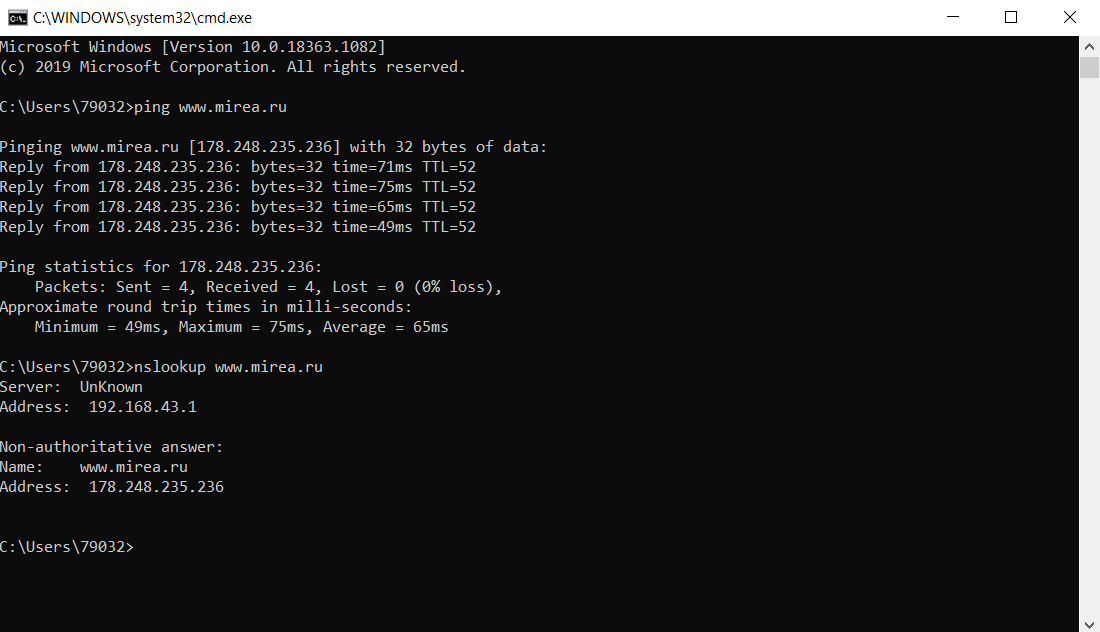
Практика 2

Для работы с трафиком использовался сайт <https://www.mirea.ru/>

С помощью консоли (cmd) мы узнали IP-адрес сайта МИРЭА

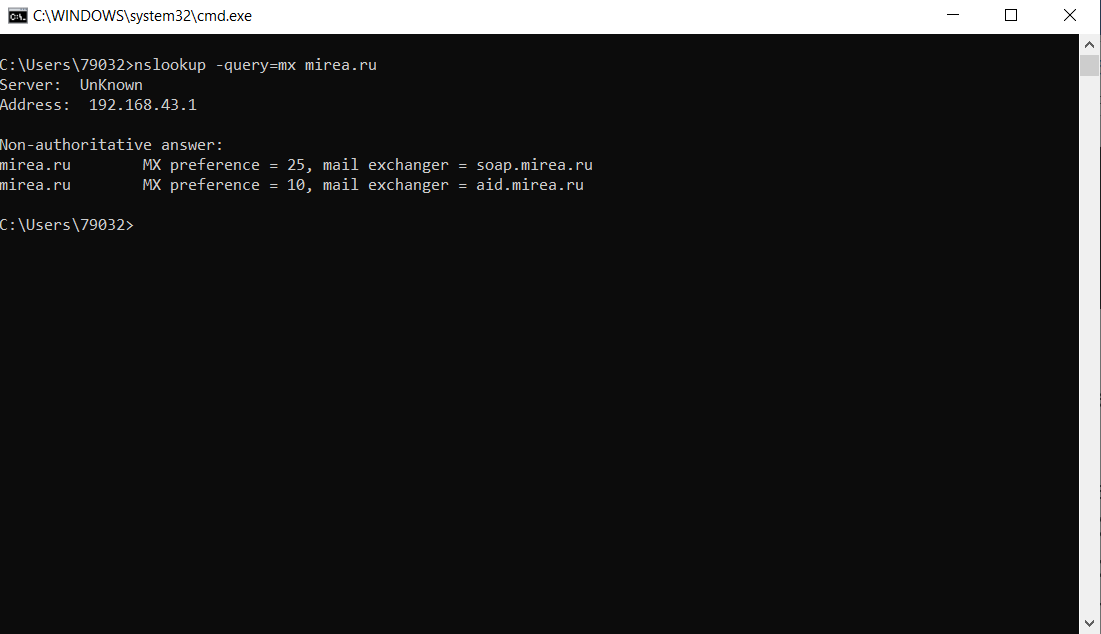
Команды: ping ‘адрес сайта’; nslookup ‘адрес сайта’

IP-адрес: 178.248.235.236



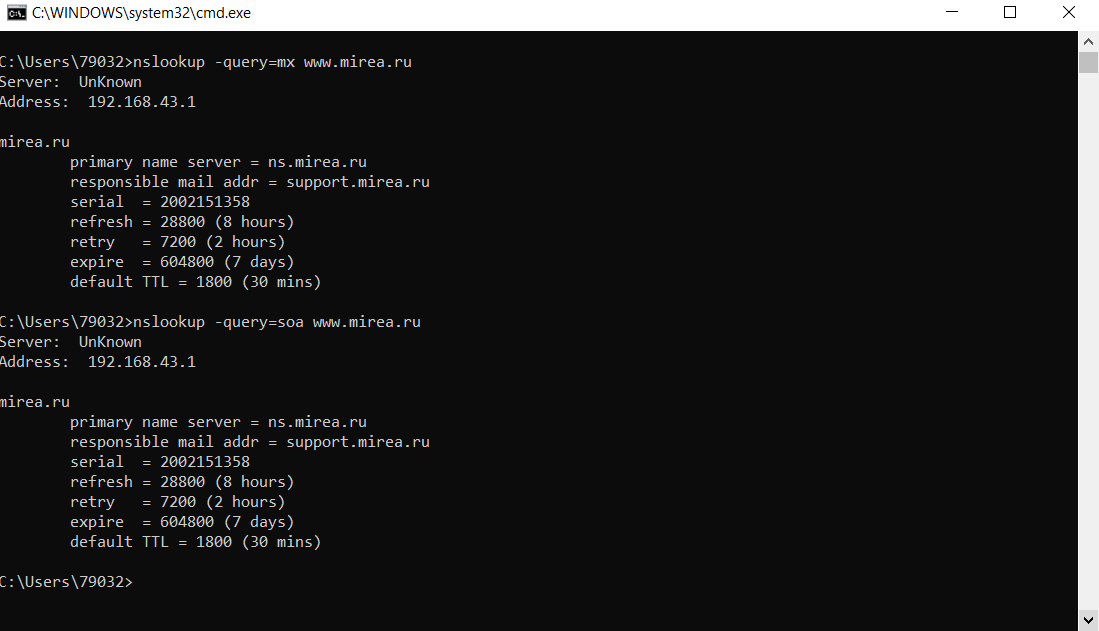
*Изучение аргументов утилиты* nslookup

Команда -query=mx



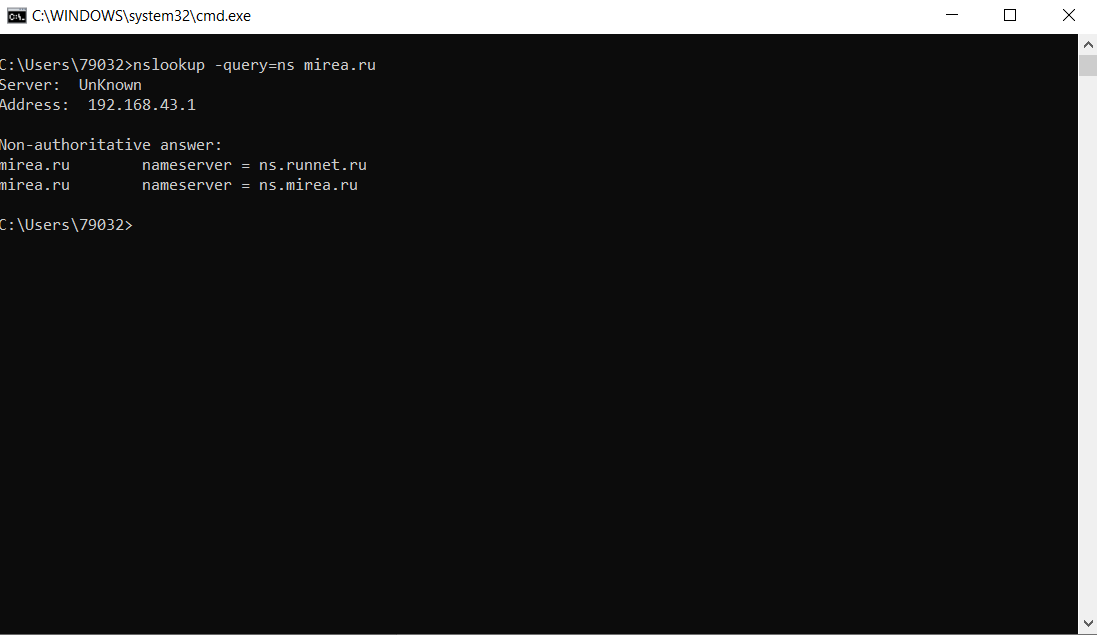
Была получена серверная почта домена

Команда -query=soa



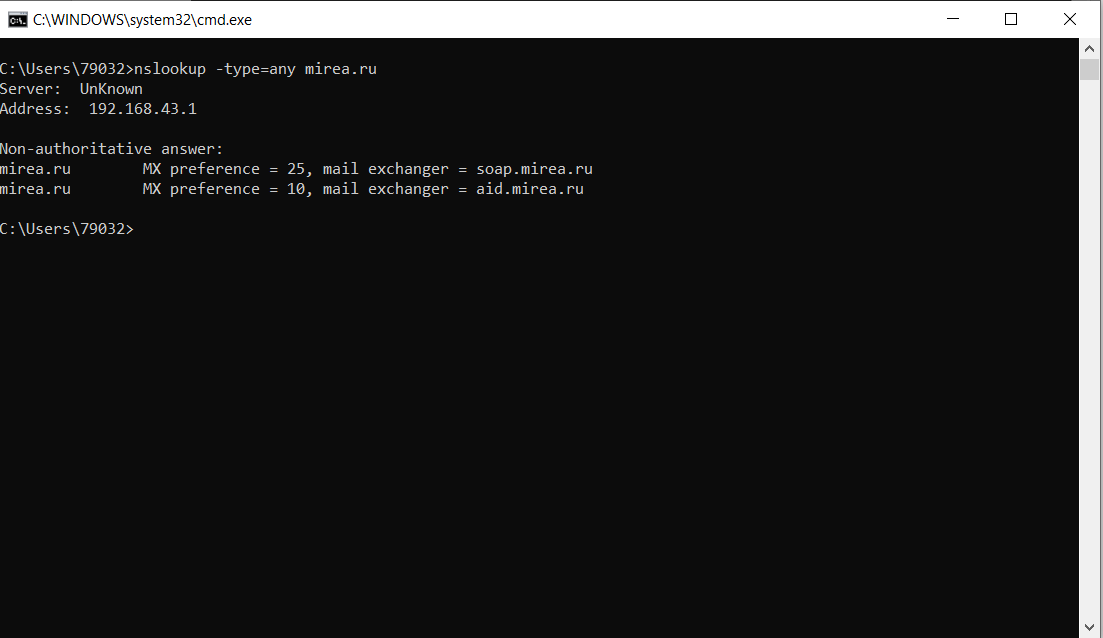
Мы получили информацию о: первичное название сервера, почту администратора сервера домена, серийный номер, период времени, через который вторичный DNS-сервер отправит запрос первичному, чтобы проверить, поменялся ли серийный номер. Интервал для повторного соединения с первичным DNS-сервером, если он по каким-то причинам не смог ответить на запрос.

Команда -query=ns



Получили доменное имя DNS-сервера

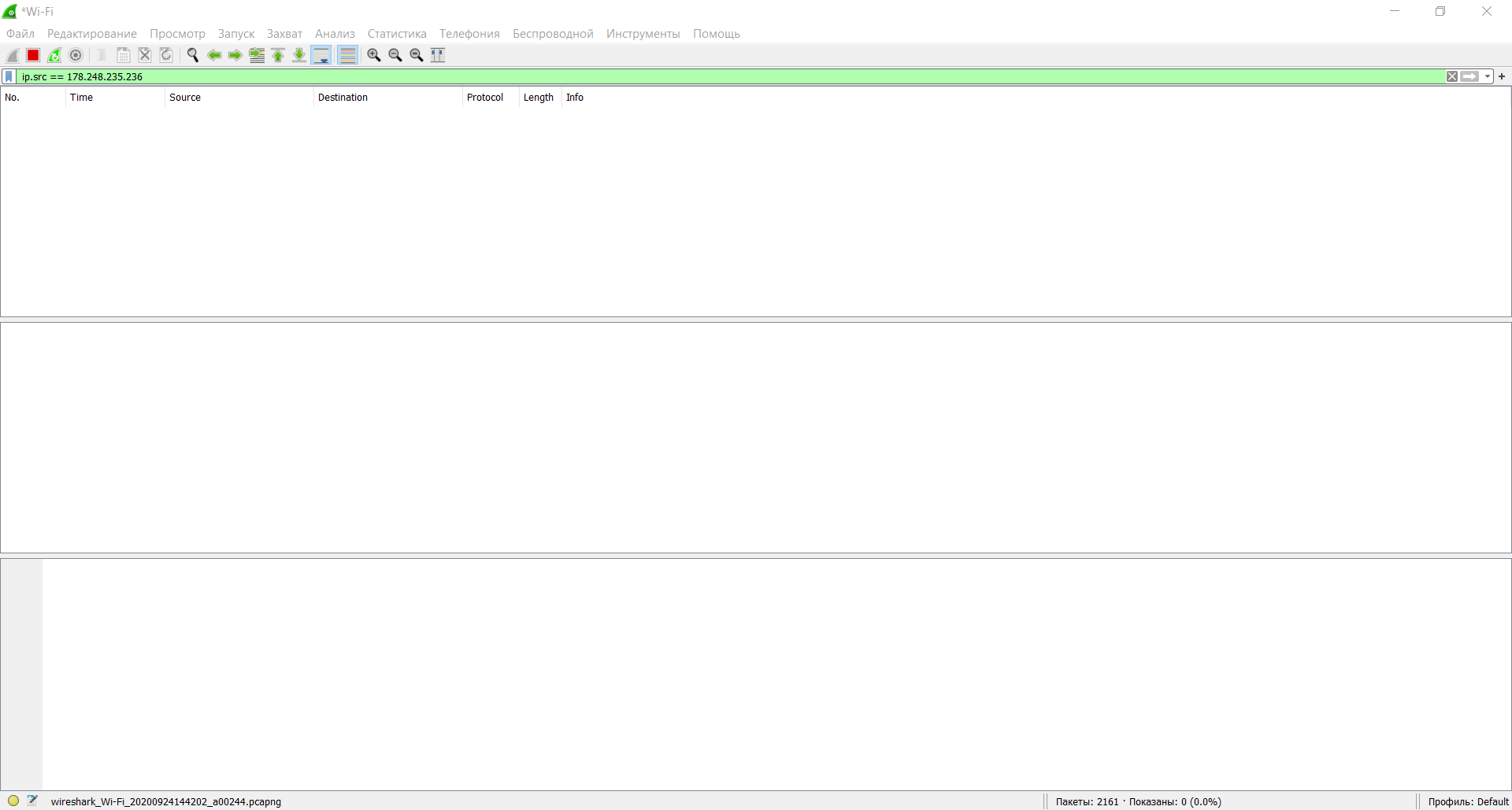
Команда -type=any



Данная команда выводит то же, что и команда -query=mx

Анализ трафика с помощью WireShark

Фильтр ip.src



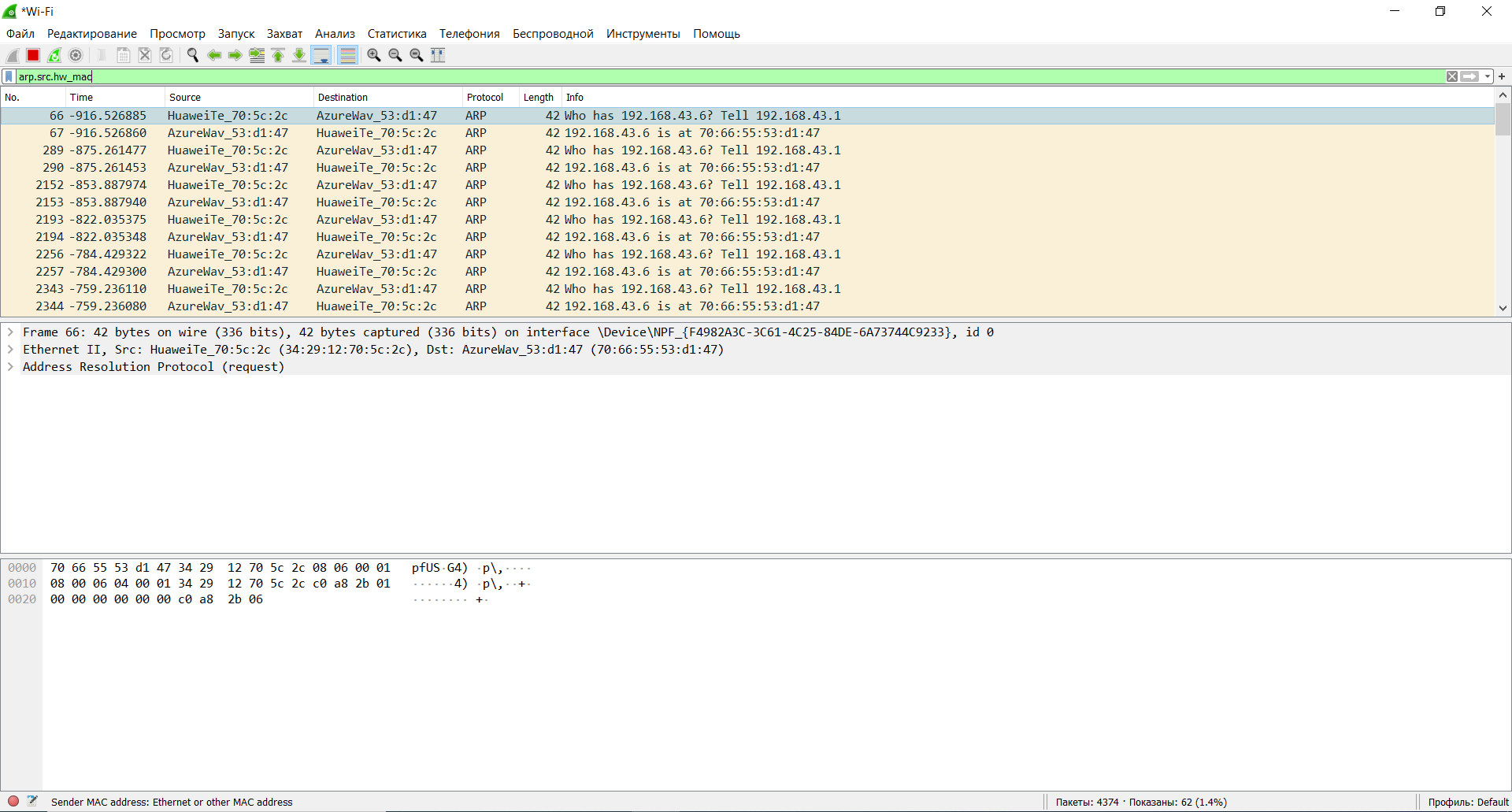
При этом фильтре ничего не произошло(

ip.dst отвечает за трафик, отправленный на IP

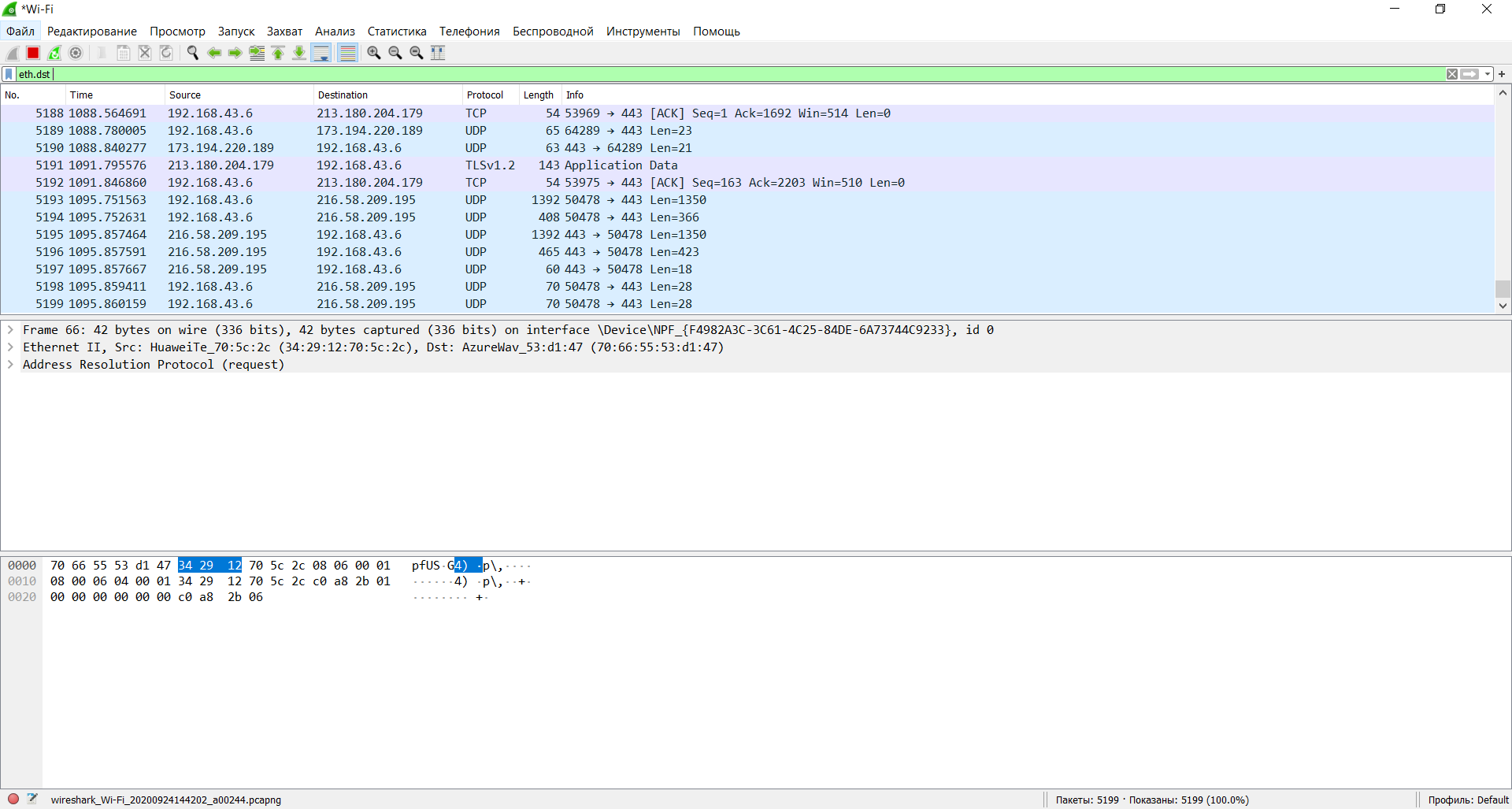
ip.addr отвечает за фильтрацию трафика, в котором упоминается этот IP

udp.src - не работает

arp.src.hw\_mac используется для фильтрации по ARP протокола по mac – адресу



eth.dst - фильтр трафика по mac - адресу получателя



eth.src - фильтр трафика по mac - адресу отправителя

