Отчет по лабораторной работе № 3

Анализ трафика в Wireshark

Бызова Мария Олеговна 2025-09-05

Содержание і

1 Цель работы

Целью данной работы является изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

С помощью команды ipconfig выведем информацию о текущем сетевом соединении (рис. 1)

```
C:\Windows\system32> ipconfig

Настройка протокола IP для Windows

Неизвестный адаптер Подключение по локальной сети:

Состояние среды. . . . . : Среда передачи недоступна.

DNS-суффикс подключения . . . :

Состояние среды . . . . . : Среда передачи недоступна.

DNS-суффикс подключения . . . :

Адаптер Ethernet Ethernet 2:
```

Рисунок 1: Вывод информации о текущем сетевом соединении.

Теперь используем разные опции команды (рис. 2 - 5)

```
\Windows\system32> inconfig /all
эстройка протокола TP лля Windows
 MM8 KOMDINITEDA . . . . . . . . . . . DESKTOP-URALIATR
 IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . . : Нет
Порядок просмотра суффиксов DNS . : rudn.ru
еизвестный адаптер Подключение по локальной сети:
Состояние среды. . . . . . . . Среда передачи недоступна.
DNS-суффикс полключения . . . . . :
DHCP включен. . . . . . . . . . . . . . . . . . .
ganten Ethernet Ethernet:
Состояние среды. . . . . . . . . . . . Среда передачи недоступна.
DNS-суффикс подключения . . . . . .
Onecase Connection (16) I219-LM
Автонастройка включена. . . . . . . . . . Да
anten Ethernet Ethernet 2:
```

Рисунок 2: Отображение полной конфигурации TCP/IP для всех адаптеров.

Рисунок 3: Отображение содержимого кэша сопоставителя DNS-клиента, включающее как записи, предварительно загруженные из локального файла Hosts, так и все недавно полученные записи ресурсов для запросов имен, разрешенных компьютером.

```
C:\Mindows\system32> ipconfig /registerdns

Macrooke προτοκοε IP для Mindows

Mariar регистрация залисей ресурсов DMS для всех адаптеров этого компьютера. Отчет об ошибках будет выведен в ожне "Просмотр событий" через 15 минут.

C:\Mindows\system32>
```

Рисунок 4: Инициализация динамической регистрации вручную для DNS-имен и IP-адресов, настроенных на компьютере

```
C:\Windows\system32> ірсопfig /showclassid *

Настройка протокола IP для Windows

Не удается изменить код класса DKCPv4 для адаптера Подключение по локальной сети: Не удается найти указанный файл.

Не удается изменить код класса DKCPv4 для адаптера Ethernet: Не удается найти указанный файл.

Нет классов DKCPv4, определенных для Ethernet 2.

Не удается изменить код класса DKCPv4 для адаптера ОремVPH Connect DCO Adapter: Не удается найти указанный файл.

Не удается изменить код класса DKCPv4 для адаптера Подключение по локальной сети 9: Не удается найти указанный файл.

Не удается изменить код класса DKCPv4 для адаптера Подключение по локальной сети 10: Не удается найти указанный файл.

Нет классов DKCPv4, определенных для Беспроводная сеть.

Не удается изменить код класса DKCPv4 для адаптера Сетевое подключение Bluetooth: Не удается найти указанный файл.

Не удается изменить код класса DKCPv4 для адаптера Сетевое подключение Bluetooth: Не удается найти указанный файл.

С: Windows\system32>
```

Рисунок 5: Отображение идентификатора класса DHCP для указанного адаптера.

Определим MAC-адреса сетевых интерфейсов на нашем компьютере с помощью команды GETMAC (рис. 6)



Рисунок 6: Определение МАС-адреса сетевых интерфейсов на нашем компьютере.

Установим на нашем устройстве Wireshark (рис. 7)

PS C:\Windows\system32> choco install wireshark

Рисунок 7: Установка на нашем устройстве Wireshark.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (рис. 8)

Рисунок 8: Запуск Wireshark. Выбор активного сетевого интерфейса.

На нашем устройстве в консоли определим с помощью команды ipconfig IP-адрес устройства и шлюз по умолчанию (рис. 9)

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . : rudn.ru
Локальный IPv6-адрес канала . . : fe80::c19f:aa15:e013:b32e%23
IPv4-адрес . . . . . . : 192.168.214.191
Маска подсети . . . . . : 255.255.224.0
Основной шлюз . . . . : 192.168.192.1

Адаптер Ethernet Сетевое подключение Bluetooth:
```

Рисунок 9: Определение ІР-адреса устройства и шлюза по умолчанию.

На нашем устройстве в консоли с помощью команды ping пропингуем шлюз по умолчанию (рис. 10)

```
C:\Windows\system32>ping 192.168.192.1
Обмен пакетами с 192.168.192.1 по с 32 байтами данных:
Ответ от 192.168.192.1: число байт-32 время-1мс ТТL-254
Ответ от 192.168.192.1: число байт-32 время-1мс ТТL-254
Ответ от 192.168.192.1: число байт-32 время-5мс ТТL-254
Ответ от 192.168.192.1: число байт-32 время-61мс ТТL-254
Статистика Ping для 192.168.192.1:
Пакетон: отправлено - 4, получено - 4, потеряно = 0
(0% потеры время приема-передачи в мс:
Приникальное время приема-передачи в мс:
Приникальное время приема-передачи в мс:
С:\Windows\system32>
```

Рисунок 10: Пинг шлюза по умолчанию.

В Wireshark остановим захват трафика. В строке фильтра пропишем фильтр arp or icmp и убедимся, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с нашего устройства на шлюз по умолчанию (рис. 11)

```
Закват из Беспроводная сеть.
                                                                                                                                                                                                                                                                                                                         g ×
 Файл Позвяд Вид Запуск Закват Аналио Статистика Телефония Беспроводная связь. Инструменты Справка
 Broadcast ARP 42 Gratuitous ARP for 192.168.201.226 (Reply)
        49 22.550258 Cisco_63:c1:60
                                                                   Broadcast ARP 42 Gratuitous ARP for 192,168,198,96 (Reply)
         63 24.012479 Cisco 63:c1:60
                                                                   87 44,783356 Cisco 63:c1:60
         98 57,132750 Ciaco 63:c1:60
                                                                  Broadcast AMP 42 Gratuitous AMP for 192.168.214.176 (Reply)
       188 56.212490 Cisco 63:c1:60
       182 188 788529 192 168 214 191 192 168 192 1 TOPP 74 Echo (nine) pages 8 idebr@001 secur8/4688 111-128 (punty in 183)
       183 180 791980 192 168 192 1 192 168 214 191 IOP 74 Etho (ping) reply id-0x8001, seq-18/4600, ttl-254 (request in 182)
  = 184 101.795741 192.168.214.191 [92.168.192.1 [DPP 74 Etho (ping) request idubw0001, seq.19/6864, ttl=128 (reply in 185)
       185 101.801012 192.168.192.1
                                                                   192.168.214.191 IOP
                                                                                                                    74 Echo (ping) reply id-0x0001, seg-19/4864, ttl=254 (request in 184)
        209 102.705987 102.165.214.191 192.165.192.1 IOP 74 5the (nine) request id-the9081, sen-20/5120, ttl=128 (repely in 210)
        218 182 888859 192 168 192 1
                                                                   192,168,214,191 ICPP 74 Echo (ping) reply id-9x0001, sep-28/5120, ttl=254 (remeat in 200)
       311 103 003384 103 168 314 101
                                                                  192.168.192.1 IOP 74 Echo (ping) request 16-0x0001, sea=21/5176, ttl=128 (reply in 212)
                                                                 | 19.10.11.12.1 | 10P | 14 (On (19.10) vegant 1-de-bids), red-17.9%, (11.12) (vega) is 223) | 19.11.01.12.13 | 10P | 14 (On (19.10) vegal 1-de-bids), red-17.9%, (11.12) (vegat 1-de-bids) | 19.11.01.12.13 | 10P 
        212 103 804528 192 168 192 1
        433 110,0001EG Cisco_65;c1;60
        477 116.668211 Ciaco 63:c1:68
        516 129 587562 Circo 631c1168
       517 129.828753 Cisco 63:c1:68
       $30 137 861381 Circo 631/1/60
    Frame 184: 74 butes on vice (502 bits). 74 butes captured (502 bits) on interface (Device)ARE (5534)228 | 2000 78 18 a7 58 9s ab 80 93 37 80 28 dc 88 98 45 80 m.
   Ethernet II, Src: Intel_00:28idc (00:93:37:00:28idc), Ost: Cisco_60:9c:eb (70:18:27:60:9c:eb) | 00:10: 00 3c df 90 00:00 00 10: 00 00 c0 ald db bf c0 all c
                                                                                                                                                                     0010 40 01 00 00 44 48 00 01 00 13 61 63 65 65 65 ... Mt. ... who def
     Internet Protocol Version 4. Sec. 192.168.214.191. Det: 192.168.192.1
                                                                                                                                                                    0010 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklen opgratuv
    Internet Control Message Protocol
                                                                                                                                                                   0040 77 61 62 63 64 65 66 67 68 69
                                                                                                                                                                                                                                                             wabcdefg hi
```

Рисунок 11: Остановка захвата трафика. Фильтр arp or icmp.

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark (рис. 12 - 13)

```
- 622 96.618183 192.168.214.191
                                          192,168,192,1
                                                                          74 Echo (ping) request id:8x80001, seq:21/5376, ttl:128 (reply in 623)
     623 96.639688
                                                              TOPP
                                                                          74 Echo (ping) reply id=0x0001, seq=21/5376, ttl=254 (request in 622)
     627 97 654215 192 168 214 191 192 168 192 1
                                                             TONE
                                                                         74 Echo (nine) request idebr@@ft. seq=22/5632, ##1=128 (reply in 628)
v Frame 622: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NFF_(E5143228 | 0010 70 18 a7 60 % ob 00 93 37 00 28 dc 08 00 45 00 p · · · · · 7. ( · · E
     Section number: 1
                                                                                                         0010 00 3c 75 ba 00 00 80 01 00 00 c0 a8 d6 bf c0 a8
   ) Interface 14: 0 (\Device\MPF (E6343E28-ED2D-4447-82ED-900E116EC7C4))
     Incapsulation type: Ethernet (1)
     Arrival Time: Oct 7, 2025 18:02:25.887595000 RTZ 2 (arms)
     UTC Arrival Time: Oct 7, 2825 15:82:25.887595888 UTC
     Epoch Arrival Time: 1759849145.887595000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 1.441934888 seconds]
     [Time delta from previous displayed frame: 1.650293000 seconds]
     [Time since reference or first frame: 96.638183800 seconds]
     Franc Humber: 622
     Frame Length: 74 bytes (592 bits)
     Canture Length: 74 bytes (592 bits)
     [from is marked: false]
      [Frame is ignored: False]
     [Protocols in frame; eth; ethertype; ip; icep; data]
     [Coloring Rule Name: ICMP]
     [Coloring Bule String: icmp || icmpv61
 V Ethernet II. Ser: Intel 80:28 dc (80:93:37:00:28:dc). Dat: Claro 60:9c:eb (70:18:a7:60:9c:eb)
   > Destination: Cisco_60:9c;eb (78:18:a7:68:9c;eb)
   > Source: Intel 80:28:dc (80:93:37:00:28:dc)
     Type: Thut (Bubbbb)
     (Stream Index: 0)
  Internet Protocol Varsion 4, Sec. 192,168,214,191, Dat. 192,168,192.1
Internet Control Bessare Protocol
```

Рисунок 12: Кадр ICMP — эхо-запрос.

```
192,168,214,191
                                                                             74 Echo (ping) reply id=0x0001, seq=21/5376, ttl=254 (request in 622)
                                                                             74 Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 628)
V Frame 623: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \(\text{Device\BPS} (F6541628) \) 0000 \(\text{00} 0.01 17 00 28 ds 70 18 s/ 60 0s eb 00 00 45 00
                                                                                                              0010 00 3c 75 ba 00 00 fe 01 2c f4 c0 a8 c0 01 c0 a8 0020 d6 bf 00 00 55 46 00 01 00 15 61 62 63 64 65 66
     Section number: 1
                                                                                                                                                                         UE abodef
  > Interface id: 0 (\Device\NFF (E6363E28-FD2D-4647-B2FD-980F116FC7C4))
                                                                                                              0010 67 68 69 6a 6b 6c 6d 6a 6f 78 71 72 73 74 75 76 shirklen opporatus
     Encapsulation type: Ethernet (1)
                                                                                                              0040 77 61 62 63 64 65 66 67 68 69
                                                                                                                                                                        wabcdefg hi
     Arrival Time: Oct 7, 2025 18:02:25.809100000 STZ 2 (nema)
     HTC Accipal Time: Oct. 7, 2835 15:82:25 889188888 HTC
     Epoch Arrival Time: 1759849345.889100000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.001505000 seconds]
     [Time delta from previous displayed frame: 0.001505000 seconds]
     [Time since reference or first frame: 96.6395858990 seconds]
     Frame Number: 625
     Frame Langth: 74 butes (592 hits)
     Capture Length: 74 bytes (592 bits)
     Eframe is marked; Falsel
     [Frame is ignored: False]
     (Protocols in frame: ethiethertype:in:icen:data)
     [Coloring Rule Name: ICMP]
     [Coloring Rule String: icmp || icmpv6]
  Ethernet II. Src: Cisco 60:9c;eb (70:18;e7:60:9c;eb), Dat; Intel 00:28;dc (00:93:37:00:28;dc)
  > Destination: Intel_00:28:dc (00:93:37:00:28:dc)
  > Source: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
     Type: IPvd (0x0000)
     (Stream Index: 0)
  Internet Protocol Version 4, Src: 192,168,192,1, Dat: 192,168,214,191
  Internet Control Heavage Protocol
```

Рисунок 13: Кадр ICMP — эхо-ответ.

Изучим кадры данных протокола ARP и данные в полях заголовка Ethernet II (рис. 14)

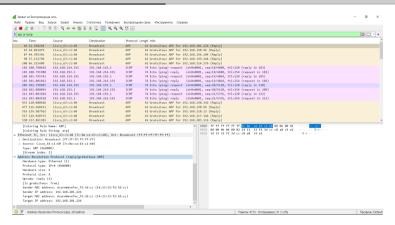


Рисунок 14: Изучение кадров данных протокола ARP и данных в полях заголовка Ethernet II.

Начнём новый процесс захвата трафика в Wireshark. На нашем устройстве в консоли пропингуем по имени адрес ping vk.com (рис. 15)

Рисунок 15: Пингуем по имени адрес vk.com.

B Wireshark остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP (рис. 16 - 17)

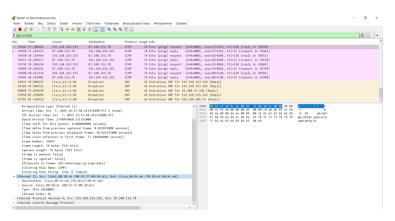


Рисунок 16: Кадр ICMP — эхо-запрос.

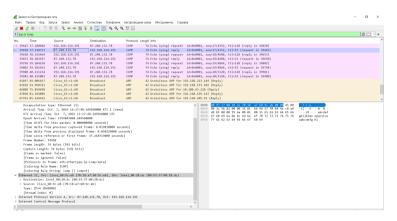


Рисунок 17: Кадр ICMP — эхо-ответ.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (рис. 18)



Рисунок 18: Запуск Wireshark. Выбор активного сетевого интерфейса.

На устройстве в браузере перейдём на сайт, работающий по протоколу HTTP (http://httpbin.org/) и поперемещаемся по ссылкам и разделам сайта в браузере (рис. 19)



Рисунок 19: Открытие в браузере сайта

B Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов и ответов (рис. 20 - 21)

```
42622 645.840375 10.193.235.206 44.210.206.228 HTTP 504 GET / HTTP/1.1
  42713 646,287639 10.193,235,206 44,210,206,228 HTTP 420 GET /flasgger static/swagger-ui.css HTTP/1.1
v Frame 42622! 584 bytes on wire (4892 bits), 584 bytes captured (4892 bits) on interface \Device\MPF_(E6: 0000 76 81 8d 19 ae eb 08 93 37 00 28 dc 08 00 45 00
    Section number: 1
  > Interface id: 0 (\Davice\NPF (E6343E28-FD2D-4647-E2FD-9DDF116FC7C4))
    Enrangulation type: Ethernet (1)
                                                                                                      0000 26 31 2e 31 8d 8a 48 66 73 74 3e 38 34 34 2e 32
    Arrival Time: Oct 7, 2025 14:45:12,986863000 RTZ 2 (2000a)
    UTC Arrival Time: Oct 7, 2025 11:45:12.986063000 UTC
    Enoch Acadust Time: 1759837513 986863888
                                                                                                      0010 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31
    [Time shift for this packet: 0.000000000 seconds]
                                                                                                      0010 0d 8a 55 73 65 72 2d 41 67 65 6e 74 3a 28 4d 6f
    [Time delta from anacinus cantured frame: 8 881885888 seconds]
    [Time delta from previous displayed frame: 68,399324000 seconds]
                                                                                                                                                             ws NT 18 -8: Winfo
    [Time since reference on first frame: 645.840375000 seconds]
                                                                                                      0000 4h 69 74 2f 35 33 37 2e 33 36 28 28 4h 48 54 4d
    Frame Number: 42622
                                                                                                      10x10 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43
    Frame Length: 504 bytes (4032 bits)
    Century Langth: 504 botes (4832 bits)
     [frame is marked: False]
                                                                                                      0110 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c
     Dicage is imposed; Ealer!
                                                                                                      0120 2c 61 70 70 6c 60 63 61 74 69 6f 6e 2f 78 68 74
                                                                                                       0130 6d 6c 2b 78 6d 6c 2c 61 78 70 6c 69 63 61 74 69
                                                                                                                                                             ml+xml,a policati
     [Protocols in frame: eth:ethertype:ip:tcp:http]
                                                                                                       0140 6f 6e 2f 78 6d 6c 3h 71 3d 30 2e 39 2c 69 6d 61 cm/mml o =0.9 tma
     [Coloring Rule Name: HTTP]
                                                                                                                                                             ge/avif, image/we
     [Coloring Rule String: http://tcp.port == 80 || http2]
                                                                                                       0160 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f
V Ethernat II. Src: Intel 00:28:dc (00:93:37:00:28:dc), Ost: 76:81:8d:19:so:ob (76:81:8d:19:so:ob)
  > Destination: 76:81:8d:19:ae:eb (76:81:8d:19:ae:eh)
  ) Source: Intel 00:28:dr (00:93:37:00:28:dr)
                                                                                                       01+0 41 63 63 65 78 74 34 45 60 63 64 69 60 67 by Arcentyl produce
    Type: IPu4 (0:0100)
    (Streen index: 8)
Internet Protocol Version 4, Sec. 18,193,235,286, Dat. 44,218,286,228
Transmission Control Protocol, Ser Port: 50906, Dat Port: 80, Sea: 1, Ark: 1, Leo: 450
> Hypertext Transfer Protocol
```

Рисунок 20: Анализ информации по протоколу ТСР

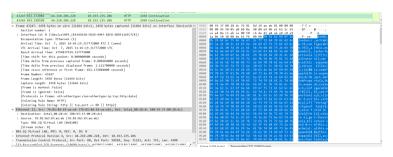


Рисунок 21: Анализ информации по протоколу ТСР

B Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов (рис. 22 - 23)

```
- 1573 48.431452 192.168.214.191 192.168.80.63 DMS 71 Standard query 0x00004 A httpbin.org
                                                                      167 Standard query response 8x8904 A httphia.org A 1,221,229,78 A 14,216,61,135 A 54,214,128,168 A 35,178,214,92 A 44,218,266,228 A 108,
   1575 48.459616 192.168.89.63
                                         192-168-214-191 DNS
v Frame 1573: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\APF (1634312) 0000 70 18 a7 60 9c eb 00 93 37 00 28 dc 08 00 45 00 p.
                                                                                                      0010 00 39 05 cc 00 00 80 11 00 00 c0 a8 d6 bf c0 a8 .9...
                                                                                                      0020 50 3f fa at 00 3t 00 2t at 06 00 04 01 00 00 01 D1 5 K
   \ Teterface id: 8 (\Decire\MPE (F6343F28:FD30-4447-82F0-900F116FC7C4)\)
                                                                                                      0020 90 37 Te e5 00 35 00 25 a8 86 00 04 01 00 00 01 P/ 5 5
     Encapsulation type: Ethernet (1)
                                                                                                      0040 72 67 00 00 01 00 01
     Arrival Time: Oct 7, 2025 15:03:17.694898000 RTZ 2 (3uma)
     UTC Arrival Time: Oct 7, 2825 12:85:17.694898000 UTC
     Teach Acrival Time: 1759838597.694898888
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.000306000 seconds]
     [Time delta from previous displayed frame: 0.000306000 seconds]
     [Time since reference or first frame: 48.431452000 seconds]
     Frame Number: 1573
     Frame Longth: 71 bytes (568 bits)
     Capture Length: 71 bytes (568 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: ethiethertyne:in:udo:dox]
     [Colonies Rule Hame: 1001]
     [Coloring Rule String: udp]
 Ethernet II. Sec. Intel 00:28 dc (00:93:37:00:28 dc). Det: Clace 60:9c:eb (70:18:a7:60:9c:eb)
   > Destination: Cisco 60:9c:eb (70:18:a7:60:9c:eb)
   ) Source: Intel_00:28:dc (00:93:37:00:28:dc)
    Type: IPv4 (0v0000)
    Estream Index: 81
  Tetappet Postocol Macsine A. Sec. 193, 168, 214, 191, Duty 192, 168, 88, 63
  User Datagram Protocol, Src Port: 65253, Det Port: 53
  Domaio Name System (many)
```

Рисунок 22: Анализ информации по протоколу UDP.

```
1575 48,459616 192,168,00.63 192,168,214,191 DNS 167 Standard query response 0x0004 A httpbin.org A 3,221,229,78 A 34,236,61,135 A 54,234,120,160 A 35,170,234,92 A 44,210,206,228 A 100
v Frame 1575; 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF (F634 0000 60 93 37 00 28 dc 70 18 a7 60 9c ab 08 60 45 60
                                                                                               0010 00 90 61 f5 00 00 7f 11 31 0f c0 all 50 3f c0 all ...a.... 1...P7.
    Section number: 1
                                                                                               0020 d6 bf 00 35 fe e5 00 85 00 ee 00 04 81 80 00 01
  \ Totacface id: 0 (\Davica\NBS (F6343E38-E030-4447-83E0-5005114EC3C4))
                                                                                               2010 80 05 00 00 00 00 07 58 74 74 70 57 50 50 01 01 6f
    Encapsulation type: Ethernet (1)
                                                                                               0050 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00
    Arrival Time: Oct. 7, 2025 15:03:17 723062000 877 2 (mass)
                                                                                               0050 28 00 04 03 dd o5 4e c0 0c 00 01 00 01 00 00 00 (....N.
    UTC Arrival Time: Oct 7, 2025 12:03:17,723062000 UTC
                                                                                               0000 28 00 04 22 ec 3d 87 c0 0c 00 01 00 01 00 00 00 (......
                                                                                               00770 28 00 04 36 ca 78 a0 c0 0c 00 01 00 01 00 00 00
    Enoch Arcival Time: 1759838597, 223862888
                                                                                               [Time shift for this nacket: 8 000000000 seconds]
                                                                                               [Time delta from previous captured frame: 0.018092000 seconds]
                                                                                               00±0 20 00 04 64 1d 93 a1
    [Time dalta from provious displayed frame: 8 838164888 secondal
    [Time since reference or first frame: 48.459616000 seconds]
    From Longth: 167 bytes (1336 bits)
    Capture Length: 167 bytes (1336 bits)
    (Frame is marked; False)
    (Frame is ignored: Eales)
    (Protocols in forms; athrethestons incode dos)
    [Coloring Bule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Sec: Cisco 60/9c/eb (70/18/a7/60/9c/eb), Dst: Intel 00/28/dc (00/93/37/00/28/dc)
  > Destination: Total 00:28:4c (00:93:37:00:28:4c)
  > Source: Cisco_60:9c:eb (70:18:a7:60:9c:ab)
    Type: IPv4 (0x0000)
    Esturan Index: 81
 Internet Protocol Varsion 4, Src: 192,168,89.63, Dat: 192,168,214,191
  Hiser Datagram Protocol. Sec Poet: 53. Det Poet: 65253
  Domain Name System (response)
```

Рисунок 23: Анализ информации по протоколу UDP.

B Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов (рис. 24 - 25)

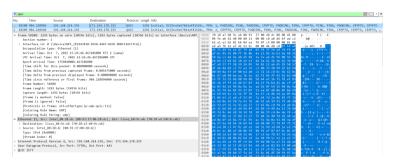


Рисунок 24: Анализ информации по протоколу QUIC.

```
58388 684 338896 193 168 314 191
                                                                                                                         173 104 170 21C MITC 1202 Total In DOTA AND CONTROL OF SWILL A DANDING DING DANDING DING COVERN DING COVERN DING COVERN DANDING DING COVERN DANDING COVERN COVERN COVERN COVERN COVERN COVERN DANDING COV
      58289 984.228928 192.168.214.191
                                                                                                                           173,194,178,225
                                                                                                                                                                                   OUIC
                                                                                                                                                                                                                1292 Initial, DCID=09457661af41526c, PKN: 2, CKMPTO, CRMPTO, PADDIMS, PING, PADDING, PING, PADDING, PING, CKMPTO, CKMPTO, CRMPTO, CRMP
                                                                                                                           192,168,214,191
                                                                                                                                                                                                                      82 Initial, SCID-e9a57b61af41526c, PKV: 1, ACK
v Frame SECIA: 82 bytes on wire (656 bits). 82 bytes cantured (656 bits) on interface \Device\NPF (FEMALE) 000 00 93 37 00 28 dc 70 18 a7 60 9c ob 00 00 45 00
                                                                                                                                                                                                                                                                                                                     2010 08 44 00 08 40 00 th 11 47 3d ad c2 h2 al c0 al . D. . B. . . G.
                                                                                                                                                                                                                                                                                                                     0020 d6 bf 01 bb e1 b5 00 30 92 79 c0 00 00 00 01 00 .....0 y
      > Interface id: 0 (\Device\MPF (E6343E28-F020-4447-82F0-900F116FC7C4))
                                                                                                                                                                                                                                                                                                                    0030 08 e9 a5 7b 61 af 41 52 6c 00 40 16 b2 d2 0e 51 (a AR 1 0 0
           Incappulation type: Ethernet (1)
             Accival Time: Oct. 7, 2025 15:26:46 468954000 8T7 2 (2000)
                                                                                                                                                                                                                                                                                                                    0010 53 4b
             UTC Arrival Time: Oct 7, 2825 12:26:46.468954888 UTC
             Fooch Acetual Time: 1759848886-468954888
             (Time shift for this packet: 0 000000000 seconds)
             [Time delta from previous captured frame: 0.001764000 seconds]
             [Time delta from previous displayed frame: 0.001816000 seconds]
             [Time since coference on first forms: 504 330744050 records]
             Frame Number: 58212
             Frame Langth: 82 botton (656 bits)
             Capture Length: #2 bytes (656 bits)
             (Frame is marked: False)
             [Frame is ignored: False]
             [Protocols in frame: eth:ethertype:ip:ude:quic]
             [Coloring Bule Name: UDP]
             [Colonies Bule Steine: wiel
Ethernet II, Smc: Cisco_60:9c:eb (70:18:a7:60:9c:eb), Dst: Intel_00:28:dc (00:9):37:00:28:dc)
      ) Destination: Total 88:28:4c (88:93:37:88:28:4c)
      ) Source: Cinco 68:Sciab (28:18:a7:68:Sciab)
             Type: IPv4 (0x0000)
             [Stream Index: 0]
    Internet Protocol Version 4, Src: 173.194.178,225, Dat: 192.168.214.191
    User Datagram Protocol, Sec Port: 443, Ost Port: 57781
   OUTC TETE
```

Рисунок 25: Анализ информации по протоколу QUIC.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (рис. 26)



Рисунок 26: Запуск Wireshark. Выбор активного сетевого интерфейса.

На устройстве используем соединение по HTTP с сайтом для захвата в Wireshark пакетов TCP (рис. 27)

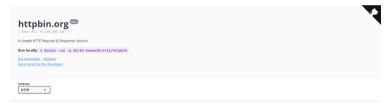


Рисунок 27: Использование соединения по НТТР с сайтом

B Wireshark проанализируем handshake протокола TCP (рис. 28 - 30)

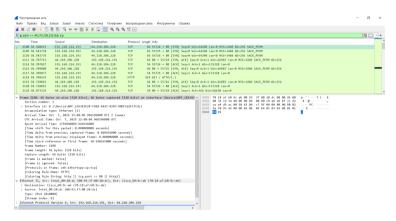


Рисунок 28: Анализ handshake протокола TCP.

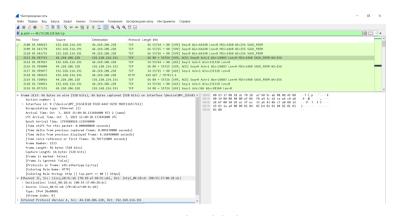


Рисунок 29: Анализ handshake протокола TCP.

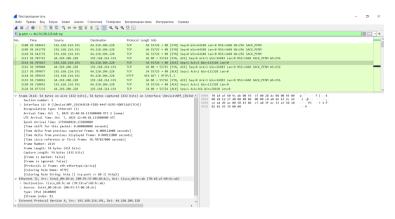


Рисунок 30: Анализ handshake протокола TCP.

В Wireshark в меню «Статистика» выберем «График Потока» (рис. 31)



Рисунок 31: График потока.

45 Выводы

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.