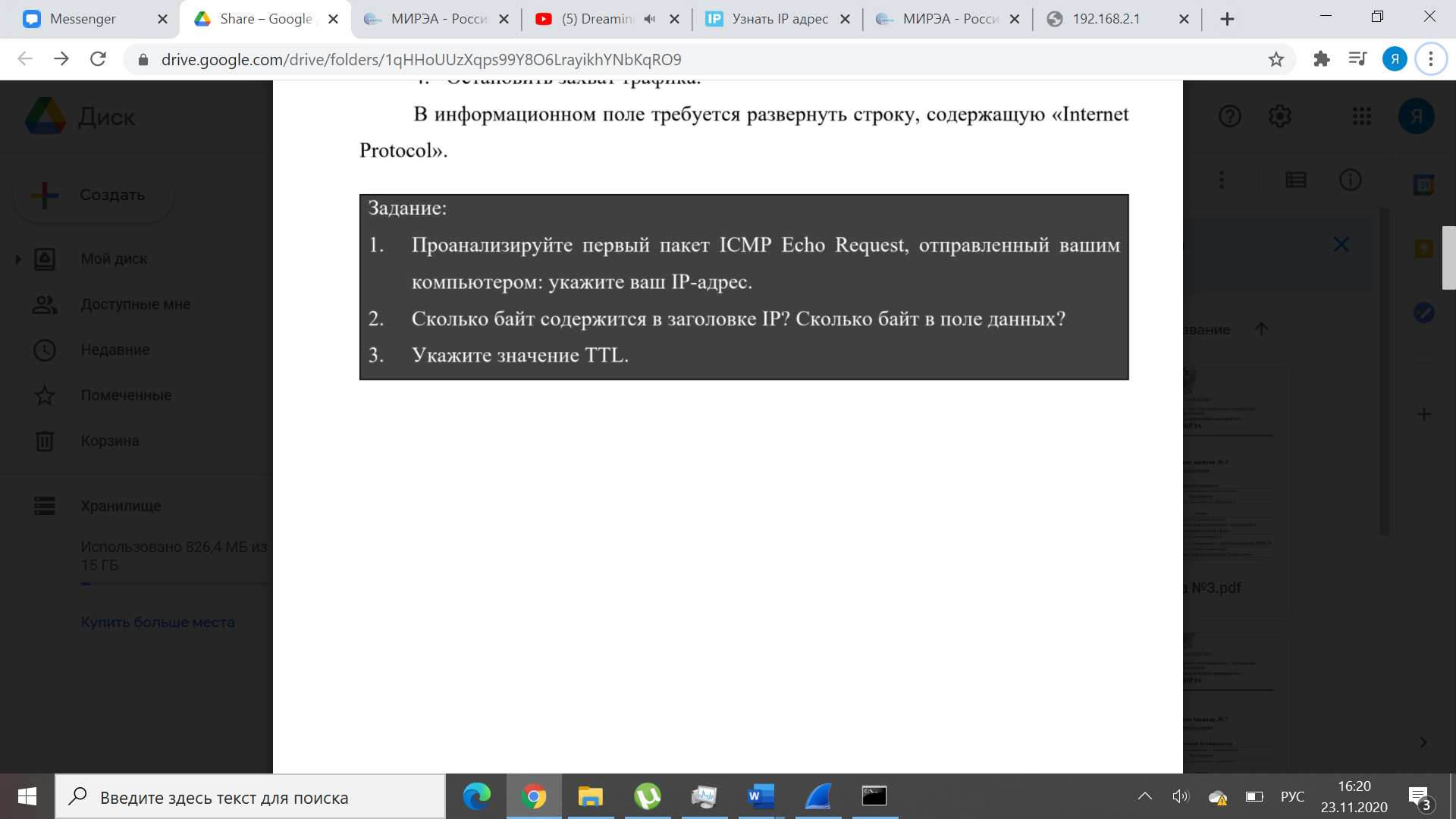
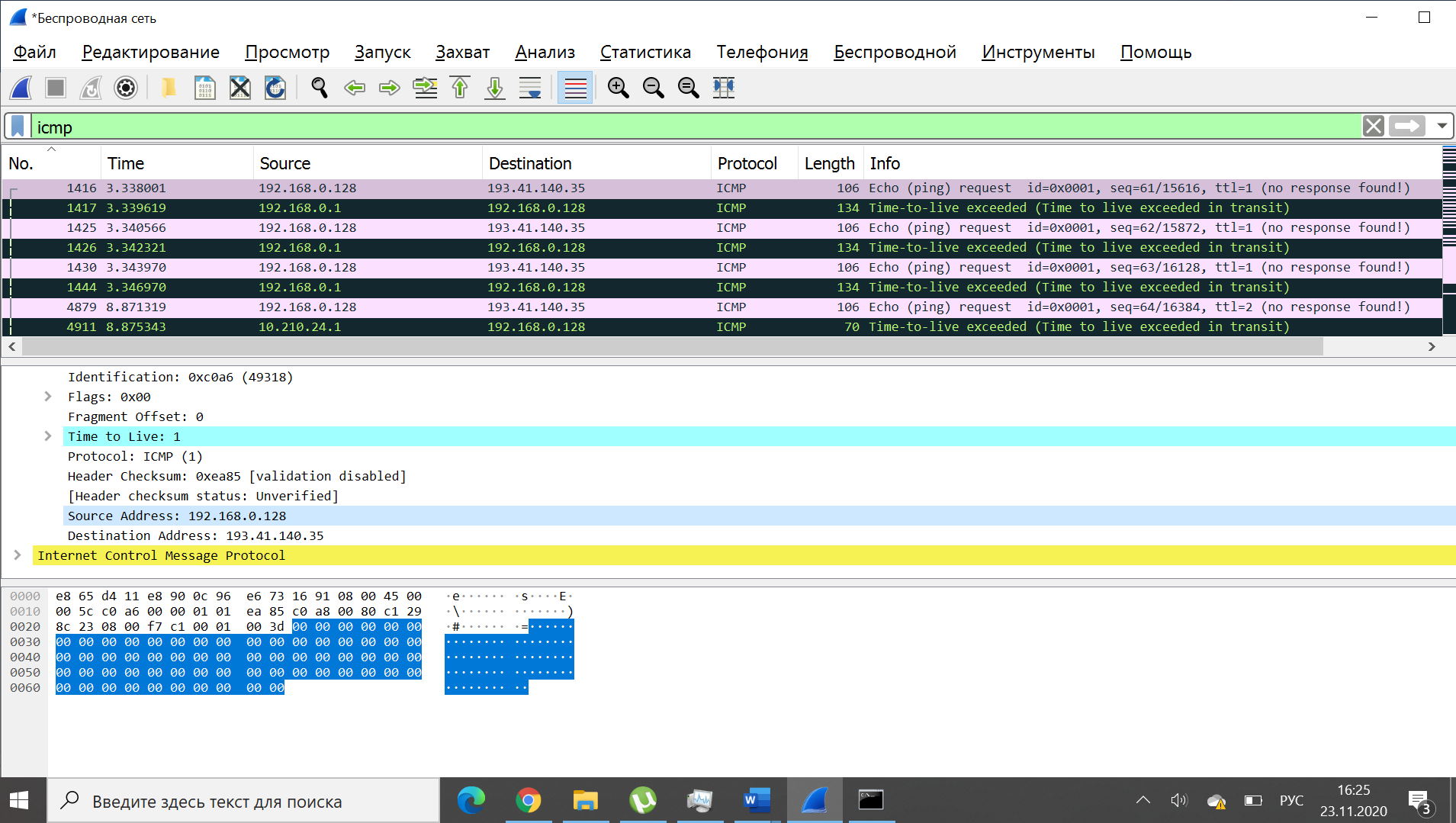
|  |
| --- |
| Описание: Описание: для прик эмбл |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего профессионального образования"Российский технологический университет"МИРЭА |
| Институт «Комплексной безопасности и специального приборостроения» |
| Кафедра «Управление и моделирование систем» (КБ-3) |
|  |

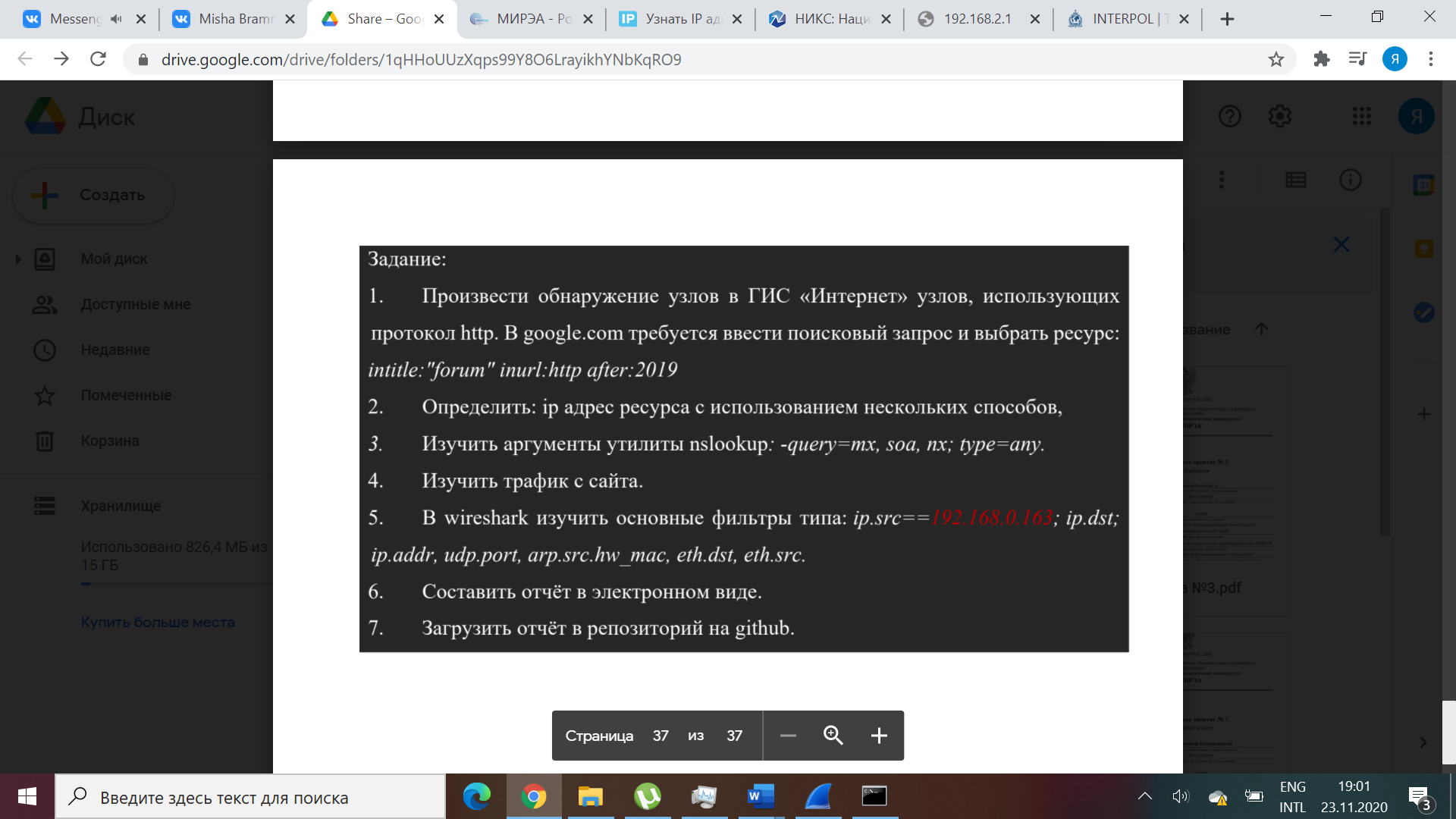
|  |  |
| --- | --- |
| **Практика №2 по дисциплине** | |
|  | |
| **« Основы информационной безопасности »**  **«АНАЛИЗ СТРУКТУРЫ СЕТЕВОГО ТРАФИКА**  **С ПОМОЩЬЮ ПРОГРАММЫ WIRESHARK»** | |
|  | |
| Выполнил студент группы БИСО-03-19 | **Коннов Я.В.** |

Москва 2020

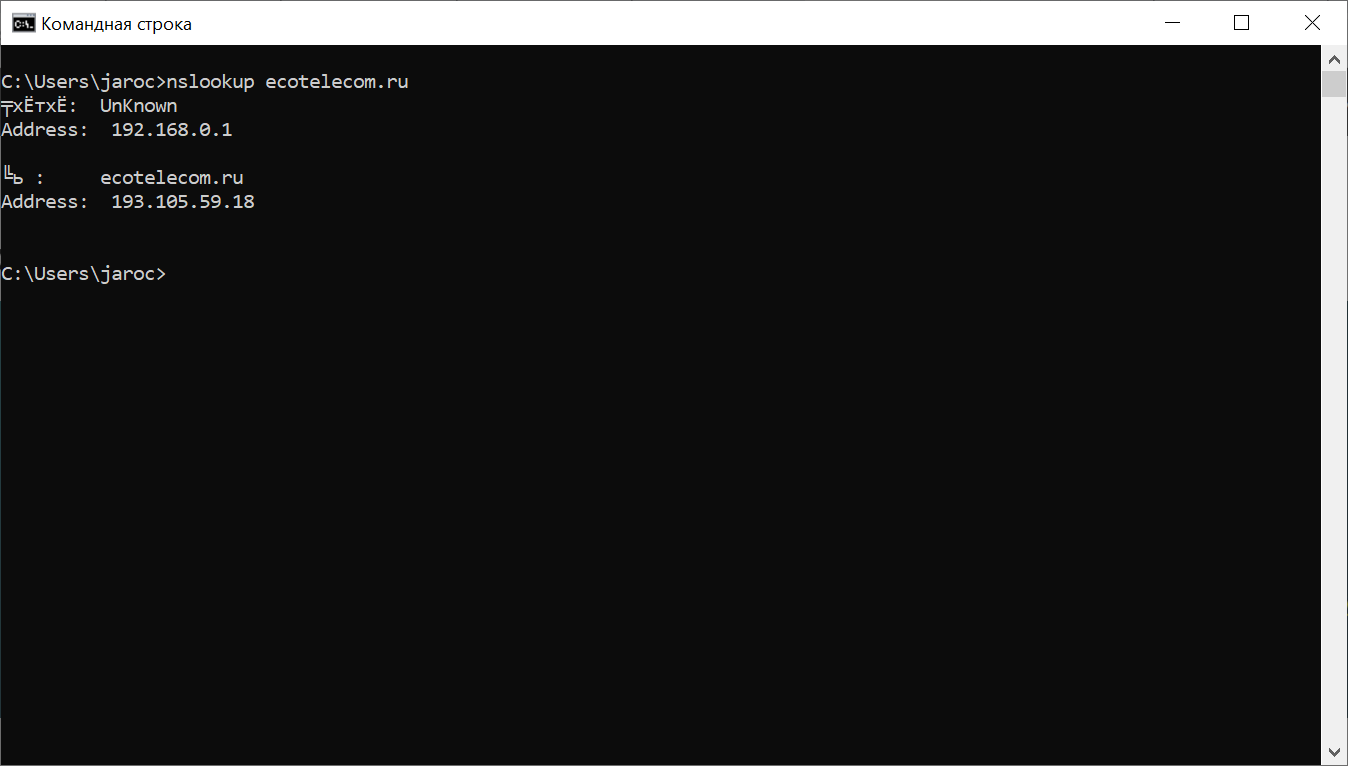


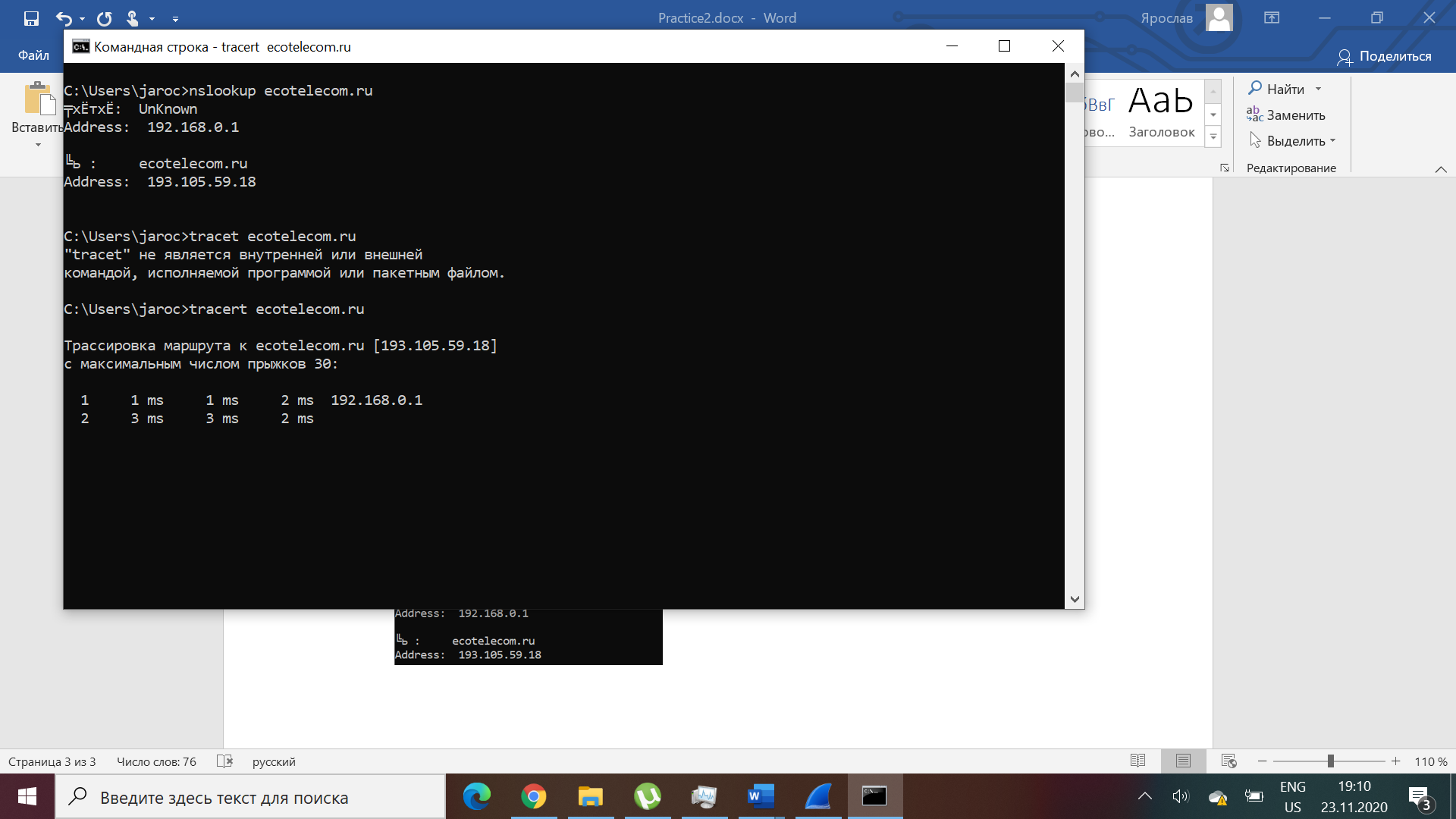


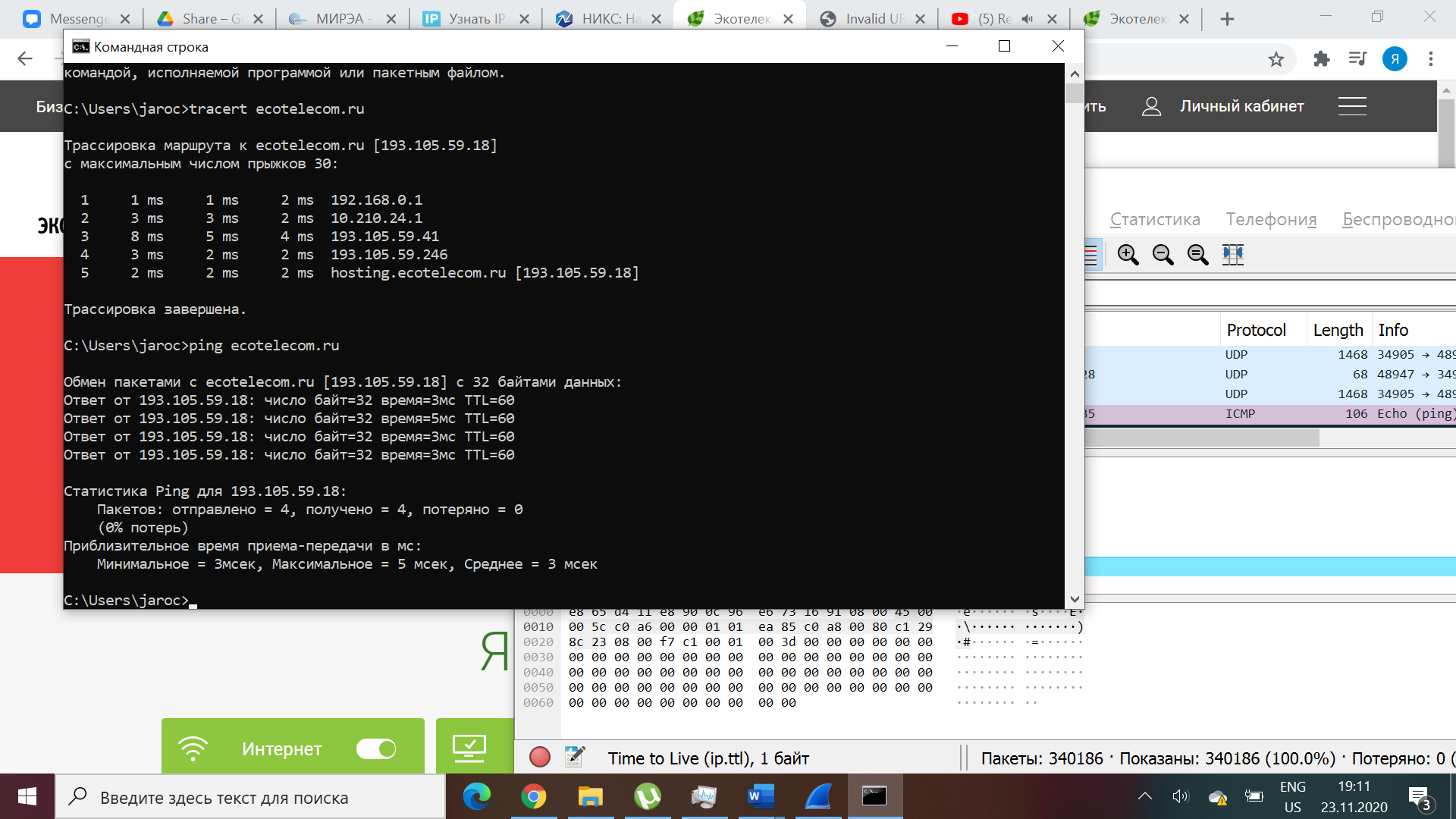
1. 192.168.01.128
2. .... 0101 = Header Length: 20 bytes (5), Data (64 bytes)
3. Time to Live: 1



2. Будем определять ip адрес <https://www.ecotelecom.ru/>

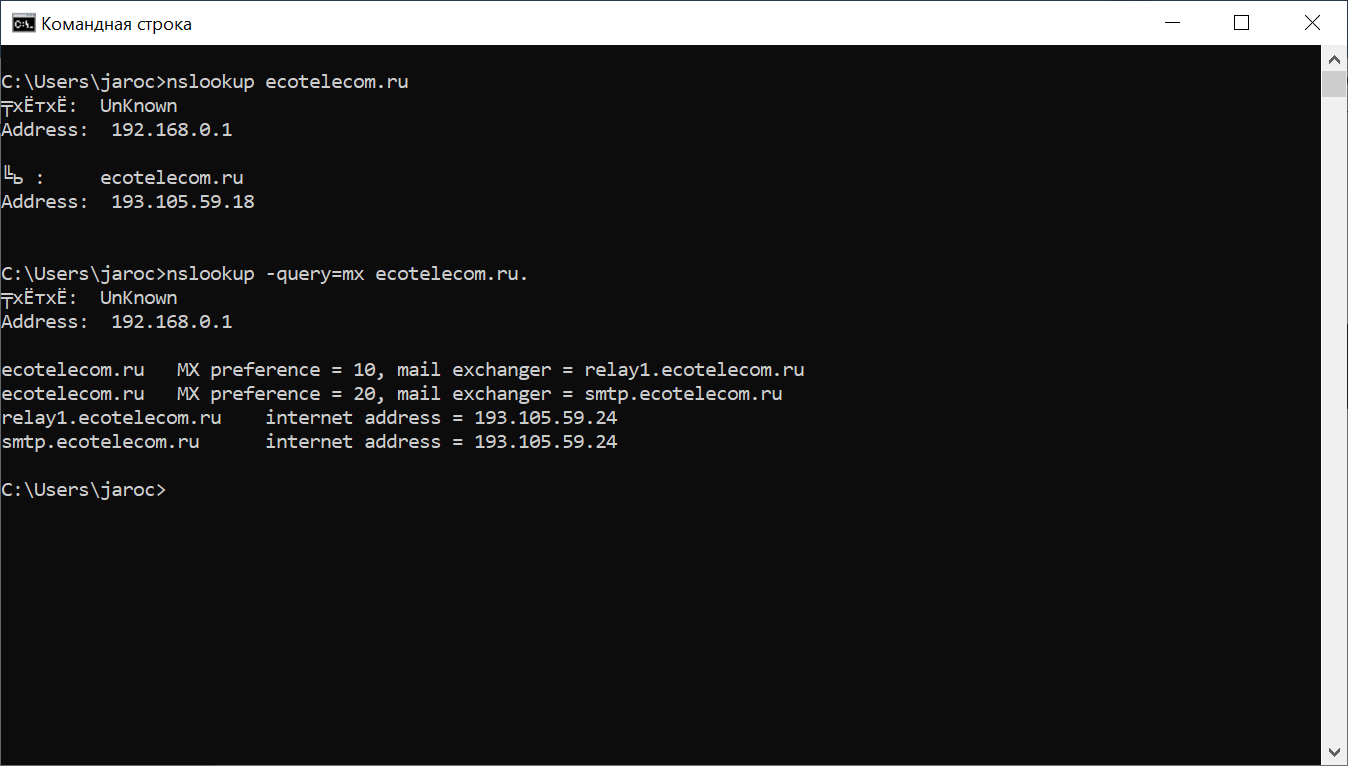






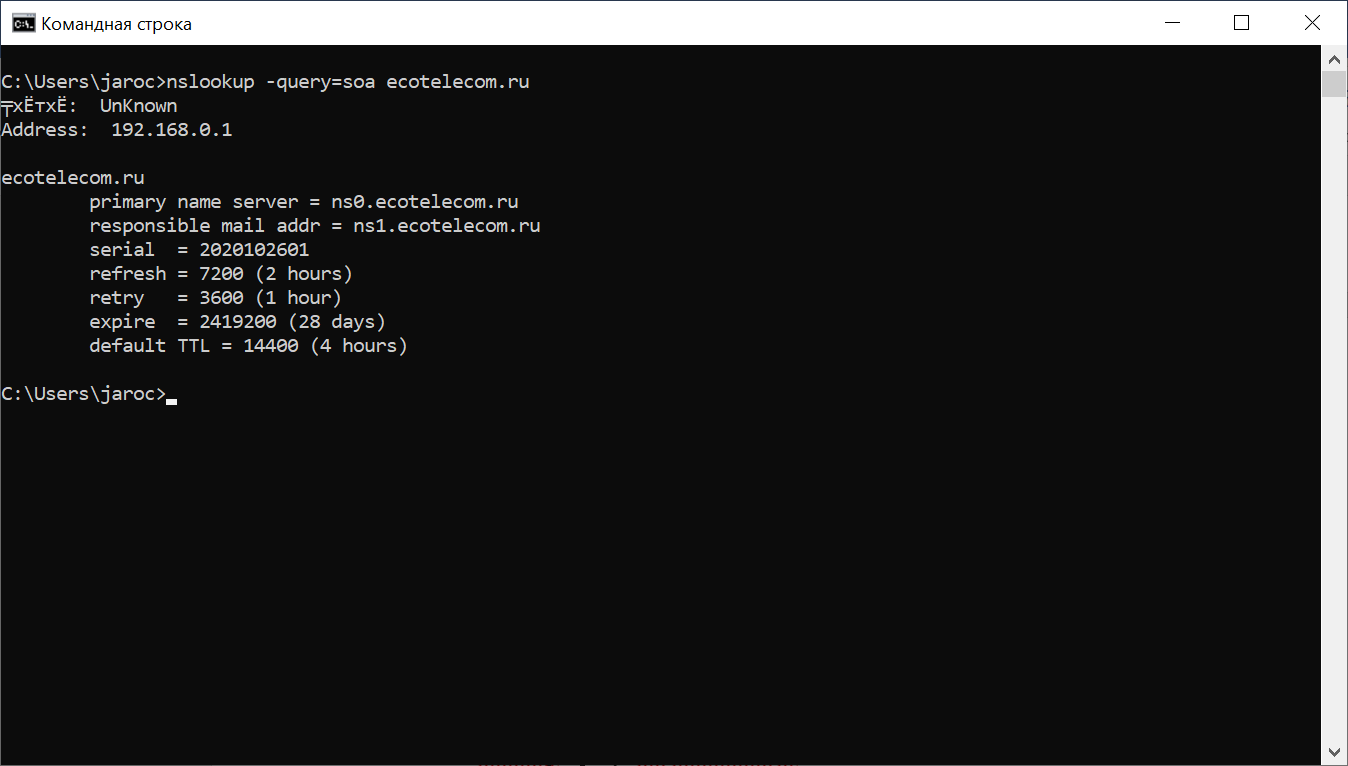
1. nslookup –query=mx ecotelecom.ru

Сервер ответит с перечислением почтовых серверов, обслуживающих домен ecotelecom.ru



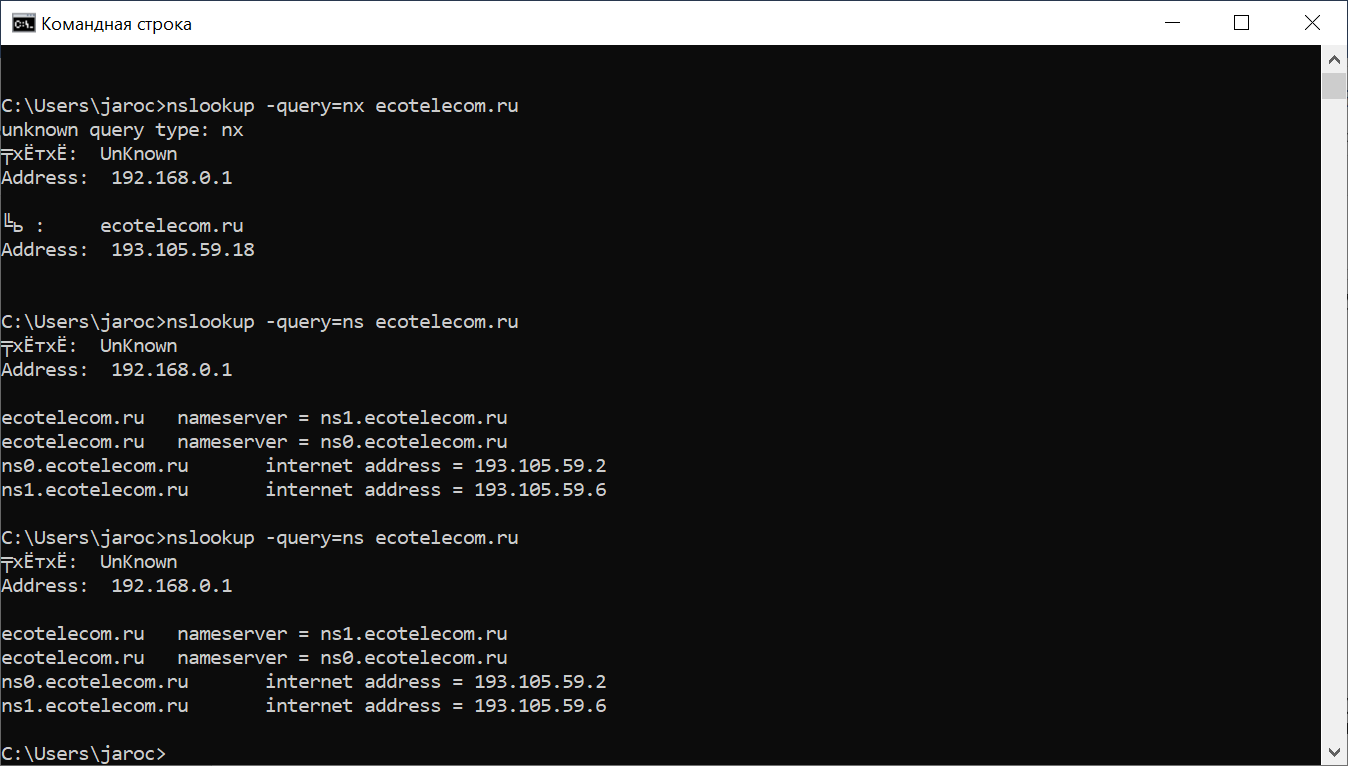
nslookup –query=soa ecotelecom.ru

SOA-запись (Start of Authority) — начальная запись зоны, которая указывает местоположение эталонной записи о домене. Она содержит в себе контактную информацию лица, ответственного за данную зону, время кэширования информации на серверах и данные о взаимодействии DNS.



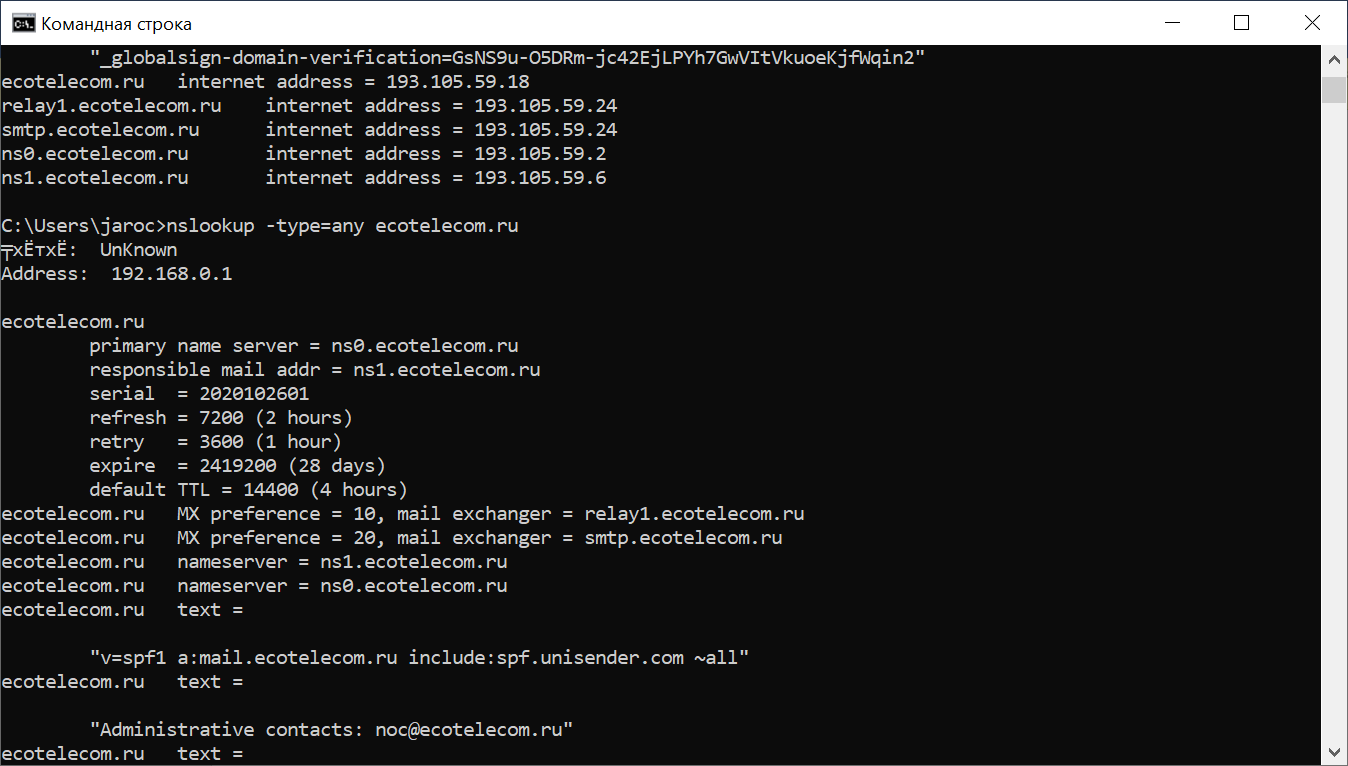
nslookup –query=nx ecotelecom.ru

Когда вы набираете в адресной строке браузера адрес сайта, то компьютер обращается к DNS серверу, указанному в настройках сетевого интерфейса. А тот в свою очередь к более NS серверам, где хранятся записи о том, какой IP-адрес соответствует данному доменному имени. Утилита nslookup позволяет определять, какие NS –сервера использует тот или иной хост (сайт).

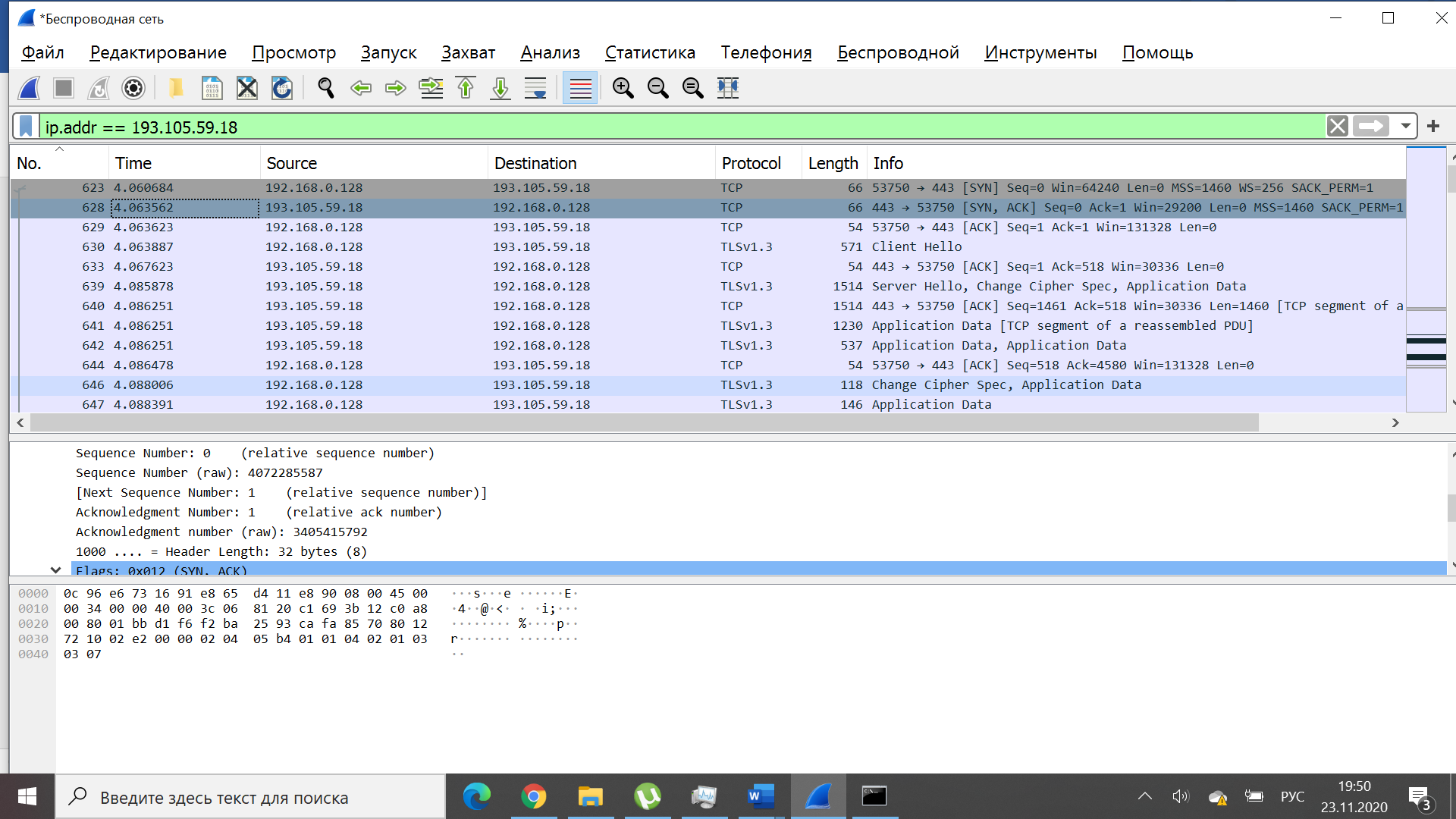


nslookup -type=any ecotelecom.ru

Утилита вернёт все возможные записи для указанного хоста



1. Для просмотра трафика с сайта поставим фильтр в Wireshark: ip.addr == 193.105.59.18



Получим от сайта пакеты TCP и TLSv1.3.  
Из этого следует, что сайт работает по расширенному протоколу HTTP - **HTTPS**, который шифрует информацию при передаче.

5. Фильтры типа ip.src, ip.dst, ip.addr отфильтруют по адресу отправителя, адресу получателя, либо по адресу отправителя или получателя соответственно.

Udp.port отфильтрует по UDP порту получателя или отправителя.

arp.src.hw\_mac отфильтрует по протоколу ARP – MAC адрес отправителя

eth.dst, eth.src отфильтрует по MAC-адресу получателя и отправителя соответственно

Источники:

<https://networkguru.ru/wireshark-filtr-po-ip-portu-protokolu-mac/>

https://ab57.ru/cmdlist/nslookup.html