|  |  |
| --- | --- |
|  | |
| 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-2) | |

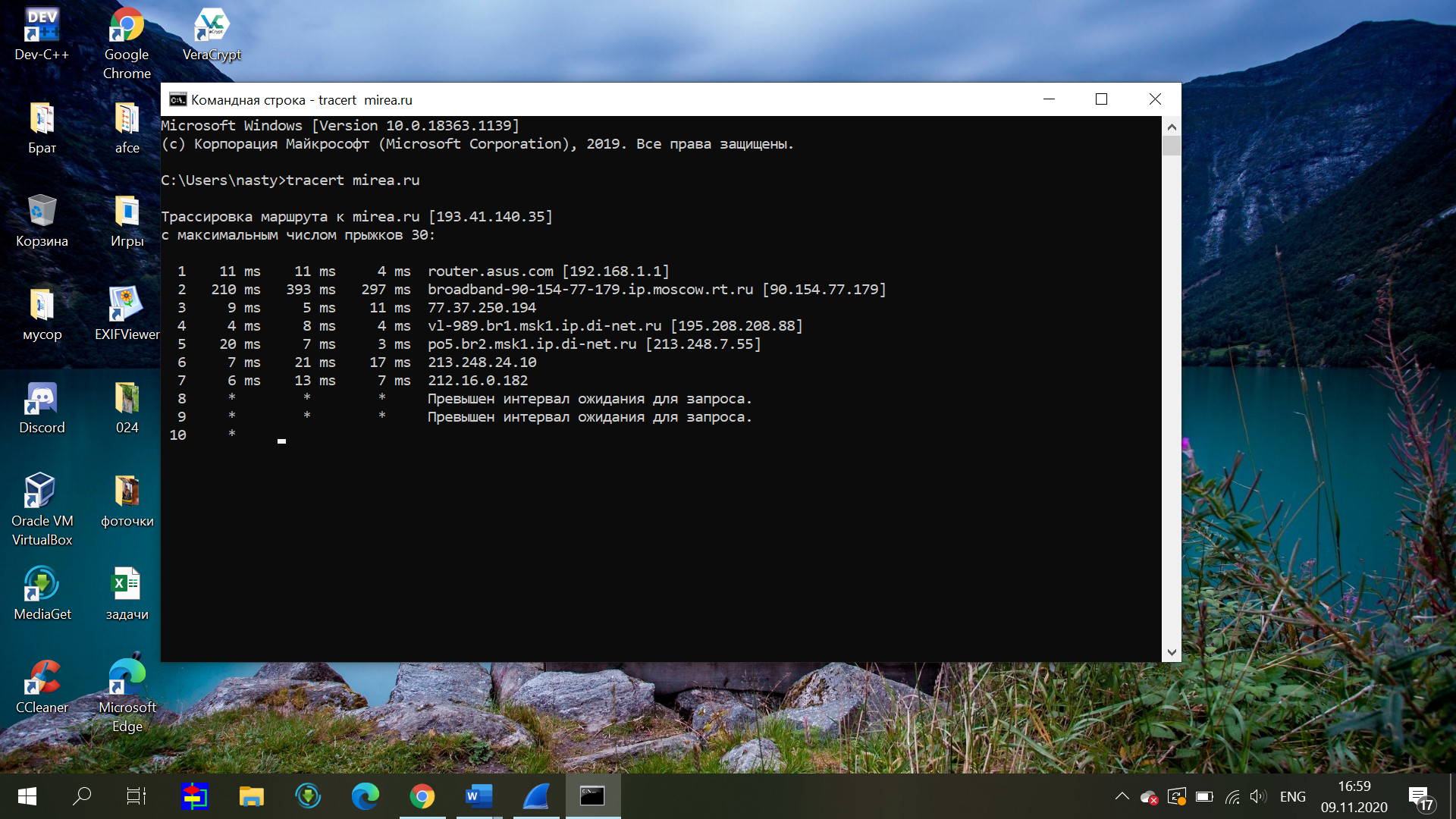
|  |  |
| --- | --- |
| **ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ** | |
| **по дисциплине** | |
| **«Основы информационной безопасности»** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Доронина Анастасия Алексеевна |
|  |  |

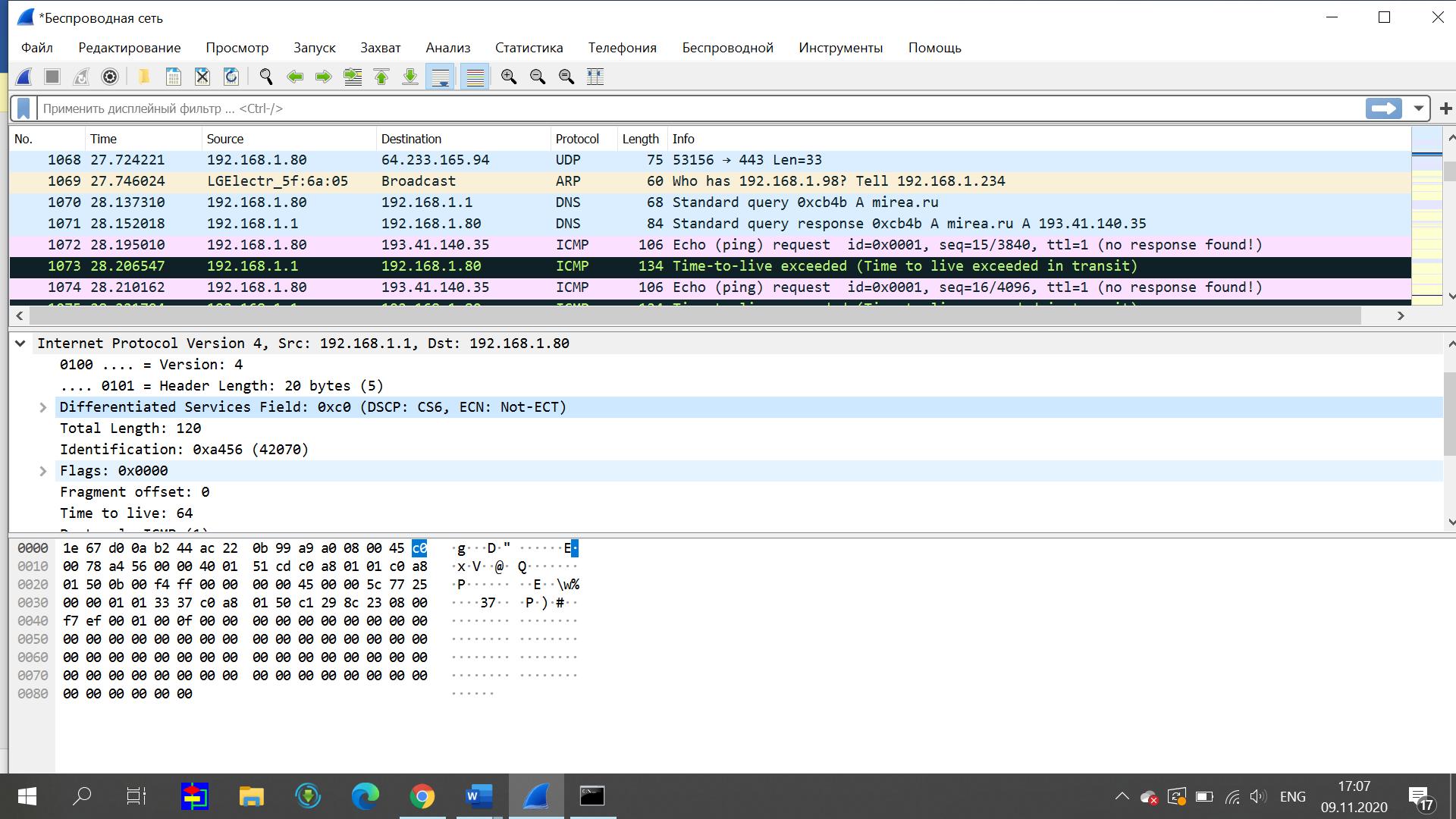
|  |  |  |
| --- | --- | --- |
| Лабораторные работы выполнены | «\_\_»\_\_\_\_\_\_\_2020г. |  |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_2020г. |  |

Москва 2020

**Практическая работа №2**

## 1.WireShark



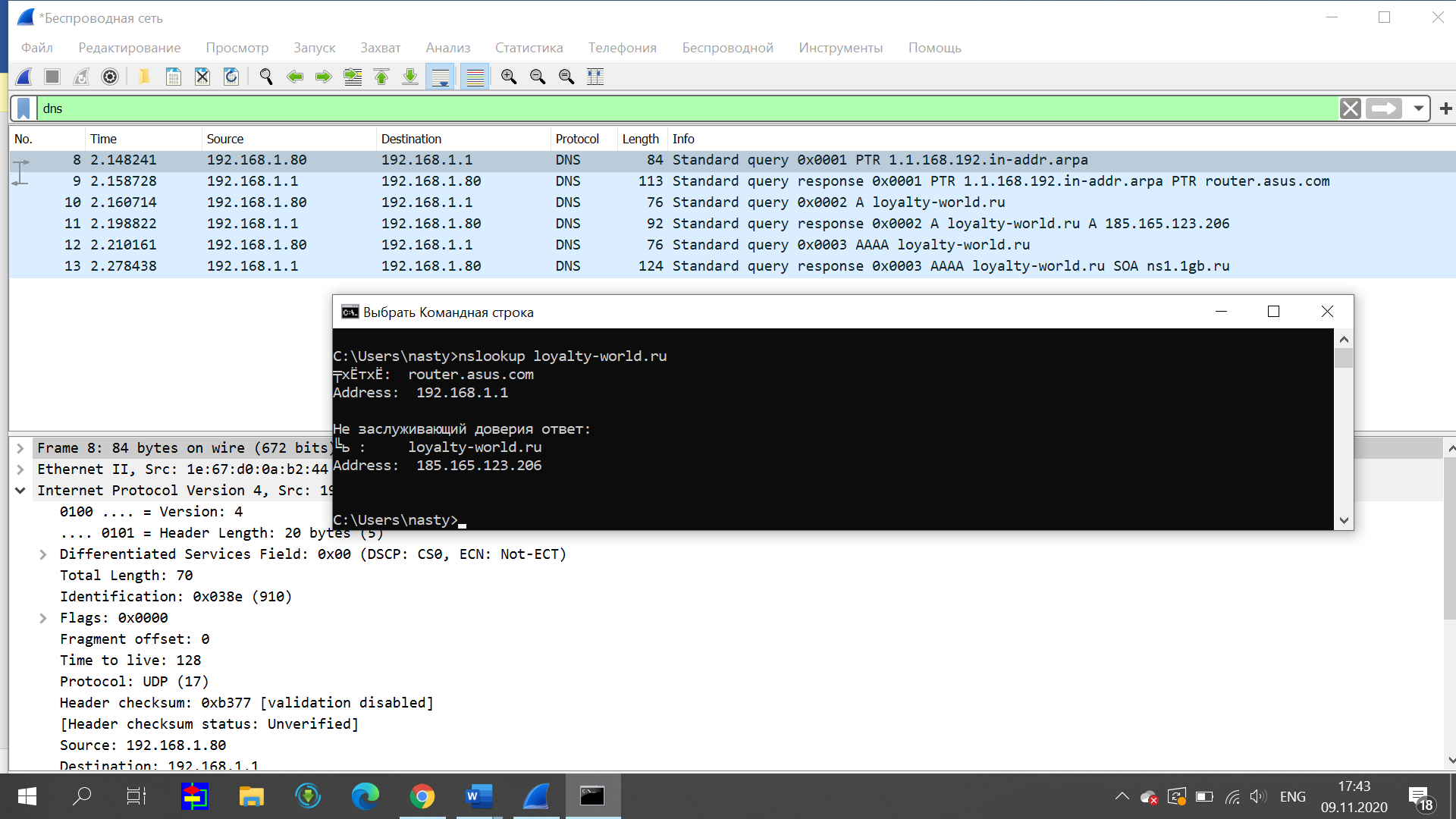


1. В заголовке 5 байт
2. Мой IP: 192.168.1.1
3. TTL: 64

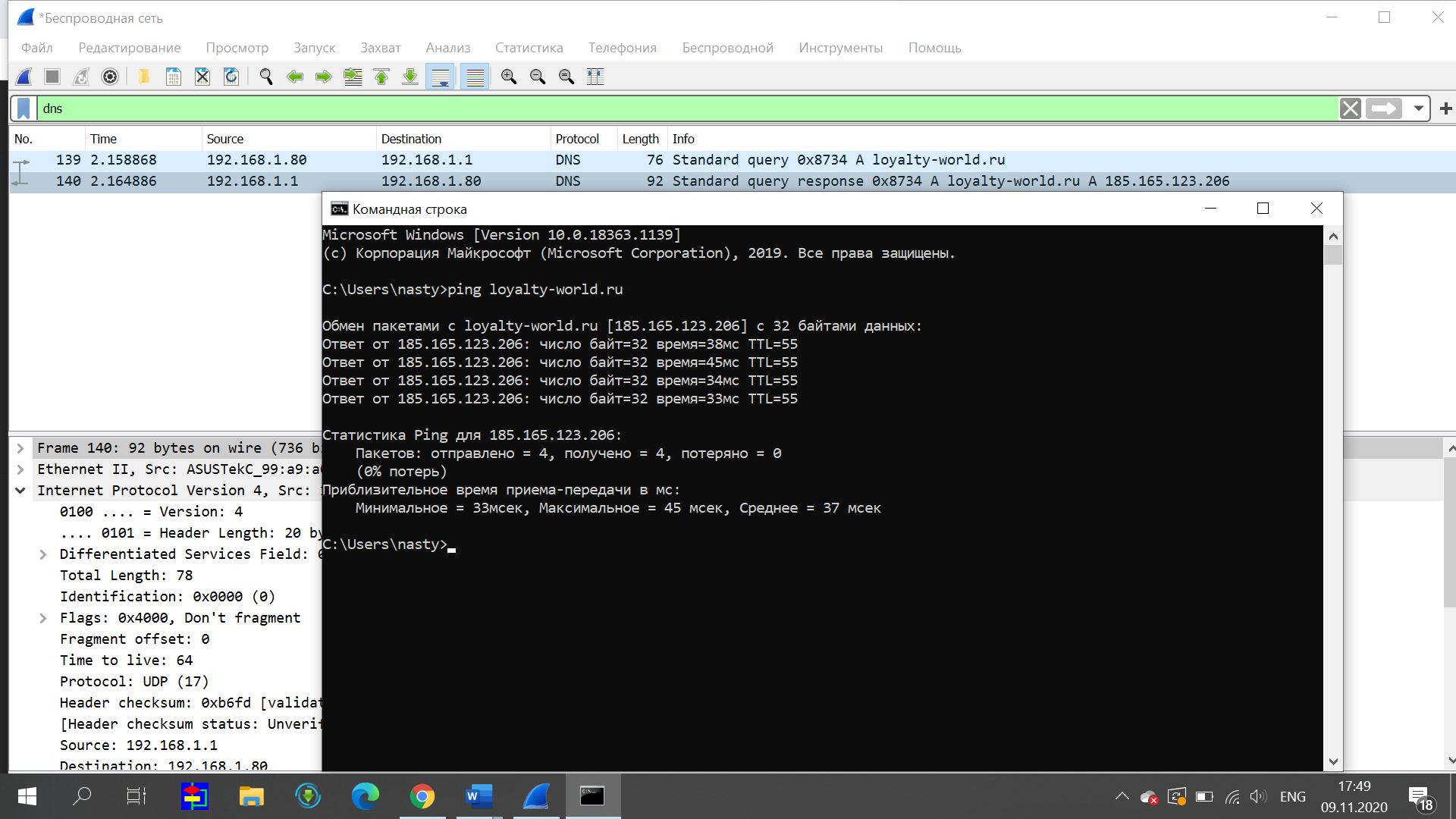
1. Ввод поискового запроса «intitle:"forum" inurl:http after:2019» и выбор ресурса «http://loyalty-world.ru»

2. Определение IP – адреса ресурса, с использованием нескольких способов.

2.1 Определение IP – адреса ресурса с помощью сетевой утилиты *nslookup.*



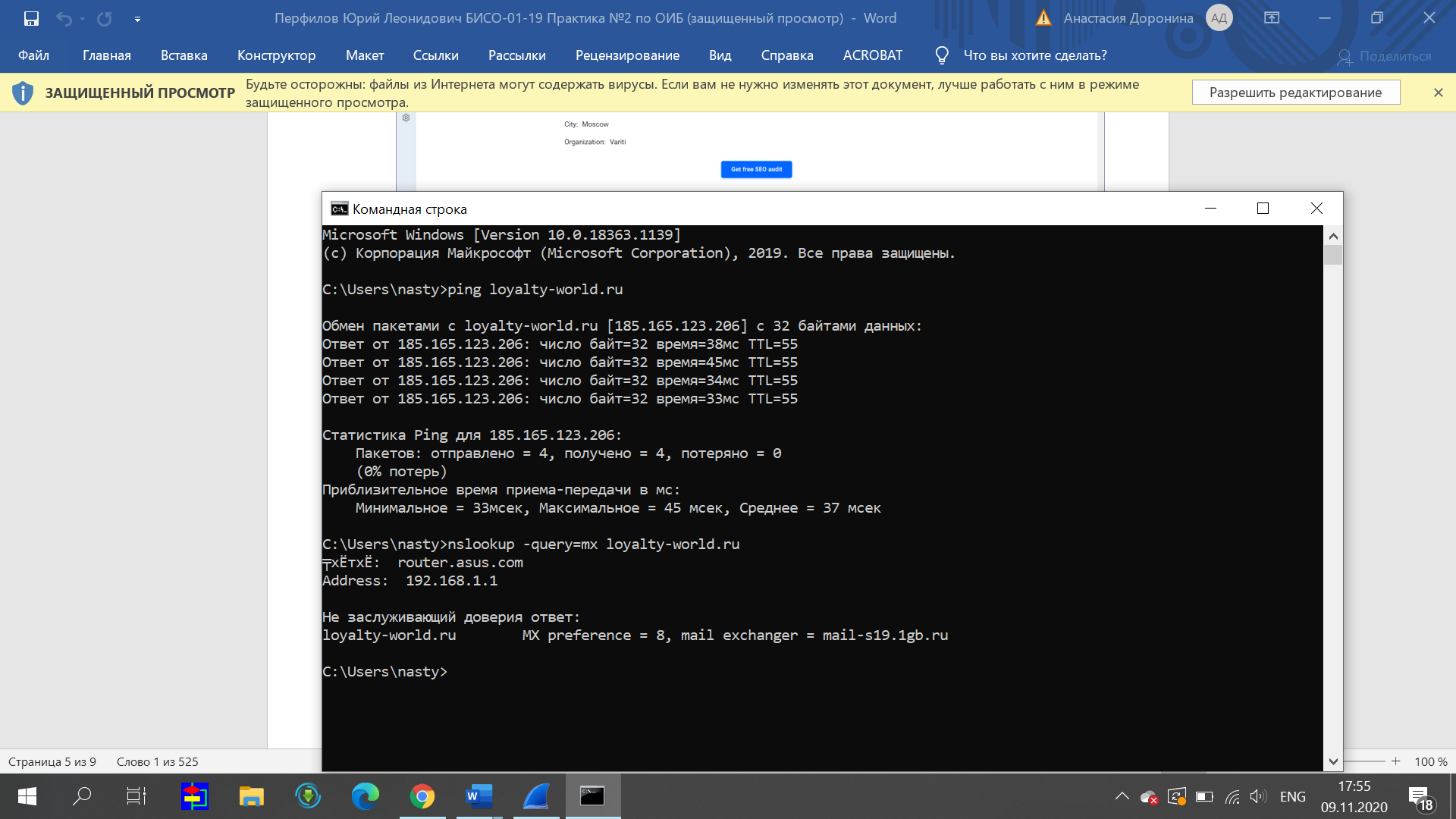
2.2 Определение IP – адреса ресурса с помощью сетевой утилиты *Ping.*



3. Изучение аргумент утилиты nslookup.

3.1 Изучение аргумента –query=mx утилиты nslookup.

С помощью данного аргумента происходит поиск записей MX, которые хранят соответствие доменного имени почтовому сервису этого домена, то есть в этих записях содержатся почтовые серверы домена, через которые должна отправляться вся электронная почта.

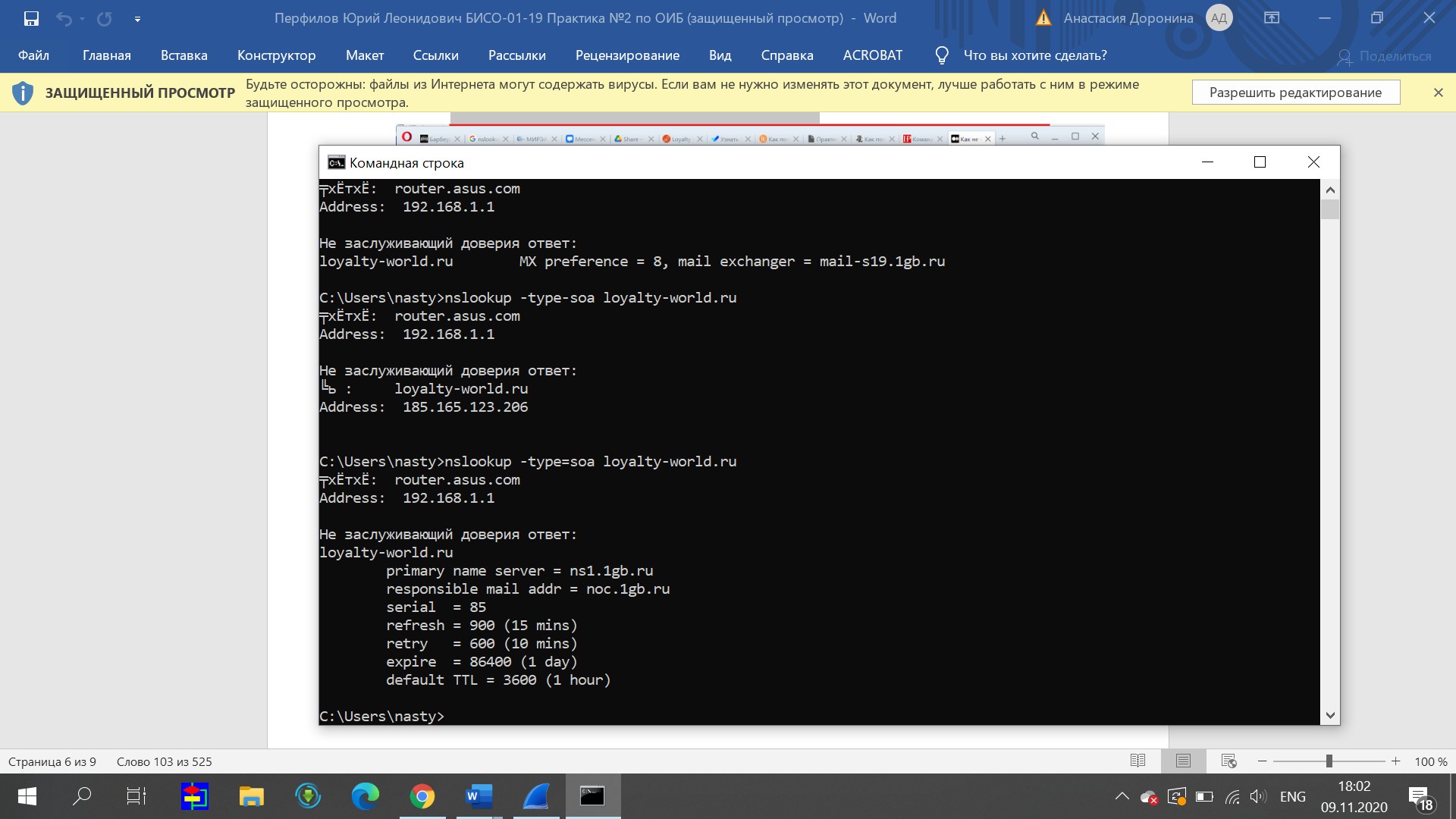


Для домена «loyalty-world.ru» есть 1 записи MX. Число рядом с именем сервера (8) означает его приоритет. Чем меньше число, тем выше приоритет. То есть при наличие других серверов и отправке письма на адрес «@loyalty-world.ru» сначала бы использовался сервер mail-s19.1gb.ru.

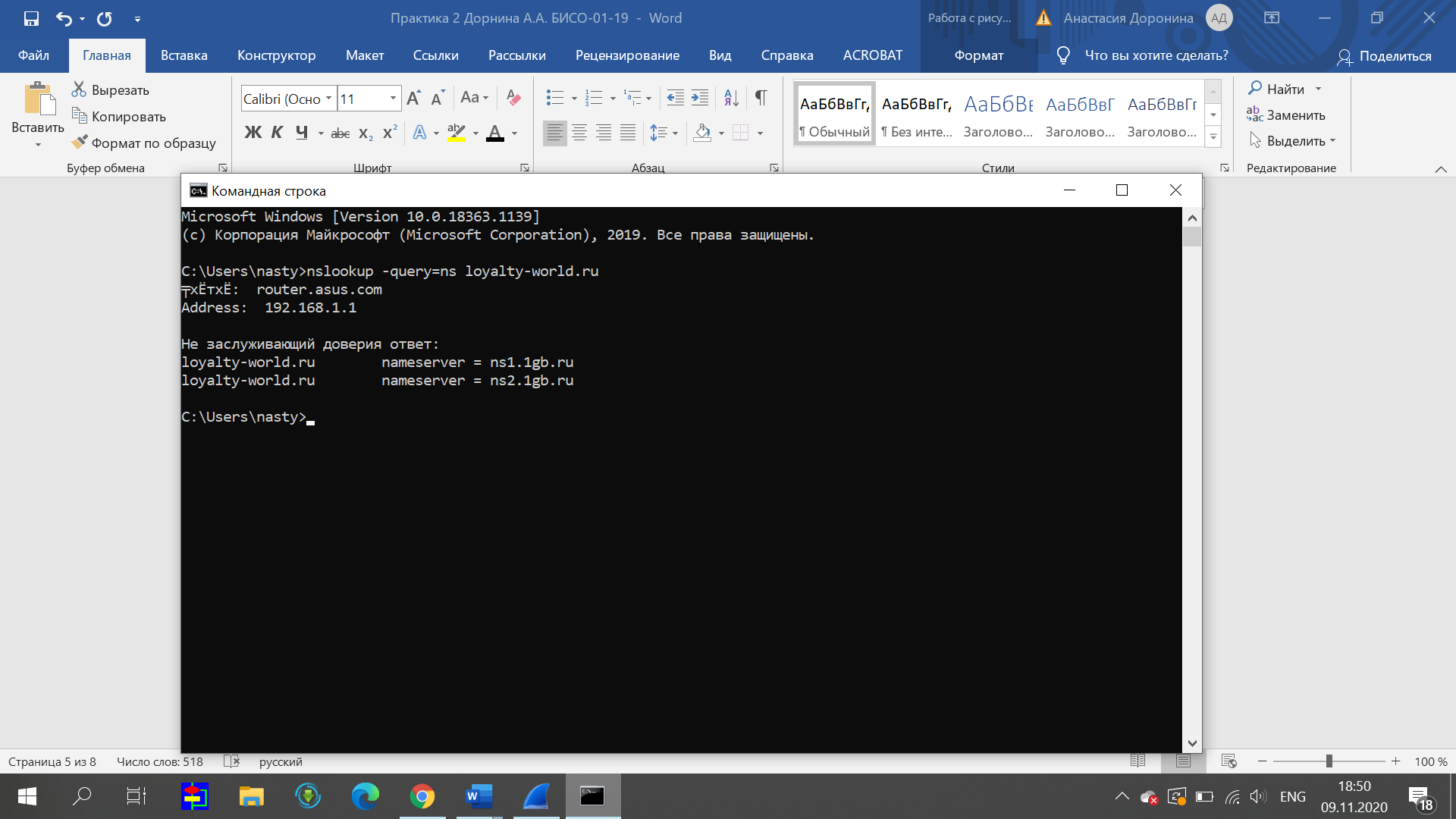
3.2 Изучение аргумента soa утилиты nslookup.

SOA – один из типов информации, которую мы можем получить. SOA или Start Of Authority предоставляет техническую информацию о домене, где

* Primary name server - происхождение полученной информации;
* responsible mail addr - адрес электронной почты администратора домена;
* serial - 32-разрядное число, которое содержит в себе серийный номер файла зоны;
* refresh - количество секунд, с момента последнего обновления, когда его нужно повторить;
* retry - количество секунд, через которое нужно повторить попытку подключения, если DNS сервер недоступен;
* expire - количество секунд, по истечении которых полученная от первичного DNS информация будет считаться устаревшей;
* minimum - минимальное количество секунд до следующего обновления.
* default TTL – стандартное время жизни пакета



3.3 Изучение аргумента ns утилиты nslookup.



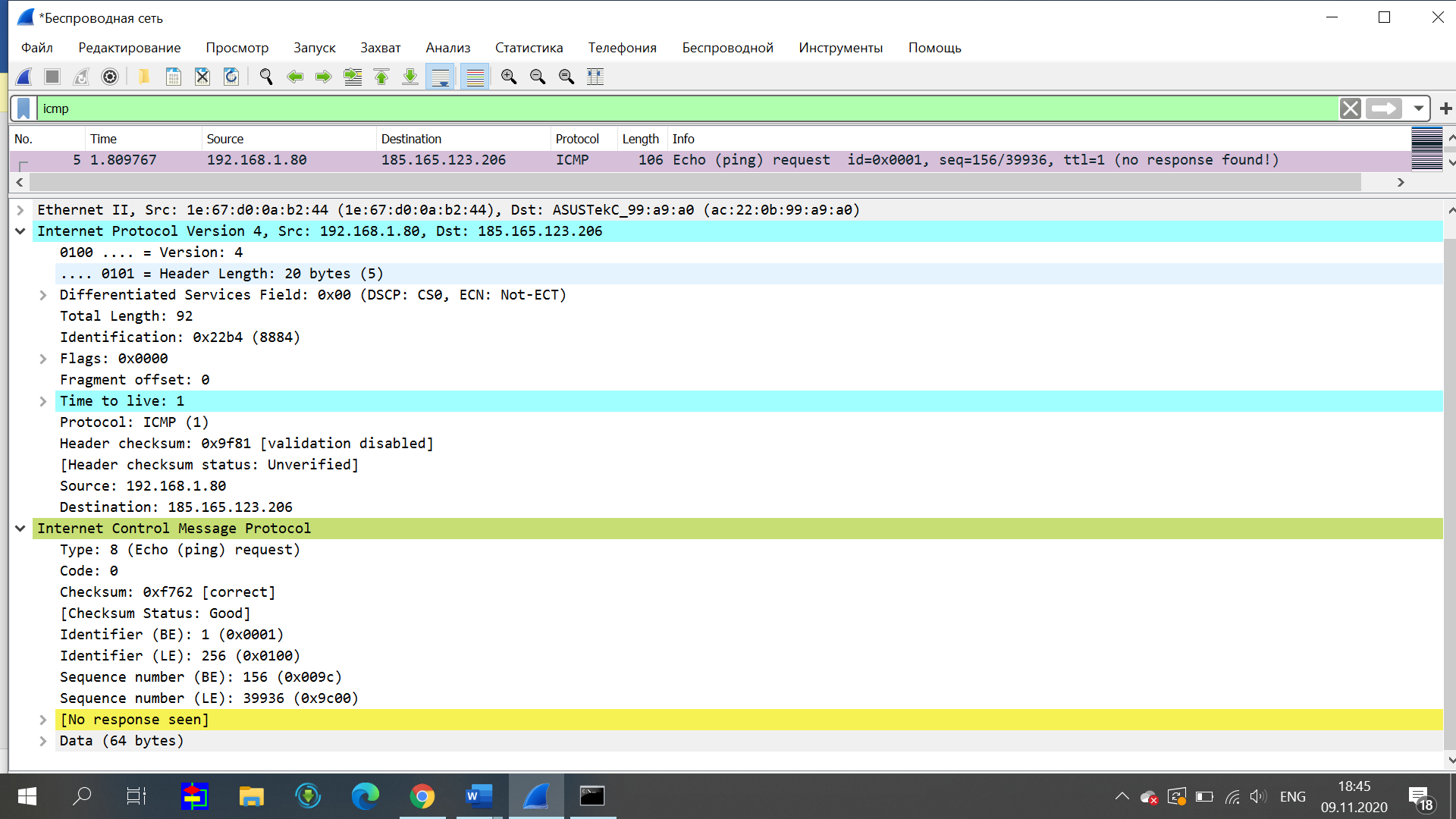
Выводит соответствие доменных имен DNS-серверам

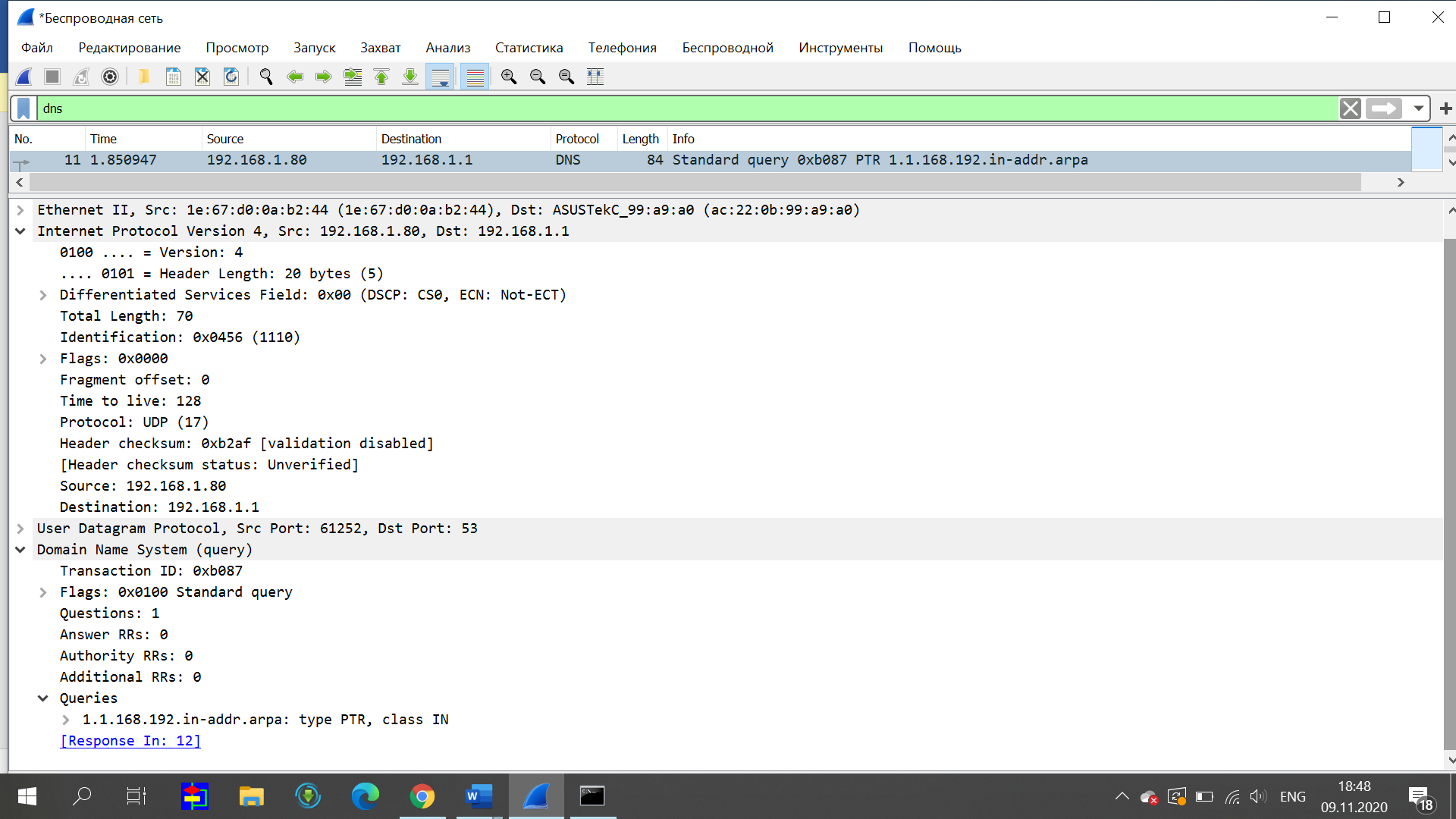
3.4 Изучение аргумента type=any утилиты nslookup.

Аргумент type=any создан для отображения любых типовых записей, а также для того, чтобы вывести все имеющиеся DNS записи в доменной зоне.

4.Трафик с сайта

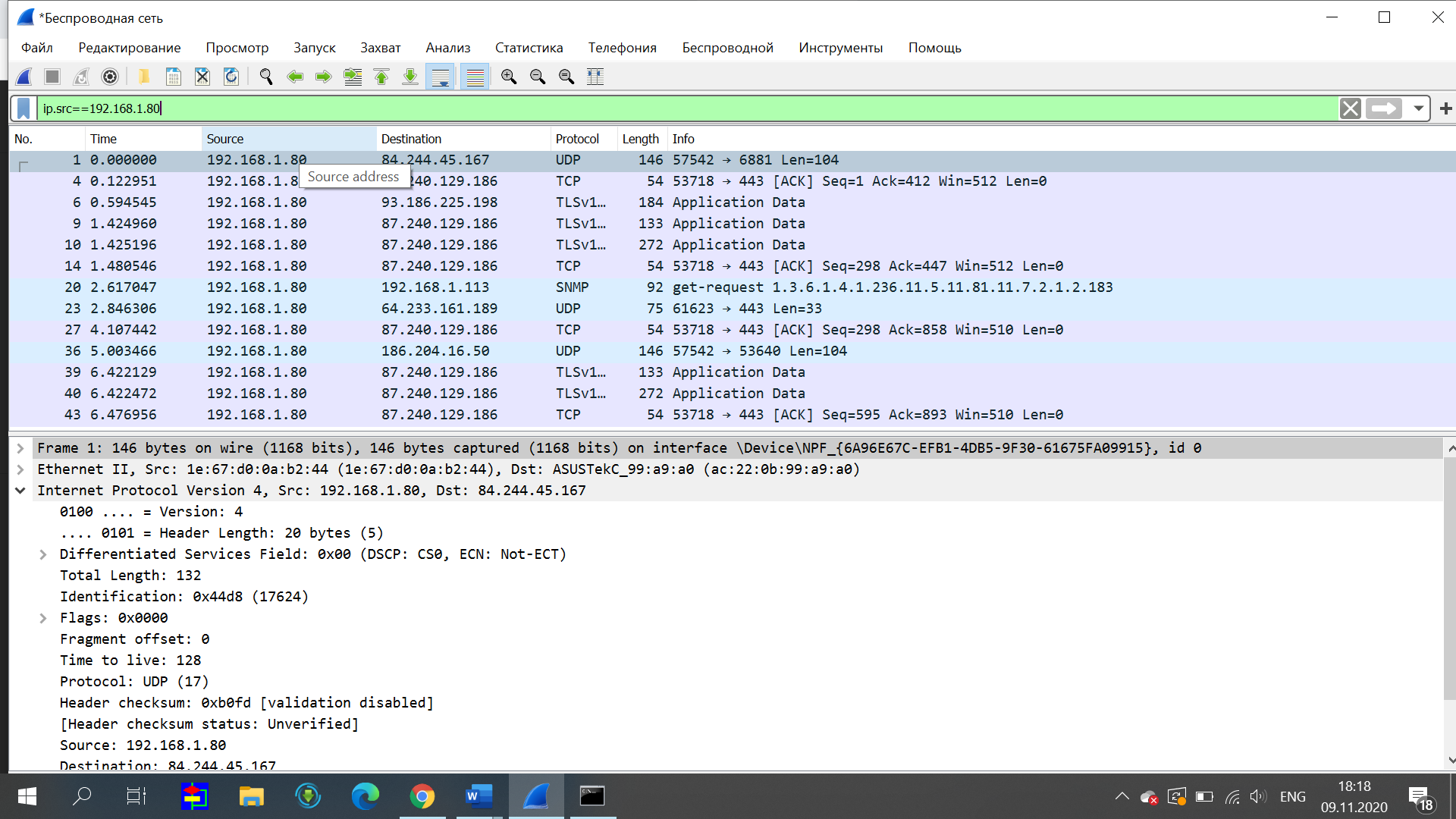
IP ресурса 185.165.123.206



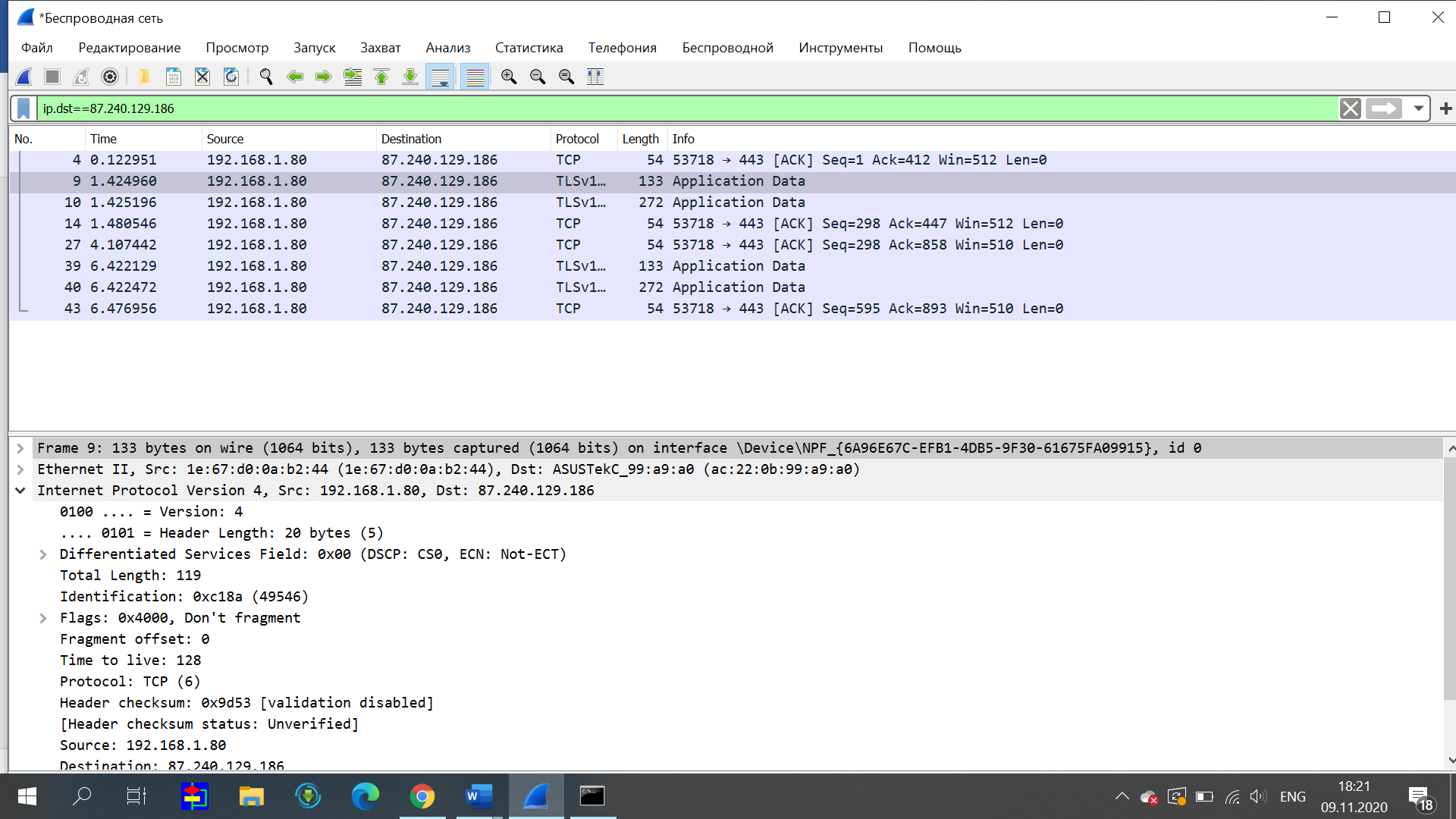


5.Изучение основных фильтров

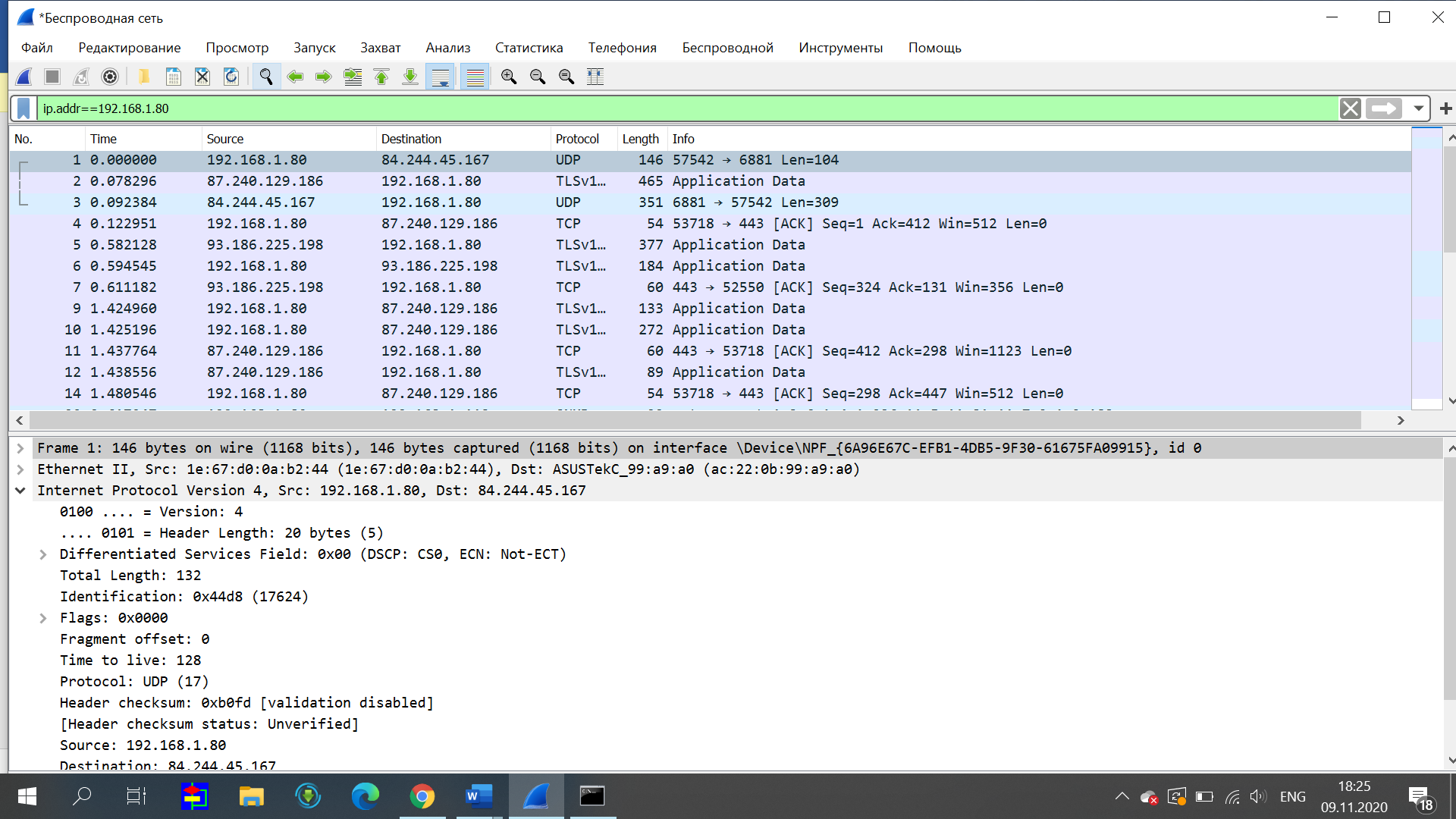
***ip.src*** - Wireshark - фильтр по IP адресу отправителя



***ip.dst*** – Wireshark - фильтр по IP адресу получателя

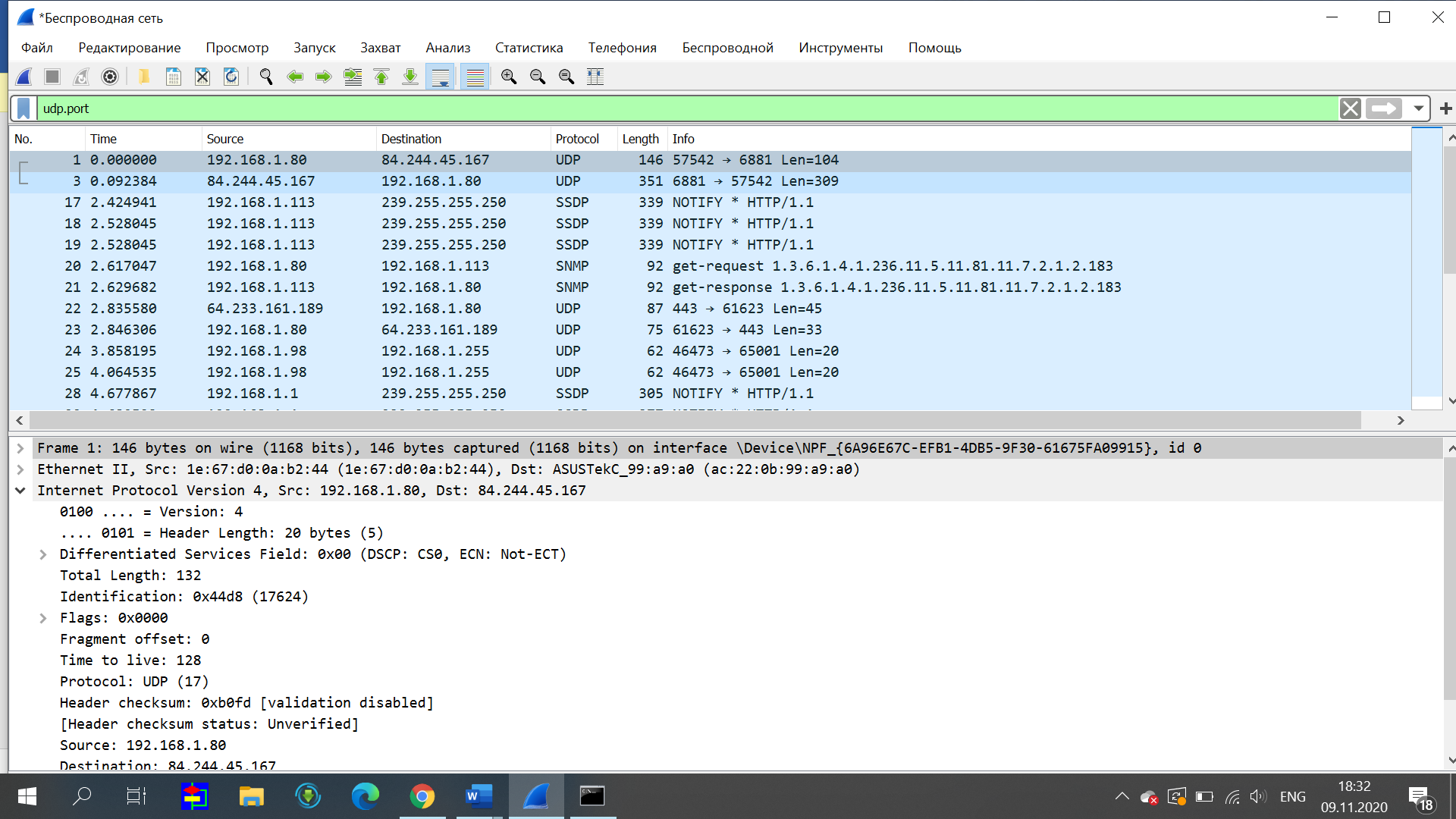


***ip.addr*** - Wireshark- фильтр по IP адресу



UDP — один из ключевых элементов набора сетевых протоколов Интернета, используемых для быстрой передачи сообщений, но не гарантирующий их доставку, целостность, а также не сохраняющий состояние отправленных сообщений.

***udp.port*** – Wireshark – фильтр по UDP порту/протоколу получателя или отправителя, где каждый порт/протокол обозначает конкретное действие, то есть, например, протокол 2 - процесс управления, порт 3 - процесс сжатия, а порт 5 - обслуживает отправку файлов и вывод отчётов при работе рабочей станции с мейнфреймами.



ARP — протокол разрешения адресов (Address Resolution Protocol) является протоколом третьего (сетевого) уровня модели OSI, используется для преобразования IP-адресов в MAC-адреса, играет важную функцию в множественном доступе сетей. Непосредственно связь между IP-адресом и MAC-адресом осуществляется с помощью ARP-таблиц, где в каждой строке указывается соответствие IP адреса MAC-адресу.

***arp.src.hw\_mac*** – Wireshark – фильтр, показывающий фреймы ARP протокола, отправленные с устройства, имеющего следующий MAC-адрес

5.6 Ethernet— семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей.

eth.dst – Wireshark – фильтр MAC-адрес получателя

eth.src – Wireshark – фильтр MAC-адрес отправителя