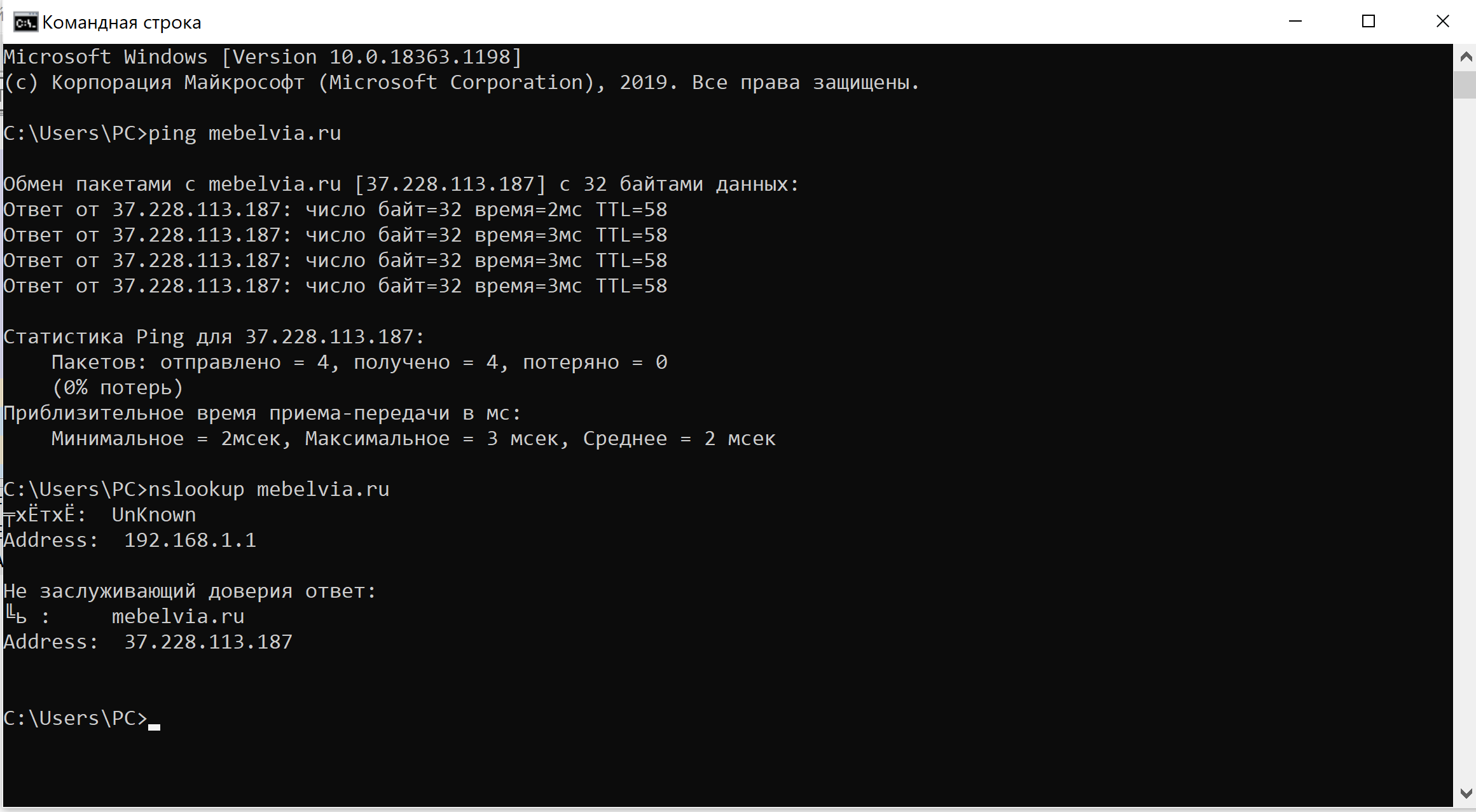
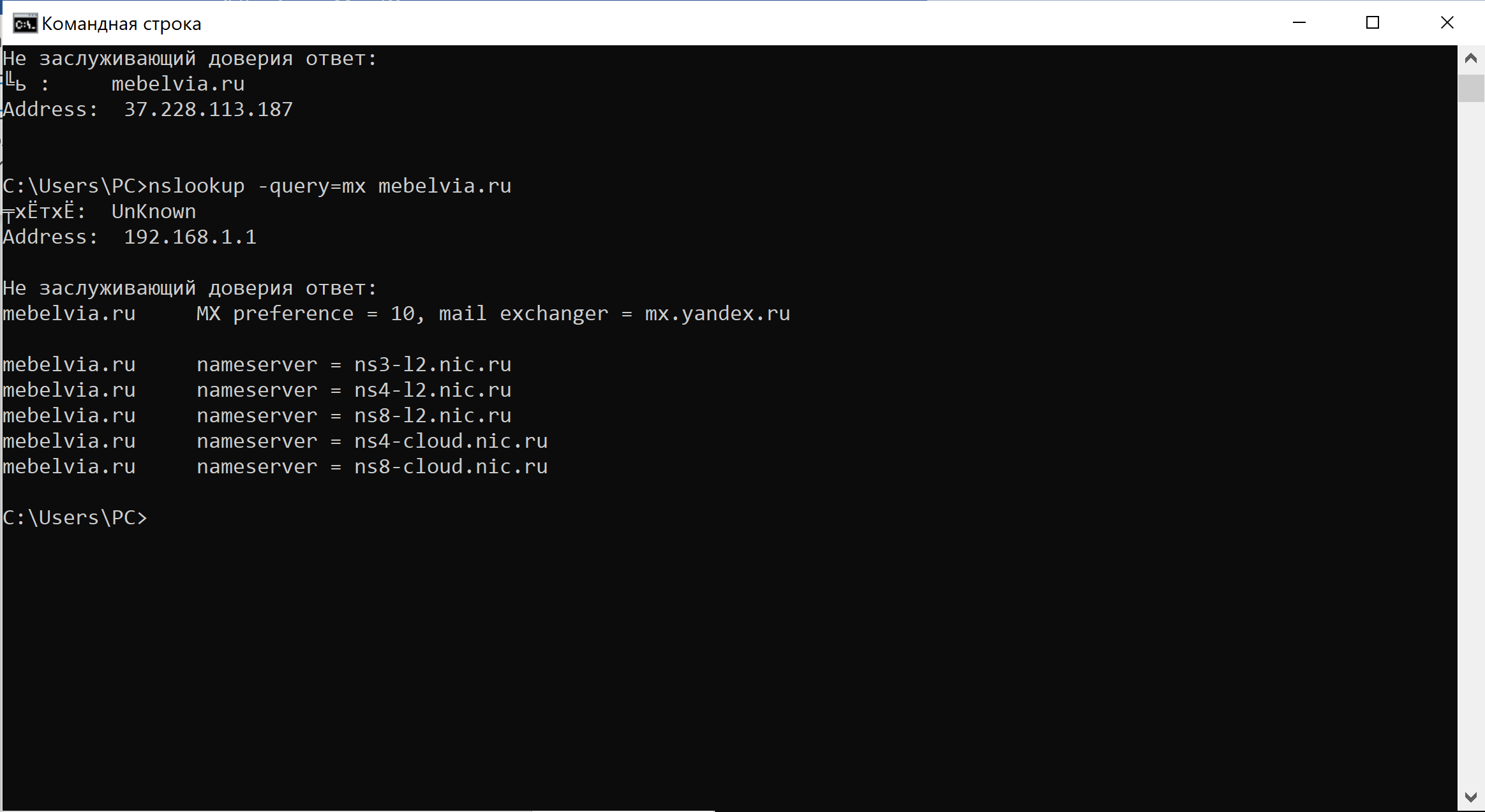
Для работы я взял сайт – mebelvia.ru

Чтобы узнать ip–адресс я использовал команды ping и nslookup в консоли:



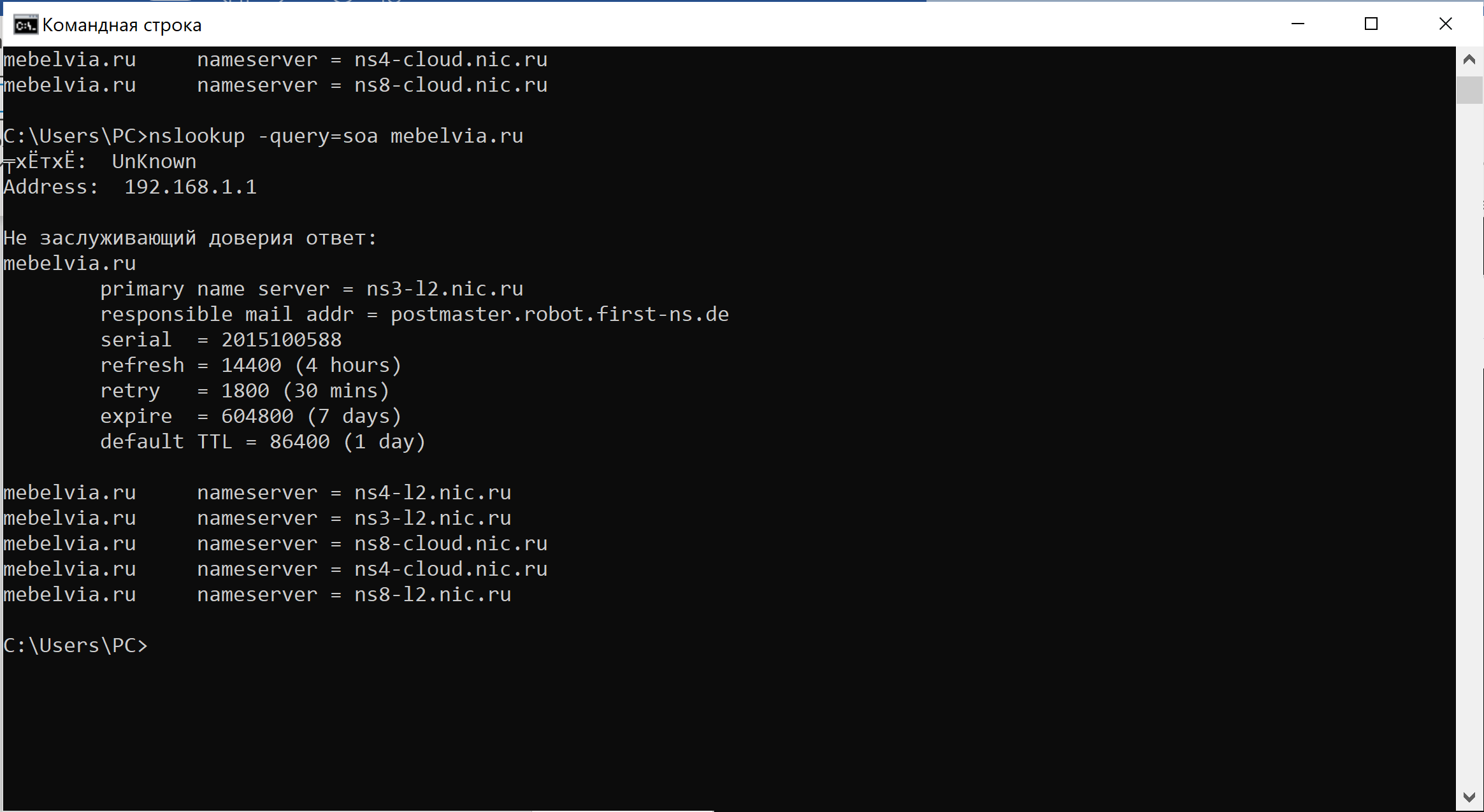
Следовательно ip-адресс – 37.228.113.187

Дальше я изучил nslookup, начал с команды -query=mx:



Выяснилось, что у этого домена серверная почта – mx.yandex.ru

После чего перешел к команде – -query=soa:

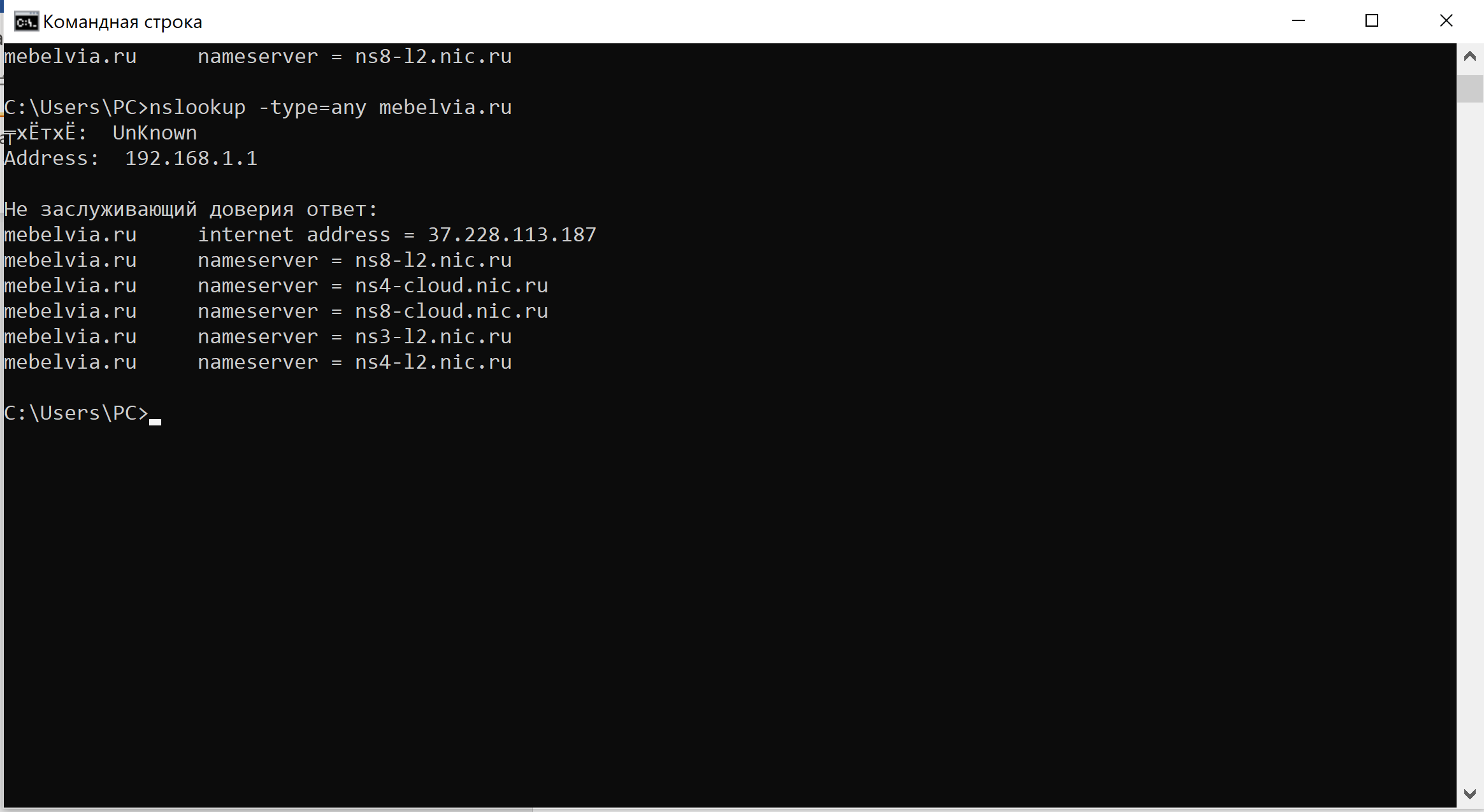


Таким образом я получил информацию о:

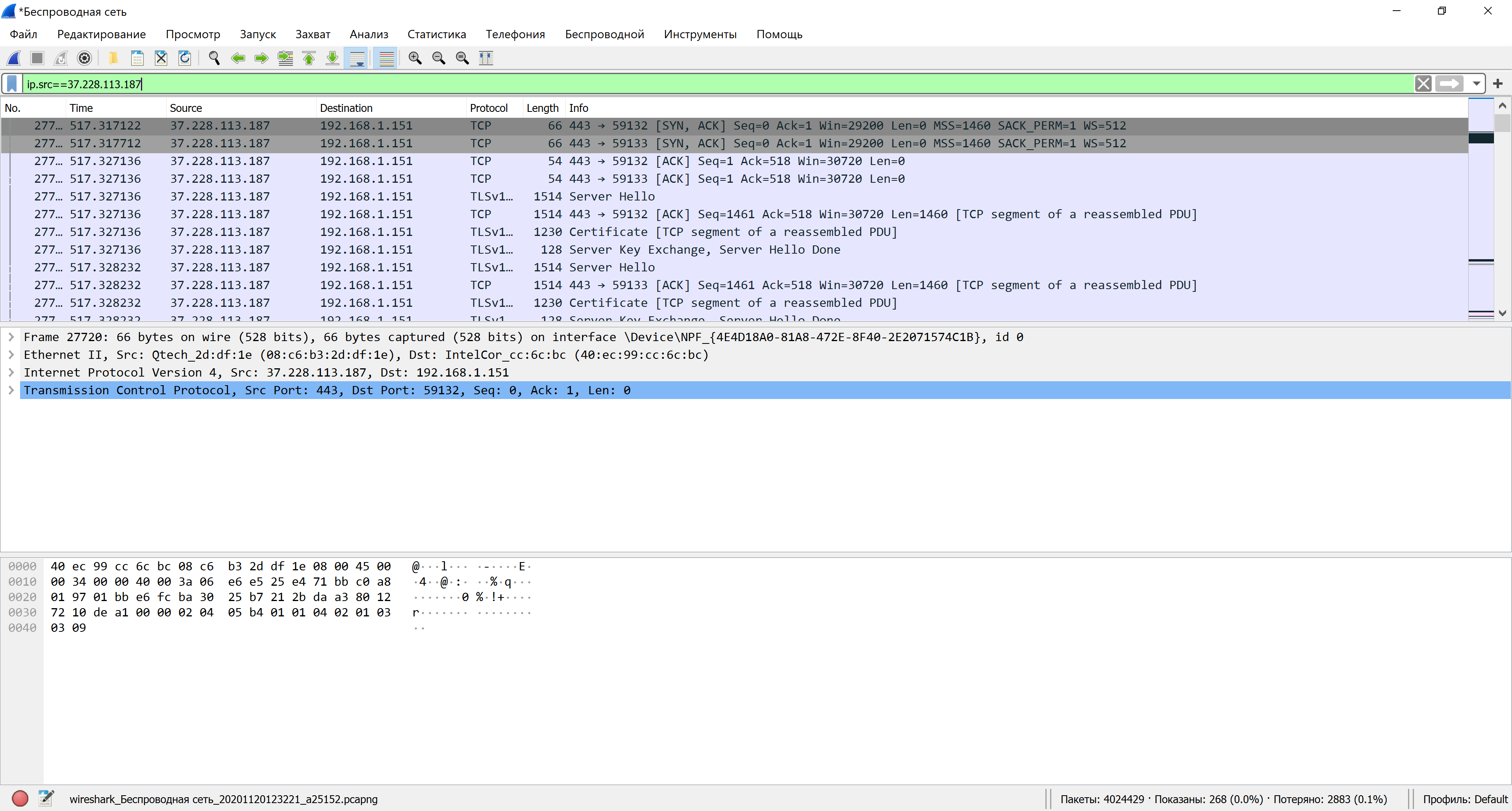
* Первичном названии сервера
* Почту администратора сервера домена
* Серийный номер
* Период времени (в секундах), через который вторичный DNS-сервер отправит запрос первичному, чтобы проверить, поменялся ли серийный номер.

Интервал для повторного соединения с первичным DNS-сервером, если он по каким-то причинам не смог ответить на запрос и т.д.

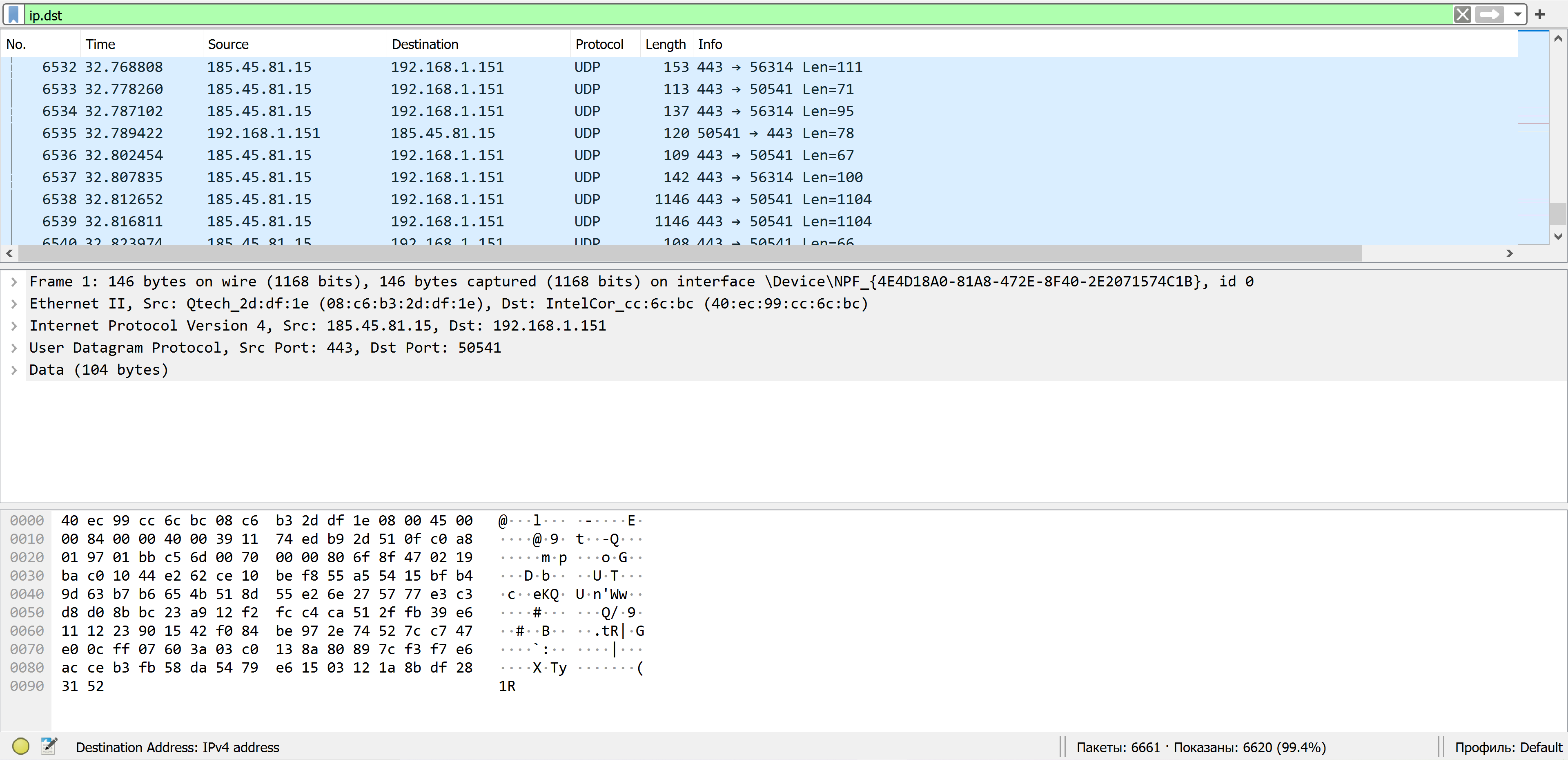
Последняя команда – -type=any:



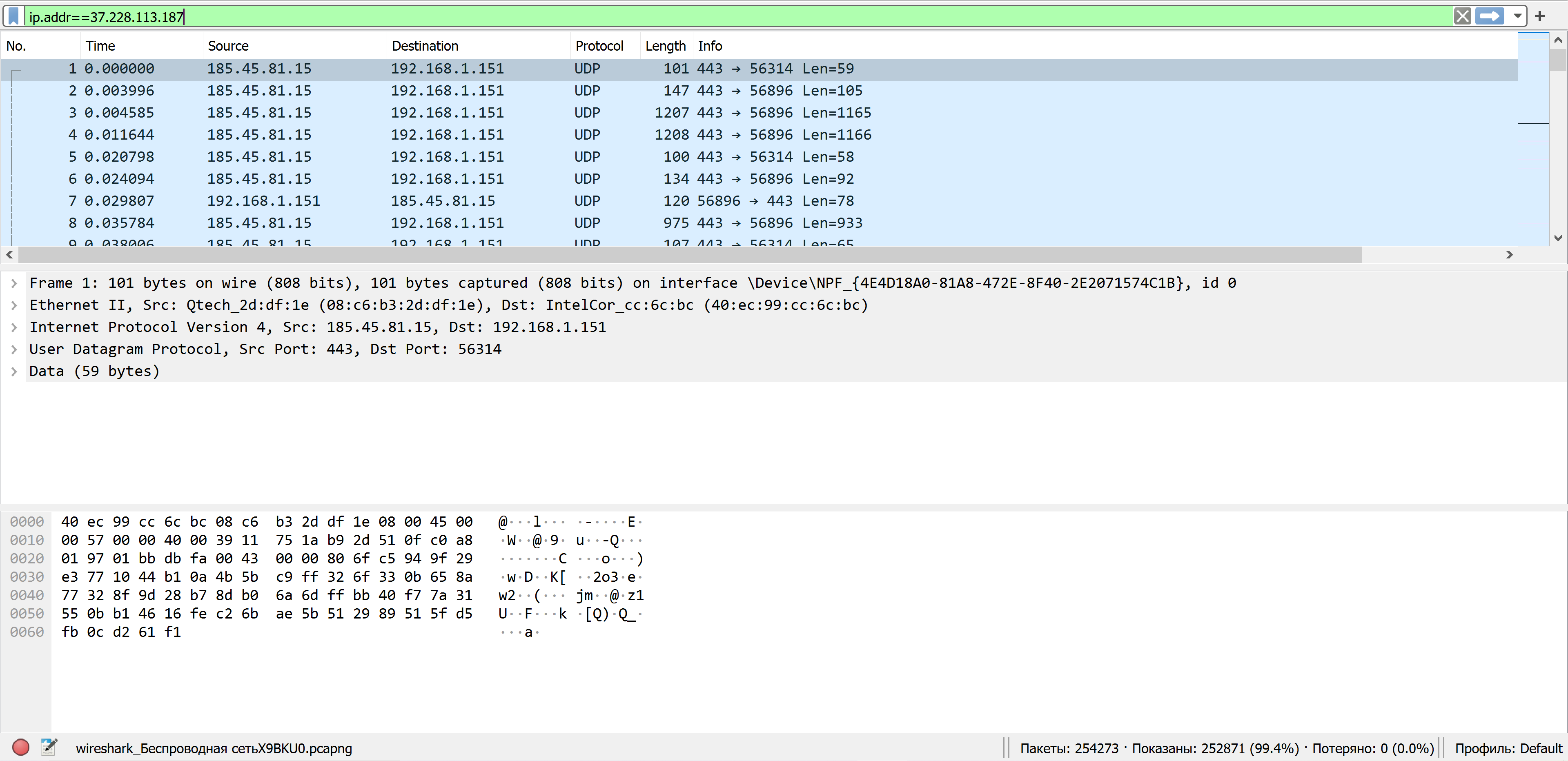
С помощью Wireshark и фильтра ip.src==37.228.113.187 я изучил трафик сайта:



ip.dst отвечает за трафик отправленный ip:

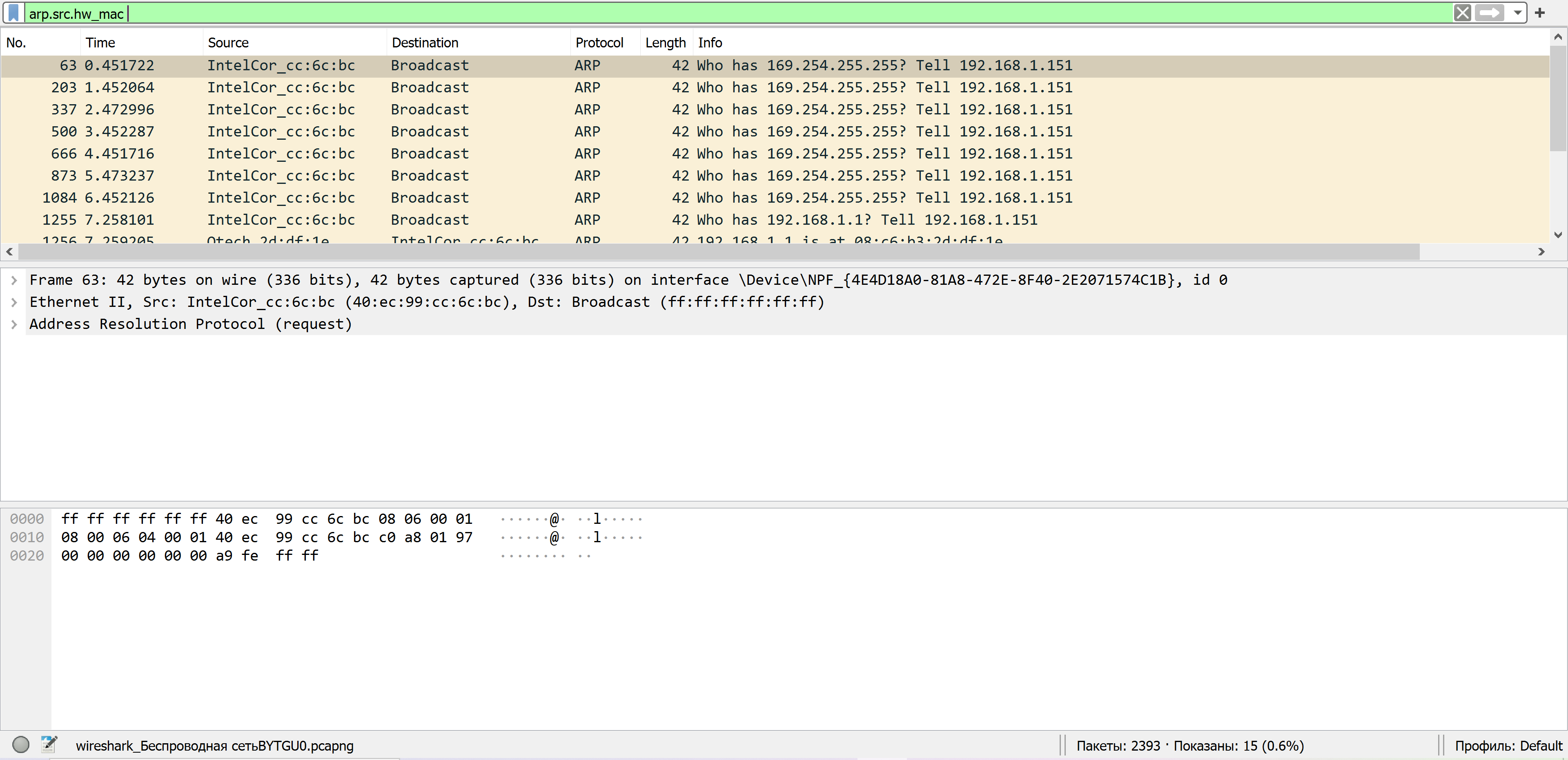


ip.addr отвечает за фильтрацию трафика:

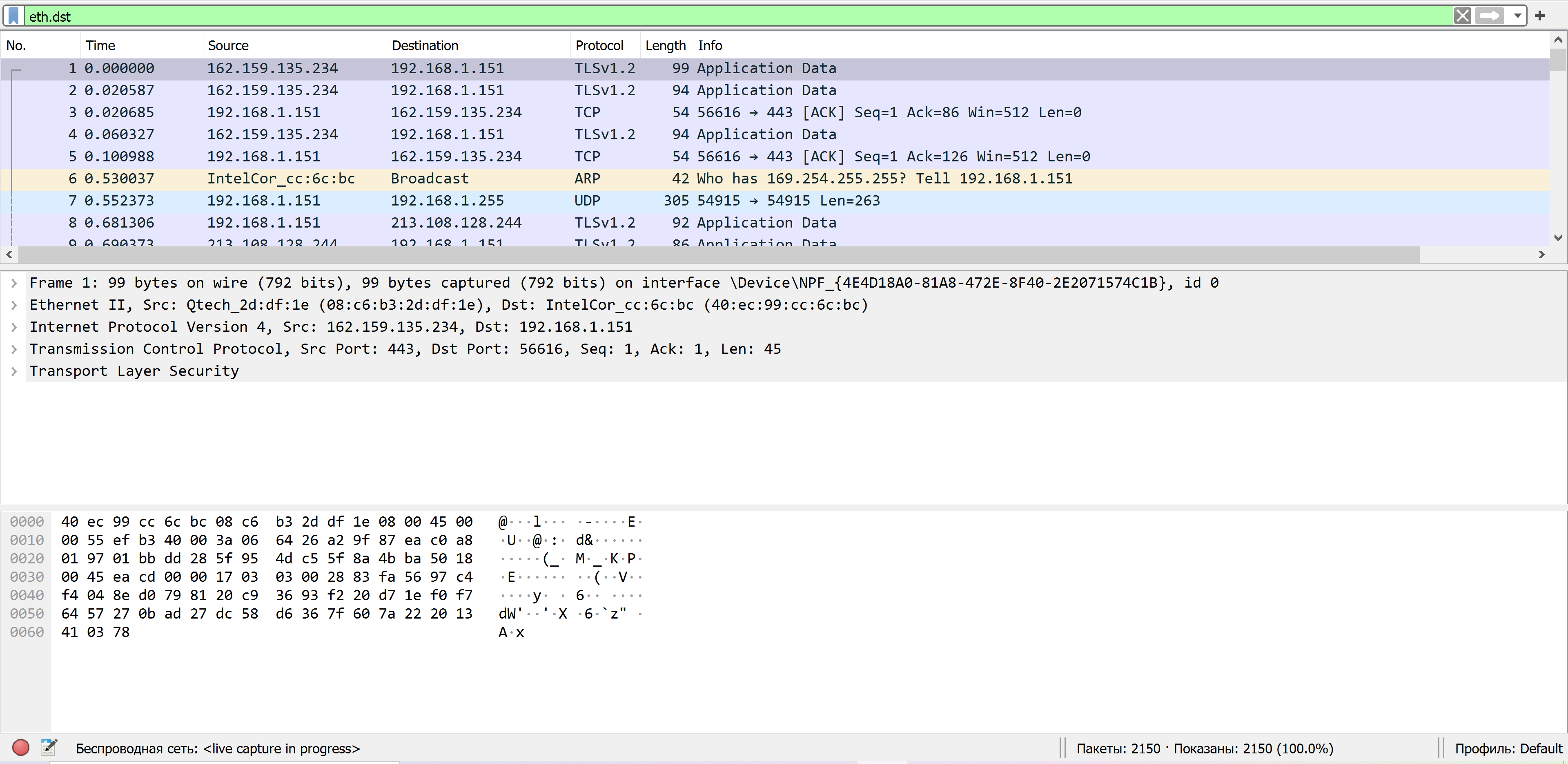


udp.port== не работает.

arc.src.hw\_mac используется для фильтрации по **arp** протокола по mac-адресу:



eth.dst это фильтр трафика по mac-адресу получателя:



eth.src это фильтр трафика по mac-адресу отправителя:

