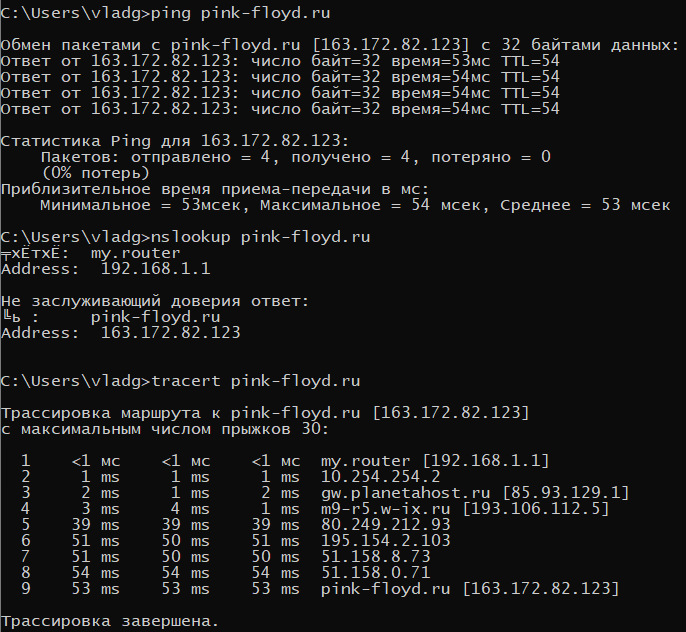
1. **Произвести обнаружение узлов в ГИС «Интернет» узлов, использующих протокол *http*. В *google.com* требуется ввести поисковый запрос и выбрать ресурс: *intitle:"forum"* *inurl:http after:2019*.**

В качестве сайта взял: <http://pink-floyd.ru>

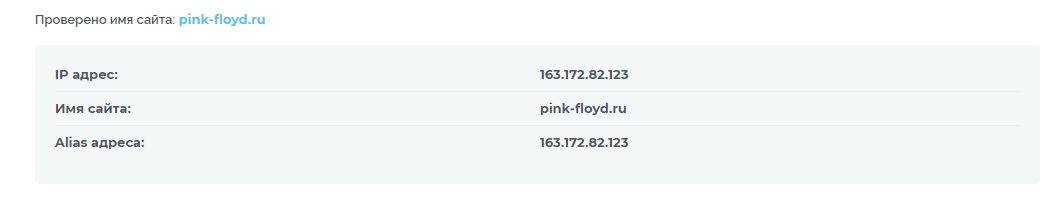
1. **Определить: ip адрес ресурса с использованием нескольких способов.**

Определил IP адрес ресурса с помощью следующих:

* Воспользовался в командной строке командами a) ***ping*** ; b) ***nslookup***; c) ***tracert***;

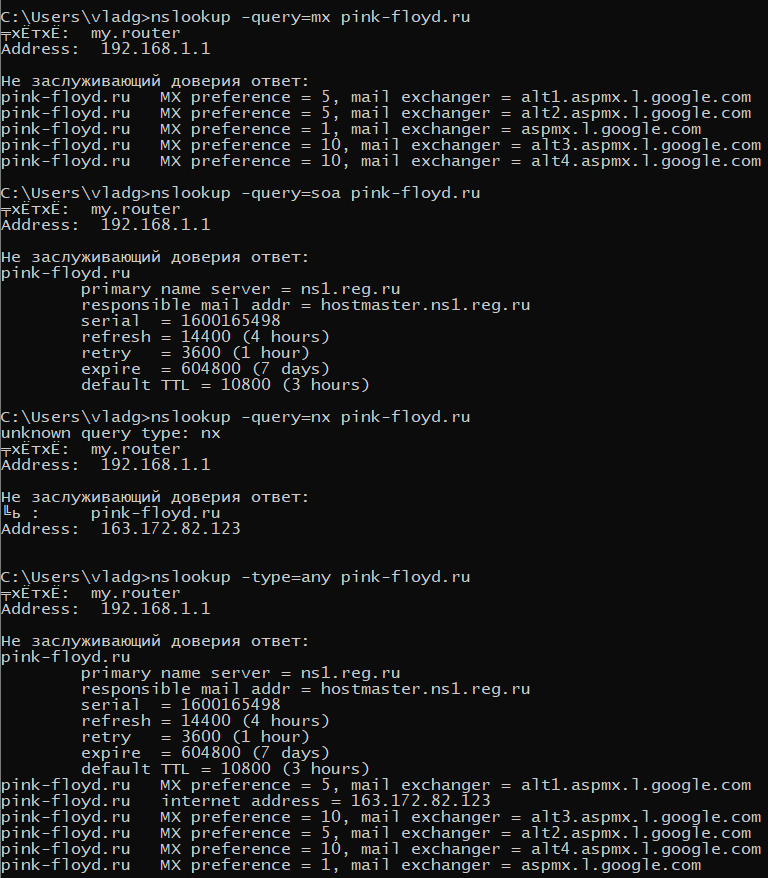


* Воспользовался сайтом ***2ip.ru***;

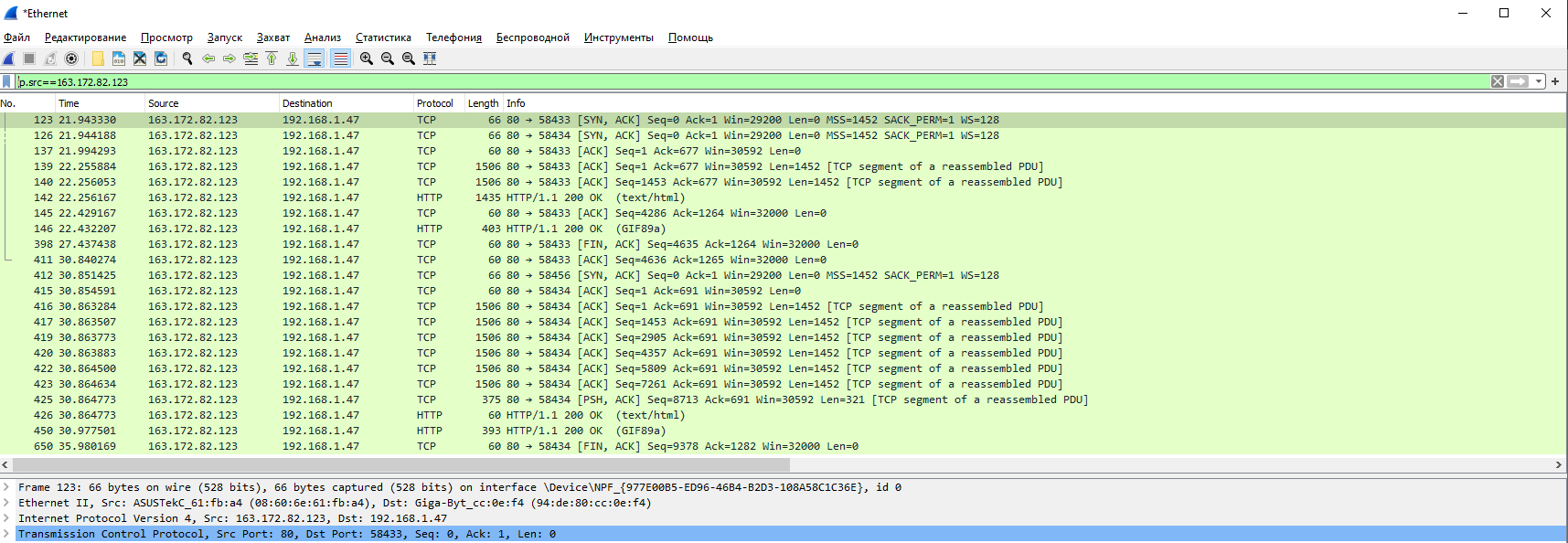


1. **Изучить аргументы утилиты *nslookup*: *-query=mx*, *soa*, *nx*; *type=any*.**

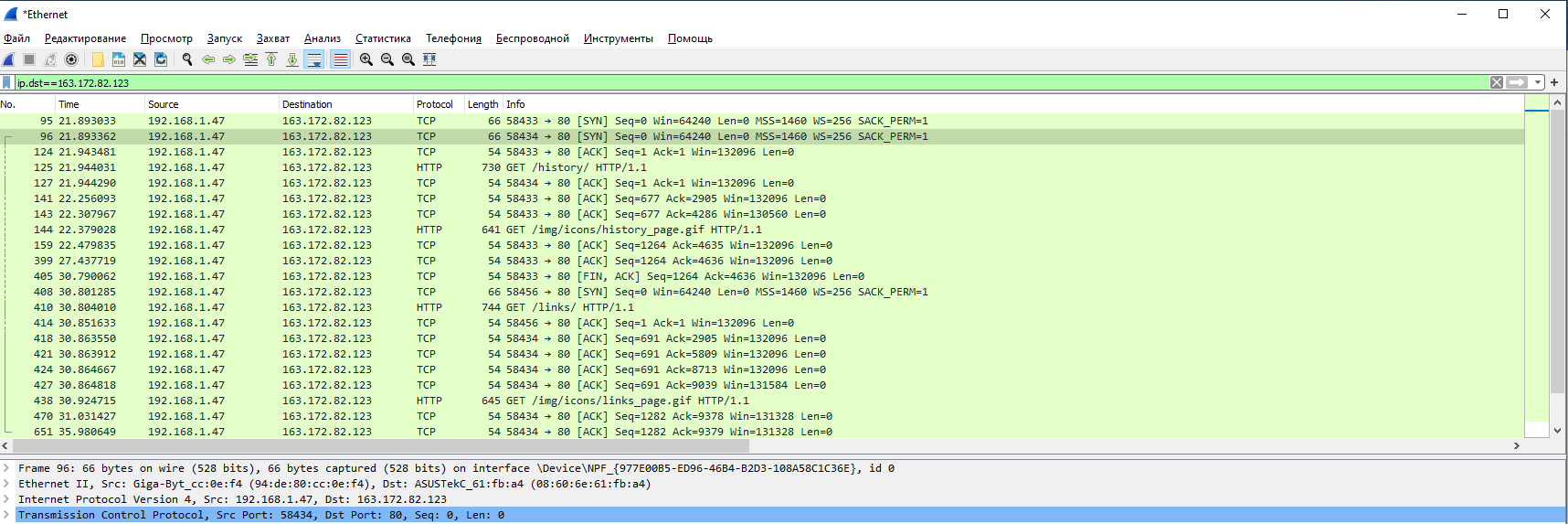
С помощью этих команд я узнал данные о сервере, домене и почте:



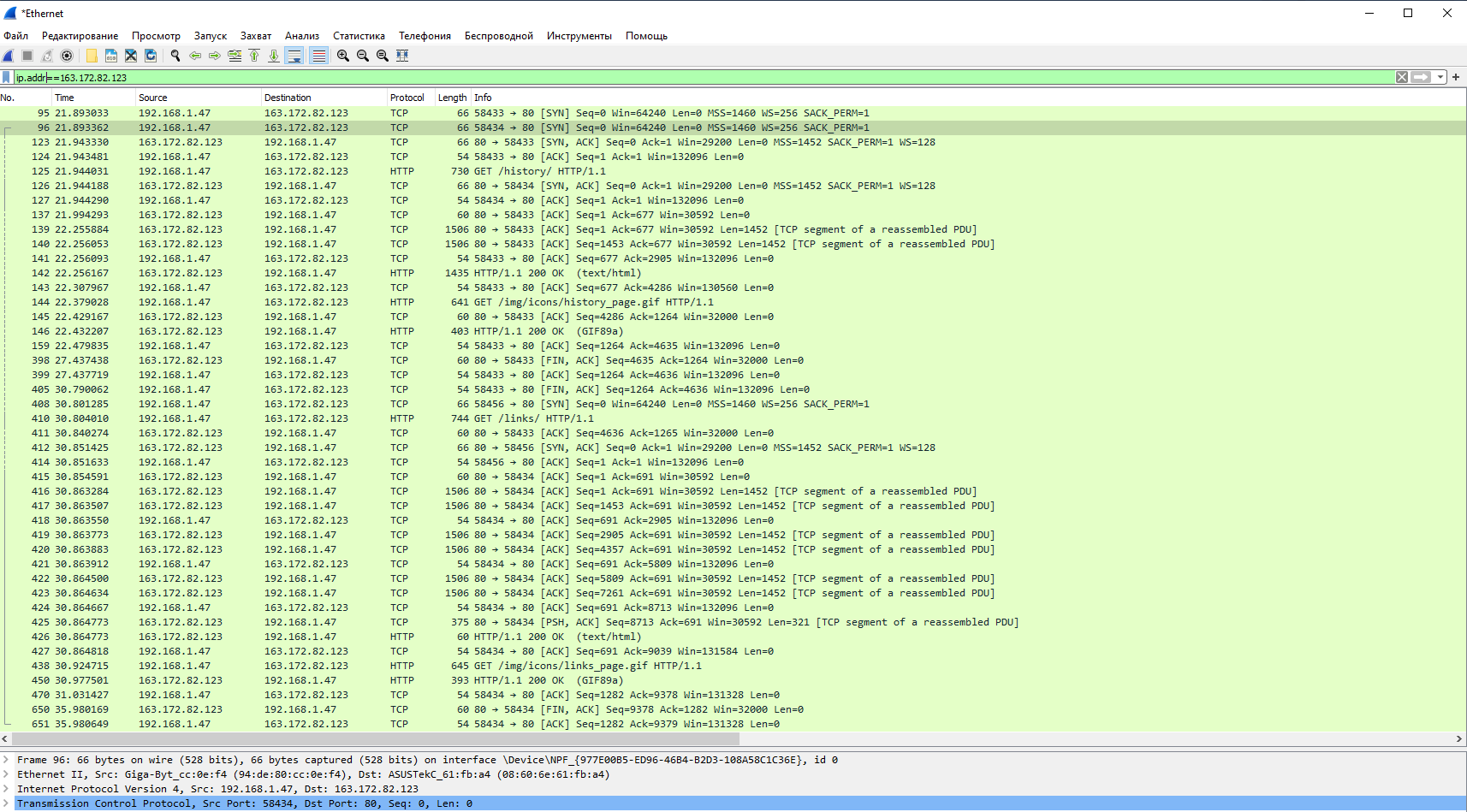
1. **Изучить трафик с сайта.**
2. **В wireshark изучить основные фильтры типа: *ip.src==192.168.0.163*; *ip.dst*; *ip.addr*, *udp.src*, *arp.src.hw\_mac*, *eth.dst*, *eth.src*.**
3. **ip.src==**"ip сайта". Данная команда осуществляет перехват трафика с сайта, который отравляет запрос на наш ip;



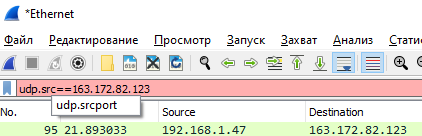
1. **ip.dst==**"ip сайта". Данная же команда осуществляет перехват трафика с нашего устройства к сайту;



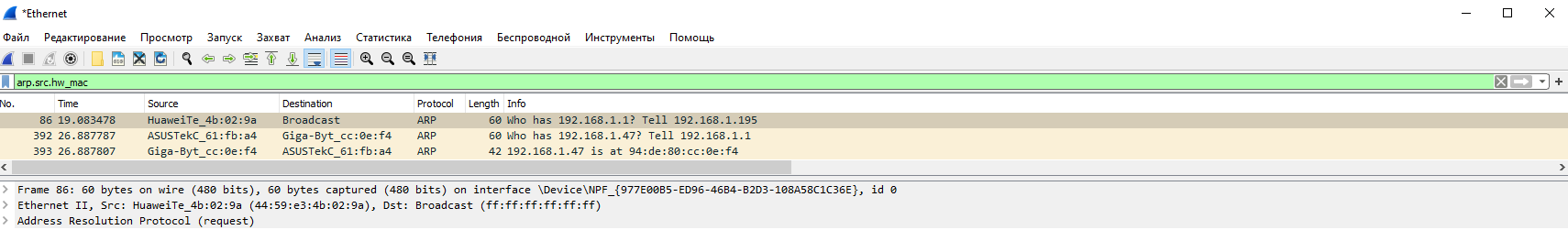
1. **ip.addr==**"ip сайта" комбинирует команды выше и показывает как трафик с сайта, так и с нашего устройства;



1. **udp.src**. Лично у меня команда не отображается, возможно имелась в виду команда **upd.srcport**, она показывает UDP отправителя;



1. **arp.src.hw\_mac** является фильтром по протоколу **arp**, показывает нам **MAC** адрес получателя;



1. **eth.src/dst** фильтрует пакету по подуровню **MAC**.