|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)** |
|  |

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 2** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Маринин Вячеслав Петрович |
|  |

Москва 2020

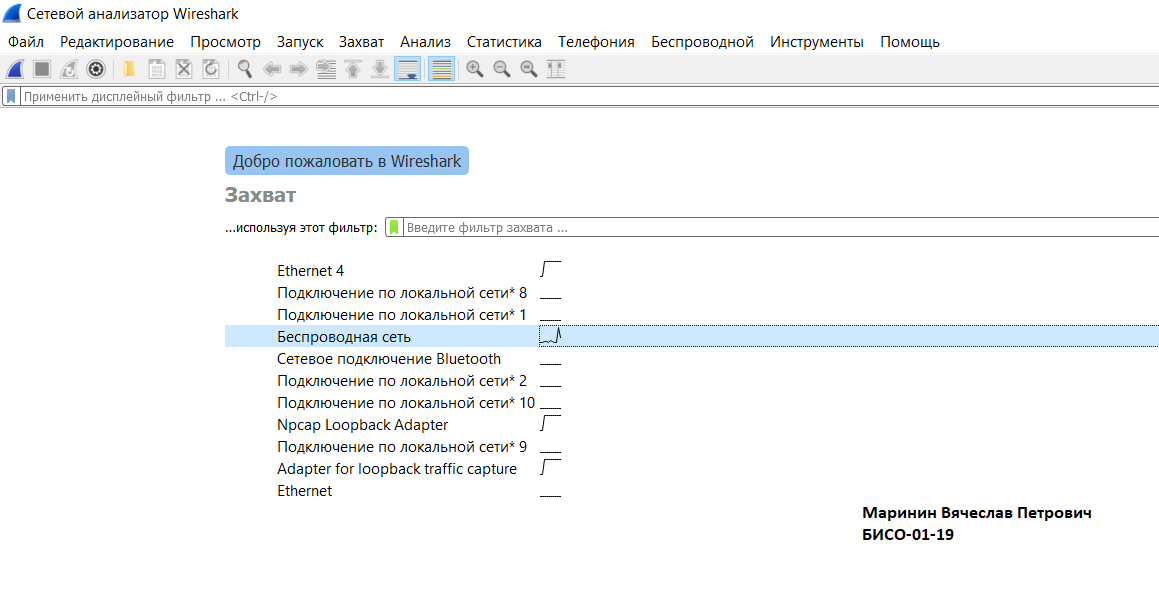
**Практика 2**

**WIRESHARK**

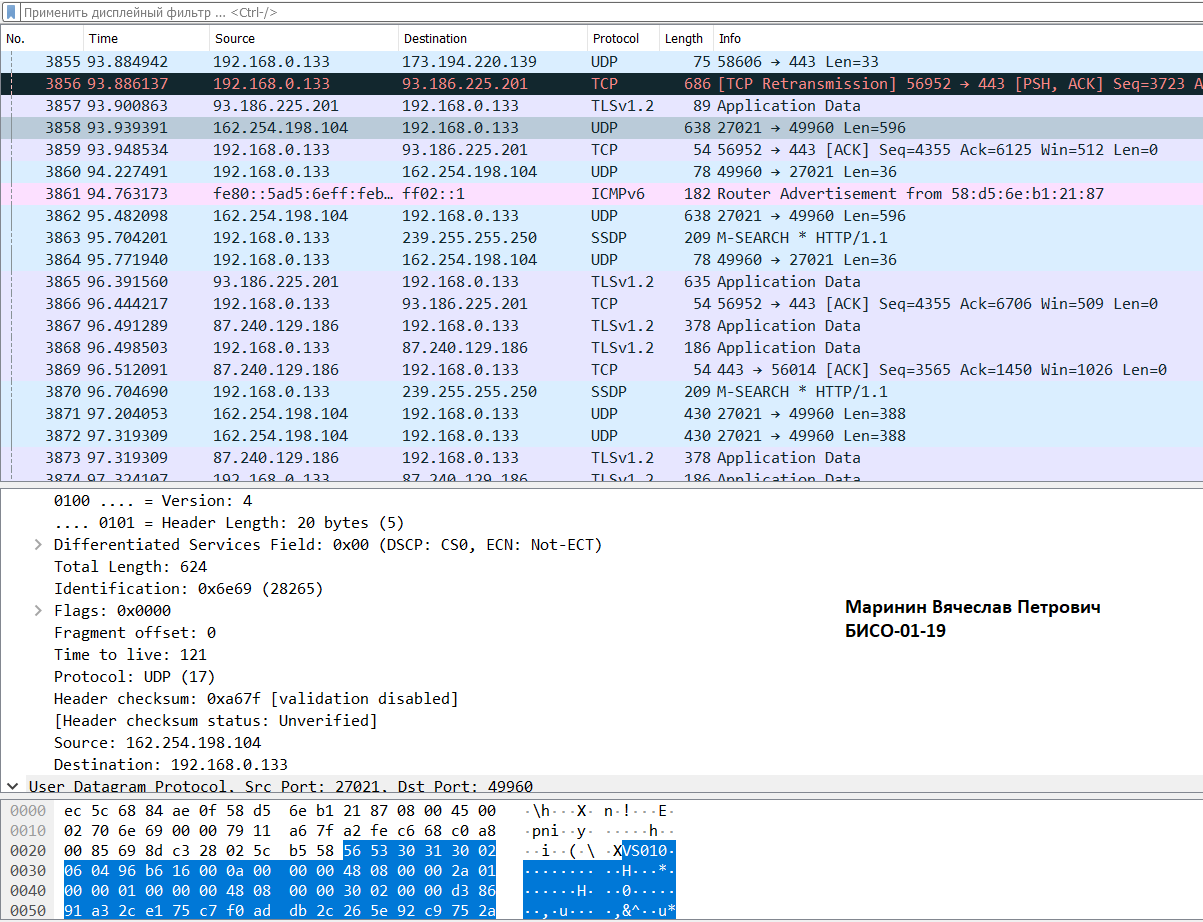
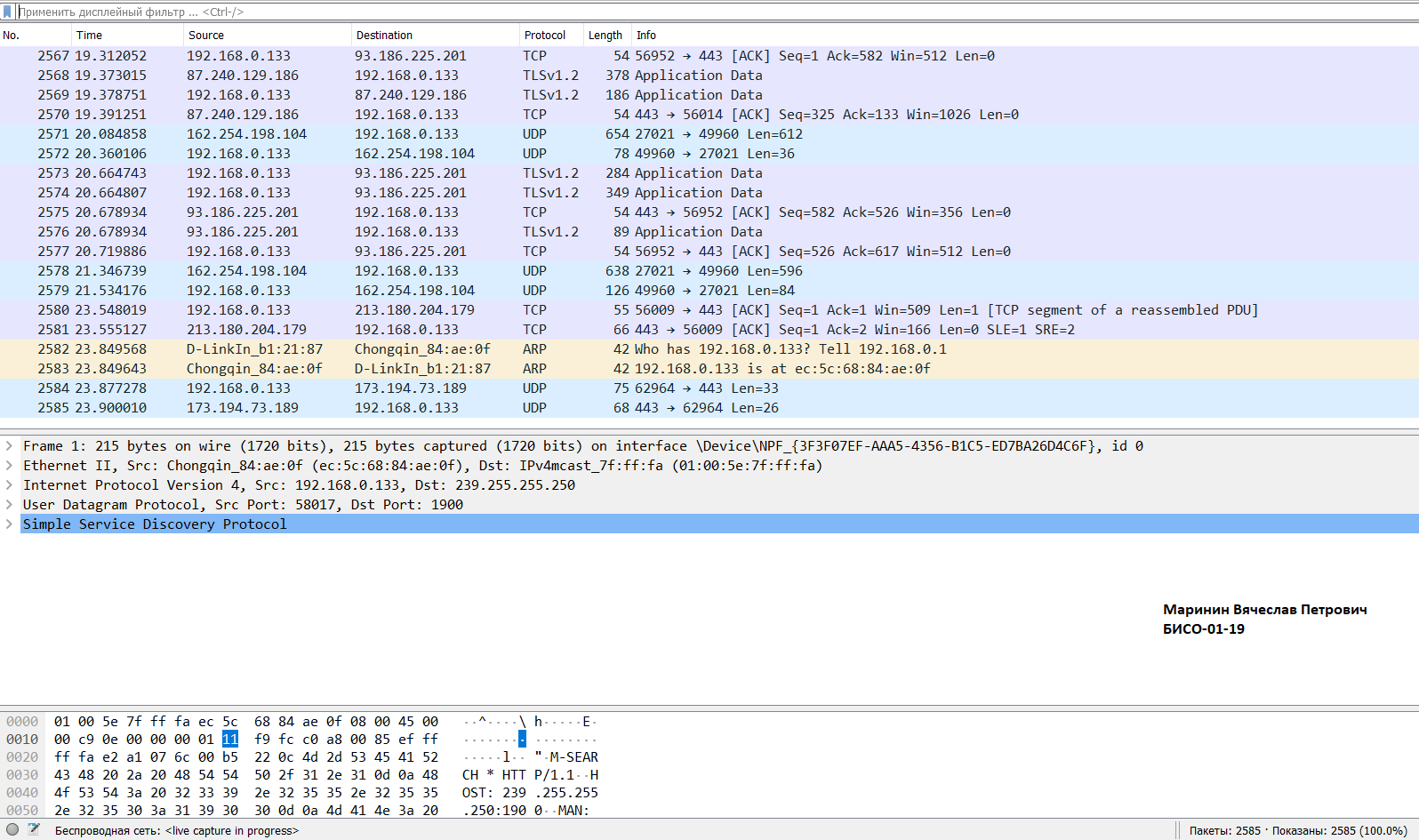
**(1)Протокол IP (стр 4)**

**Действия:**

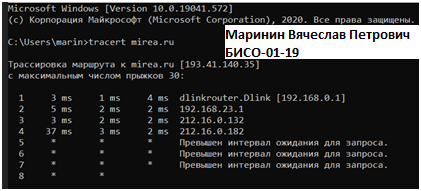
**1)**



**2)**

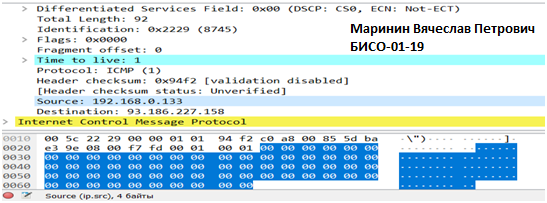
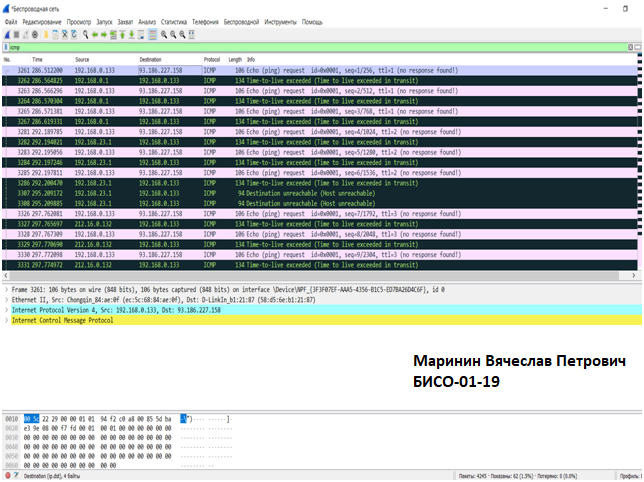


**3)**



**Задания:**

1.1))Проанализируйте первый пакет ICMP Echo Request, отправленный вашим компьютером: укажите ваш IP-адрес.



**Мой IP-адрес: 192.168.0.133**

1.2))Сколько байт содержится в заголовке IP? Сколько байт в поле данных?

**Теория:**

**Длина (размер) заголовка (4 бита)**

Заголовок IP включает обязательные поля, а также может включать в себя

дополнительные поля, которые называются опциями. В этом поле записывается

полная длина как обязательной части, так и опций.

**Размер пакета (общая длина, 16 бит)**

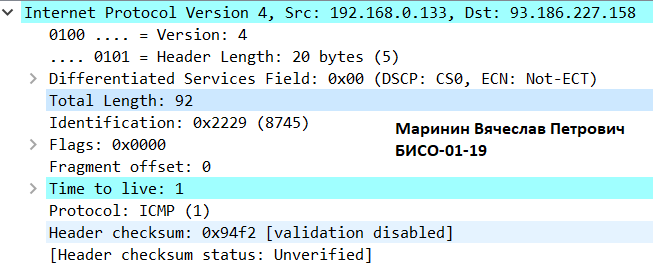
Общая длина – длина пакета, включая заголовок и данные. Минимальный

размер – 20 байт (заголовок без данных), максимальный

– 65535 байт. Пакеты большего размера подвергаются фрагментации (делению на

части).

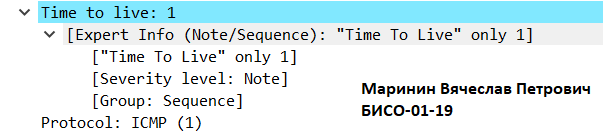
**Информация по пакету:**



**Header Length: 20 bytes (5)**

**Total Length: 92**

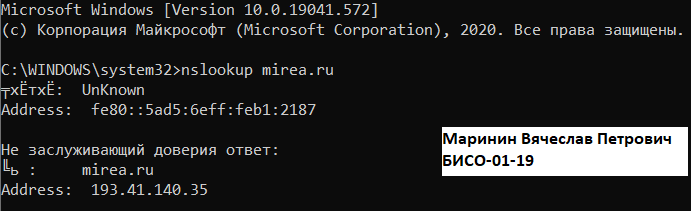
1.3)) Укажите значение TTL.



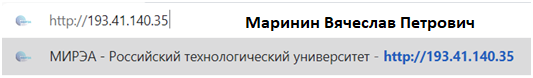
**(2)Протокол DNS (стр 13)**

**Действия:**

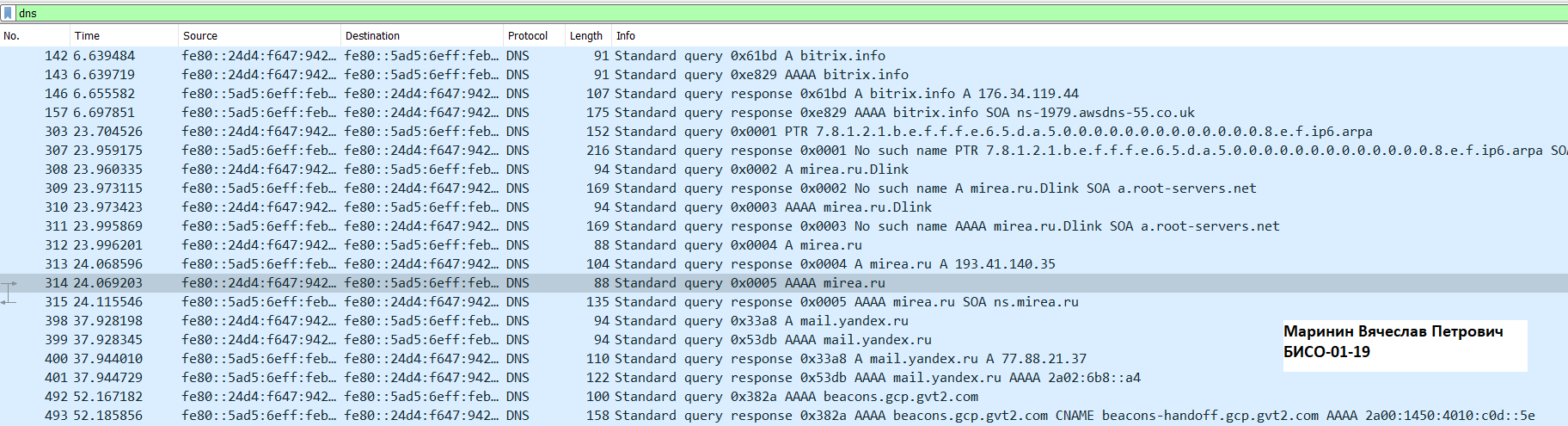
1)



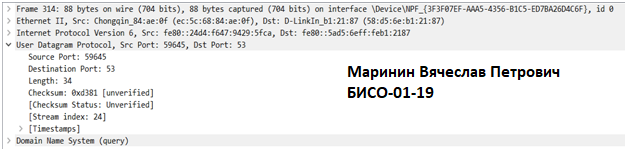
2)



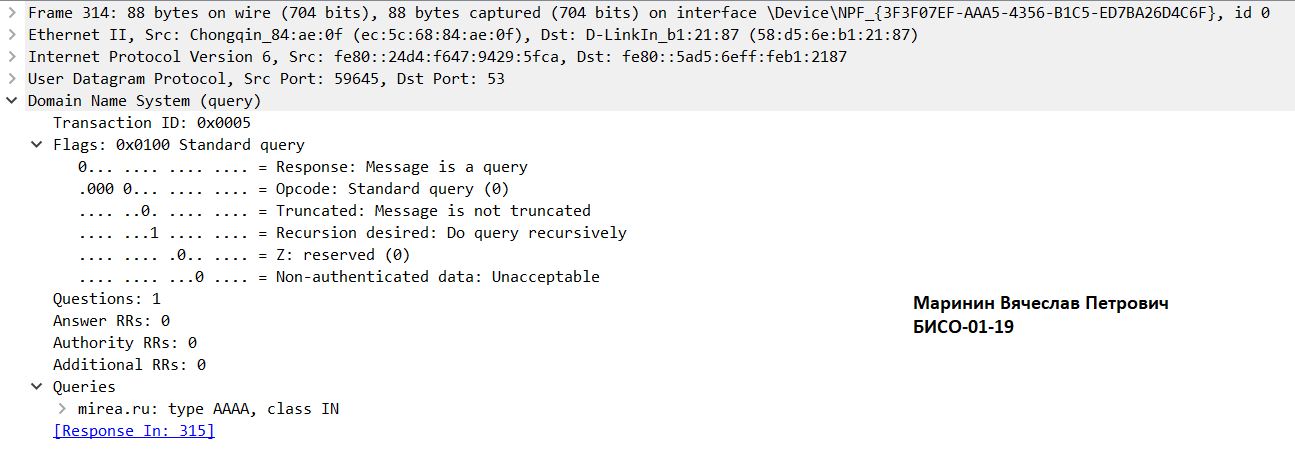
3)



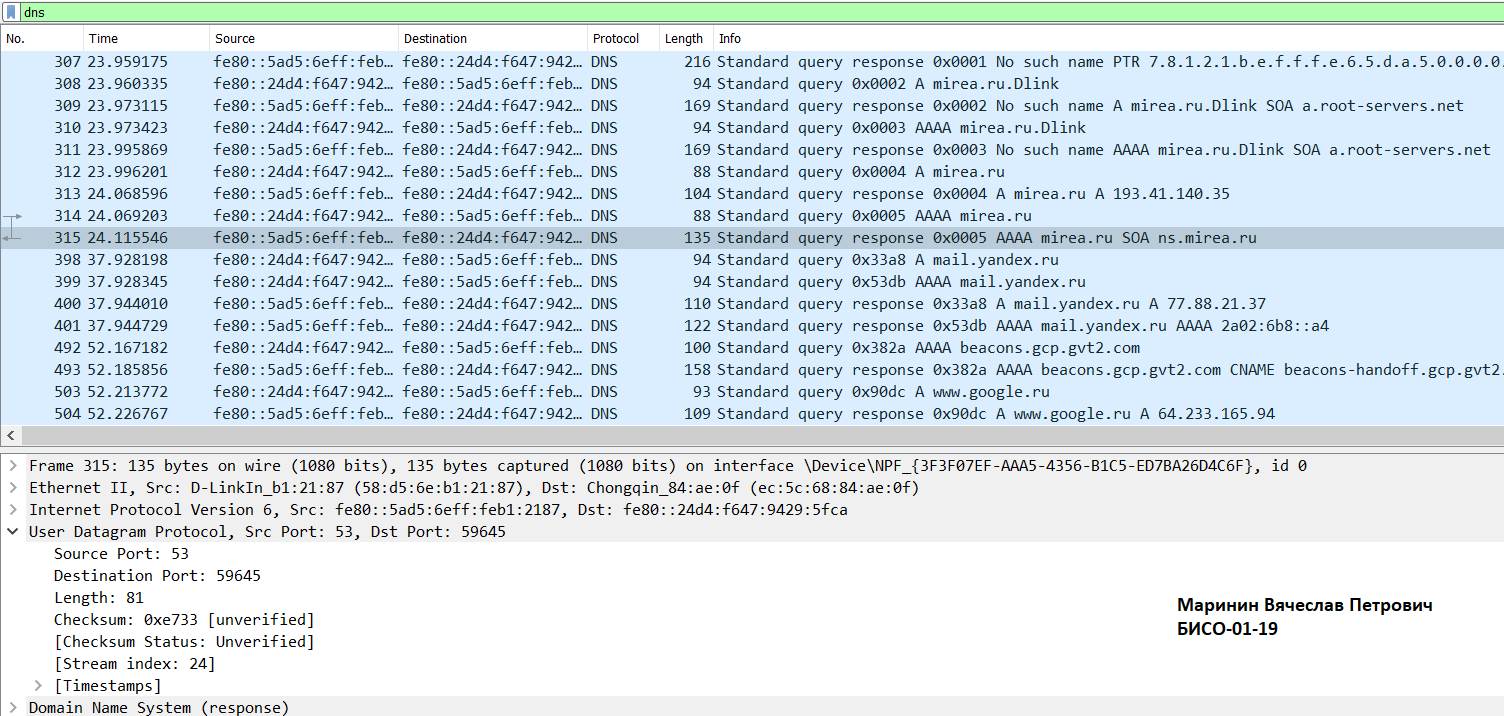
**3.5)**



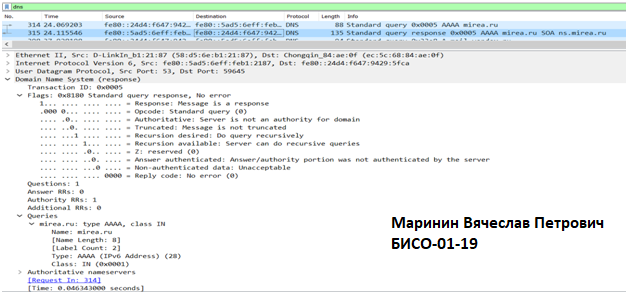
**3.6)**



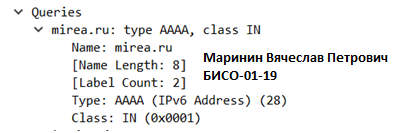
**3.7)**



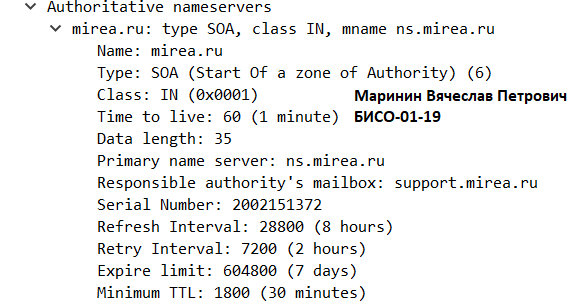
**3.8)**



**3.9)**



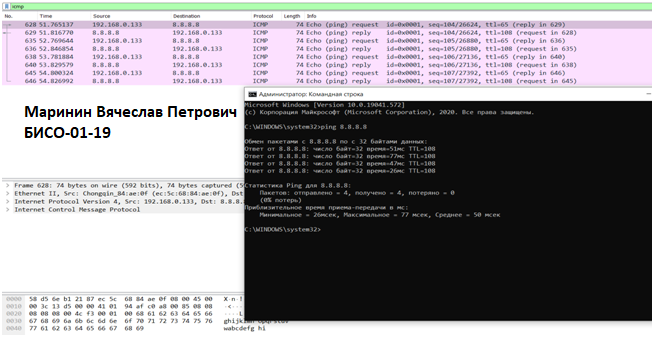
**3.10)**



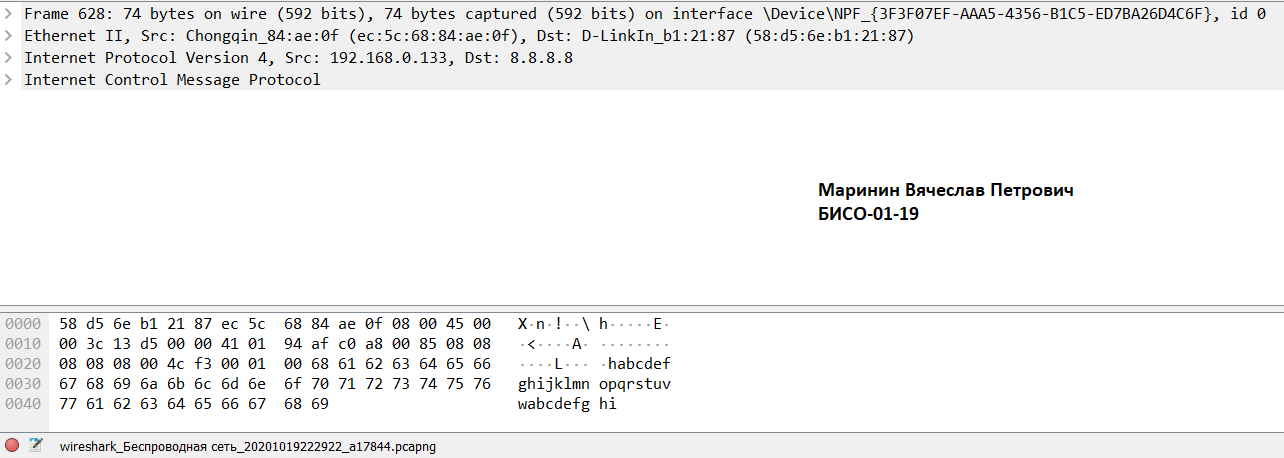
**(3)Протокол ICMP (стр 20)**

**Действия:**

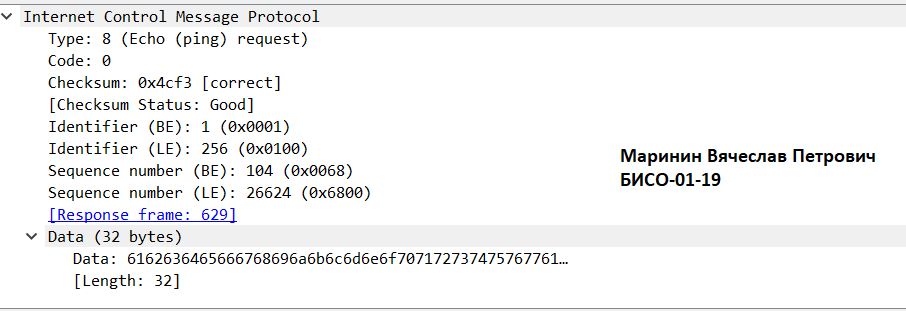
**1)**



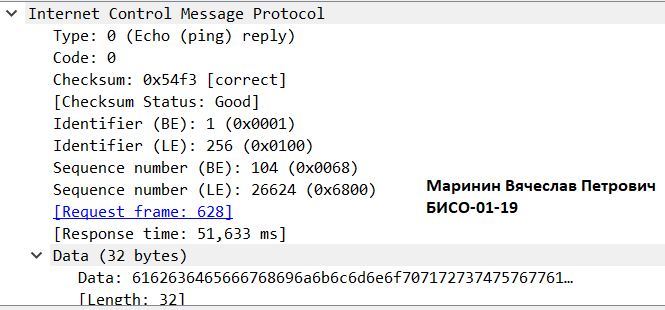
**2)**



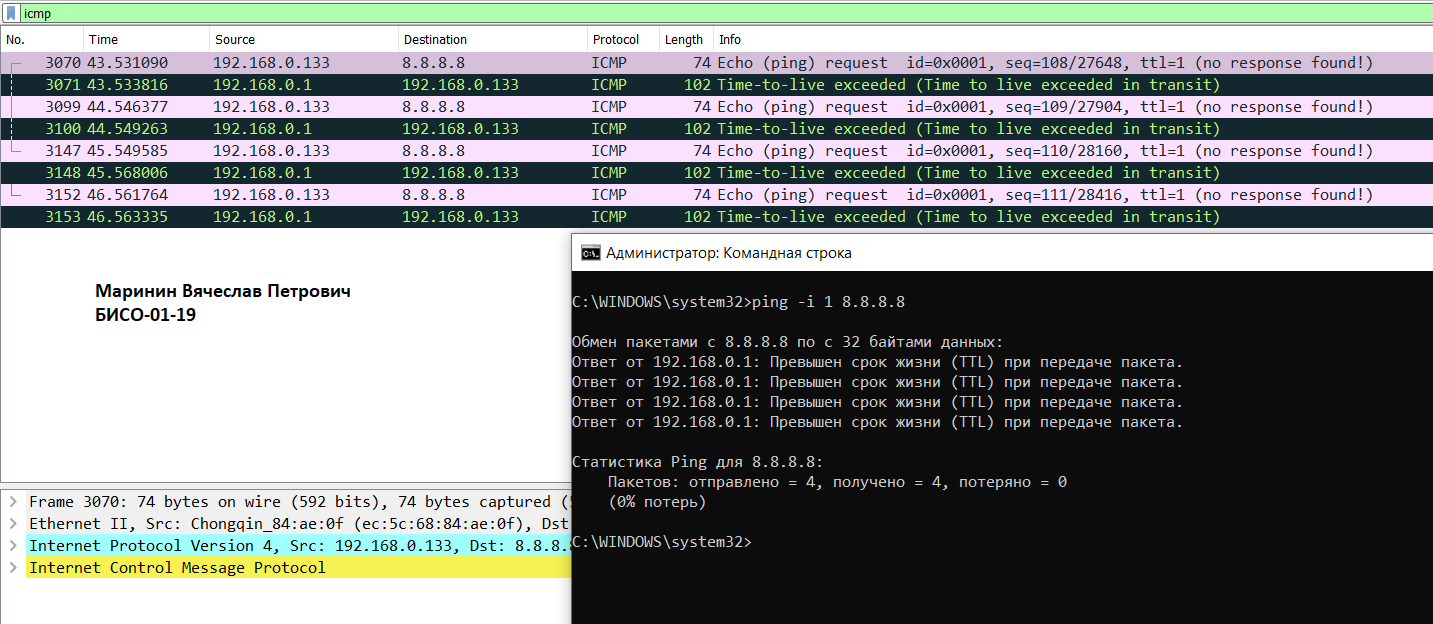
**4.4**



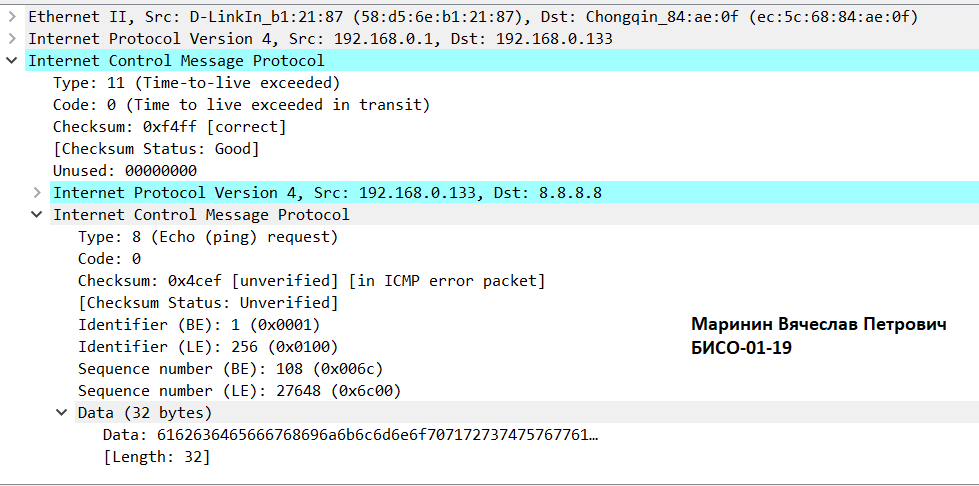
**4.5**



**3)**



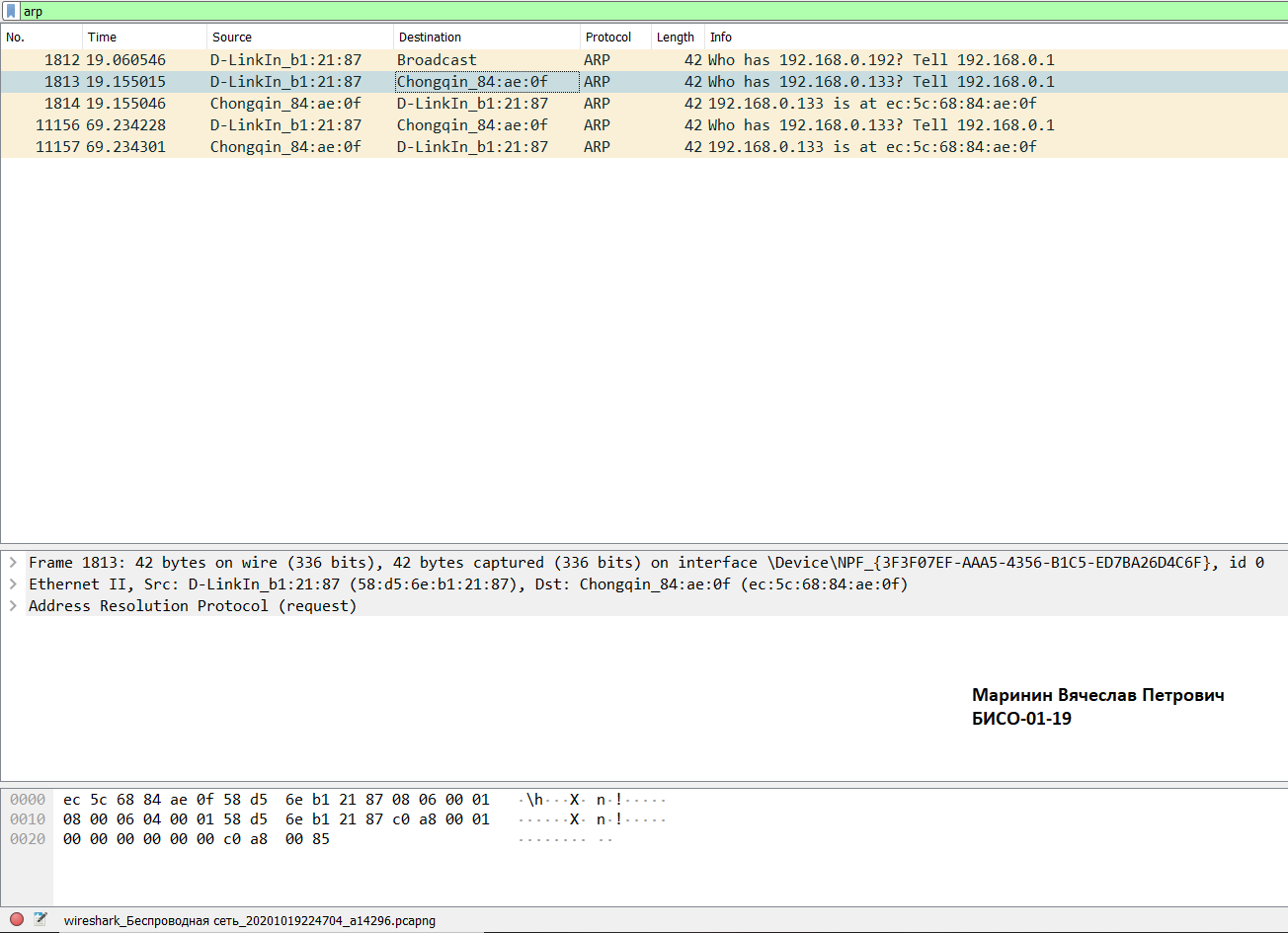
**4)**



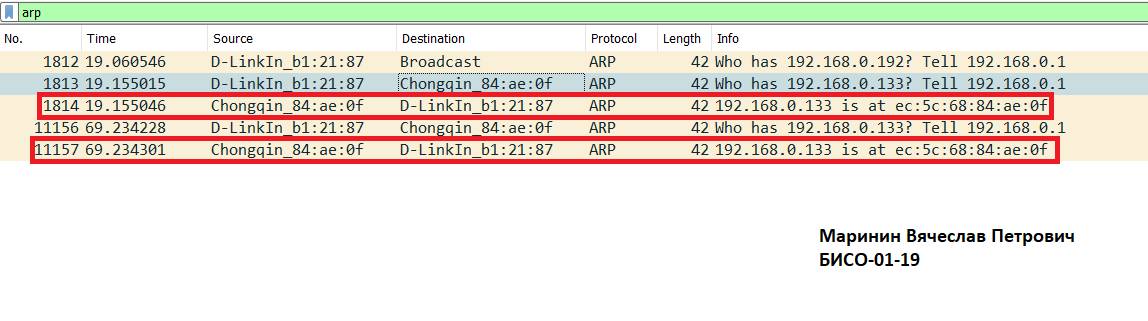
**(4)Протокол ARP (стр 25)**

**Действия:**

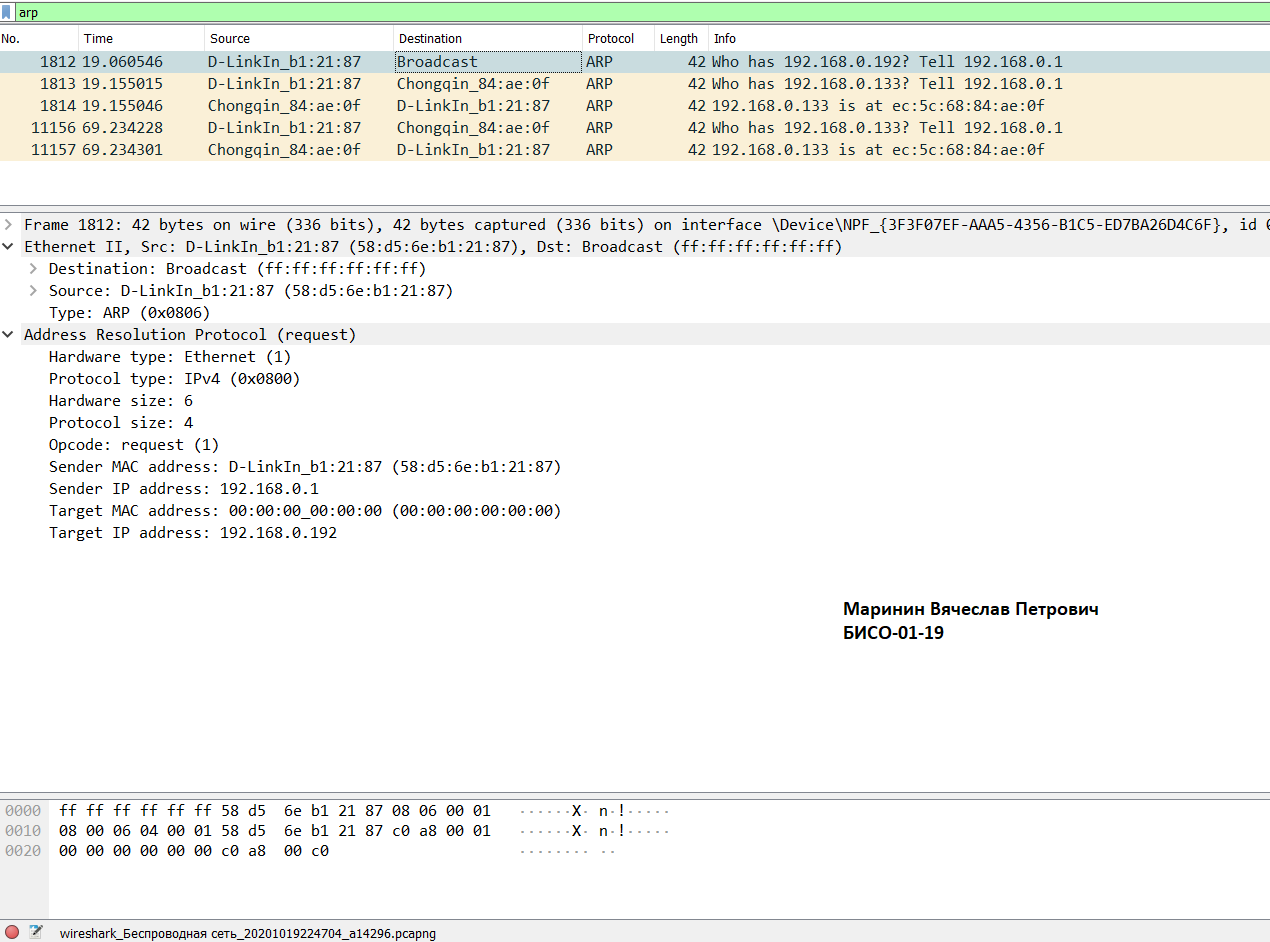
**1)**



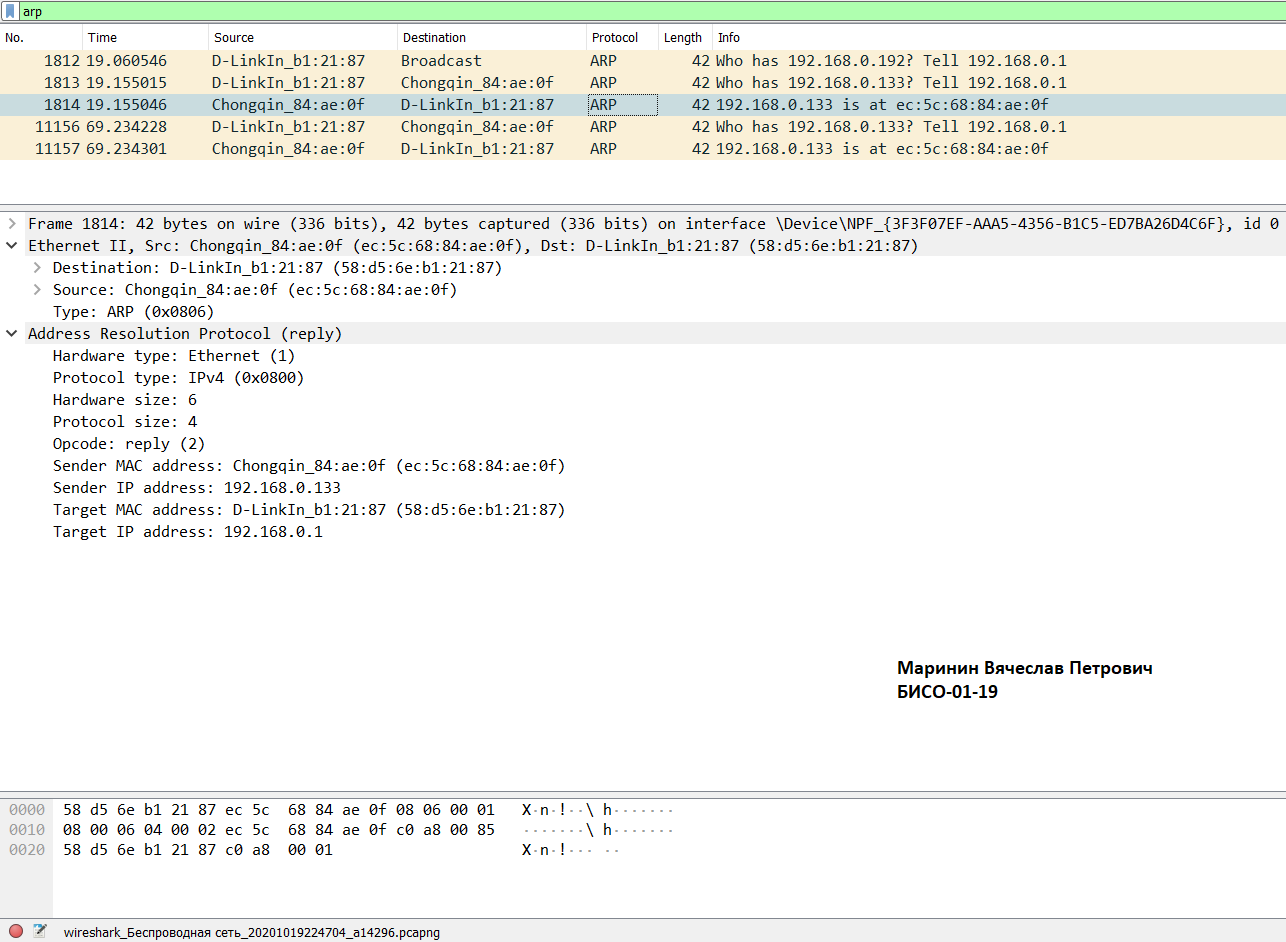
**2)**



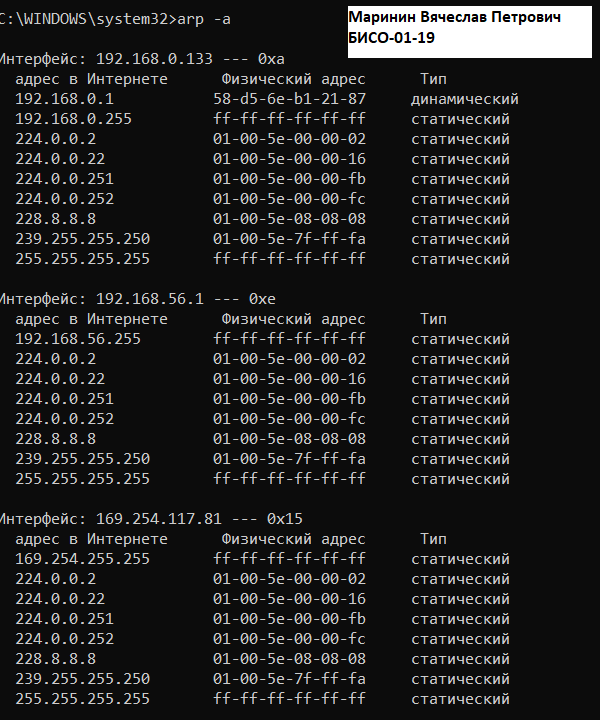
**5.5**



**5.6**



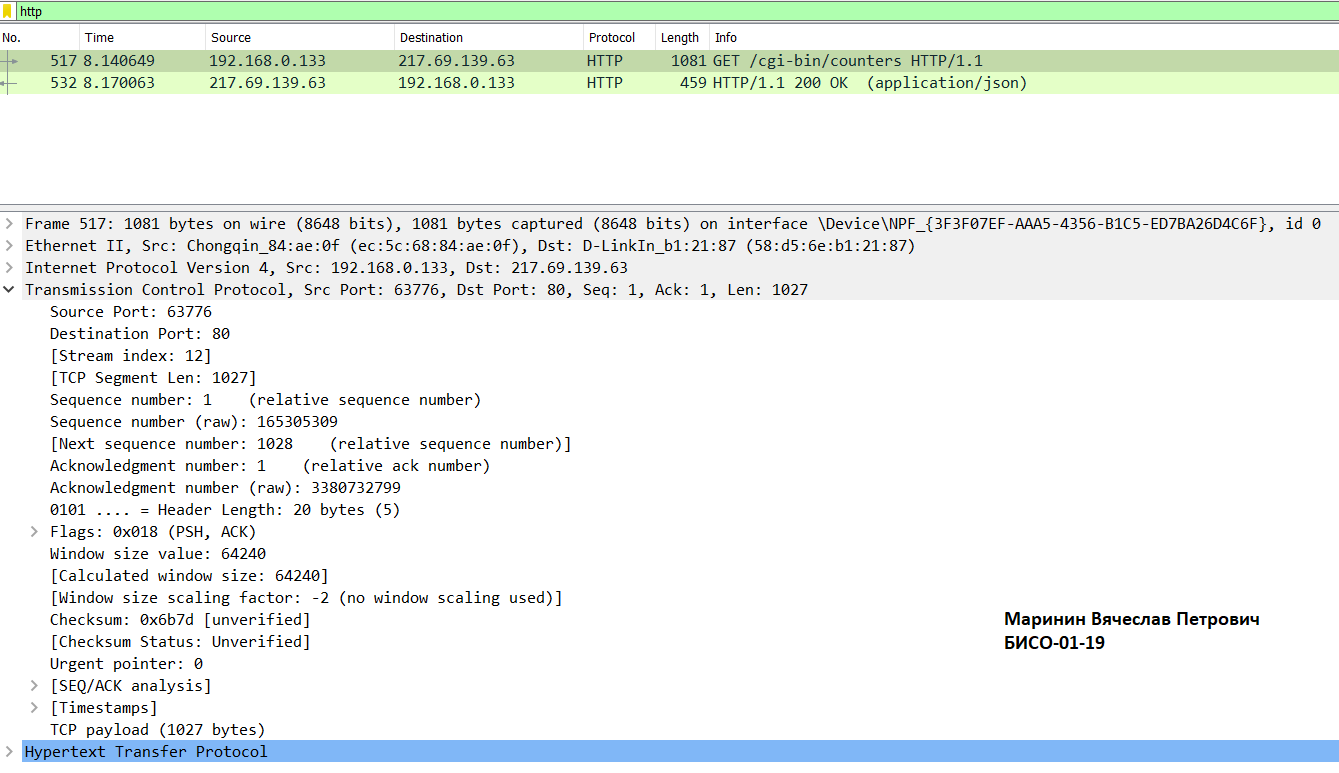
**3)**



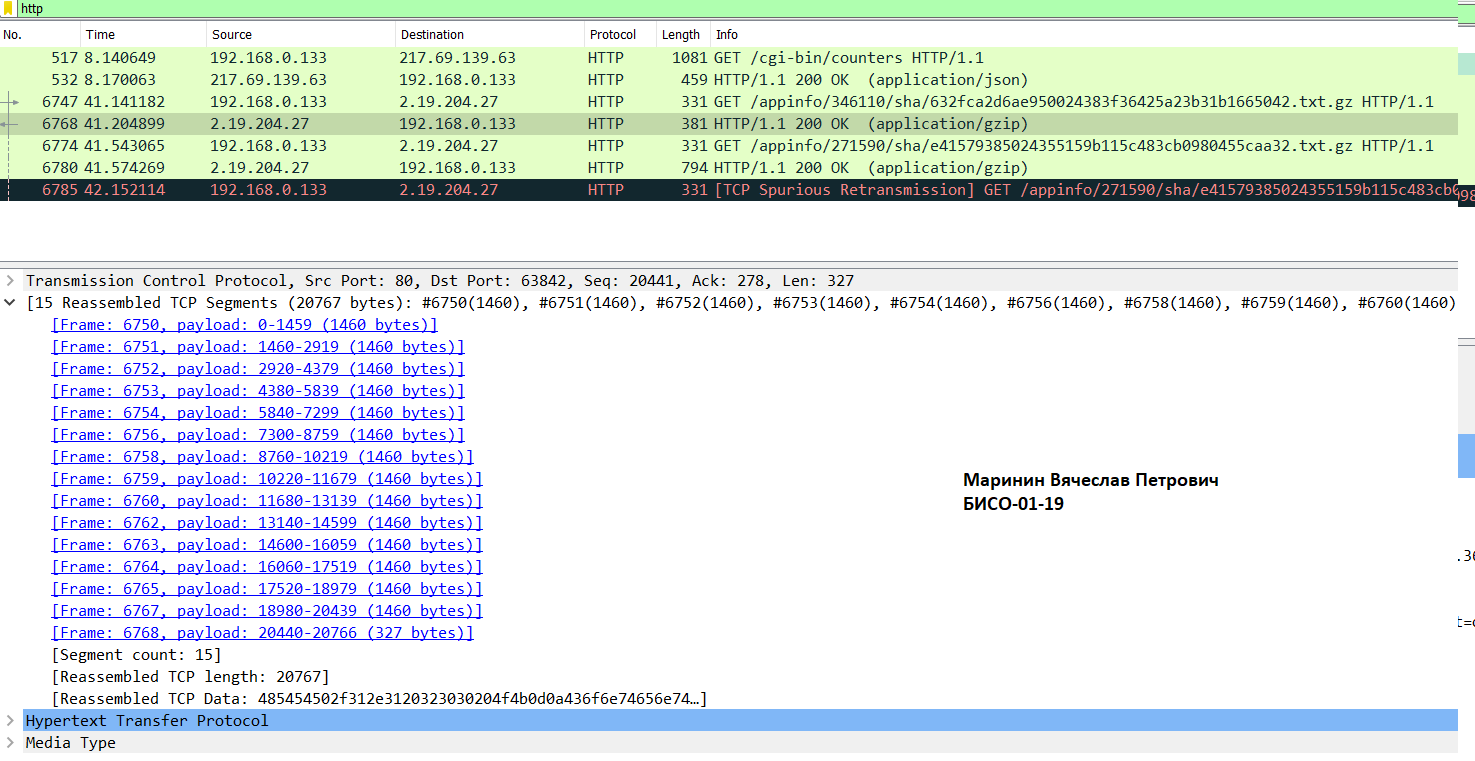
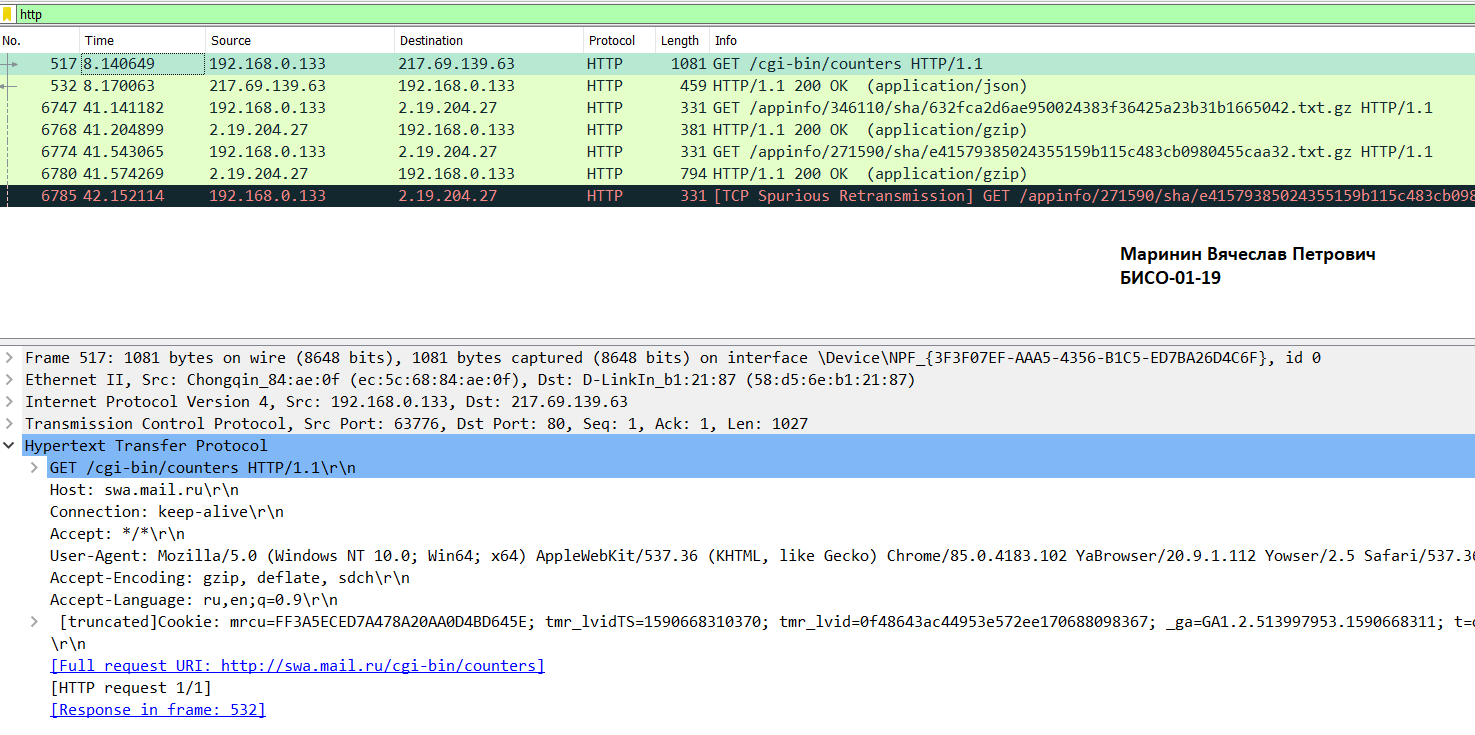
**(5)Протокол HTTP (стр 31)**

**Действия:**

**1)**

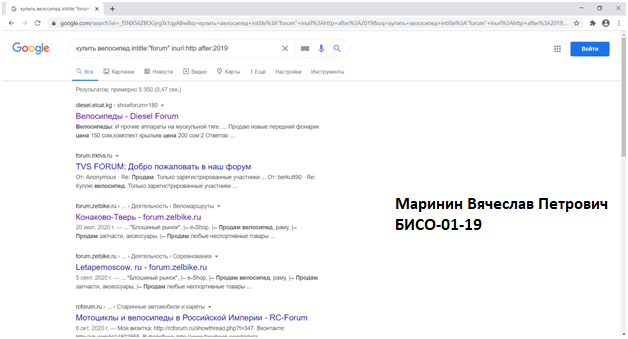


**2)**



**Задание:**

**1)**

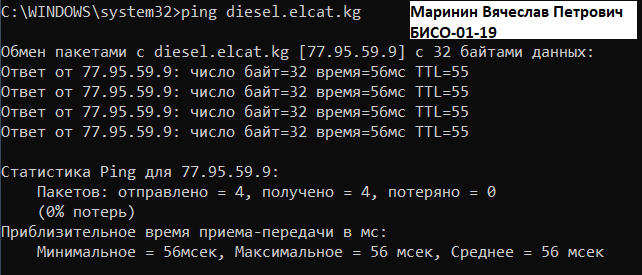


**2)** **Определить: ip адрес ресурса с использованием нескольких способов**

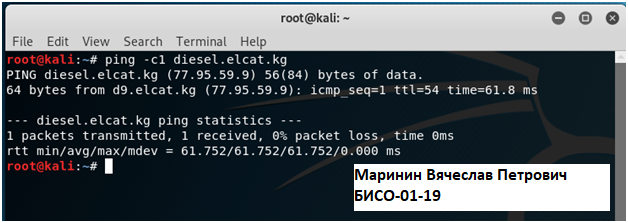
1-ая ссылка в перечне “Diesel Forum”

<http://diesel.elcat.kg/index.php?showforum=180>

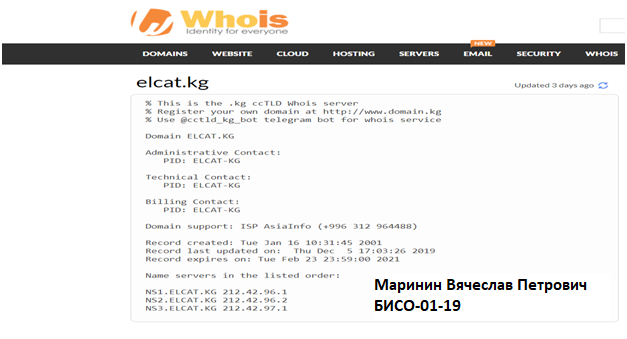
**2.1) Трассировка IP-адреса сайта с использованием командной строки**



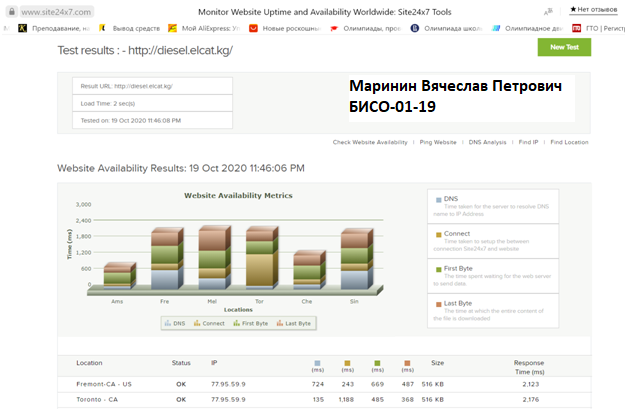
**2.2) Использование терминала на MAC или Linux**



**2.3) Использование WHOIS-истории**

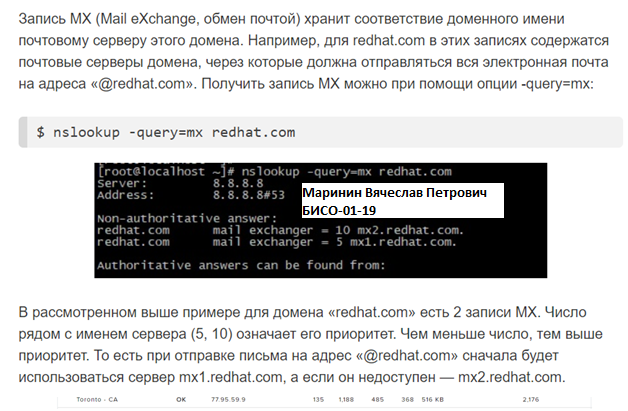


### 2.4) Использование веб-сервисов

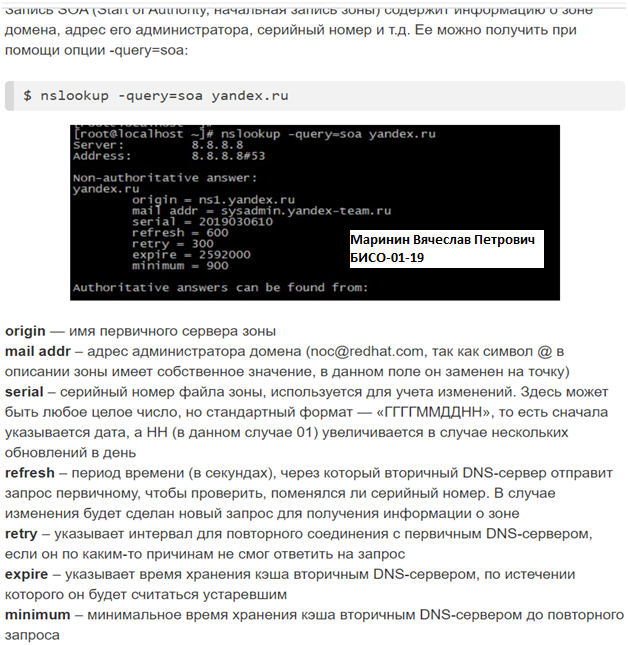


### 3) Изучить аргументы утилиты nslookup: -query=mx, soa, nx; type=any.

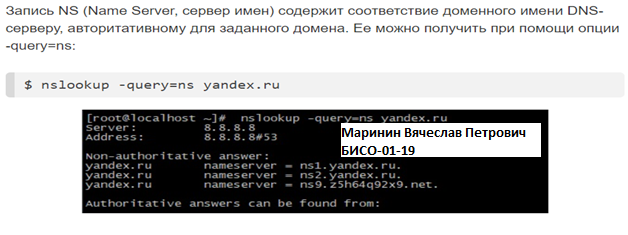
### 3.1) -query=mx



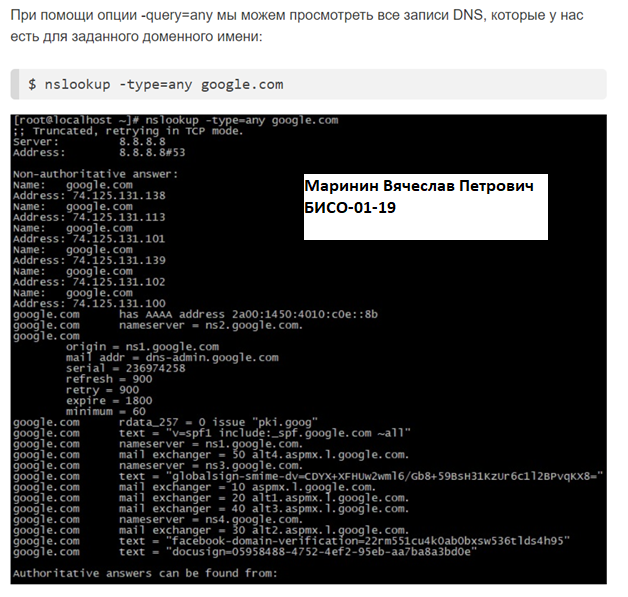
**3.2) –query=soa**



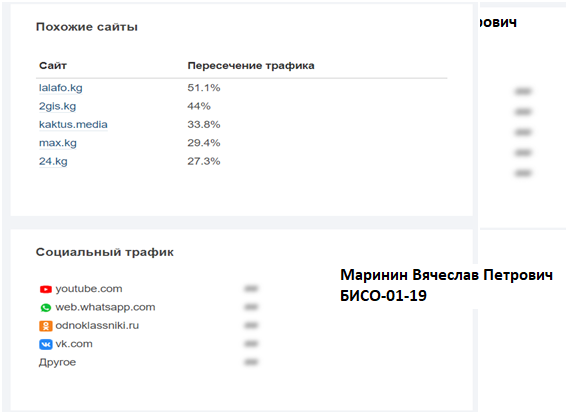
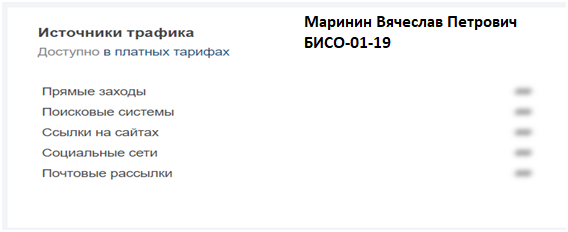
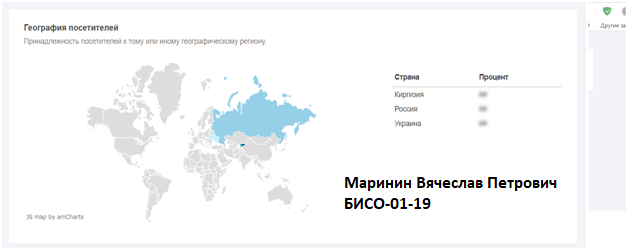
**3.3) –query=nx**



**3.4) type=any**



**4)** **Изучить трафик с сайта.**

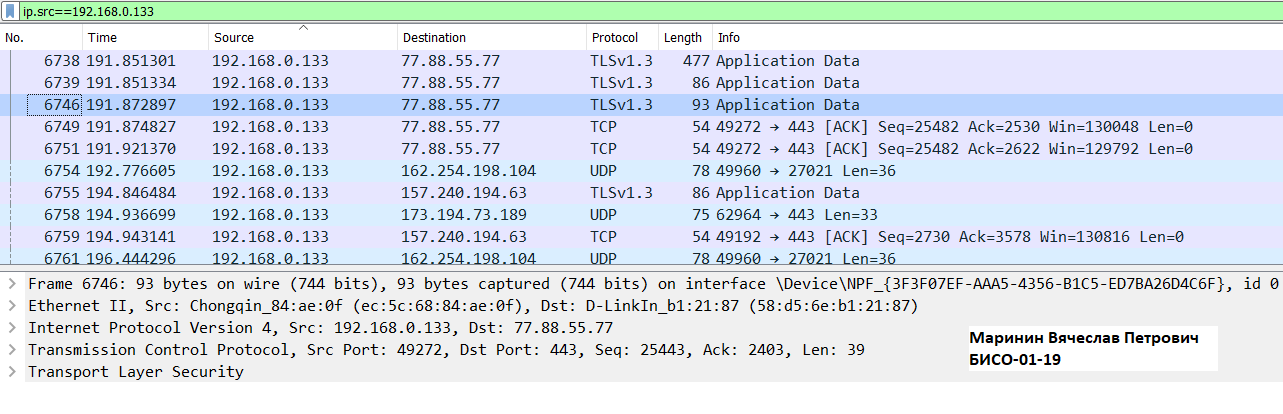


**5)** **В wireshark изучить основные фильтры типа: ip.src==192.168.0.163; ip.dst;**

**ip.addr, udp.port, arp.src hw\_mac, eth.dst, eth.src.**

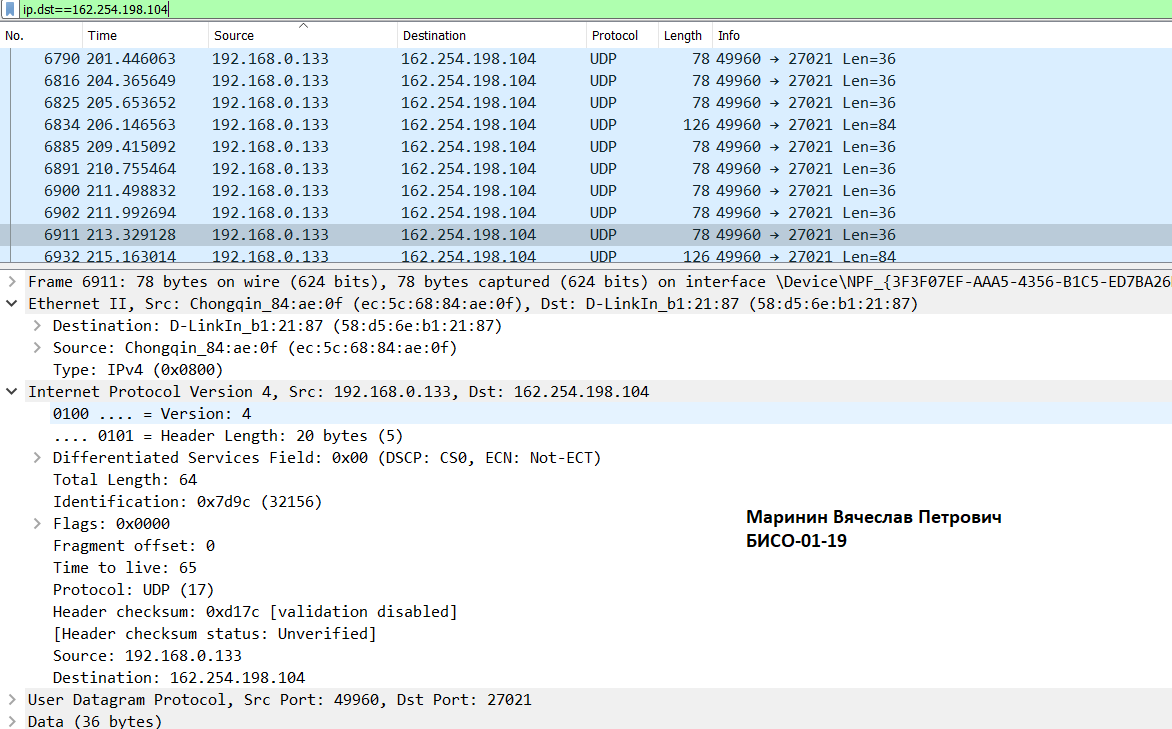
**5.1) ip.src==192.168.0.133**

Фильтрация пакетов по IP-адресу отправителя



**5.2) ip.dst**

Фильтрация пакетов по IP-адресу получателя



**5.3) ip.addr**

Определение пакетов вне зависимости от направления трафиков

**5.4)udp.port**

UDP порт получателя или отправителя

**5.5) arp.src hw\_mac**

Протокол ARP – MAC-адрес получателя

**5.6) eth.dst**

MAC-адрес получателя

**5.7) eth.src**

MAC-адрес отправителя