РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

Анализ трафика в Wireshark

дисциплина: Сетевые технологии

Студент: Саргсян Арам Грачьяевич

Группа: НПИбд 02-20

МОСКВА

2022 г.

ЦЕЛЬ РАБОТЫ:

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP

ХОД РАБОТЫ

1. С помощью команды ipconfig /all вывел полную информацию о моем текущем соединении. (Рис. 1)

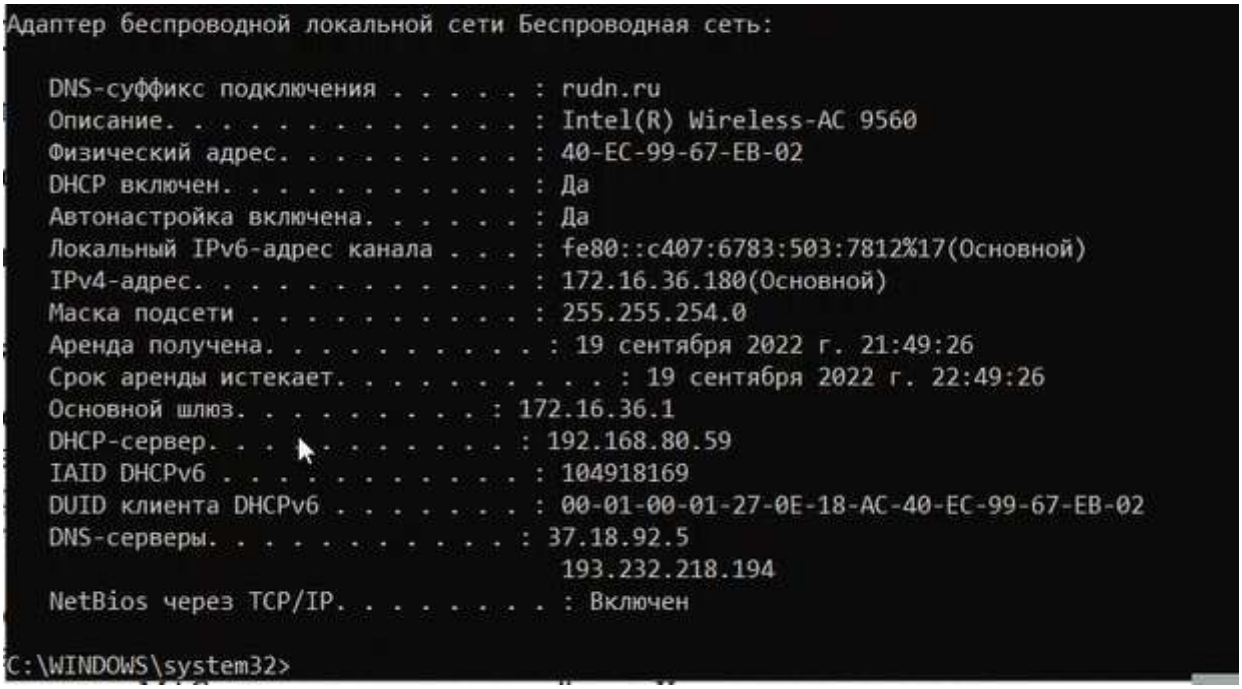

Рис. 1

2. Определил Mac-адреса (Физические адреса) своих устройств. Первые три байта определяют производителя. Последние сетевой три интерфейс устройства. Адреса глобальные и индивидуальные. (Рис. 2). Например(40-EC-99)—производитель (Intel), а (-67-EB-02)—сетевой интерфейс.

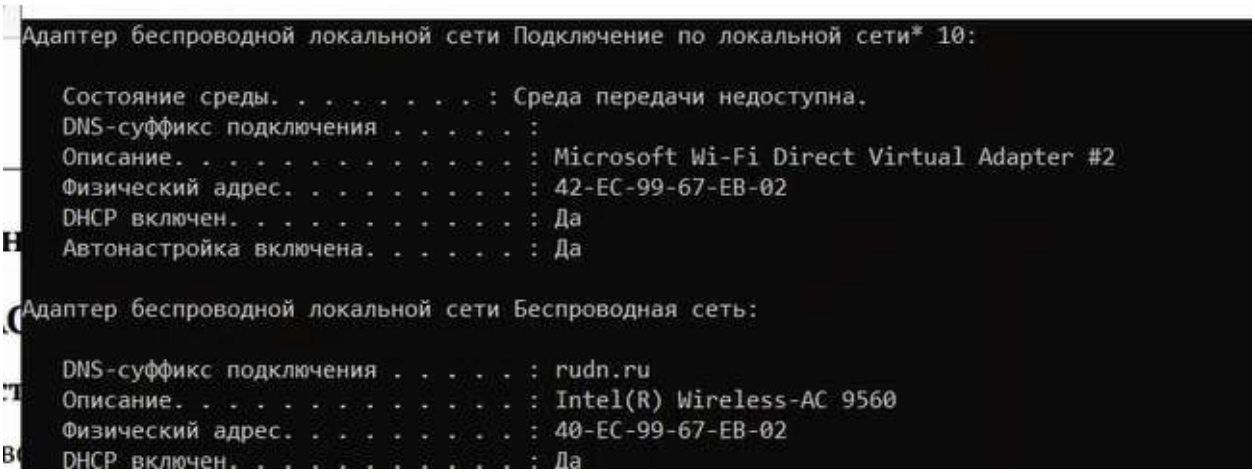

Рис. 2

3. Установил Wireshark, выбрал нужный сетевой интерфейс, запустил захват трафика. В

командной строке пропинговал шлюз по умолчанию. (Рис. 3)

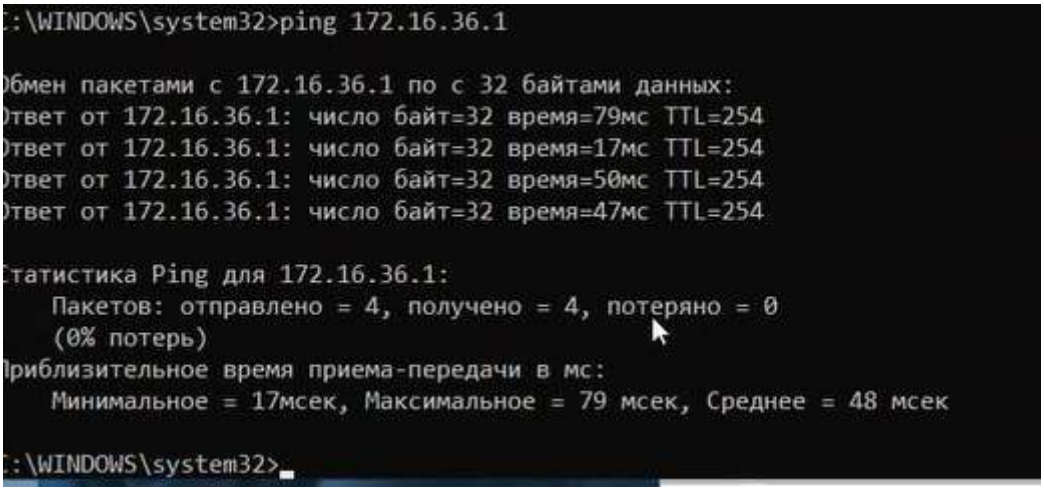

рис. 3

4. В Wireshark остановил захват трафика. В строке фильтра прописал фильтр arp or icmp. Проанализировал эти файлы. (Рис. 4-6)

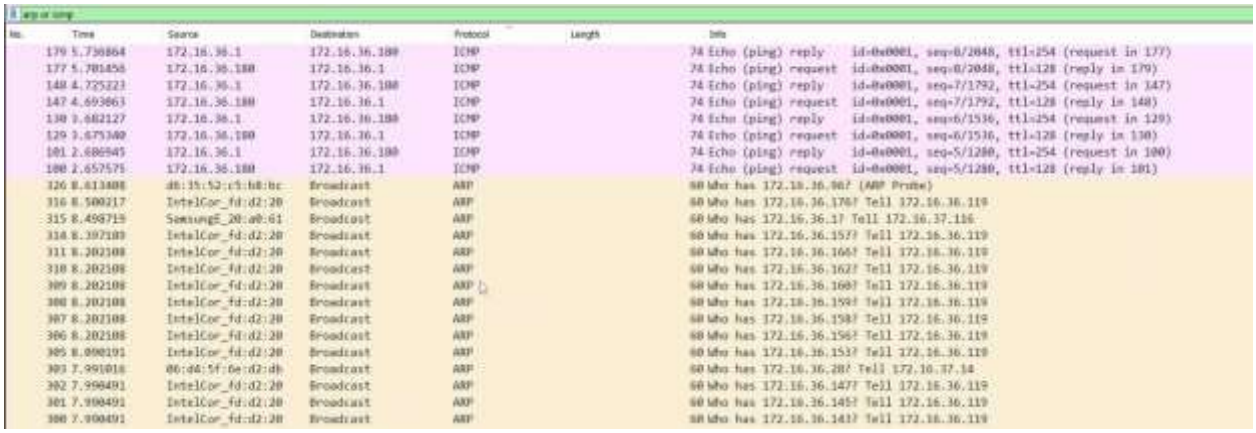

Рис. 4

5. При эхо-запросе мы имеем следующие данные. Второй тип Ethernet. Длина кадра — 74. Mac-адрес источника — 40:ec:99:67:9c:d2. Mac-адрес шлюза — 70:18:a7:60:9c:d2. Оба адреса глобальные и индивидуальные. (Рис. 5).

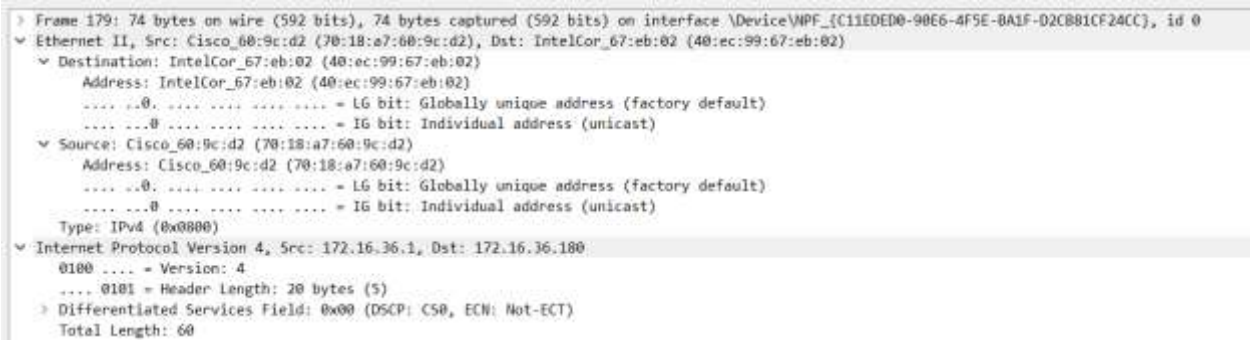

Рис. 5

6. При эхо-ответе у нас просто поменялись местами шлюз и источник. (Рис. 6).

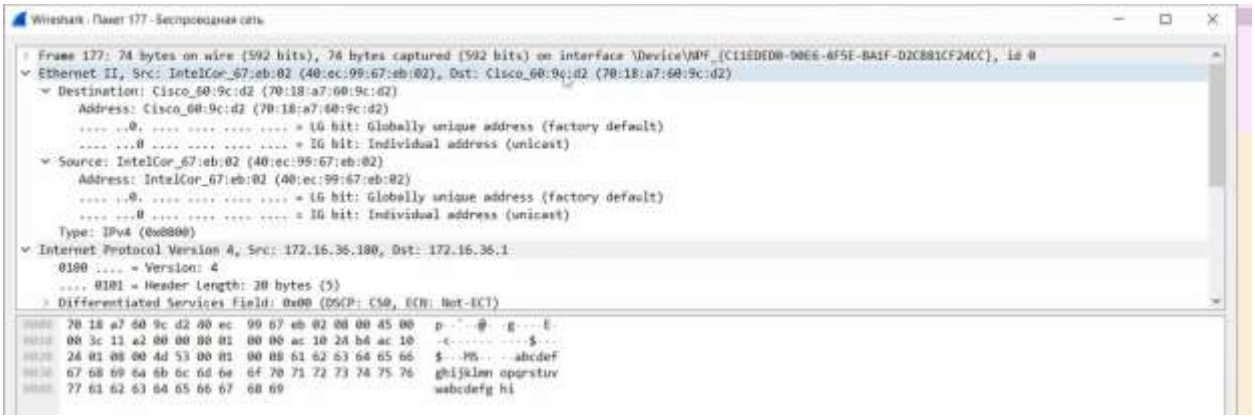

Рис. 6

7. Проанализировал файл с протоколом ARP. Изучил данные в заголовке Ethernet. Мы имеем следующие данные. Второй тип Ethernet. Длина кадра — 74. Mac-адрес источника — d6:35:52:c5:b8:bc. Mac-адрес шлюза — ff:ff:ff:ff:ff:ff. Такой адрес означает, что он доступен для всех компьютеров сети. Источник локальный индивидуальный. Шлюз локальный групповой. (Рис. 7)

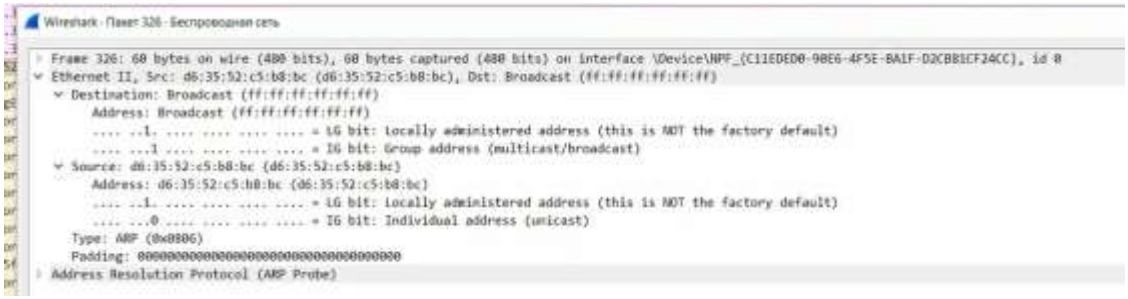

рис. 7

8. Начал новый процесс захвата трафика. Пропинговал сайт mail.ru. Остановил захват трафика. (Рис. 8)

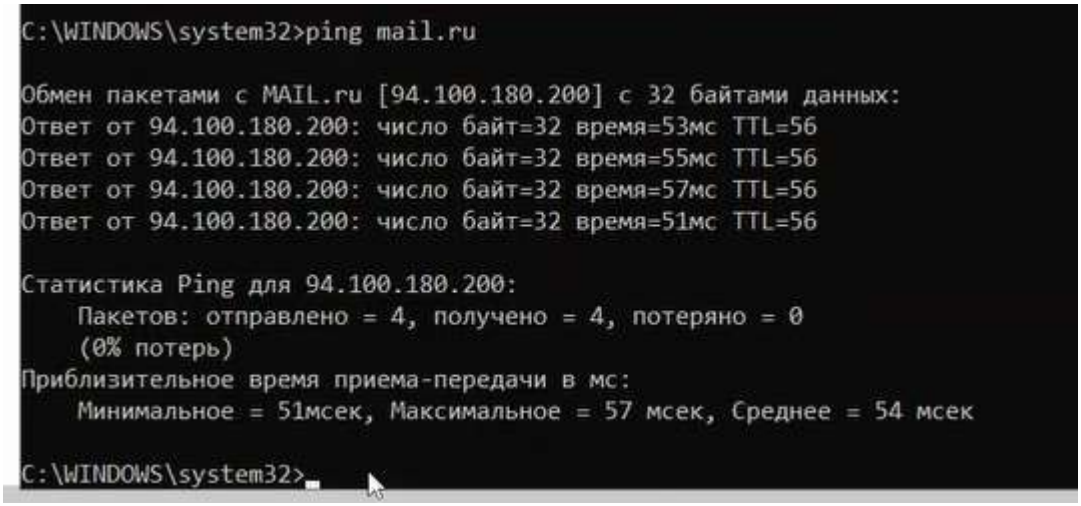

рис. 8

9. Получил следующую информацию. Mac-адрес источника — 70:18:a7:60:9c:d2. Mac-адрес шлюза — 40:ec:99:67:eb:02. Оба адреса глобальные индивидуальные. (Рис. 9)

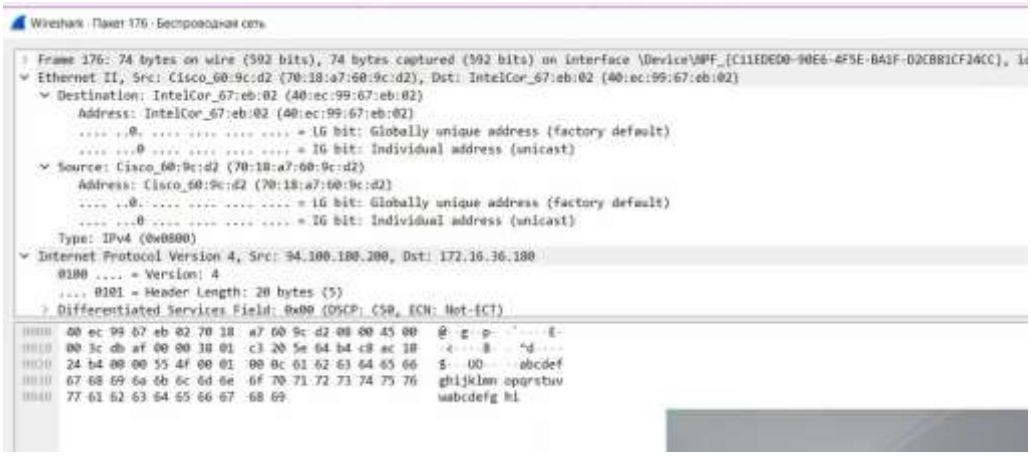

рис. 9

10. Запустил Wireshark, начал захват. Открыл сайт CERN, работающий по протоколу HTTP. Потыкал по разделам сайта. В Wireshark в строке фильтра указал http. (Рис. 10)

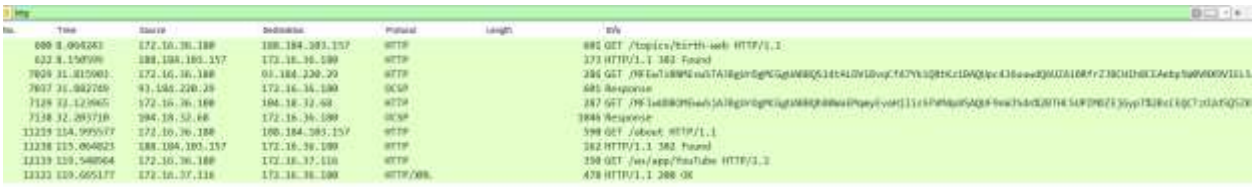

Рис. 10

11. Проанализировал информацию в случае запроса. Mac-адрес источника — 40:ec:99:67:eb:02. Mac-адрес шлюза —70:18:a7:60:9c:d2. Оба адреса глобальные индивидуальные. Длина кадра 601. (Рис. 11)

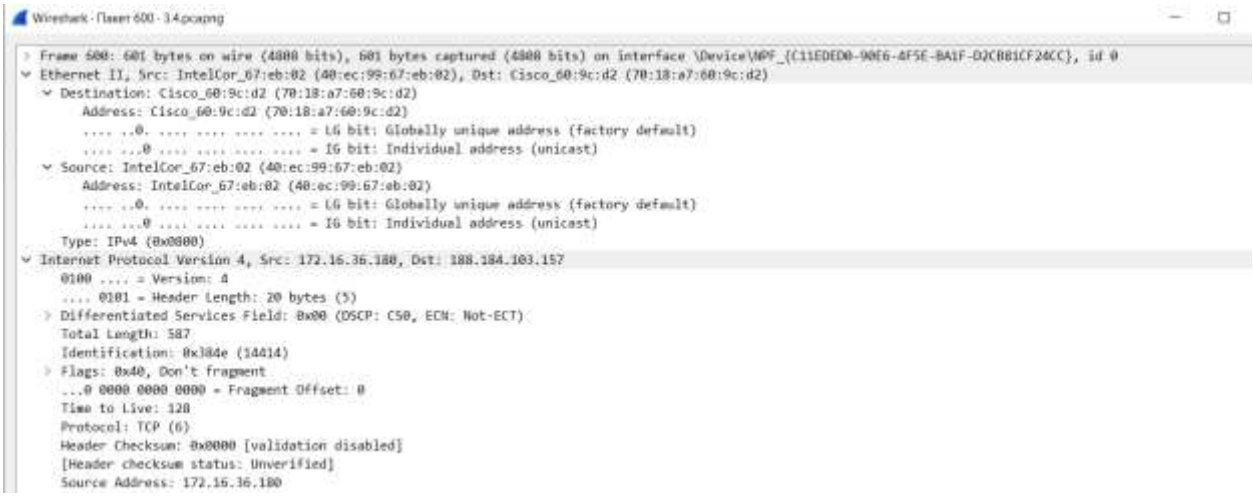

Рис. 11

12. Получил следующую информацию при. Mac-адрес источника — 70:18:a7:60:9c:d2. Mac-адрес шлюза — 40:ec:99:67:eb:02. Оба адреса глобальные индивидуальные. Длина кадра —173. (Рис. 12)

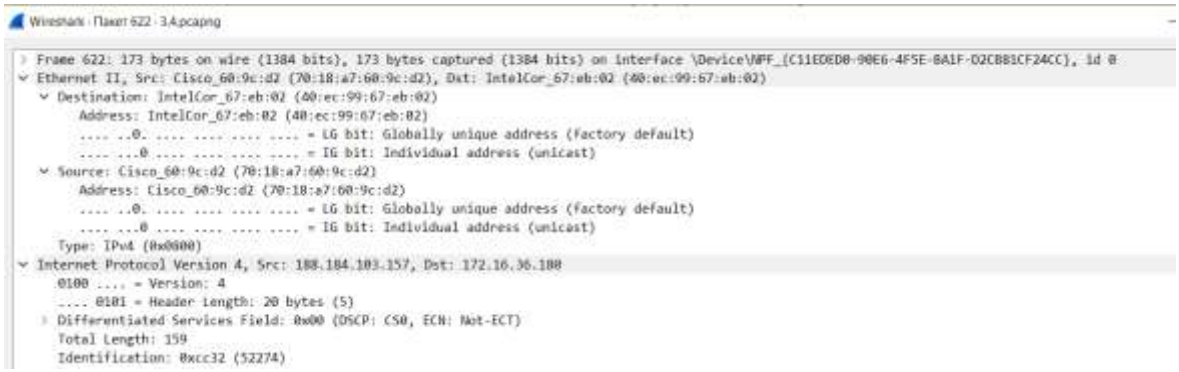

рис. 12

13. Прописал в фильтре протокол DNS. Нашёл информацию в случае запроса. Длина кадра—93. Mac-адреса — 70:18:a7:60:9c:d2. Mac-адрес шлюза — 40:ec:99:67:eb:02, и наоборот в ответе. IP источника 172.16.36.180, шлюза, 37.18.92.5. (Рис. 13-14).

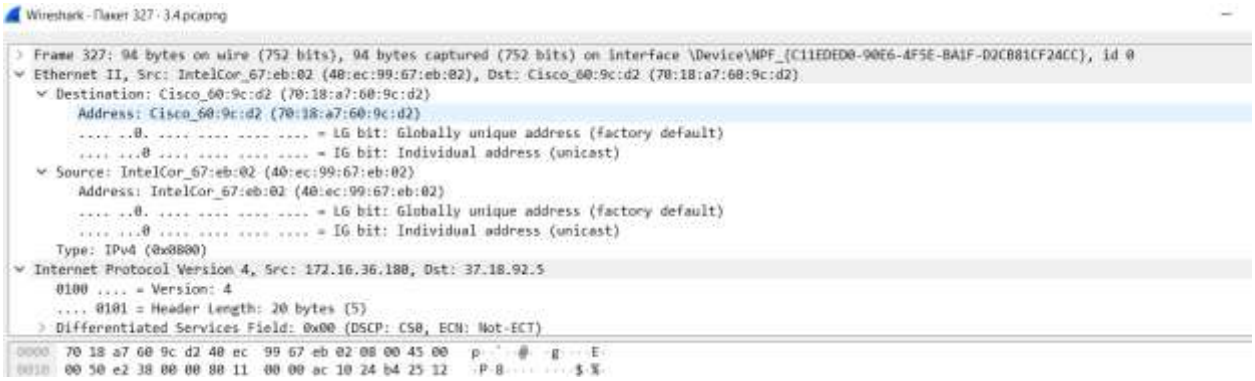

Рис. 13

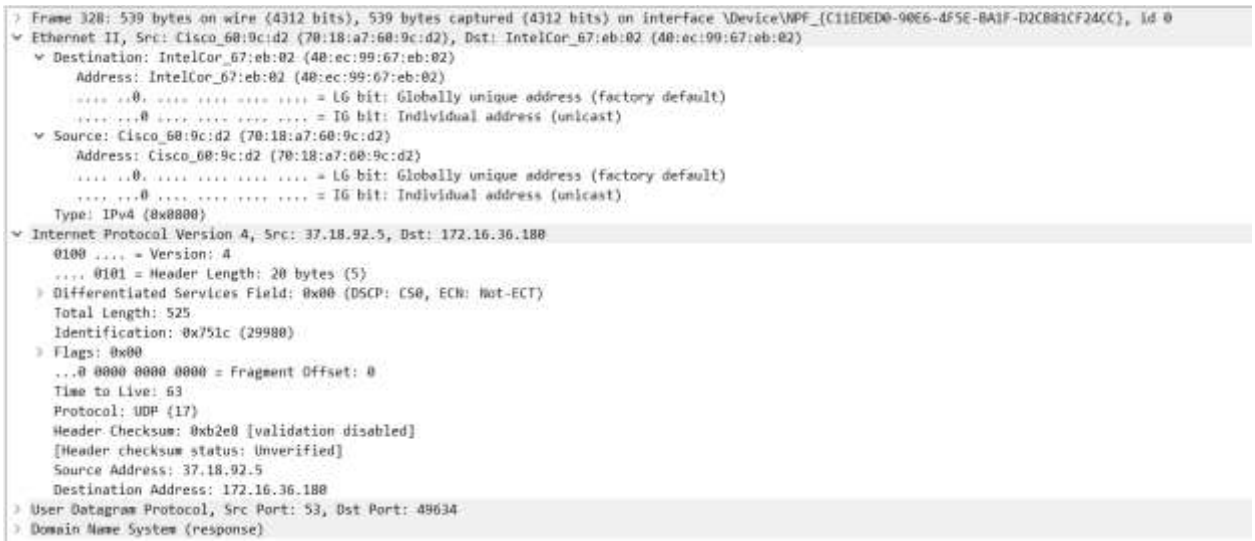

Рис. 14

14. Попробовал ввести фильтр quic. Программа не нашла файлов с этим протоколом. (Рис. 15).

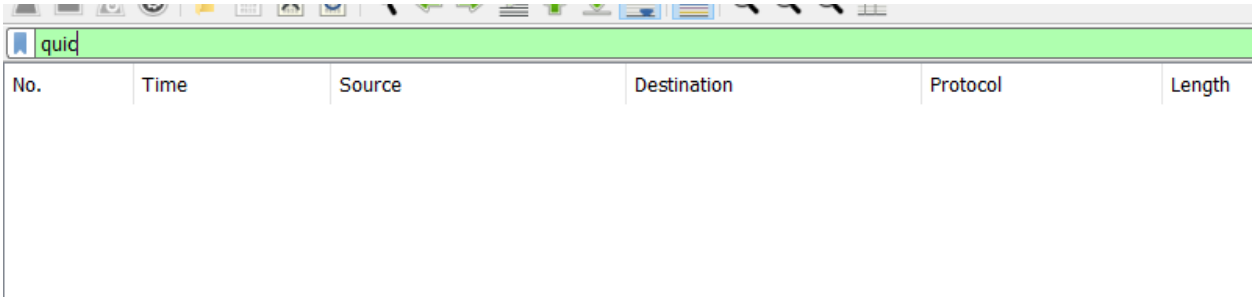

Рис. 15

ВЫВОД

Я изучил посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP. Понял, как найти Mac-адреса, их типы и другую информацию. Разобрался с протоколами ARP, ICMP, QUIC, HTTP.