Отчет по дисциплине «Основы информационной безопасности»

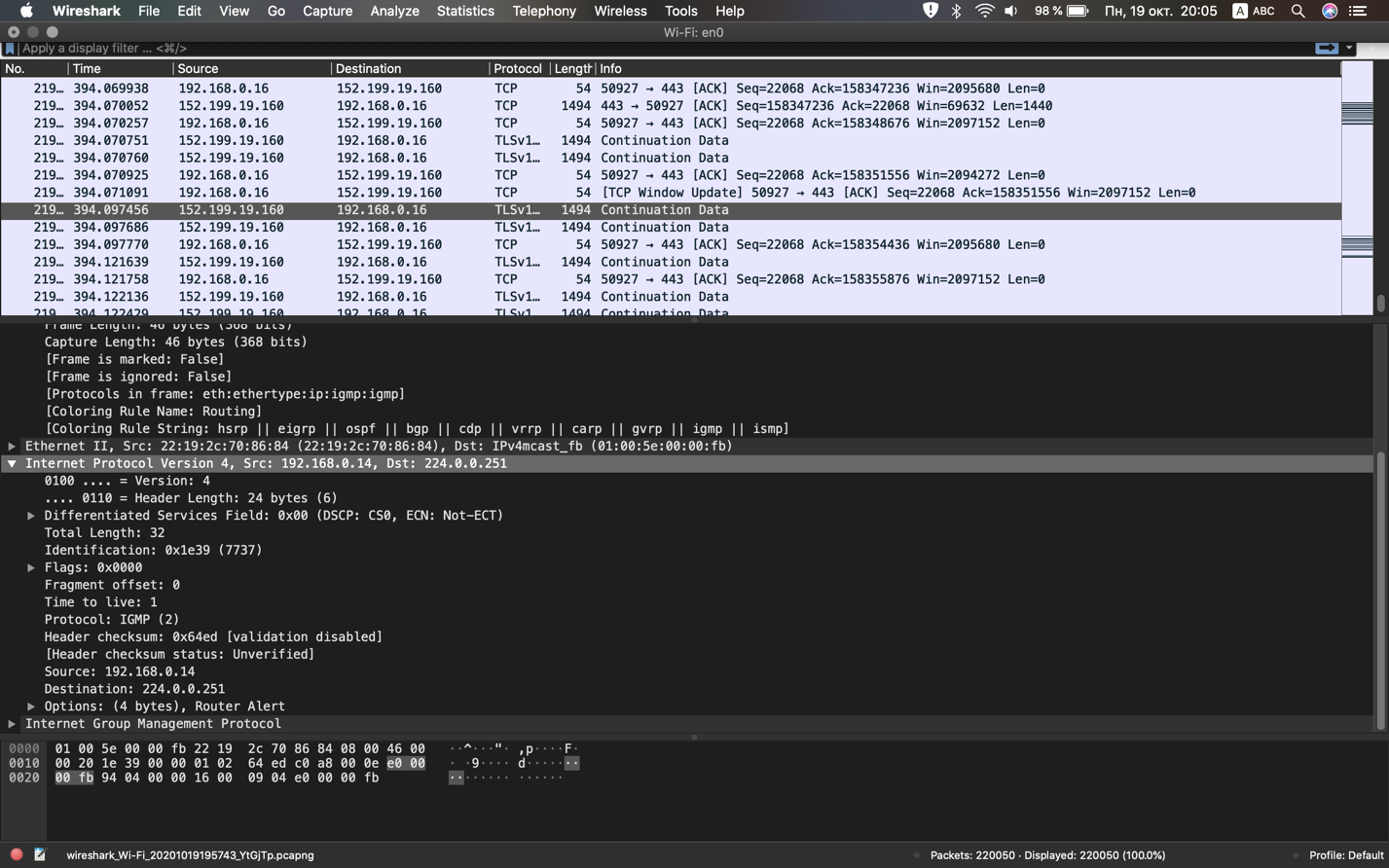
на тему «Анализ структуры сетевого трафика

с помощью программы WireShark»

Выполнил студент РТУ МИРЭА,

ИКБСП, БИСО-01-19 Крюковская Екатерина Алексеевна

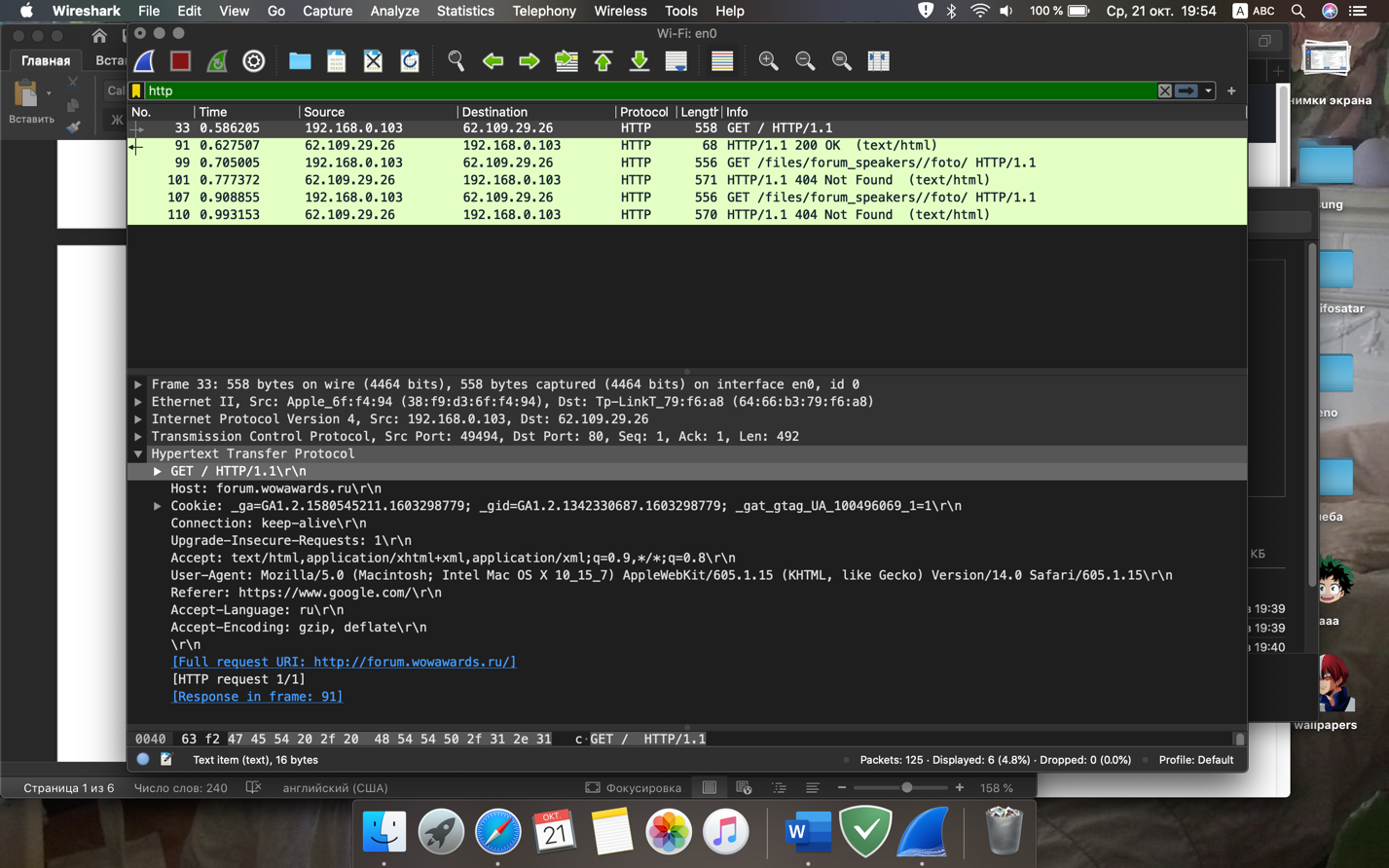
1.WireShark



1. IPv4: 192.168.0.16
2. В заголовке 24 байтов, 6 байт в поле данных
3. TTL: 1

2.HTTP

1. Версия HTTP 1.1
2. IP компьютера: 192.168.0.103 - IP адрес сервера: 62.109.29.26
3. Код состояния HTTP: 200
4. Длина тела сообщения: 558

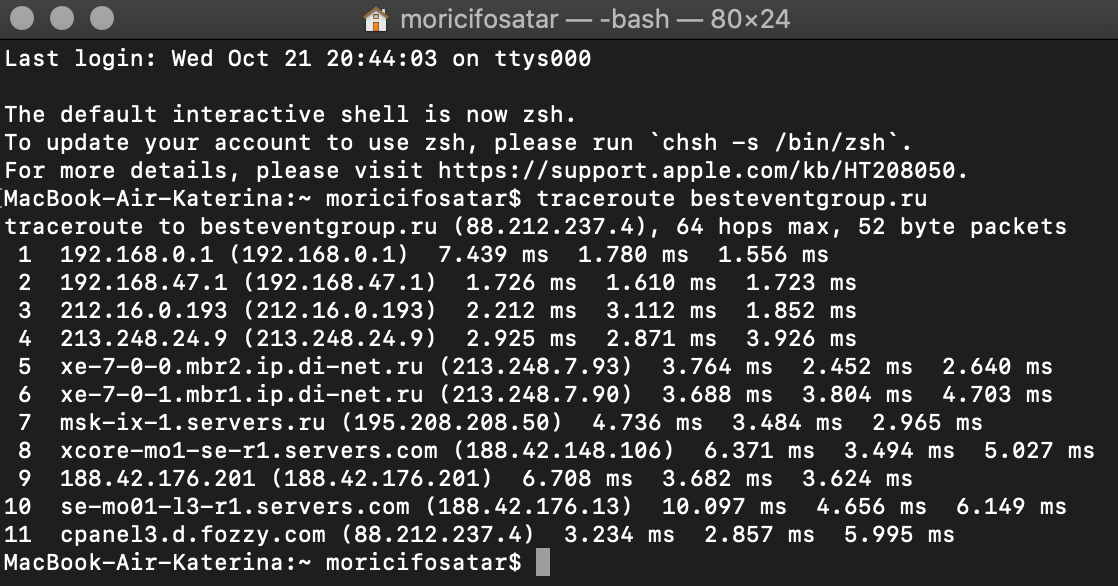


3.Исследование ресурса

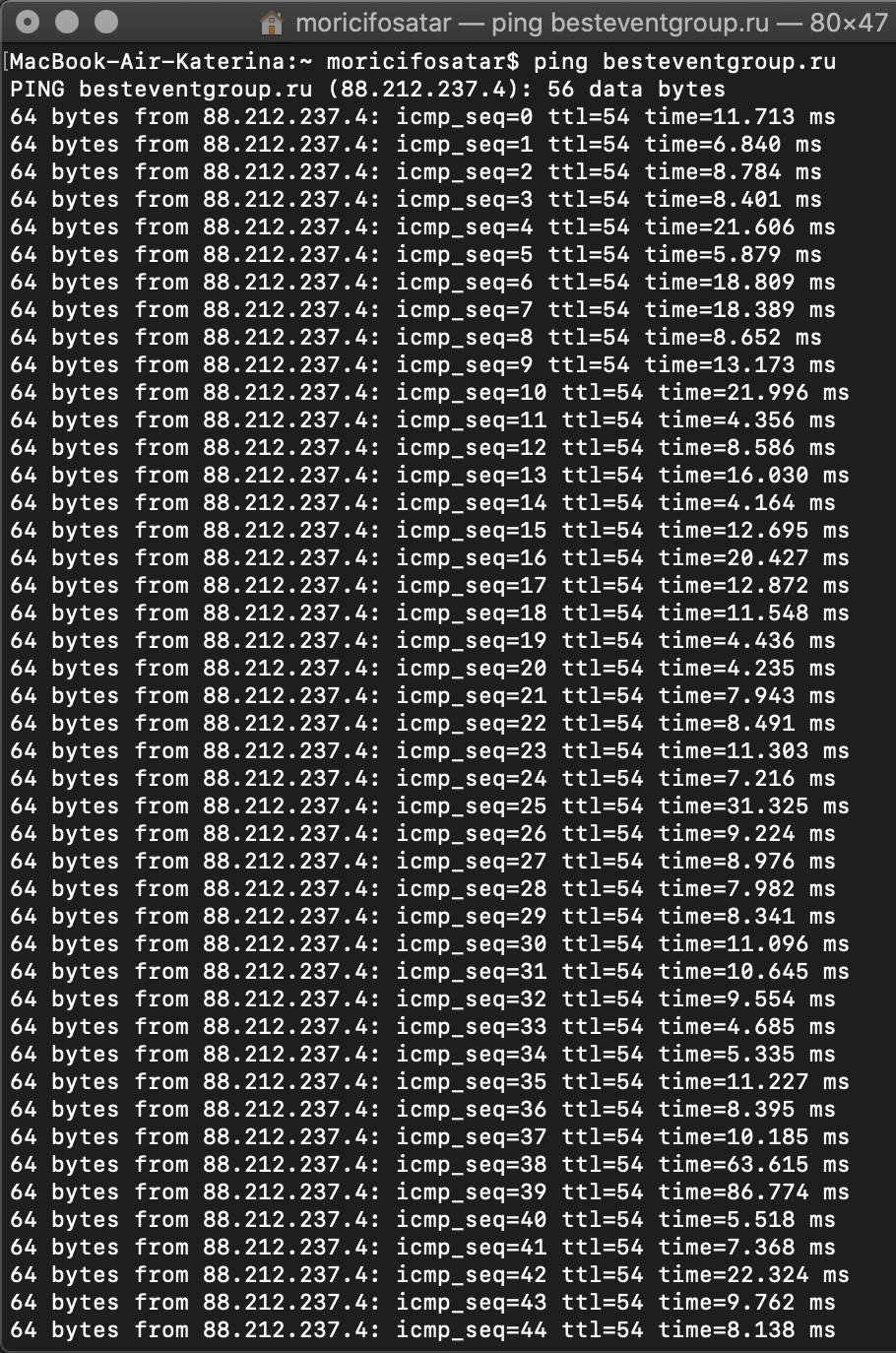
Ресурс besteventgroup.ru



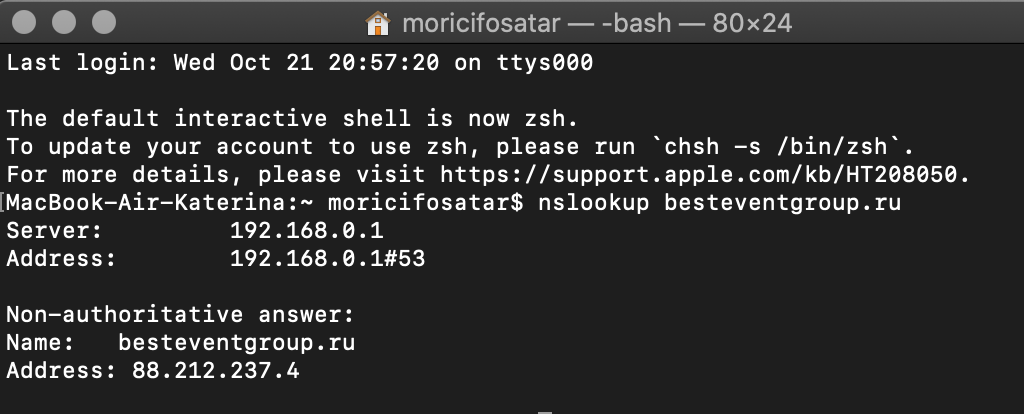
ip адрес: 88.212.237.4 (traceroute besteventgroup.ru)



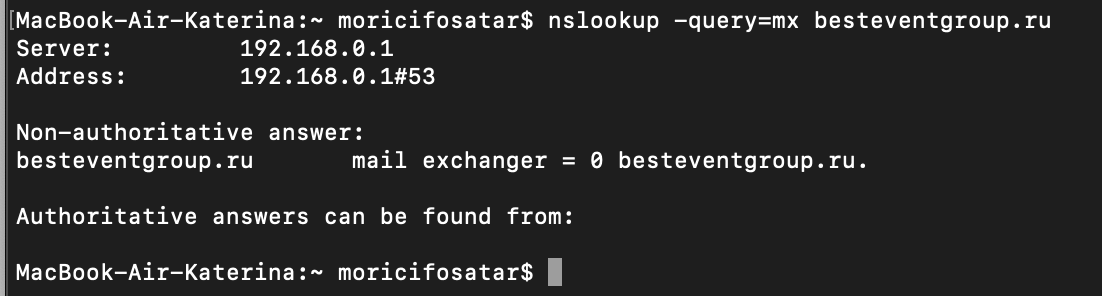
ip адрес: 88.212.237.4 (ping besteventgroup.ru)



ip адрес: 88.212.237.4 (nslookup besteventgroup.ru)

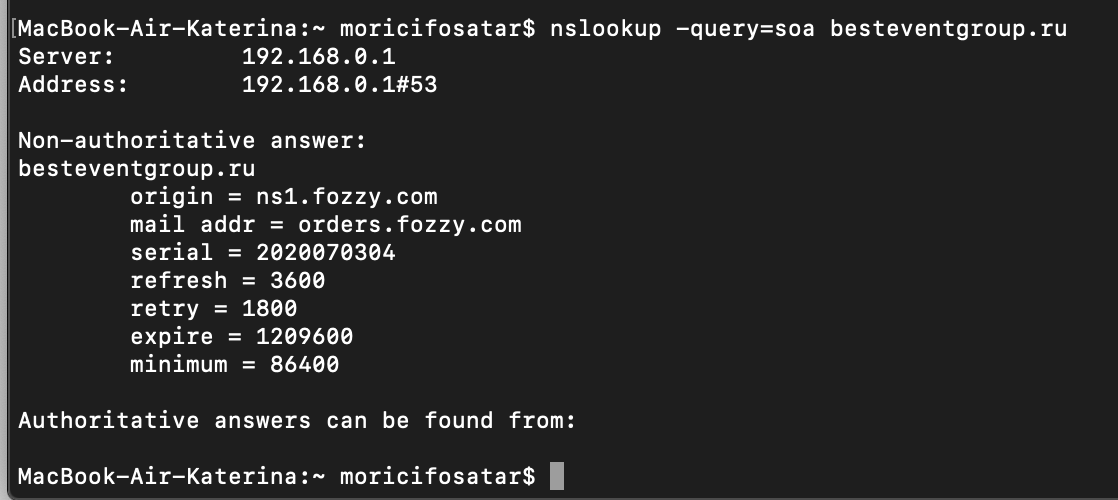


-query=mx



При вводе команды выводится соответственные доменному имени почтовые сервера. Также указан приоритет MX preference – чем меньше значение, тем больше вероятность отправки через этот сервер на best.event@bk.ru.

-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.

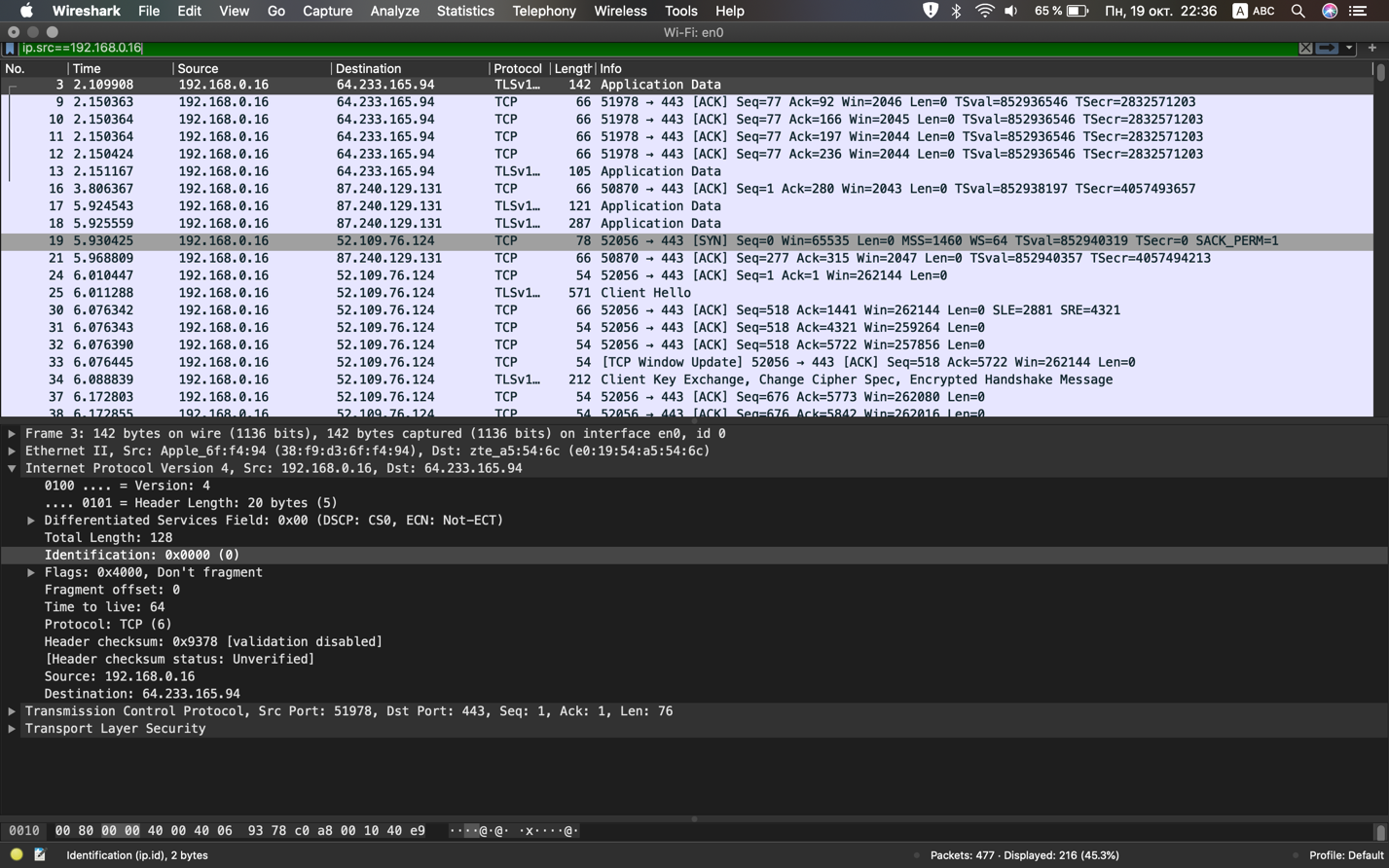
-query=ns



Показывает соответствие доменных имен DNS-серверам.

4.Фильтры WireShark (ip.src, ip.dst, ip.addr, udp.port, arp.src.hw\_mac, eth.dst, eth.src)

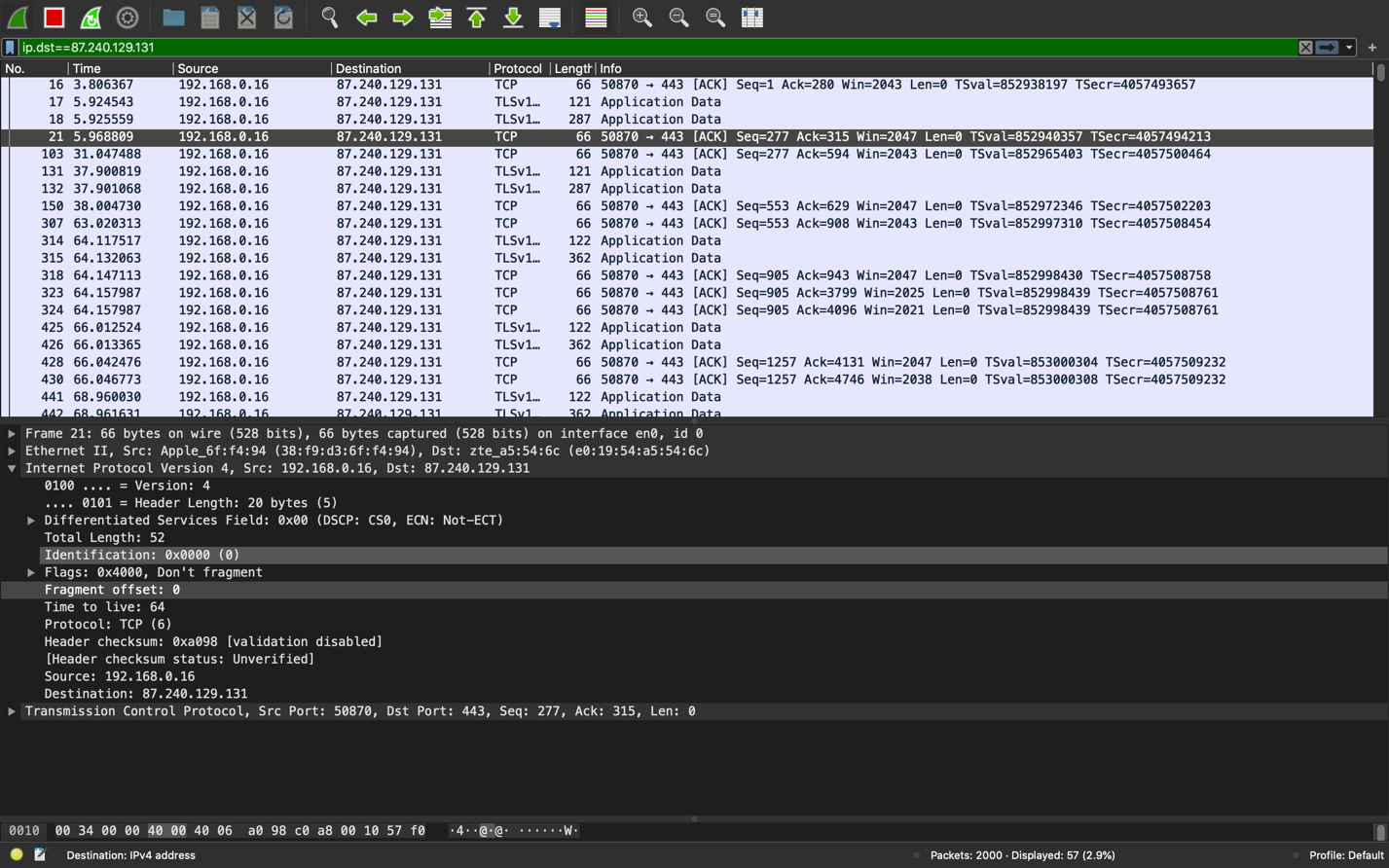
ip.src



ip.src==192.168.0.16

Покажет все захваченные пакеты с ip-адресом отправителя 192.168.0.16

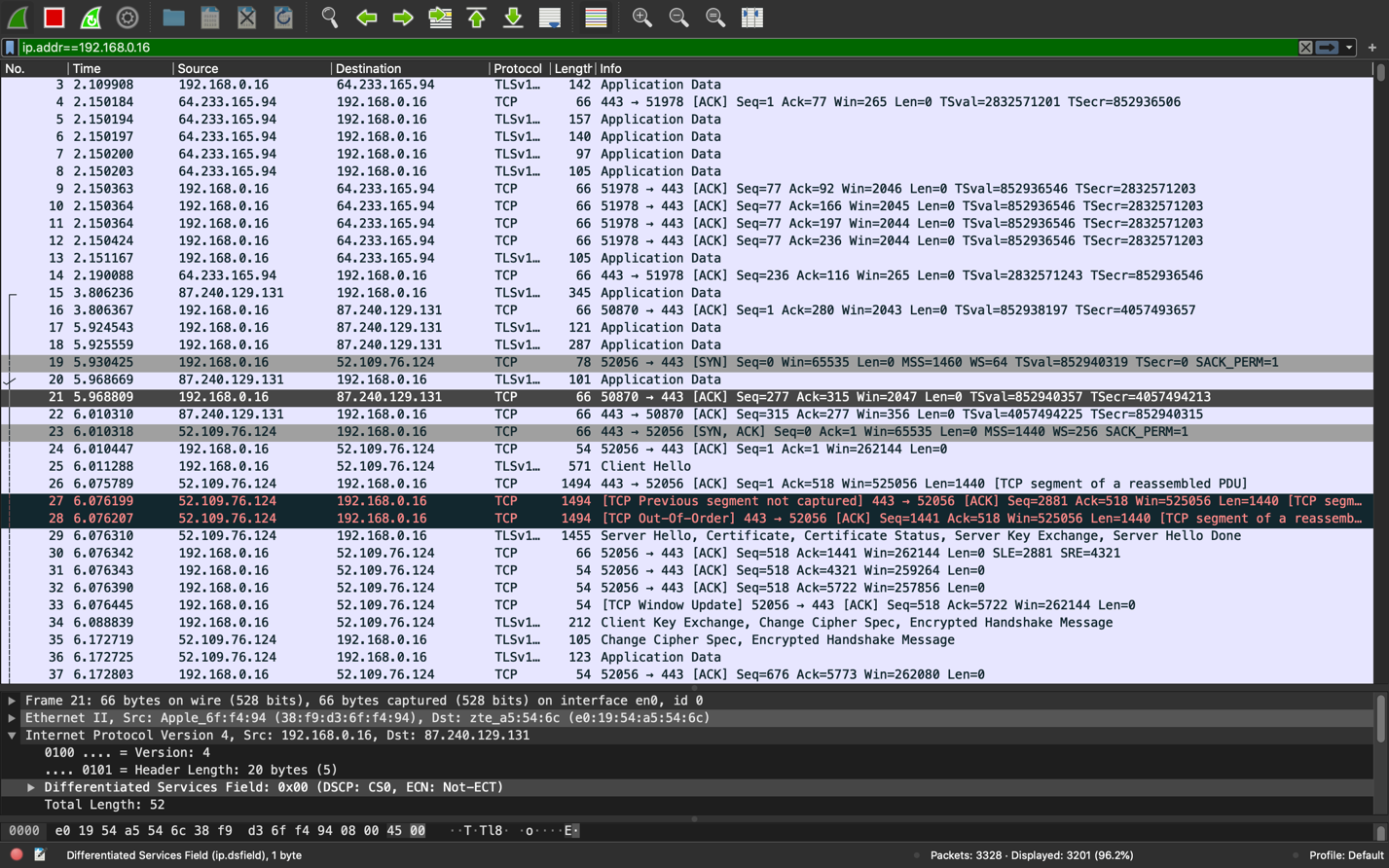
ip.dst



ip.dst==87.240.129.131

Покажет все захваченные пакеты с ip-адресом получателя 87.240.129.131

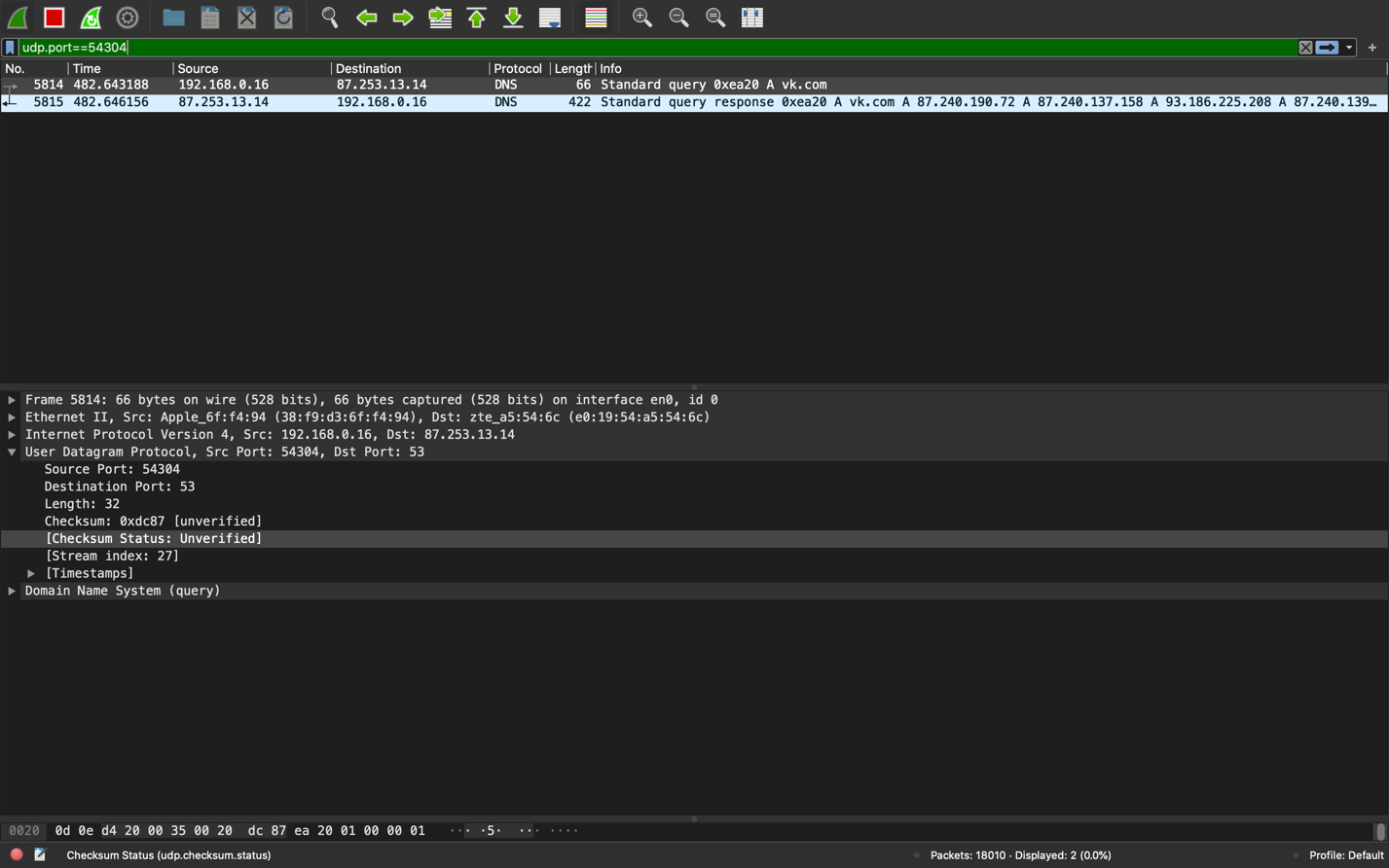
ip.addr



ip.addr==192.168.0.16

Покажет все захваченные пакеты, идущие от одного и того же IP, либо же идущие к одному и тому же IP

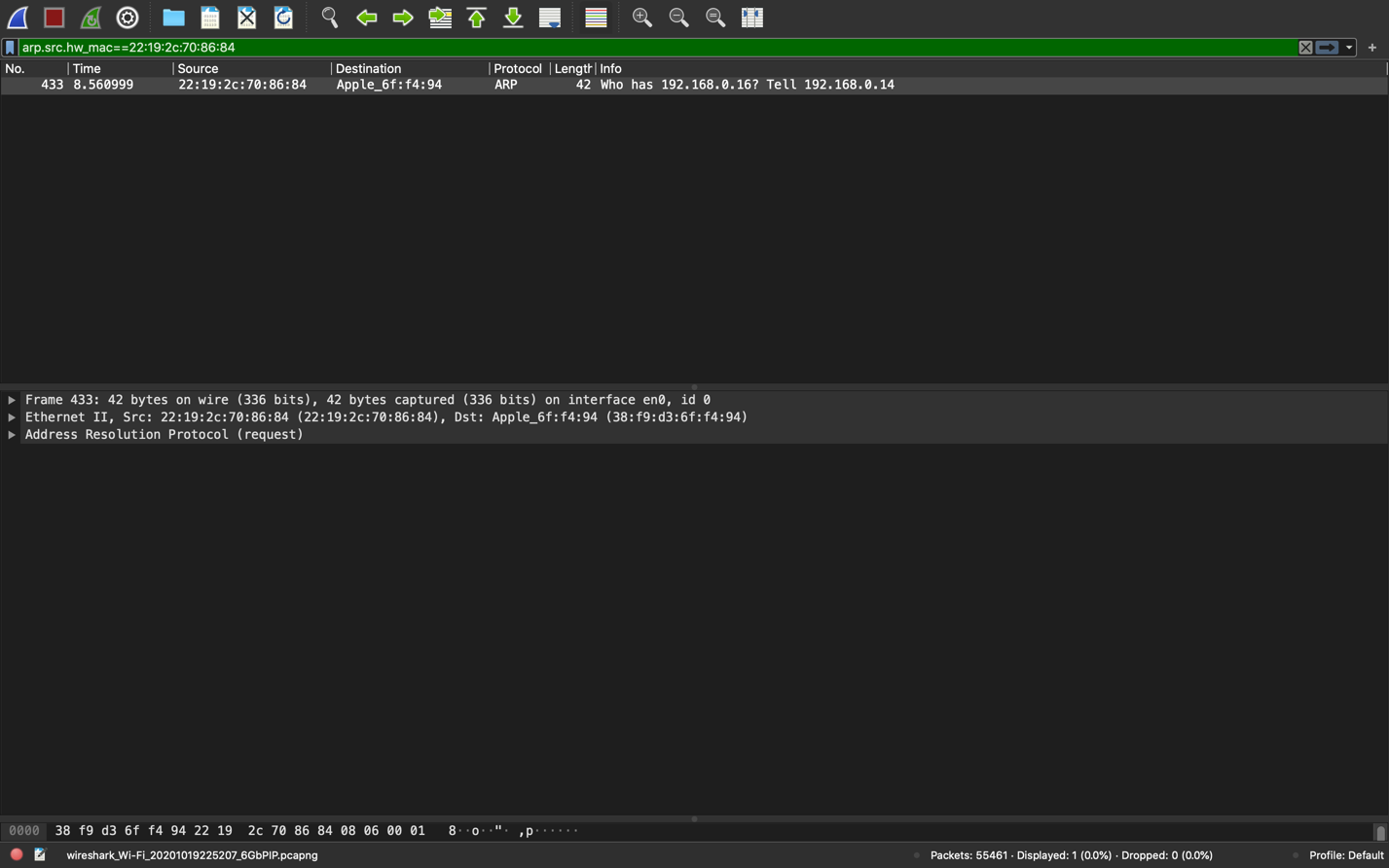
udp.port



udp.port==54304

Выведет все захваченные пакеты с udp портом 54304 отправителя или получателя

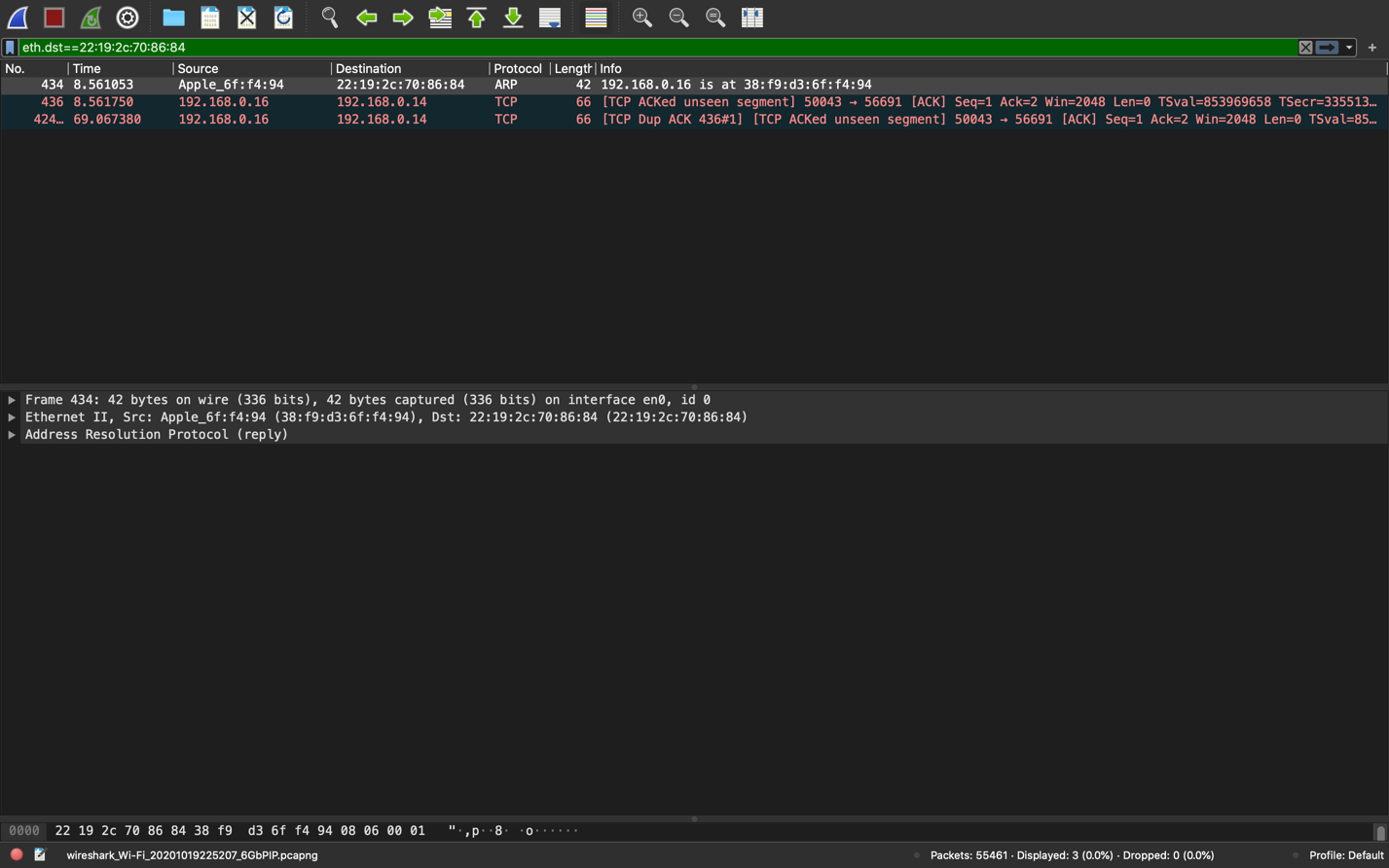
arp.src.hw\_mac



arp.src.hw\_mac==22:19:2c:70:86:84

Покажет все захваченные пакеты протокола ARP с MAC-адресом отправителя

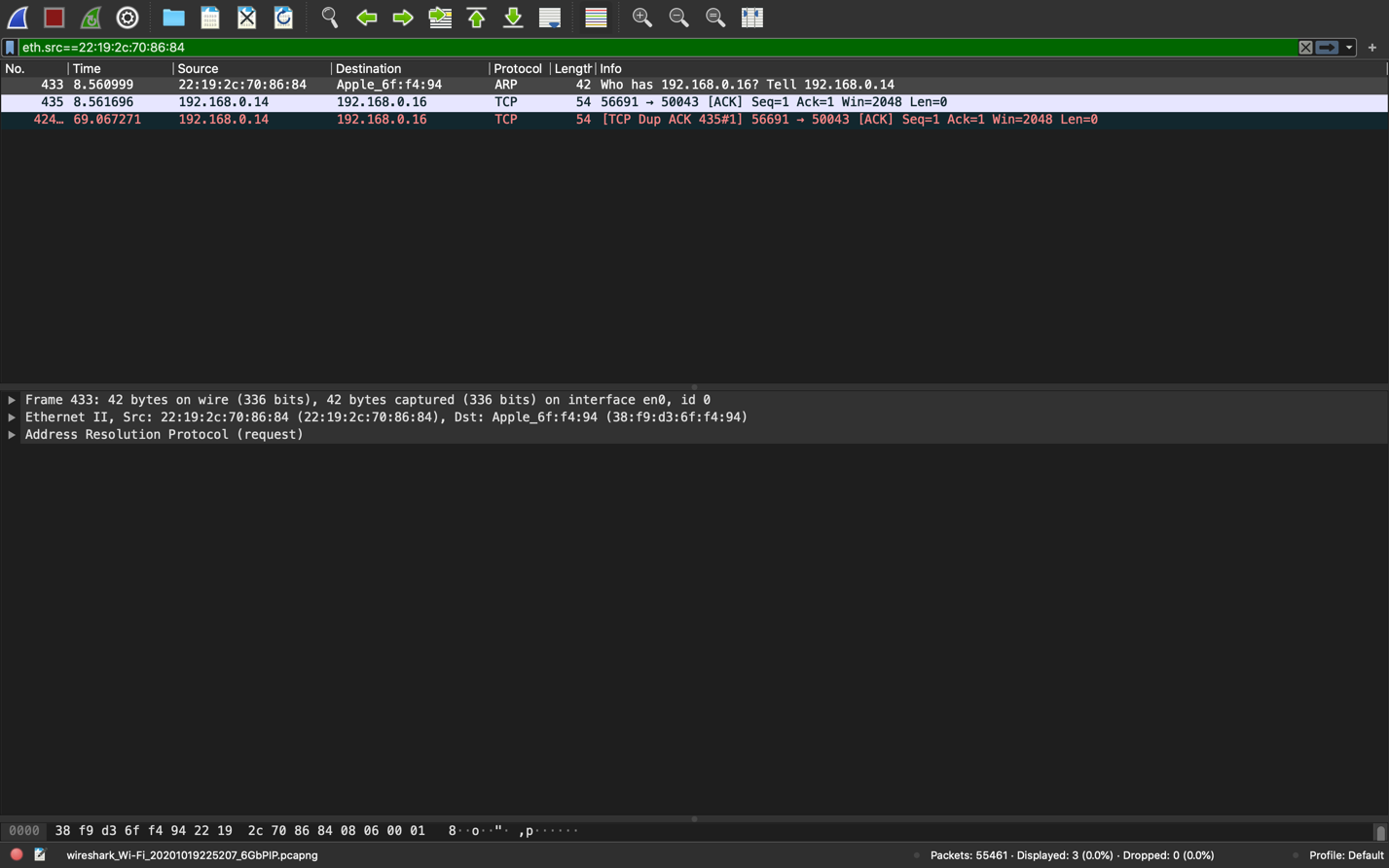
eth.dst



eth.dst==22:19:2c:70:86:84

Покажет все захваченные пакеты с MAC-адресом получателя

eth.src

****

eth.src==22:19:2c:70:86:84

Покажет все захваченные пакеты с MAC-адресом отправителя