

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 Грачьевич

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)

```
Адаптер беспроводной локальной сети Беспроводная сеть:
DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Intel(R) Wireless-AC 9560
Физический адрес. . . . . : 40-EC-99-67-EB-02
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::c407:6783:503:7812%17(Основной)
IPv4-адрес. . . . . : 172.16.36.180(Основной)
Маска подсети . . . . . : 255.255.254.0
Аренда получена. . . . . : 19 сентября 2022 г. 21:49:26
Срок аренды истекает. . . . . : 19 сентября 2022 г. 22:49:26
Основной шлюз. . . . . : 172.16.36.1
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 104918169
DUID клиента DHCPv6 . . . . . : 00-01-00-01-27-0E-18-AC-40-EC-99-67-EB-02
DNS-серверы. . . . . : 37.18.92.5
                        193.232.218.194
NetBios через TCP/IP. . . . . : Включен

C:\WINDOWS\system32>
```

Рис. 1

2. Определил Мас-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.

```
Адаптер беспроводной локальной сети Подключение по локальной сети* 10:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : 42-EC-99-67-EB-02
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:
DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Intel(R) Wireless-AC 9560
Физический адрес. . . . . : 40-EC-99-67-EB-02
DHCP включен. . . . . : Да
```

Рис. 2

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

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

```
C:\WINDOWS\system32>ping 172.16.36.1

Обмен пакетами с 172.16.36.1 по 32 байтами данных:
Ответ от 172.16.36.1: число байт=32 время=79мс TTL=254
Ответ от 172.16.36.1: число байт=32 время=17мс TTL=254
Ответ от 172.16.36.1: число байт=32 время=50мс TTL=254
Ответ от 172.16.36.1: число байт=32 время=47мс TTL=254

Статистика Ping для 172.16.36.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 17мсек, Максимальное = 79 мсек, Среднее = 48 мсек

C:\WINDOWS\system32>
```

рис. 3

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

No.	Time	Source	Destination	Protocol	Length	Info
176	5.730864	172.16.36.1	172.16.36.180	ICMP		74 Echo (ping) reply id=0x0001, seq=0/2048, ttl=254 (request in 177)
177	5.701456	172.16.36.180	172.16.36.1	ICMP		74 Echo (ping) request id=0x0001, seq=0/2048, ttl=128 (reply in 179)
148	4.725223	172.16.36.1	172.16.36.180	ICMP		74 Echo (ping) reply id=0x0001, seq=7/1792, ttl=254 (request in 147)
147	4.693663	172.16.36.180	172.16.36.1	ICMP		74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 148)
130	3.602127	172.16.36.1	172.16.36.180	ICMP		74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=254 (request in 129)
129	3.679309	172.16.36.180	172.16.36.1	ICMP		74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 130)
101	2.606945	172.16.36.1	172.16.36.180	ICMP		74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=254 (request in 100)
100	2.657575	172.16.36.180	172.16.36.1	ICMP		74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 101)
126	8.613408	40:15:52:c1:b8:bc	Broadcast	ARP		60 Who has 172.16.36.180? (ARP Probe)
316	8.500217	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.170? Tell 172.16.36.119
315	8.458719	SamsungE_20:a0:61	Broadcast	ARP		60 Who has 172.16.36.17 Tell 172.16.36.119
314	8.397189	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.157? Tell 172.16.36.119
311	8.302308	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.166? Tell 172.16.36.119
310	8.202308	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.162? Tell 172.16.36.119
309	8.202108	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.160? Tell 172.16.36.119
308	8.202108	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.159? Tell 172.16.36.119
307	8.202108	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.158? Tell 172.16.36.119
306	8.202108	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.156? Tell 172.16.36.119
305	8.090191	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.153? Tell 172.16.36.119
303	7.991016	00:04:5f:6e:d2:4b	Broadcast	ARP		60 Who has 172.16.36.28? Tell 172.16.36.119
302	7.990491	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.147? Tell 172.16.36.119
301	7.990491	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.145? Tell 172.16.36.119
300	7.990491	IntelCor_fd:d2:20	Broadcast	ARP		60 Who has 172.16.36.141? Tell 172.16.36.119

Рис. 4

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

```
> Frame 179: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C11EDED0-90E6-4F5E-8A1F-D2CB81CF24CC}, id 0
  ▾ Ethernet II, Src: Cisco_60:9c:d2 (70:18:a7:60:9c:d2), Dst: IntelCor_67:eb:02 (40:ec:99:67:eb:02)
    ▾ Destination: IntelCor_67:eb:02 (40:ec:99:67:eb:02)
      Address: IntelCor_67:eb:02 (40:ec:99:67:eb:02)
      ..0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    ▾ Source: Cisco_60:9c:d2 (70:18:a7:60:9c:d2)
      Address: Cisco_60:9c:d2 (70:18:a7:60:9c:d2)
      ..0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  ▾ Internet Protocol Version 4, Src: 172.16.36.1, Dst: 172.16.36.180
    0100 .... = Version: 4
    ....0101 = Header Length: 20 bytes (5)
    ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 60
```

Рис. 5

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

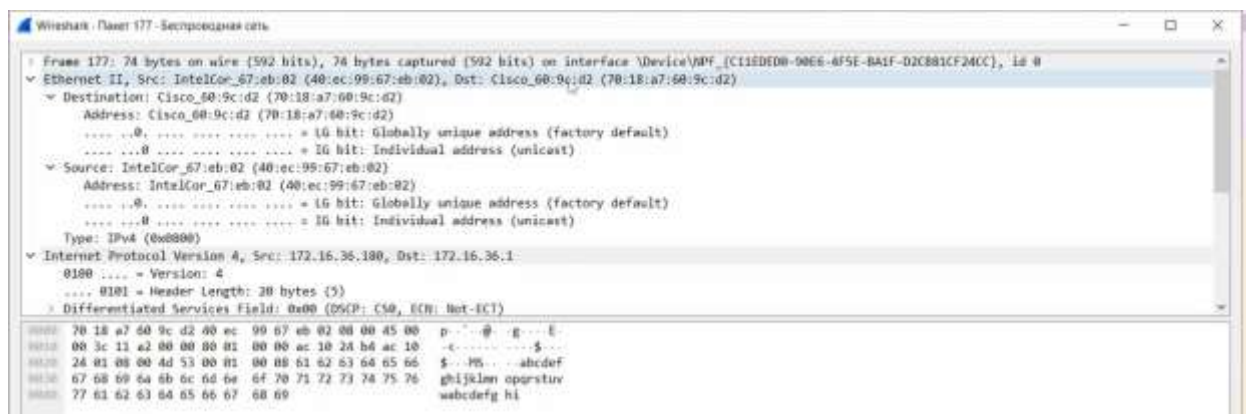


Рис. 6

7. Проанализировал файл с протоколом ARP. Изучил данные в заголовке Ethernet. Мы имеем следующие данные. Второй тип Ethernet. Длина кадра — 74. Мас-адрес источника — d6:35:52:c5:b8:bc. Мас-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)

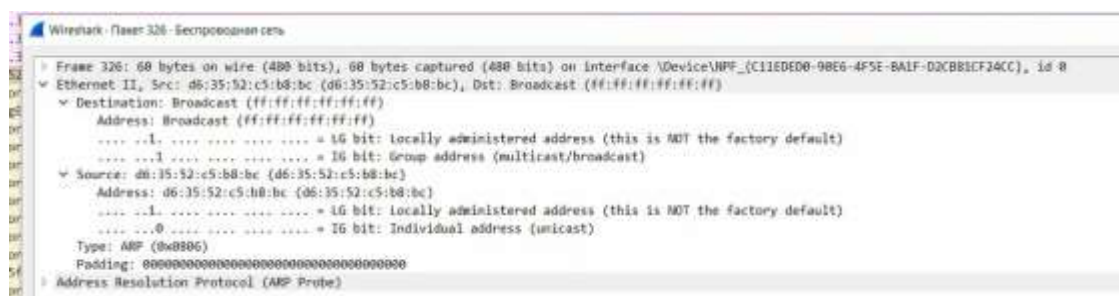


рис. 7

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

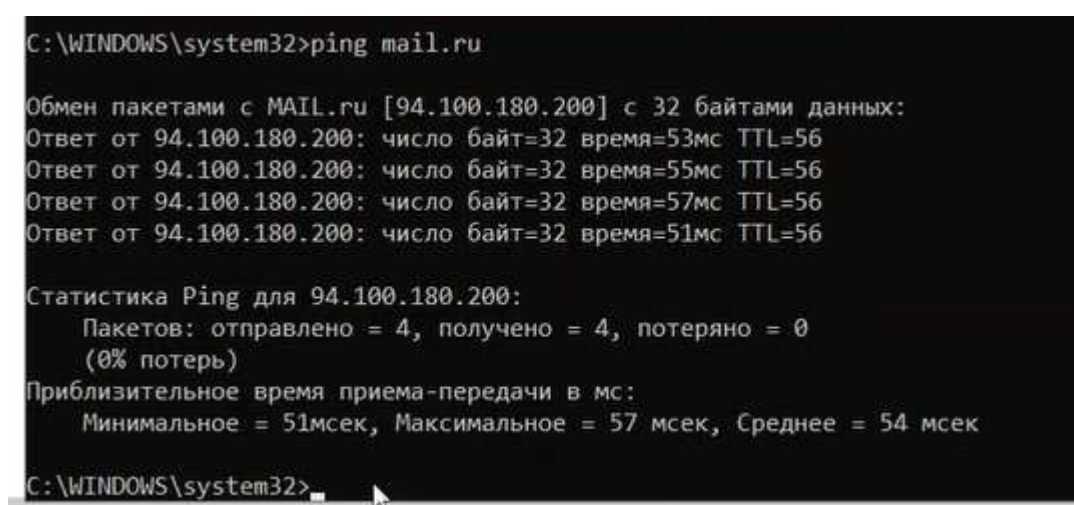


рис. 8

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

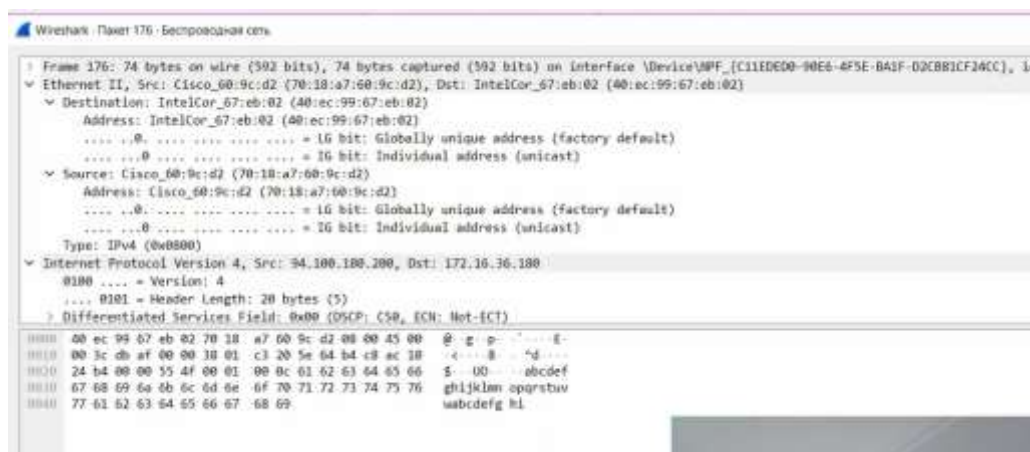


рис. 9

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)

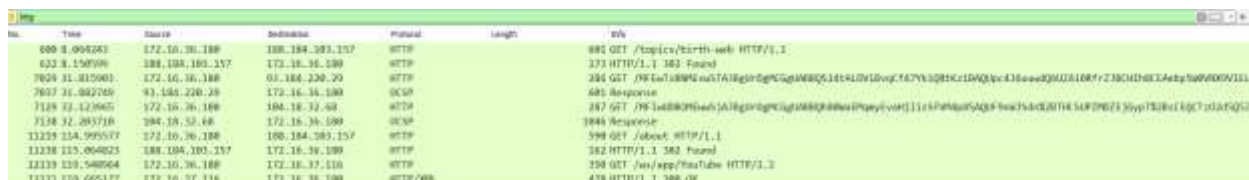


Рис. 10

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

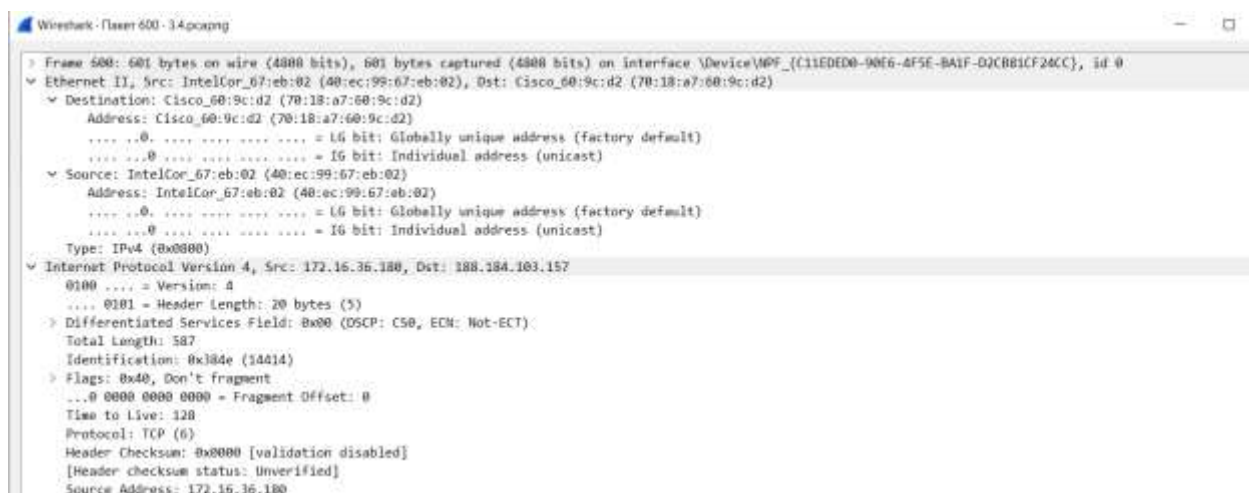


Рис. 11

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

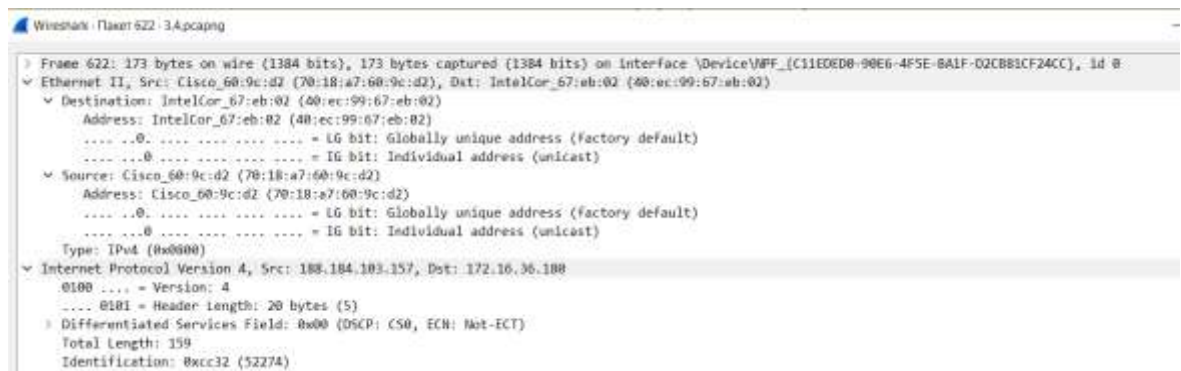


рис. 12

13. Прописал в фильтре протокол DNS. Нашёл информацию в случае запроса. Длина кадра—93. Мас-адреса — 70:18:a7:60:9c:d2. Мас-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).

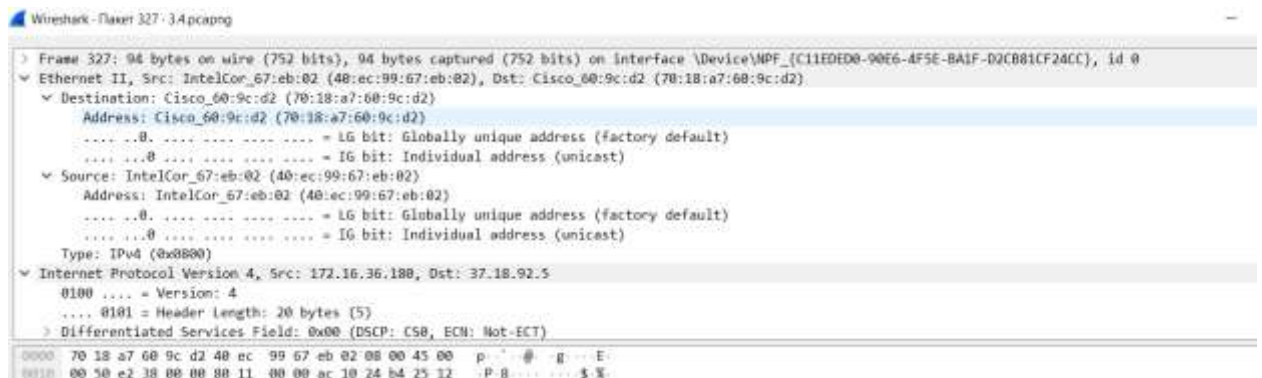


Рис. 13

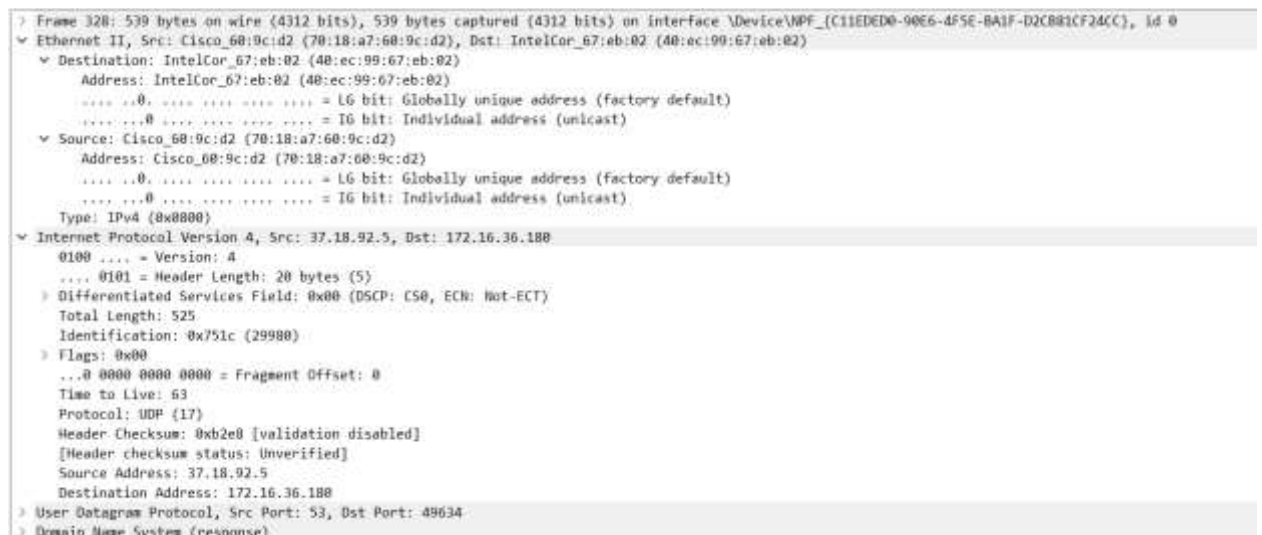


Рис. 14

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

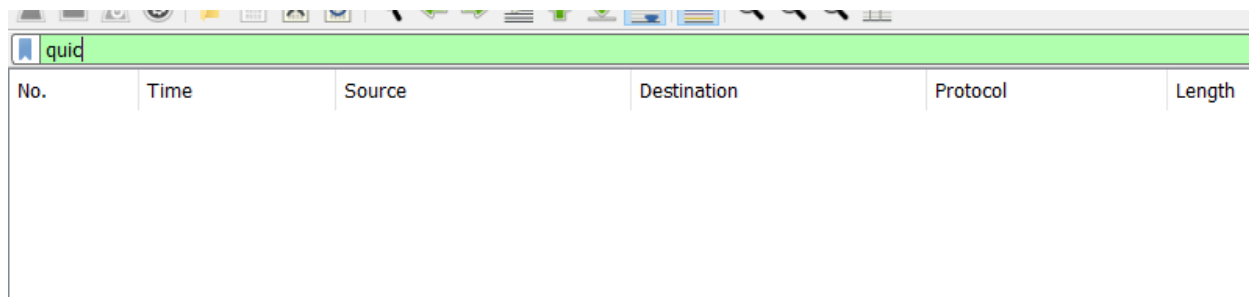


Рис. 15

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.