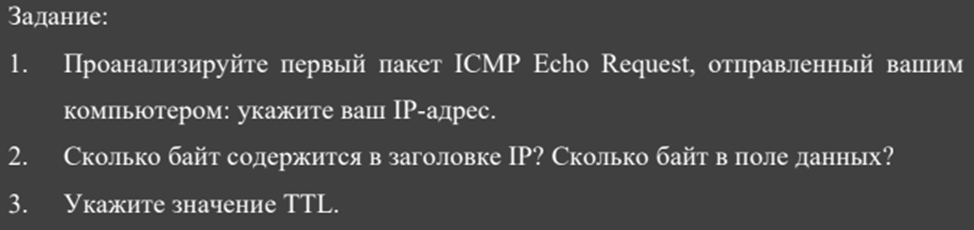
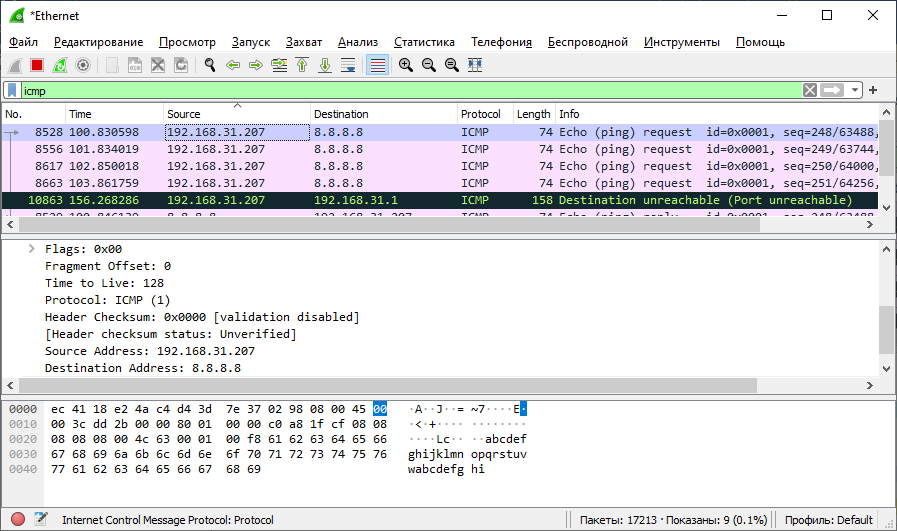
|  |
| --- |
| Описание: Описание: для прик эмбл |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего профессионального образования  **"Российский технологический университет"**  **МИРЭА** |
| Институт «Комплексной безопасности и специального приборостроения»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

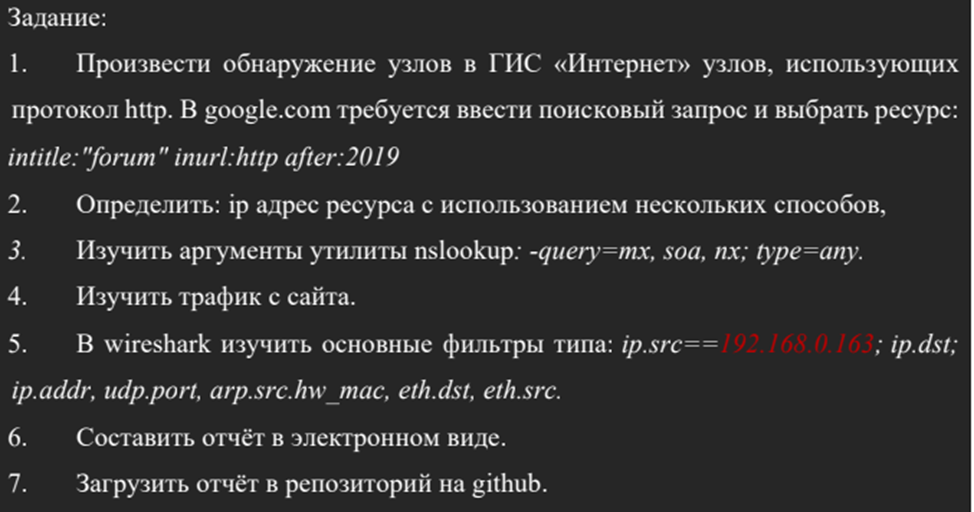
|  |  |
| --- | --- |
| **Практика №2 по дисциплине** | |
|  | |
| **« Основы информационной безопасности »**  **«АНАЛИЗ СТРУКТУРЫ СЕТЕВОГО ТРАФИКА**  **С ПОМОЩЬЮ ПРОГРАММЫ WIRESHARK»** | |
|  | |
| Выполнил студент группы БИСО-03-19 | *Чанышев А.Т.* |

Москва 2020

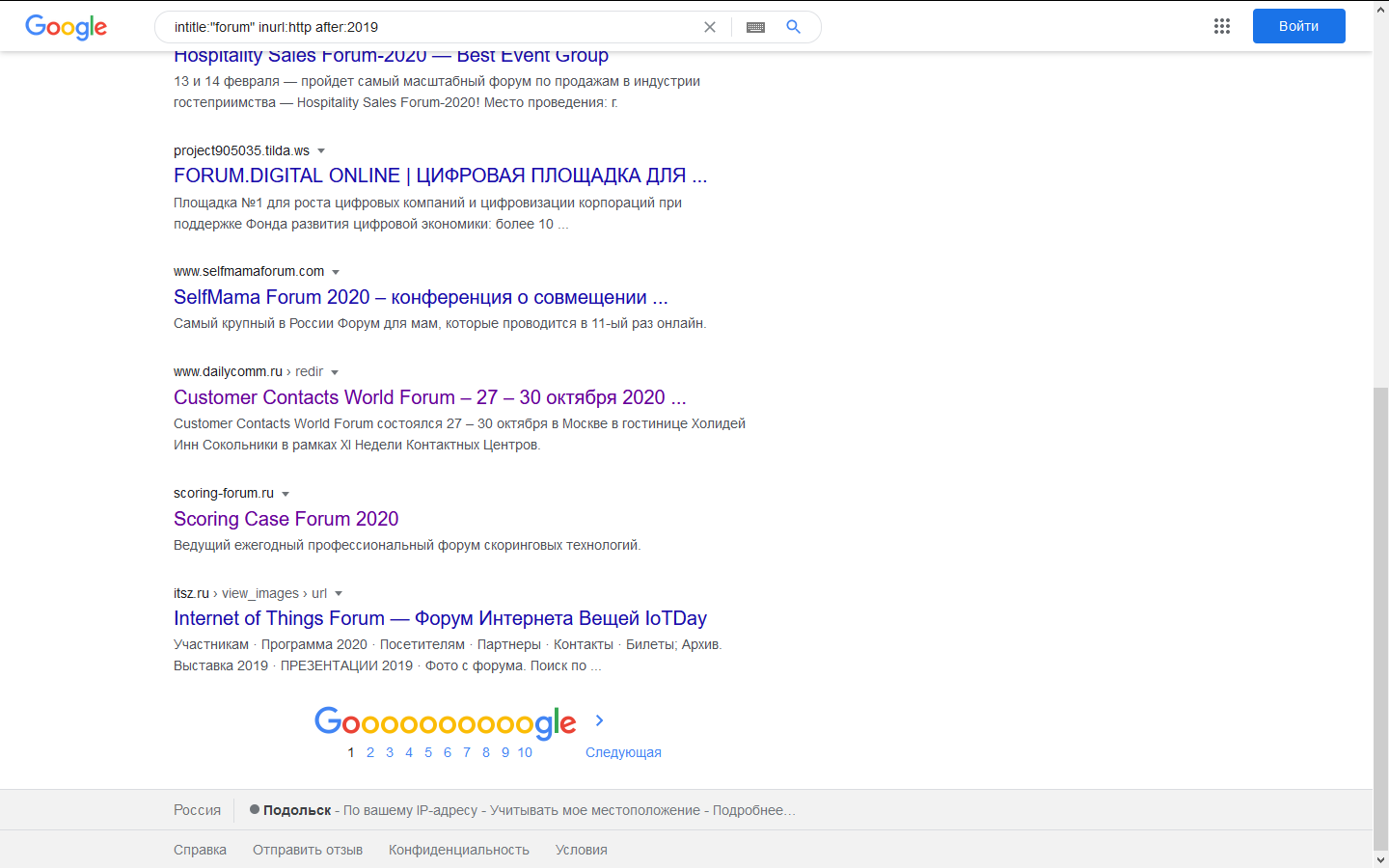
****

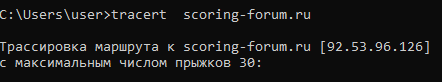


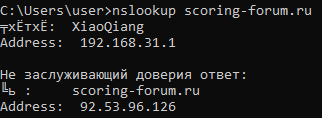
1. 192.168.31.207
2. .... 0101 = Header Length: 20 bytes (5), Data (64 bytes)
3. Time to Live: 128

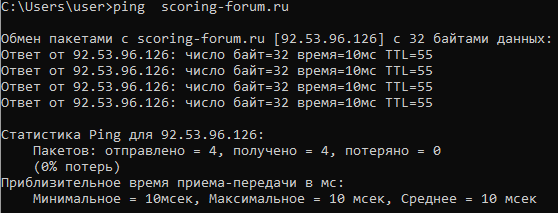
****

1. Мною был выбран сайт http://scoring-forum.ru/



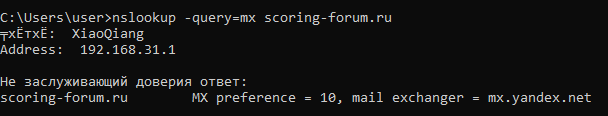
2.



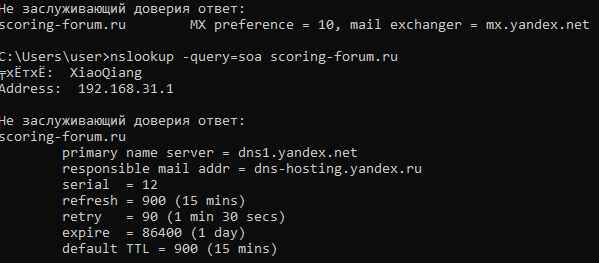


3. nslookup –query=mx scoring-forum.ru

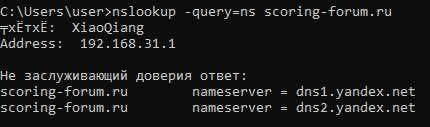
Сервер ответит с перечислением почтовых серверов, обслуживающих домен scoring-forum.ru



nslookup –query=soa scoring-forum.ru

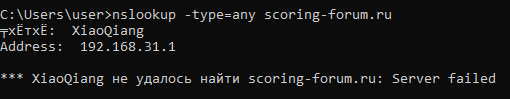


nslookup –query=ns scoring-forum.ru

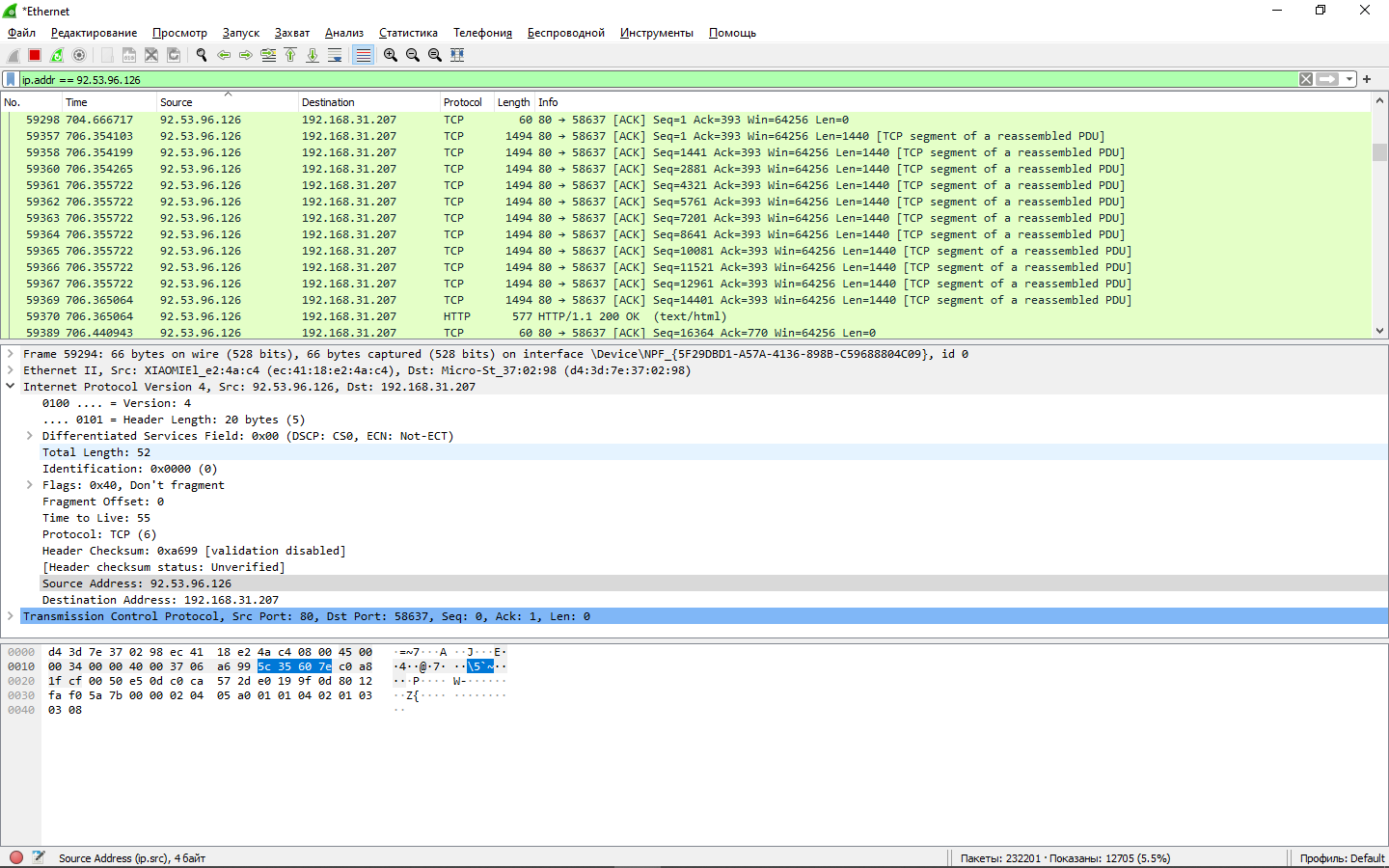


nslookup -type=any scoring-forum.ru

Утилита вернёт все возможные записи для указанного хоста



4.Для просмотра трафика с сайта поставим фильтр в Wireshark: ip.addr == 92.53.96.126



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.