**Оглавление**

[Wireshark 2](#_Toc54882477)

[HTTP (Определение ip разными способами) 3](#_Toc54882478)

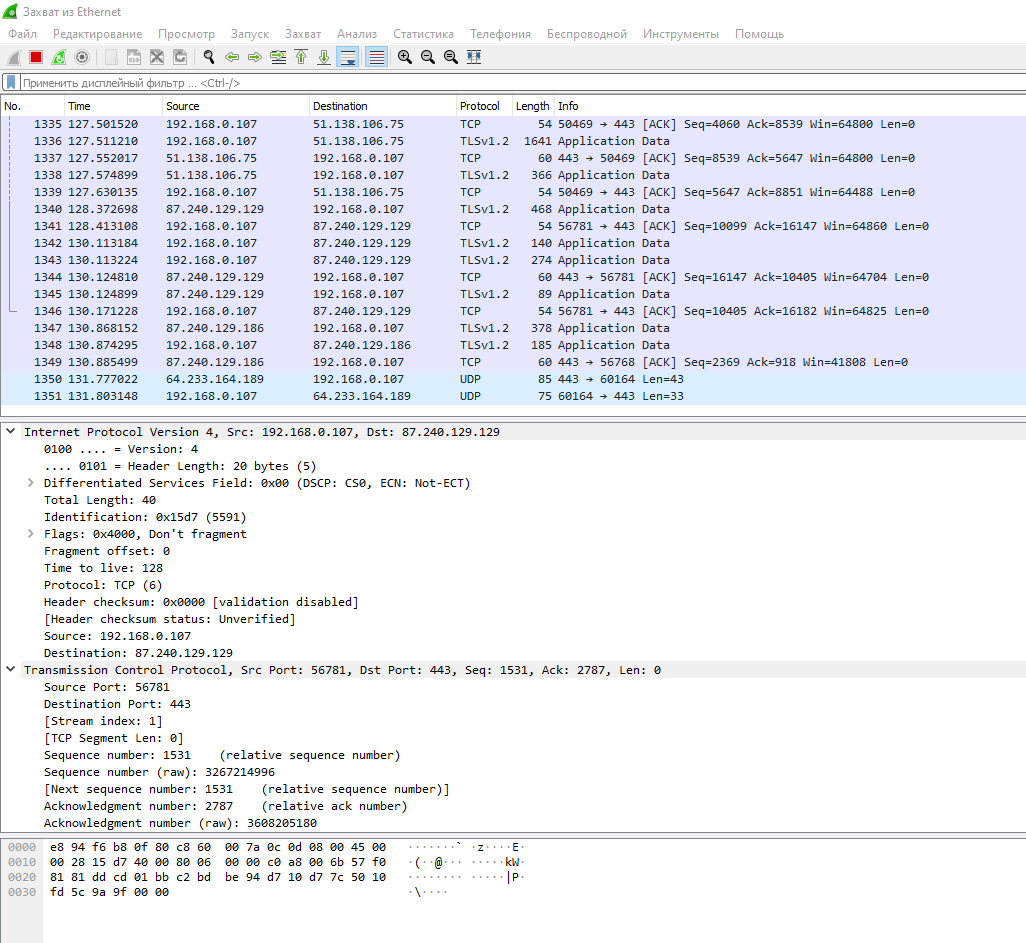
[Nslookup и соответствующие команды 4](#_Toc54882479)

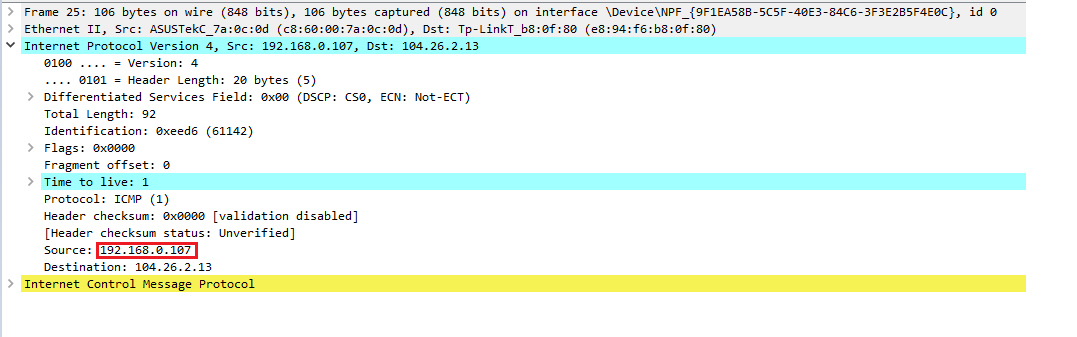
[Основные фильтры 8](#_Toc54882480)

[ICMP 12](#_Toc54882481)

[ARP 14](#_Toc54882482)

# Wireshark

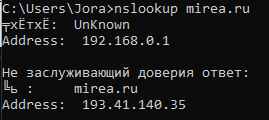




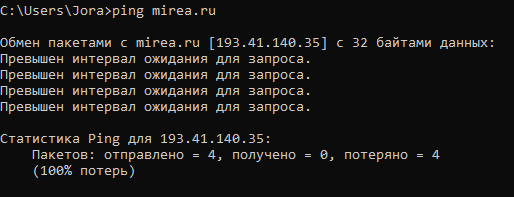
1. IPv4: 192.168.0.107
2. Заголовок содержит 20 байтов, 72 байта в поле данных
3. TTL: 1

# HTTP (Определение ip разными способами)

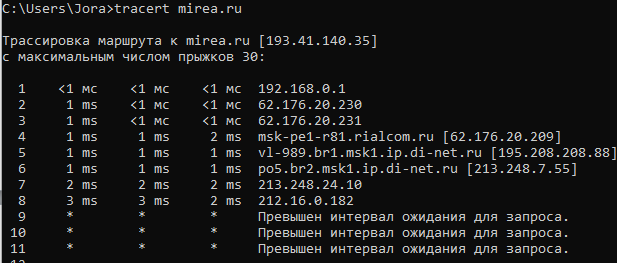
1 вариант определения IP: (сайт mirea.ru, IP: 193.41.140.35)



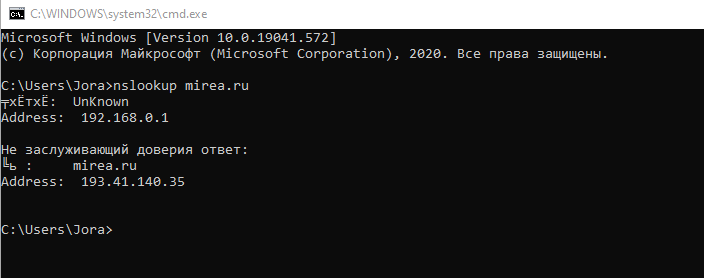
2 вариант определения IP: (сайт mirea.ru, IP: 193.41.140.35)

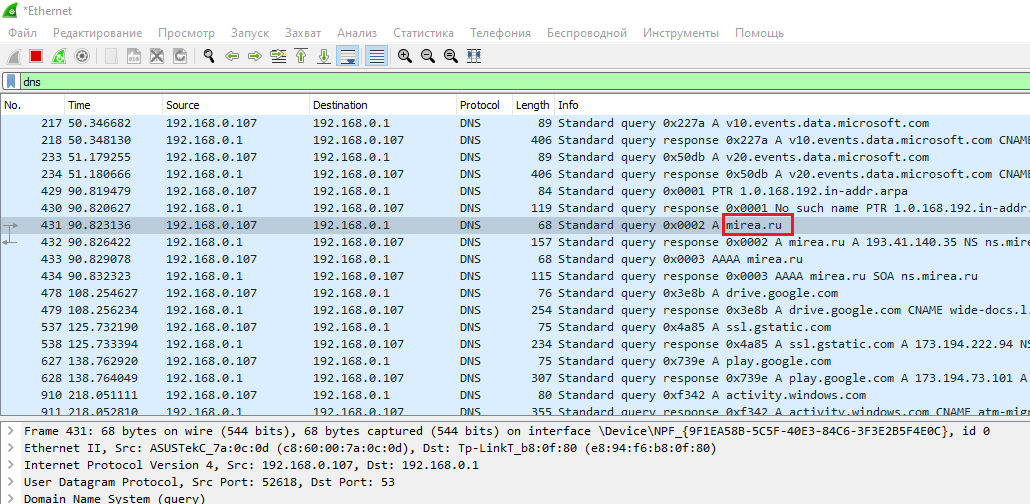


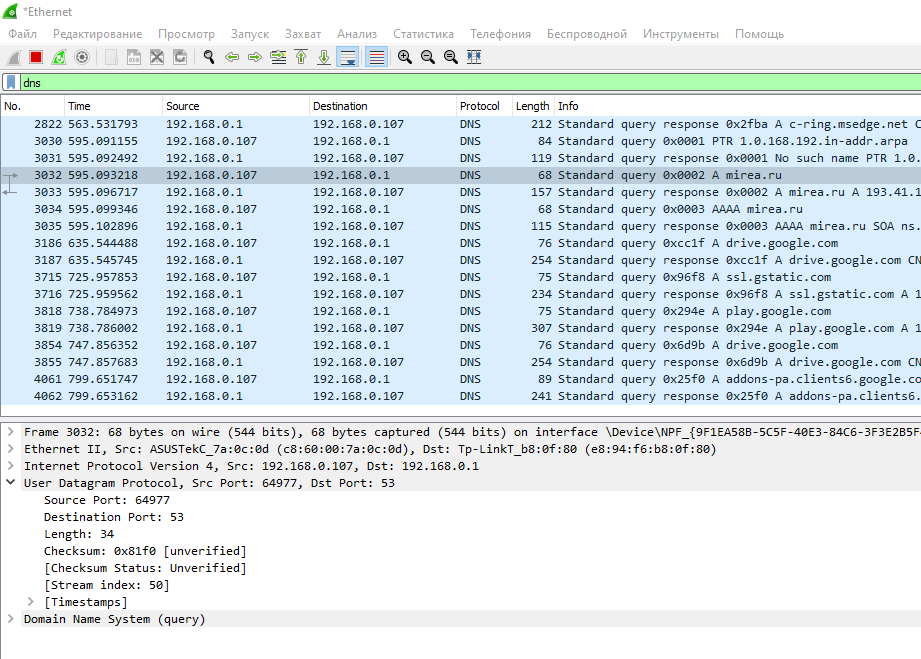
3 вариант определения IP: (сайт mirea.ru, IP: 193.41.140.35)

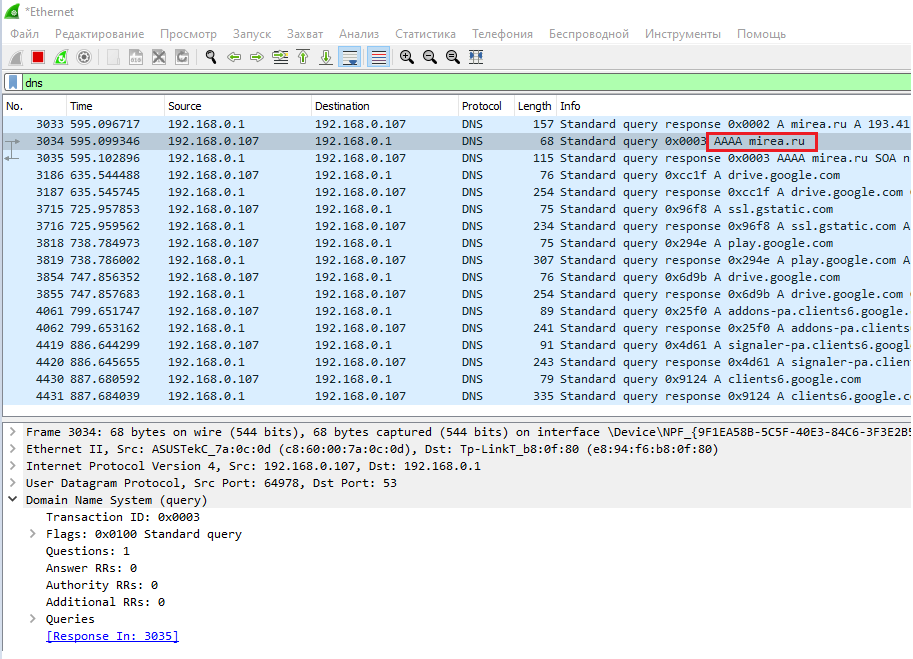


# Nslookup и соответствующие команды



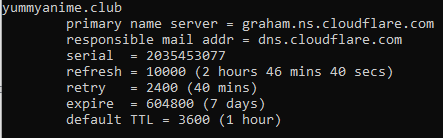






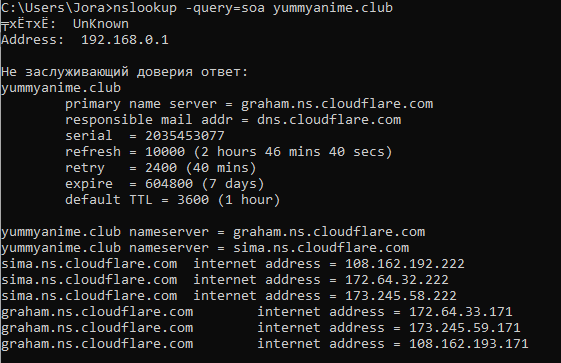
**nslookup -query=mx**

Запись MX (Mail eXchange, обмен почтой) хранит соответствие доменного имени почтовому серверу этого домена.



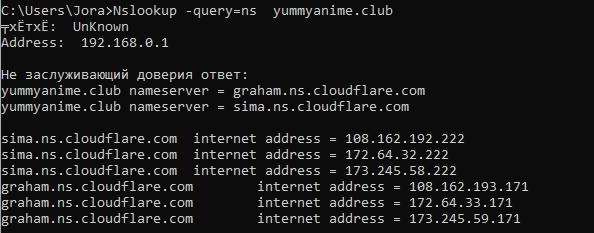
**Nslookup -query=soa**

Запись SOA (Start of Authority, начальная запись зоны) содержит информацию о зоне домена, адрес его администратора, серийный номер и т.д.



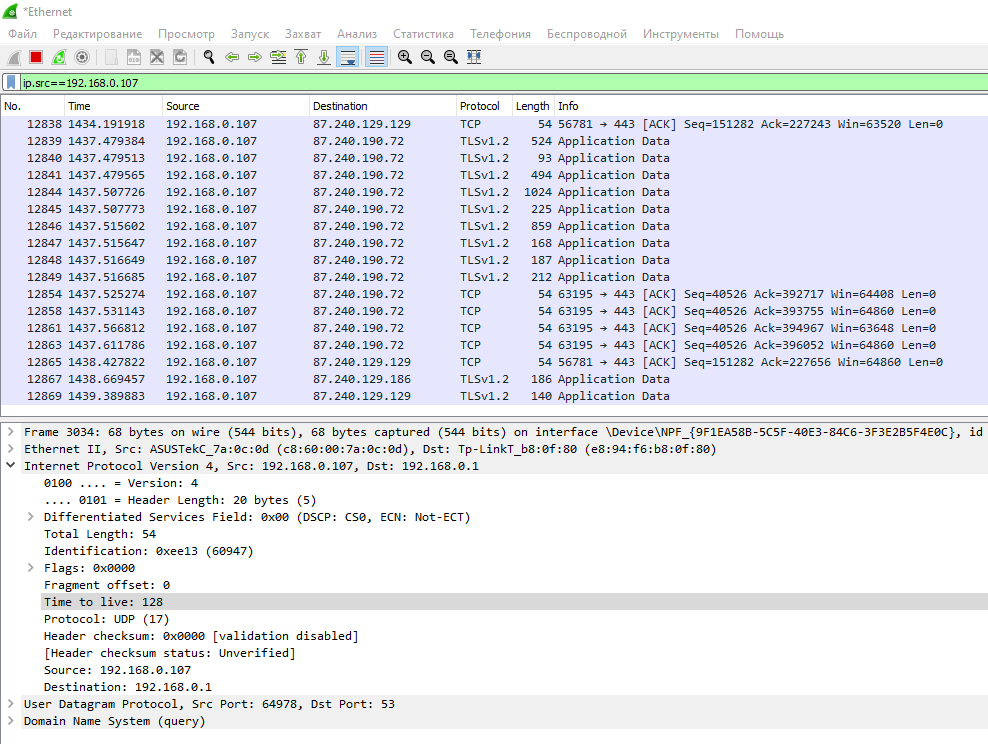
**Nslookup -query=ns**

Запись NS (Name Server, сервер имен) содержит соответствие доменного имени DNS-серверу, авторитативному для заданного домена.



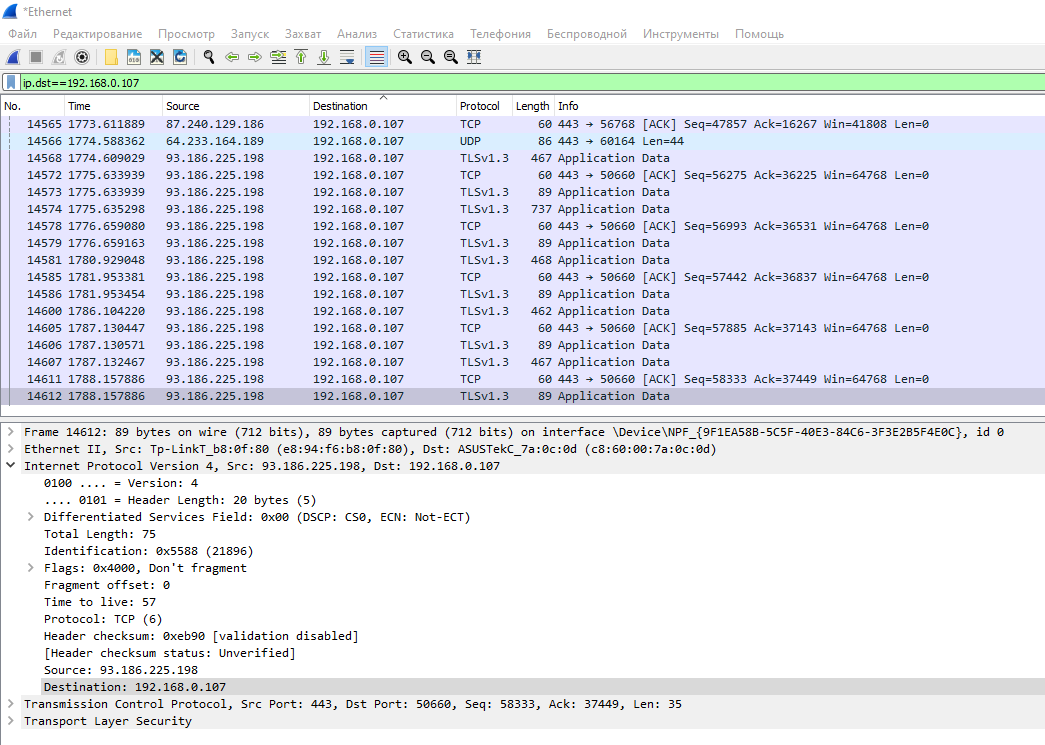
# Основные фильтры

**ip.src==**192.168.0.107



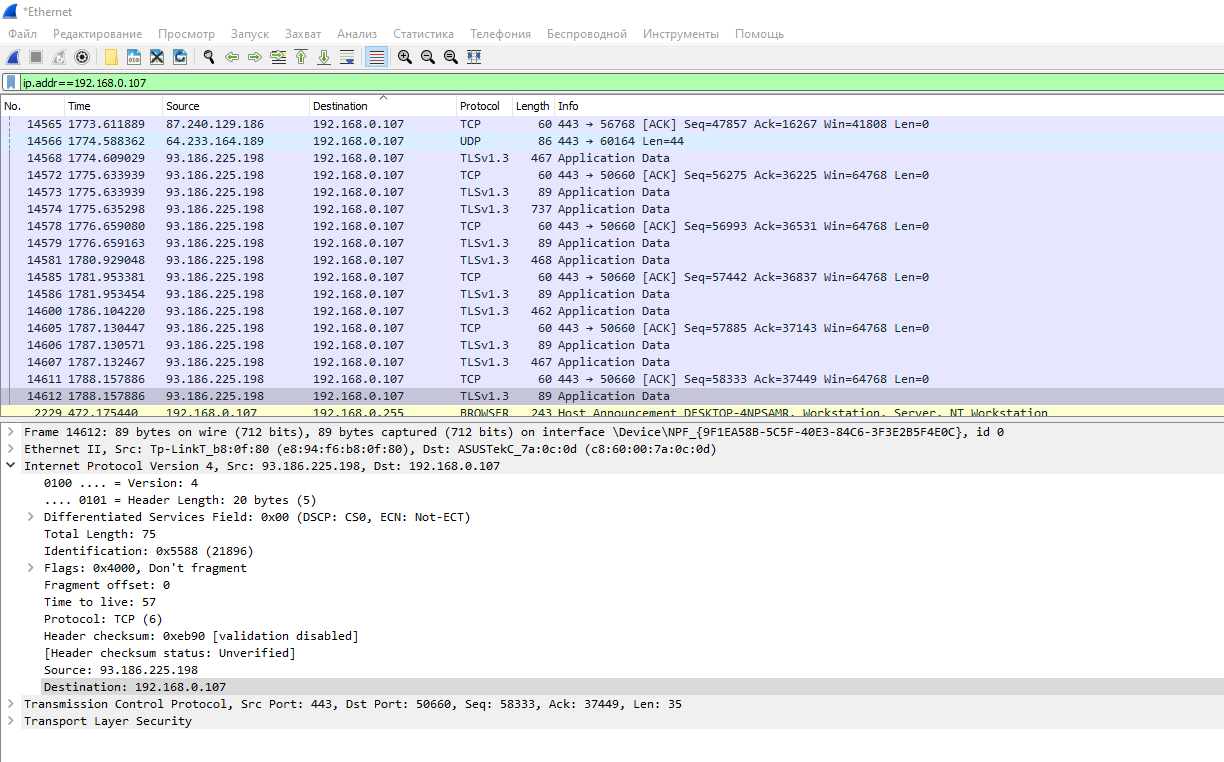
Фильтр по IP по адресу отправителя

**ip.dst==**192.168.0.107



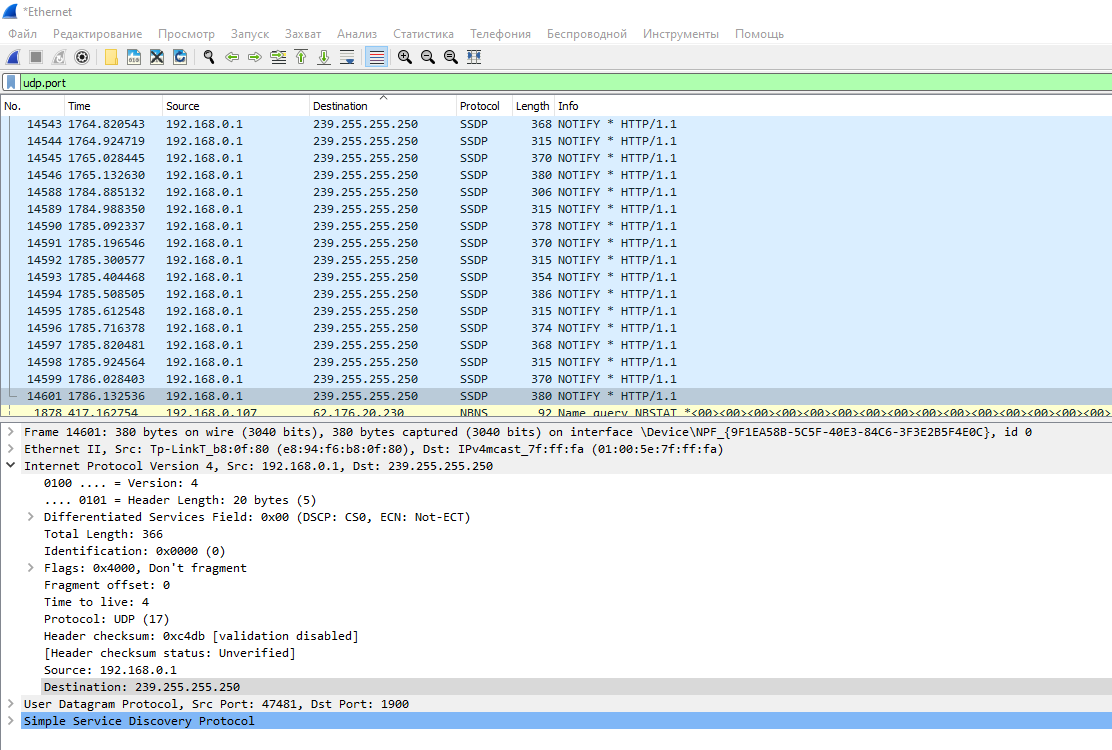
Фильтр по IP по адресу получателя

**ip.addr==**192.168.0.107



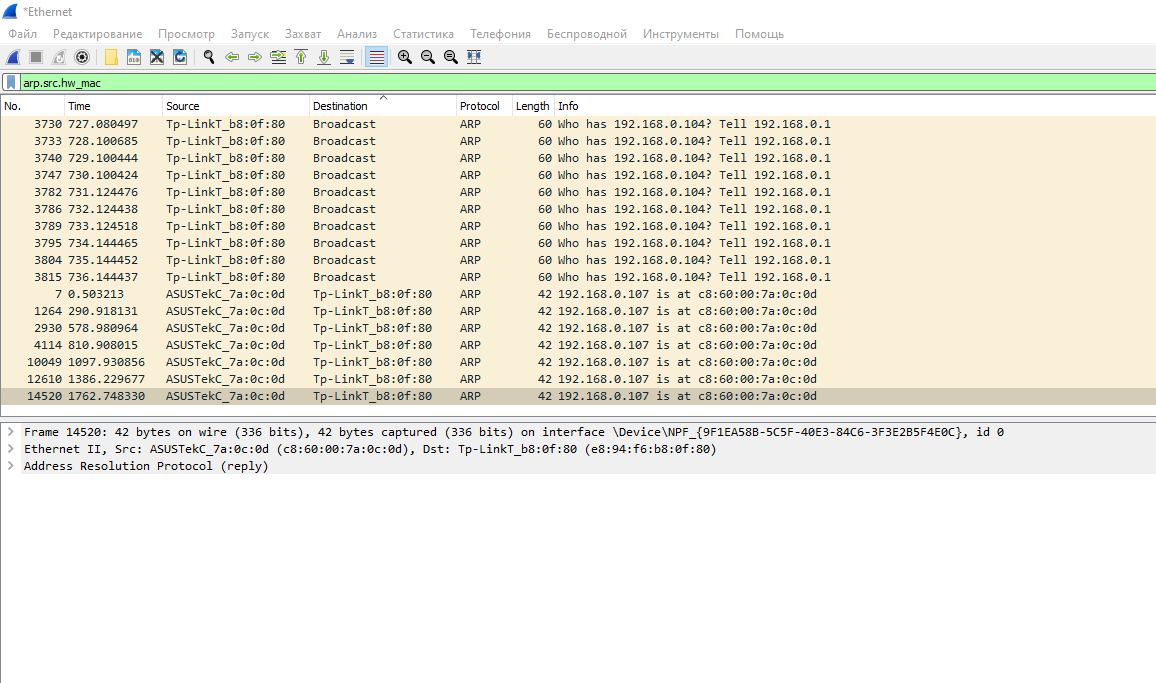
Фильтр по IP по адресу получателя и отправля

**udp.port**



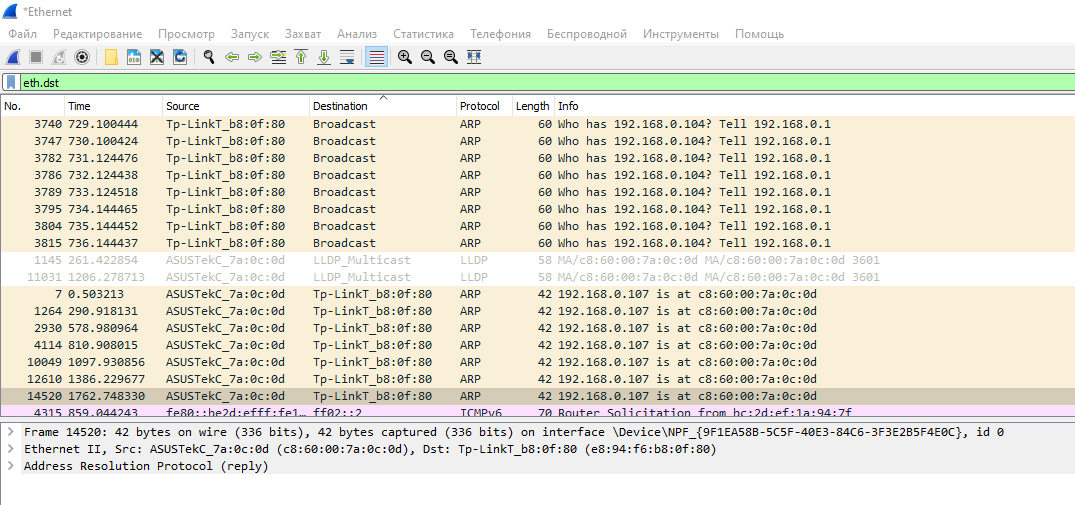
Показ захваченных пакетов, у которых Udp порт равен исходному значению

**arp.src.hw\_mac**



Протокол ARP-MAC – адреса отправителя

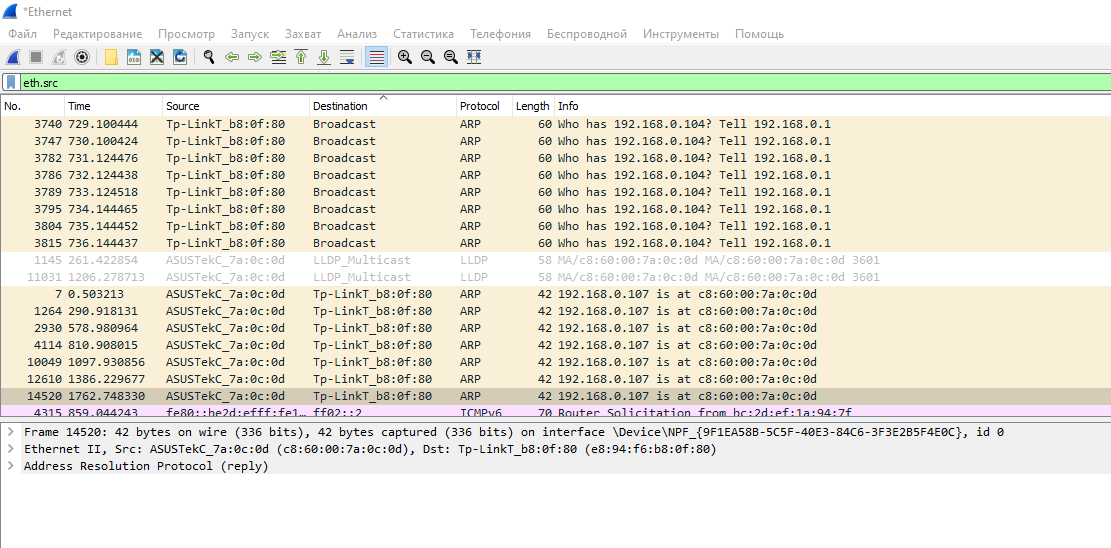
**eth.dst**



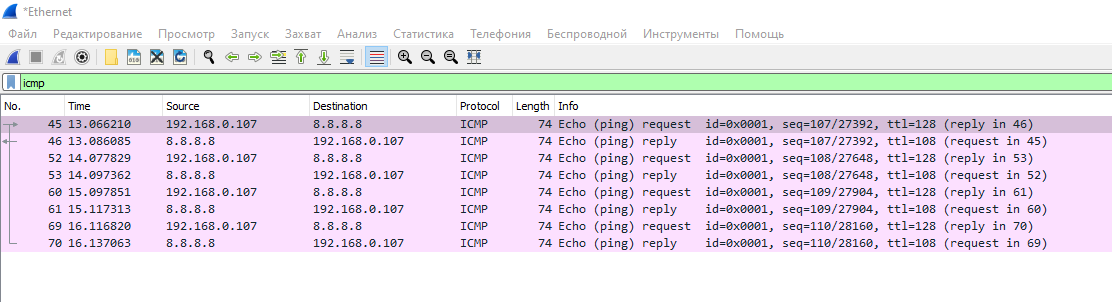
Показ MAC – адреса получателя

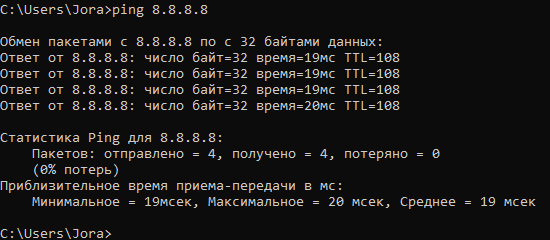
**eth.src**

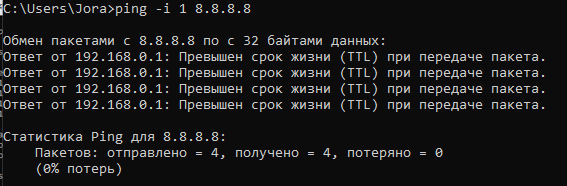
Показ MAC – адреса отправителя

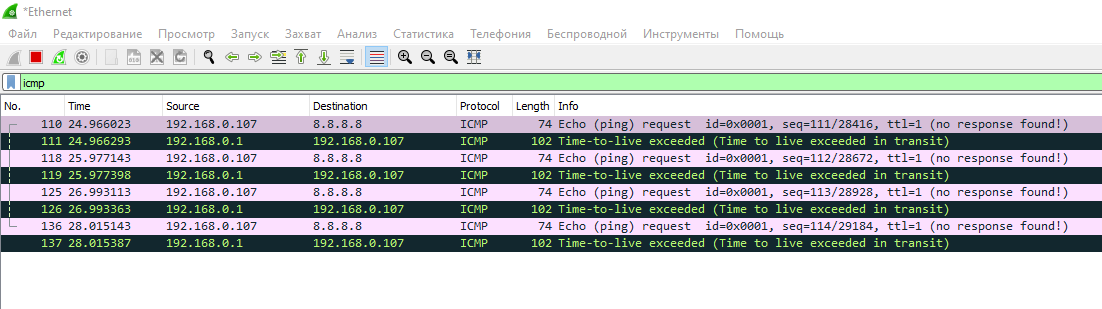


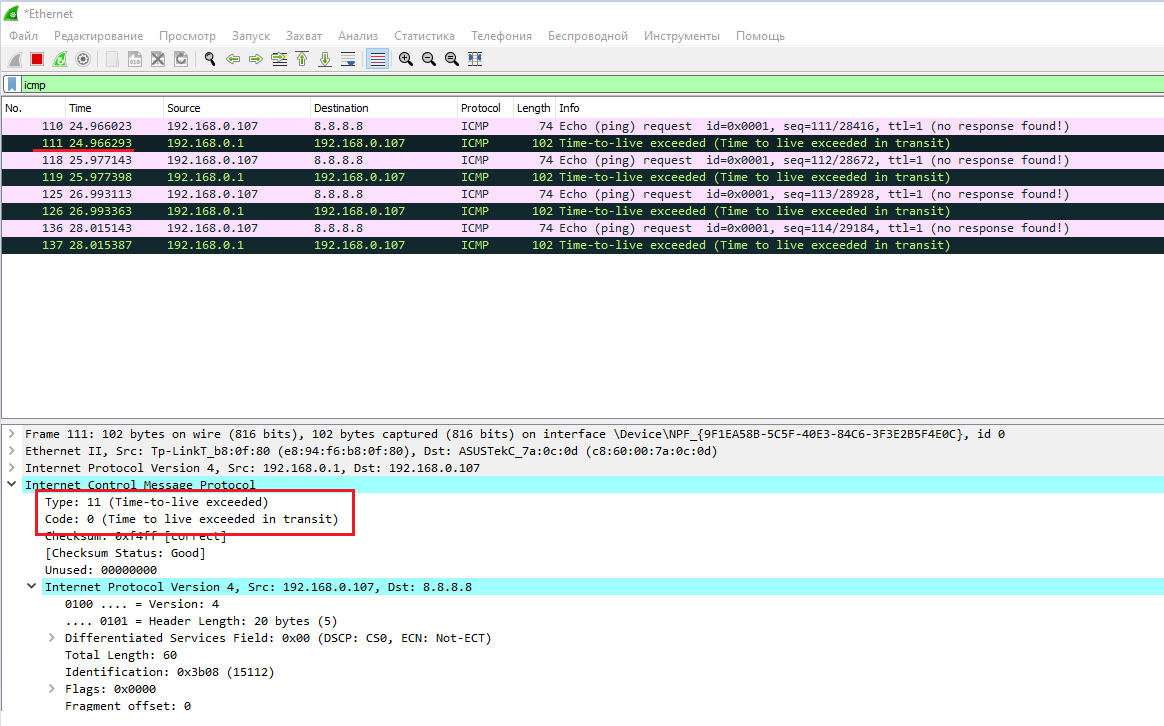
# ICMP











# ARP

