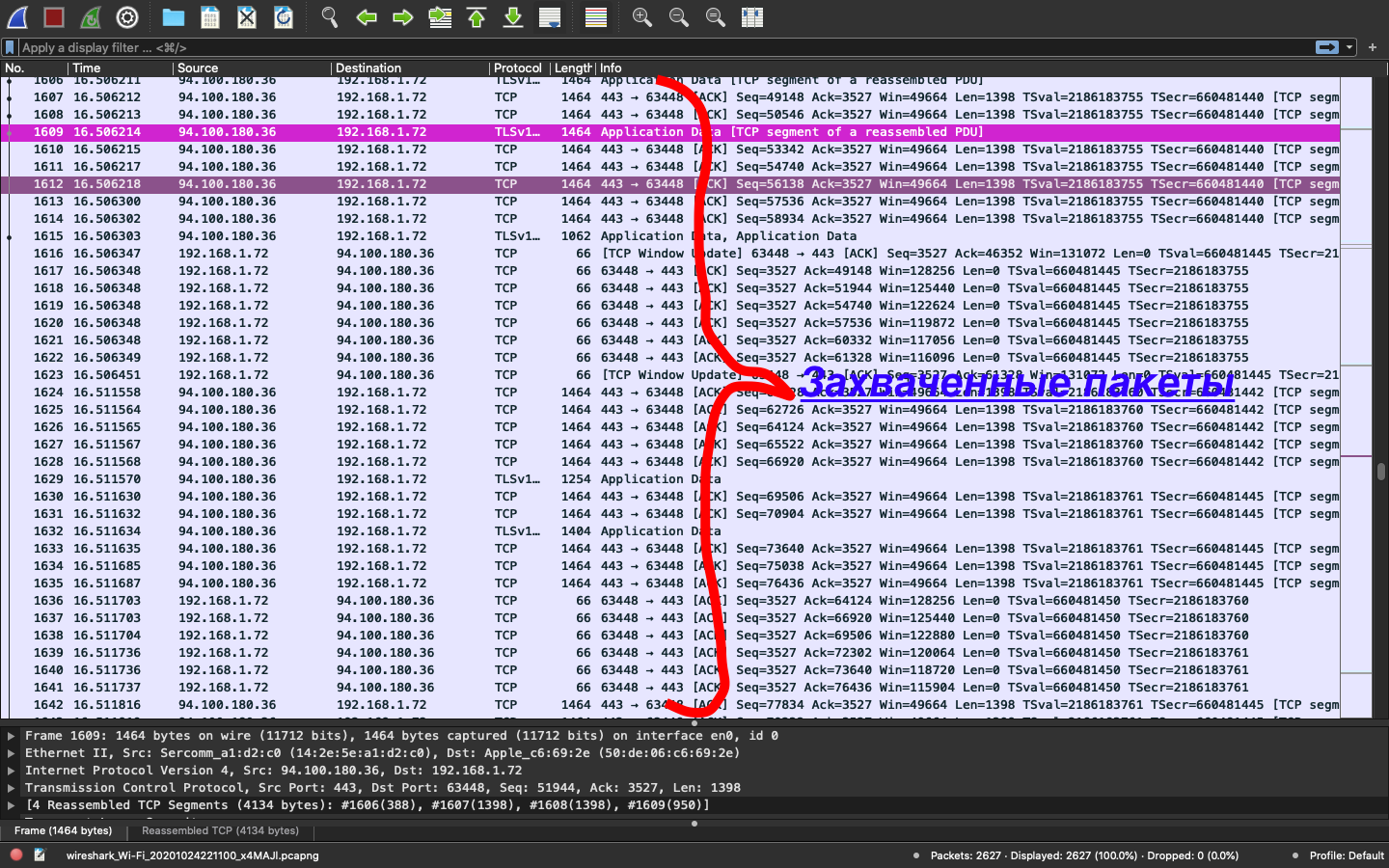
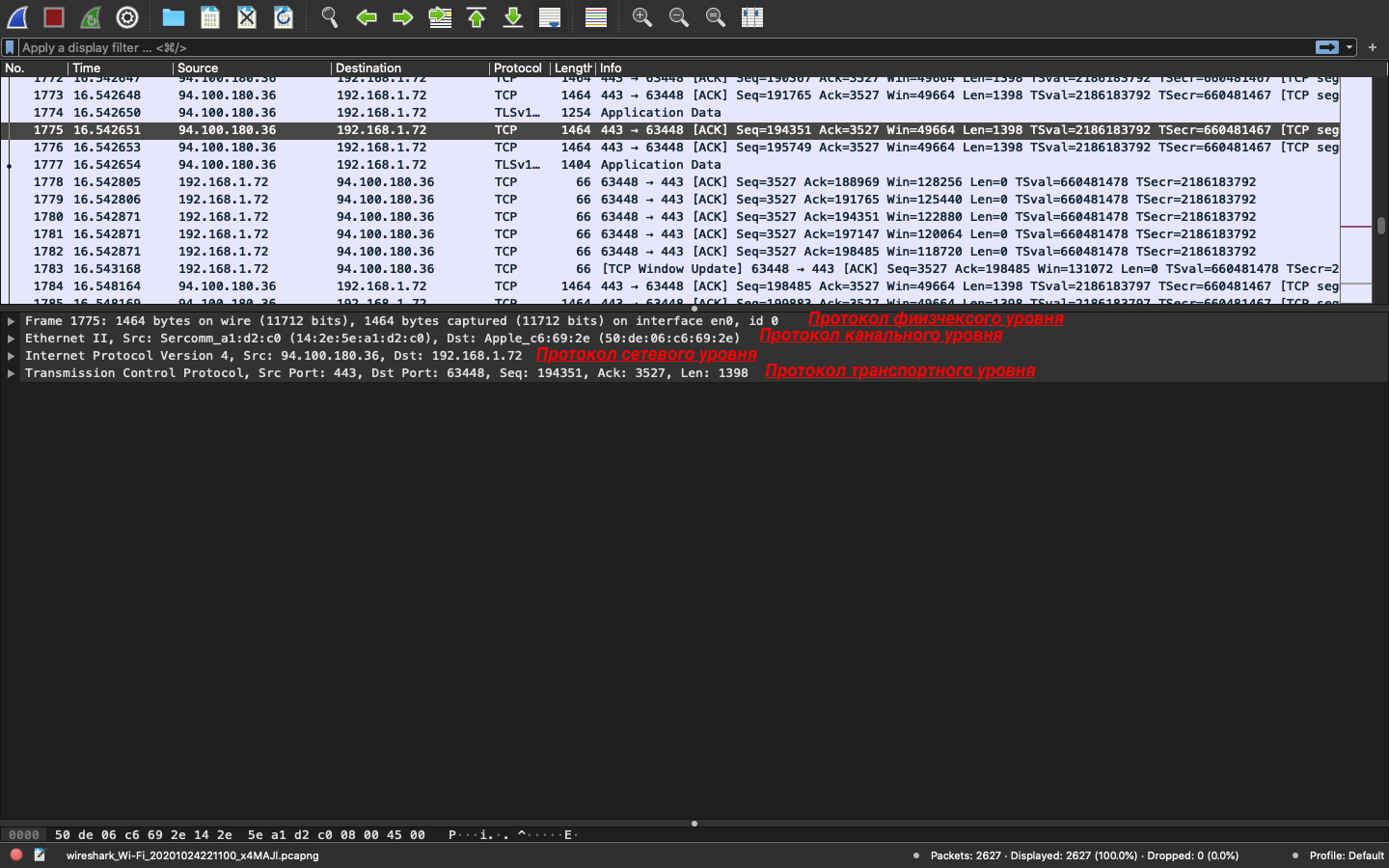
**«**АНАЛИЗ СТРУКТУРЫ СЕТЕВОГО ТРАФИКА С ПОМОЩЬЮ ПРОГРАММЫ WIRESHARK**»**

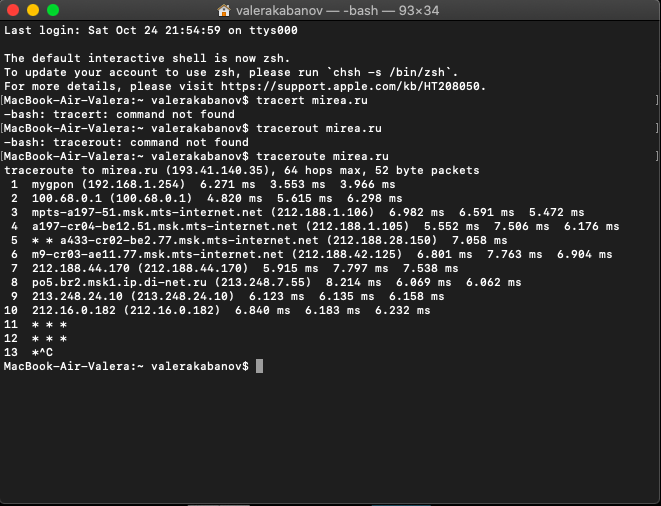
**№1**

**1)Структура пакетов**

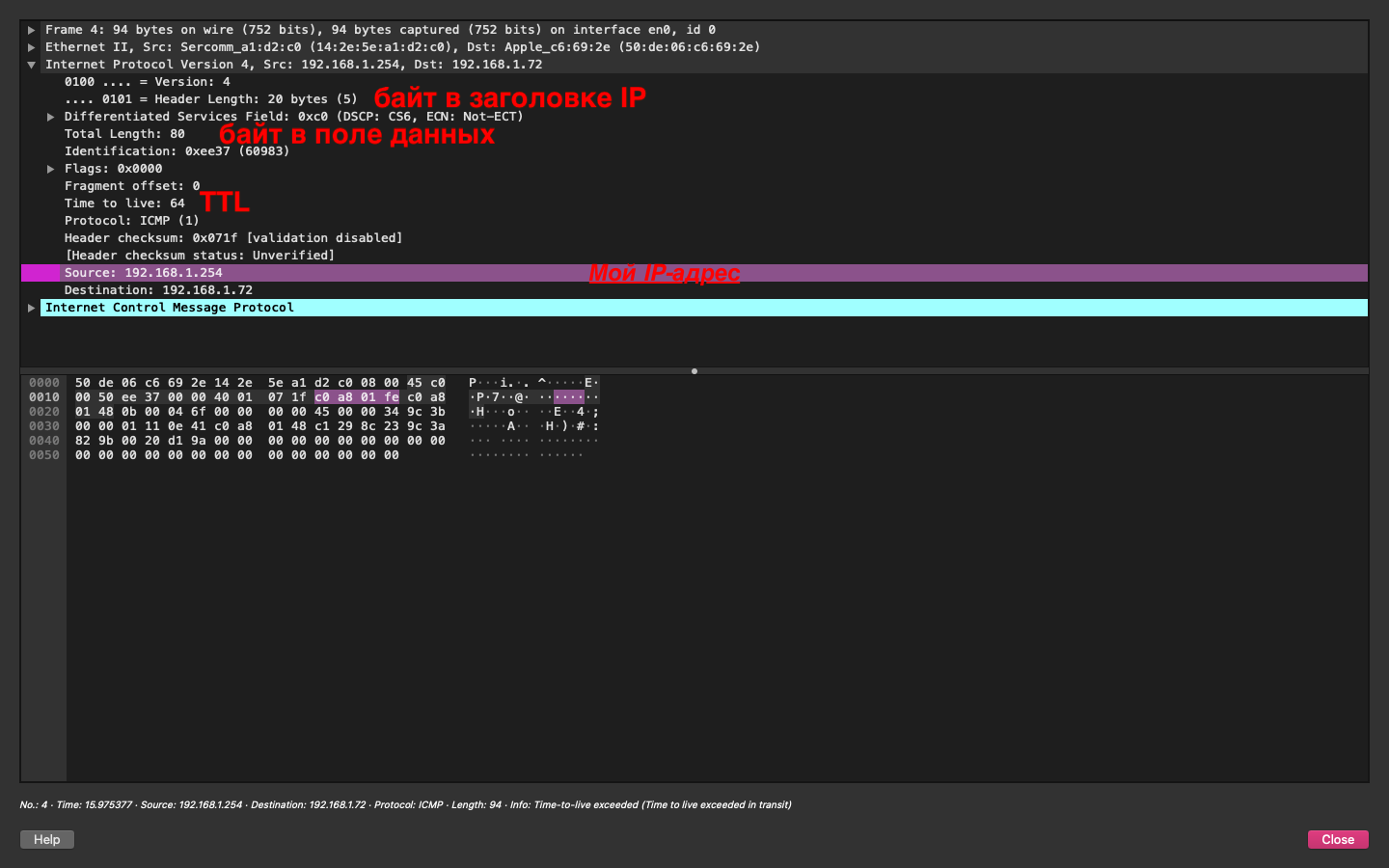


**2)Назначение заголовков**

**№2**

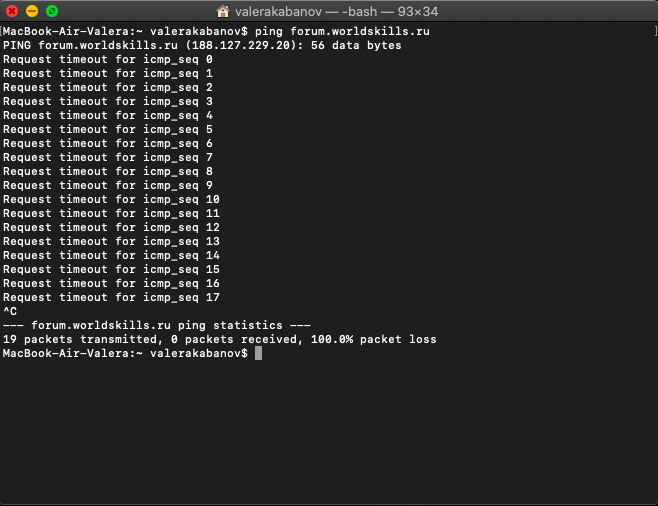
**Произвел захват трафика и вы полнил трассировку до конечного узла **

**Определил свой IP-адрес, время жизни пакета.**

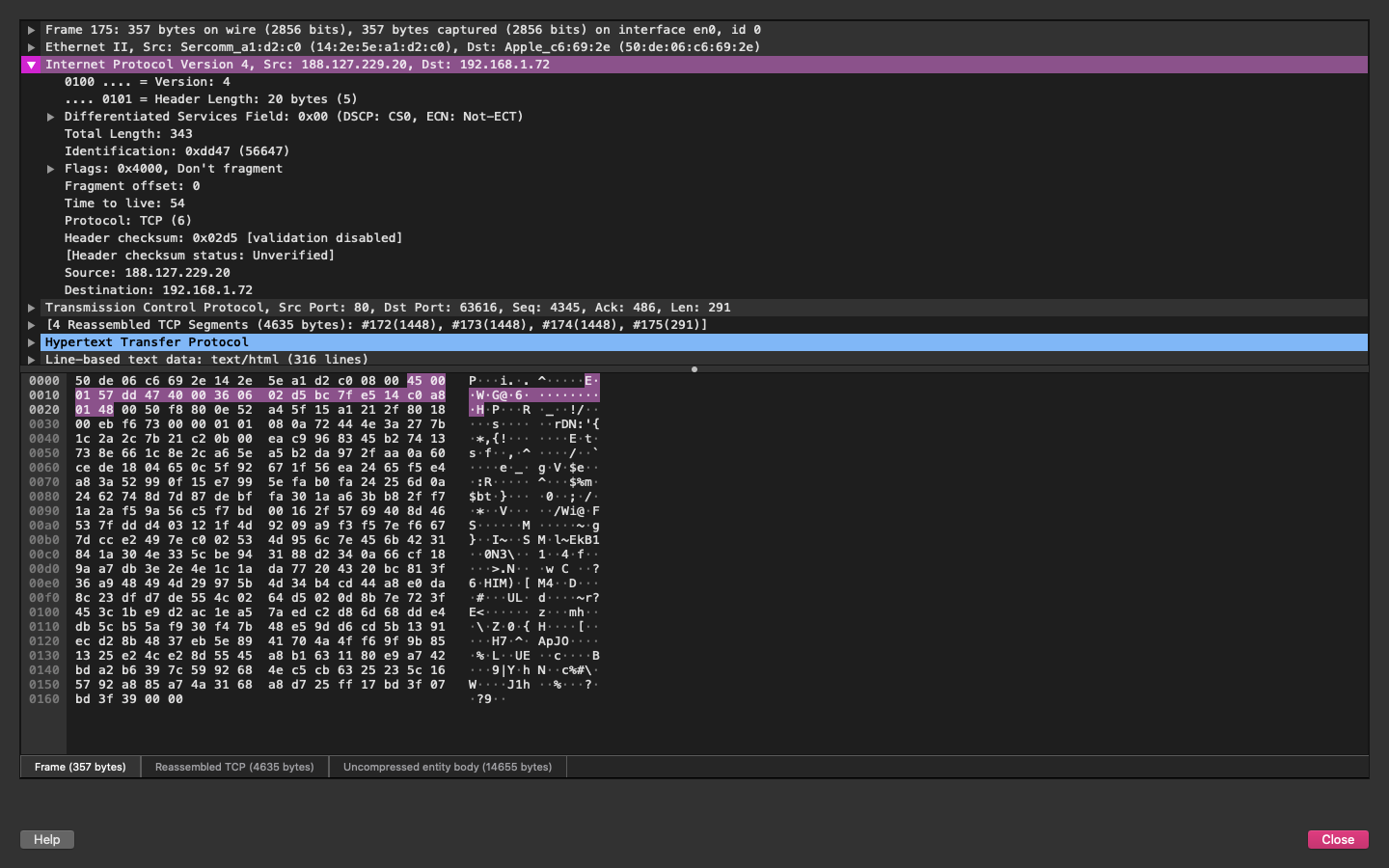
****

**№3**

**Обнаружение узлов с помощью утилиты nslookup**

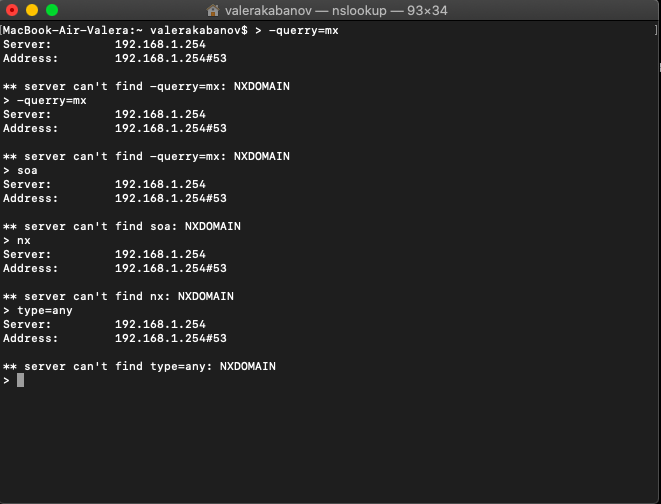
****

**Этим способом я узнал IP-адрес ресурса, но есть и друге способы. Например, с помощью Wireshark:**

****

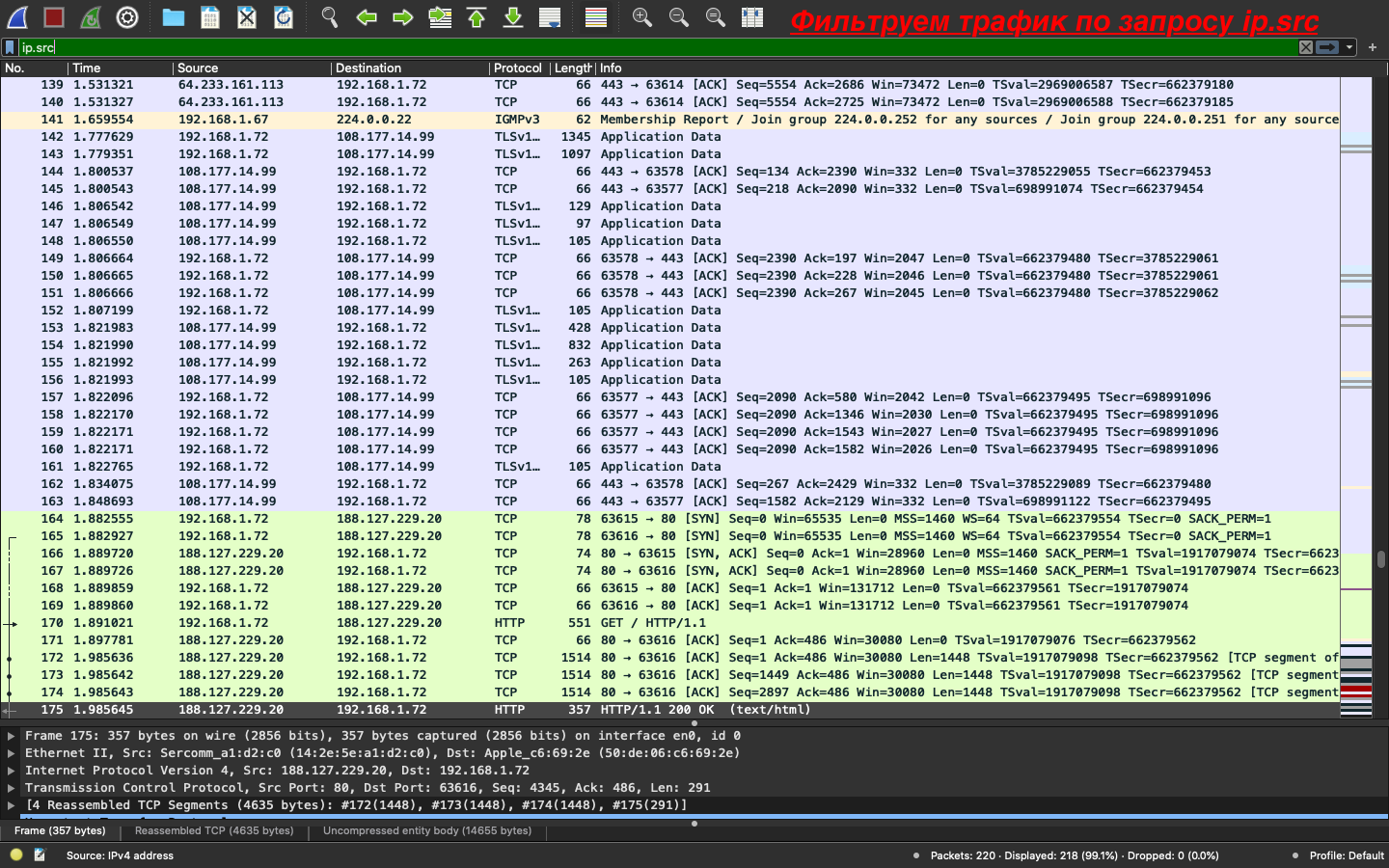
**Далее, при изучении аргументов утилиты nslookup на mac.OS**

**происходит такая штучка:**

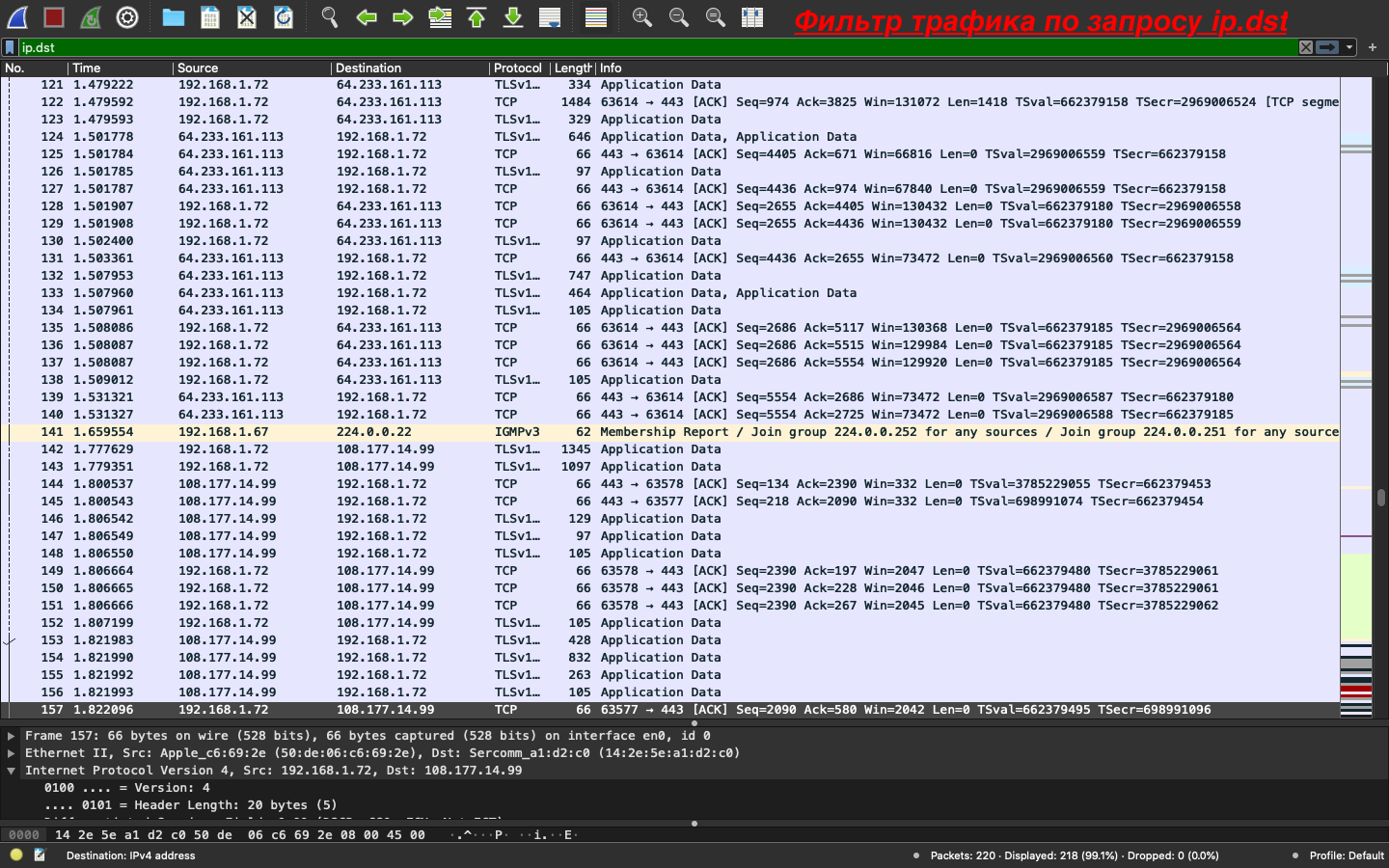
****

**Далее я изучил основные типы фильтра:**

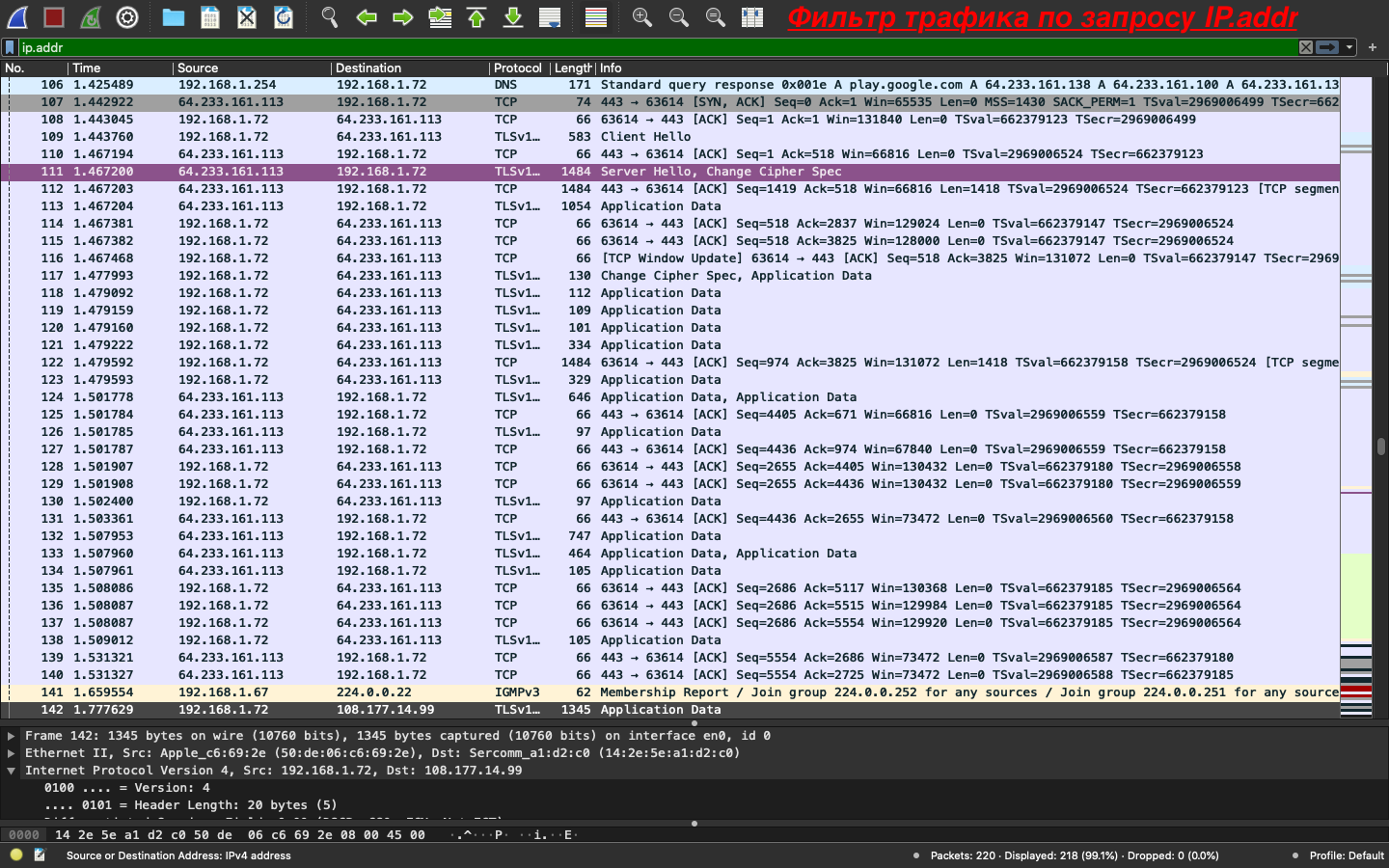
1. **Ip.src**

****

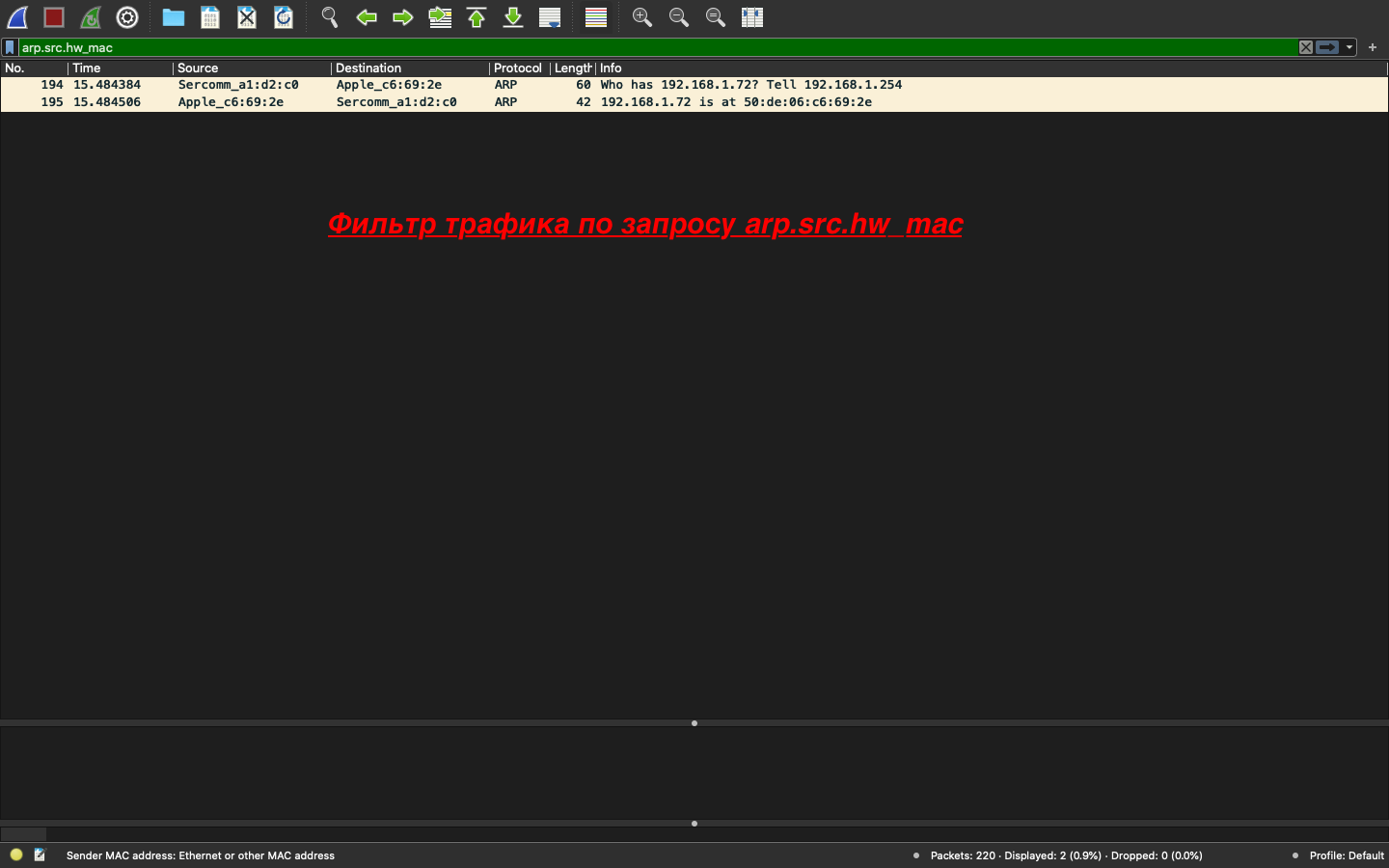
**2)ip.dst**

****

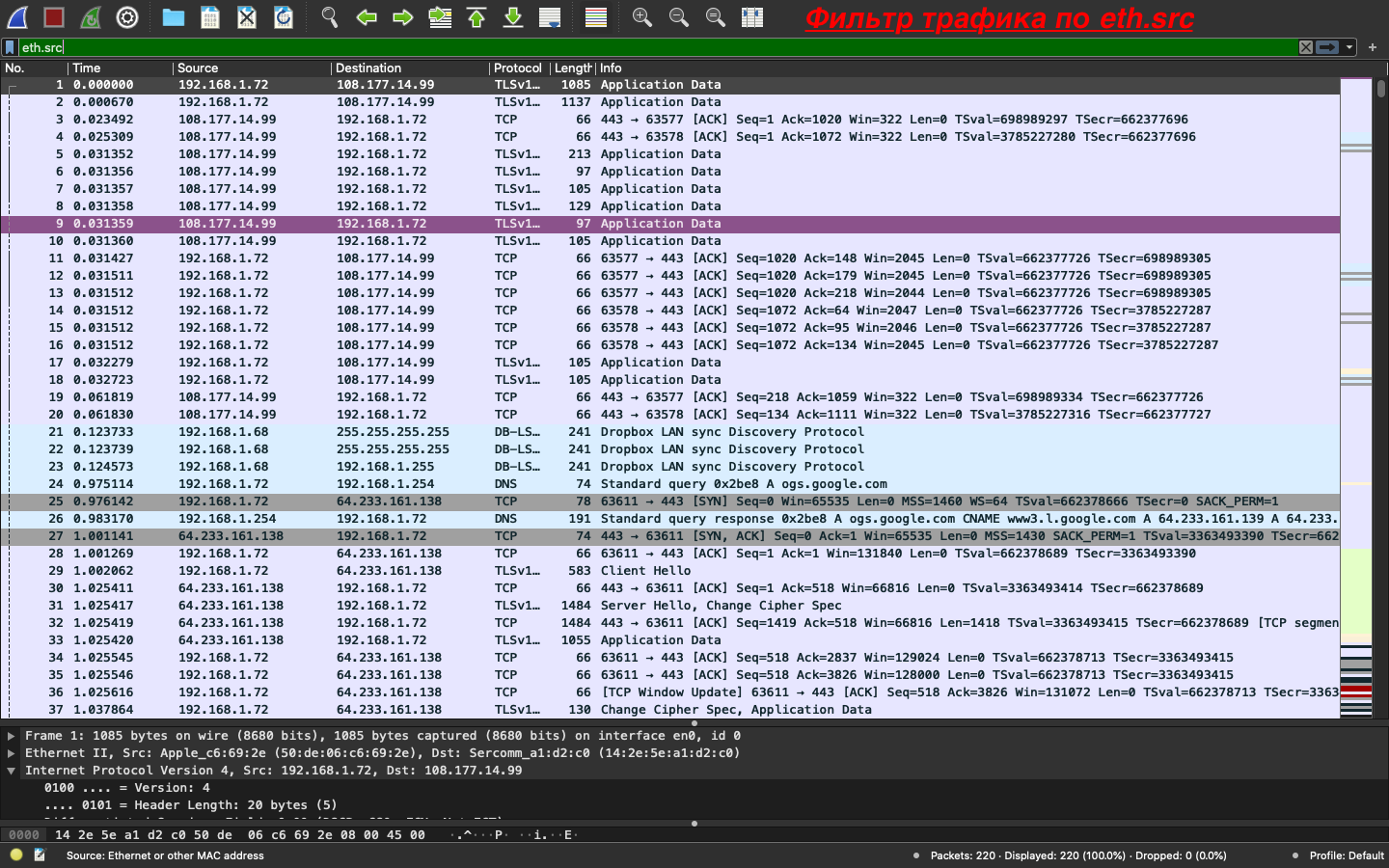
**3)ip.addr**

****

**4)arp.src.hw\_mac**

****

**5)eth.src**

****

**Конец!**