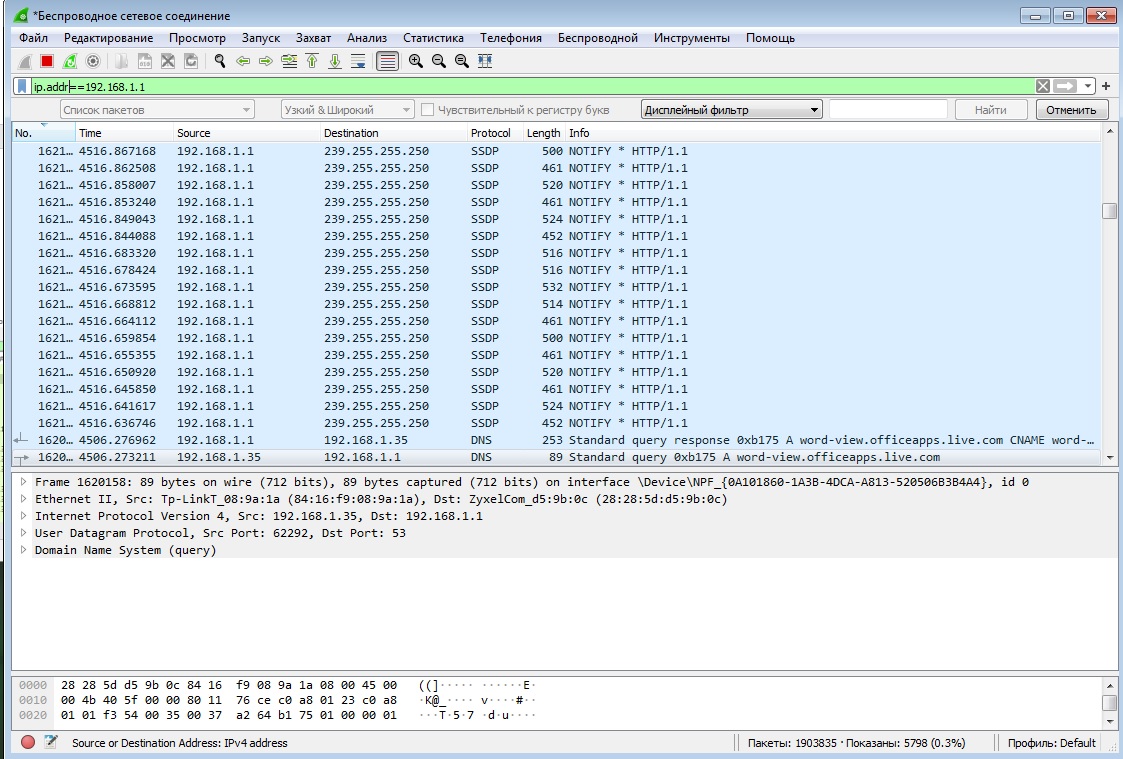
4.1) ip.src==192.168.1.1 Фильтр по IP адресу отправителя



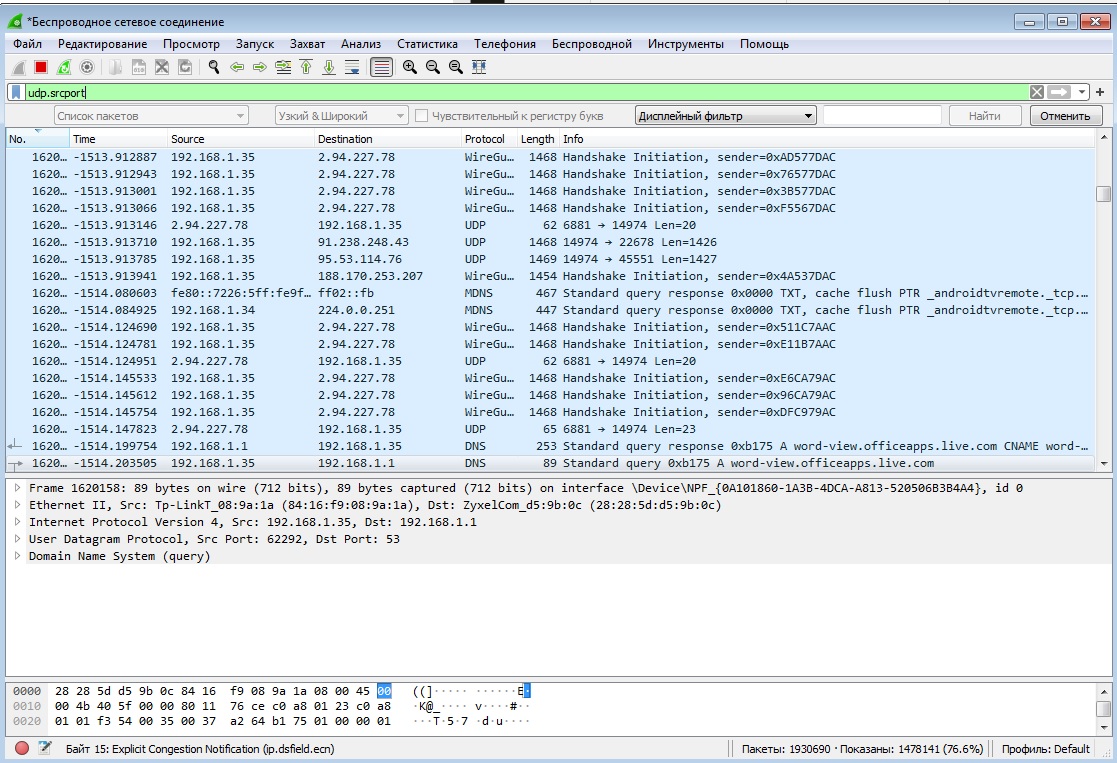
4.2) ip.dst==192.168.1.1 Фильтр по IP адресу получателя



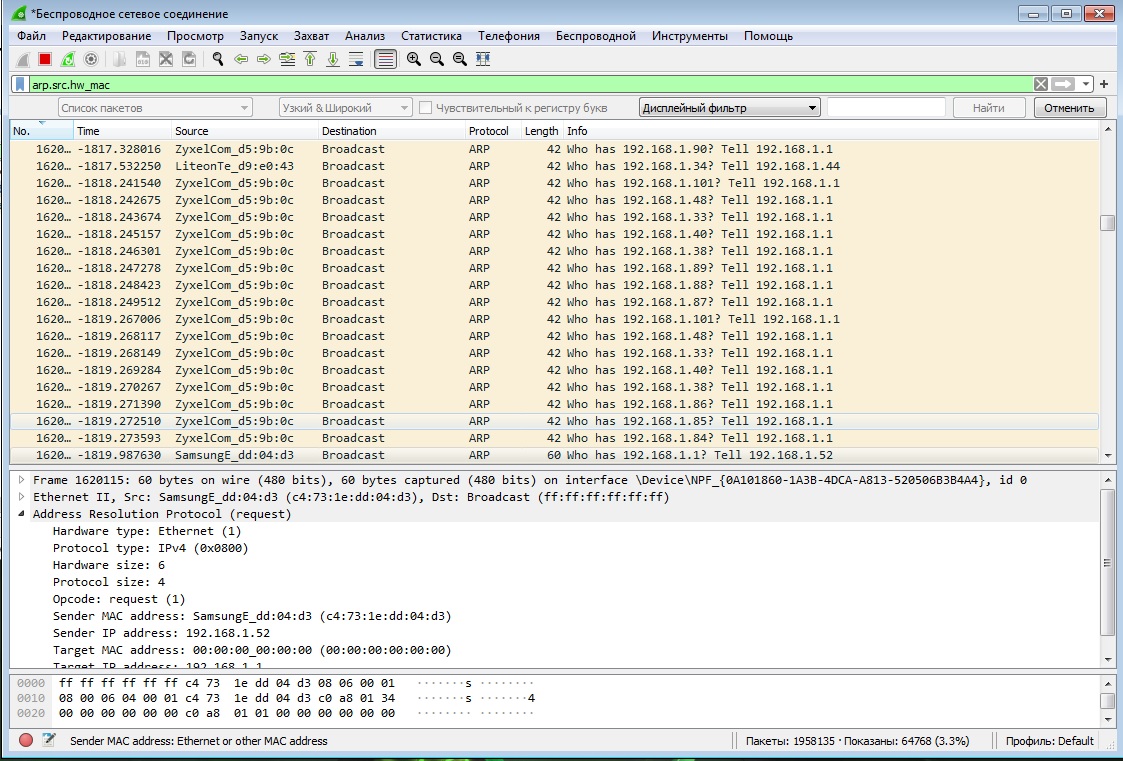
4.3) ip.addr==192.168.1.1 Фильтр по IP адресу получателя и отправителя



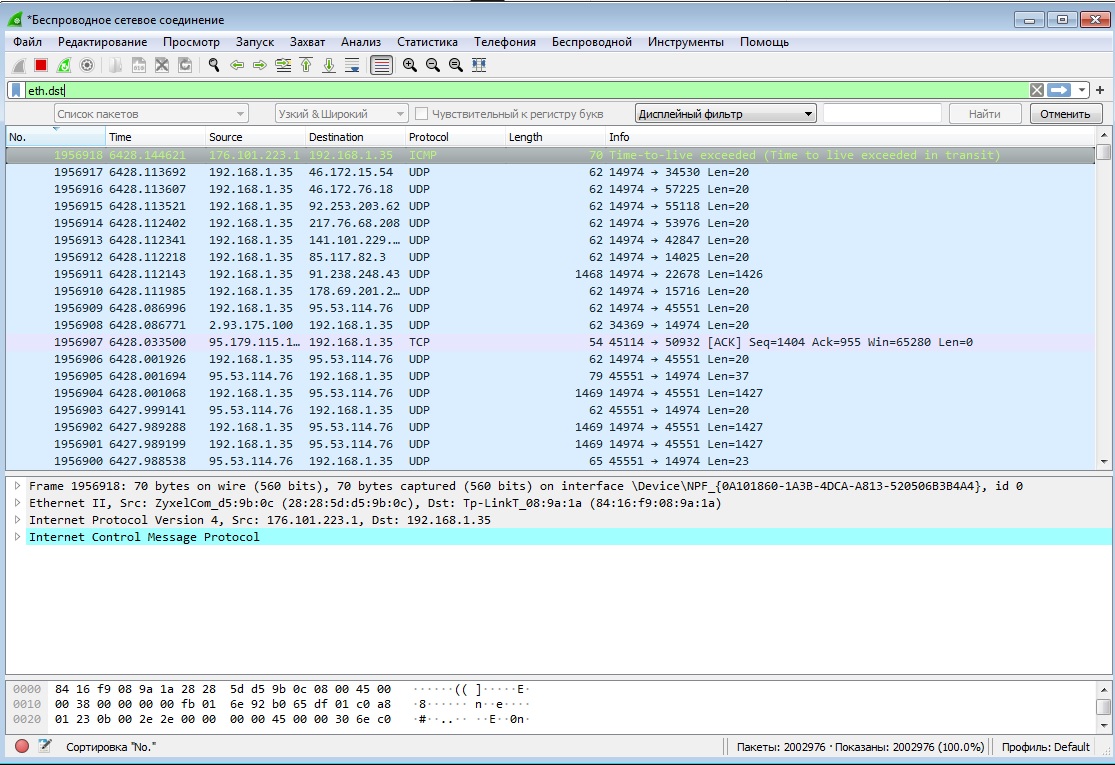
4.4) udp.srcport. Фильтр по UDP порт отправителя



4.5) arp.src.hw\_mac. Протокол ARP – MAC адрес получателя



4.6) eth.dst. MAC-адрес получателя



4.7) eth.src. MAC-адрес оправителя

