

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет программной инженерии и компьютерной техники

Дисциплина:
«Компьютерные сети»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

Выполнили:
Студент гр. Р33131
Овсянников Роман Дмитриевич

Преподаватель:
Мартынчук Илья Геннадьевич

Санкт-Петербург
2024г.

Цель работы

Изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark

Выполнение

Использоваться будет сайт discord.com

Этап 1 (ping)

```
ping.sh:
#!/bin/bash
for ((x=100; x<=10000; x+=1000)); do
    echo "Pinging discord.com with packet size $x bytes"
    ping -c 4 -s $x discord.com
    echo "

» sudo bash ping.sh
Pinging discord.com with packet size 100 bytes
PING discord.com (162.159.138.232): 100 data bytes
108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=17.096 ms
108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=15.487 ms
108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=34.495 ms
108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=15.198 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 15.198/20.569/34.495/8.073 ms
-----

Pinging discord.com with packet size 1100 bytes
PING discord.com (162.159.138.232): 1100 data bytes
1108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=18.611 ms
1108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=21.861 ms
1108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=20.323 ms
1108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=17.265 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 17.265/19.515/21.861/1.735 ms
-----

Pinging discord.com with packet size 2100 bytes
PING discord.com (162.159.138.232): 2100 data bytes
2108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=19.693 ms
2108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=23.420 ms
2108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=27.868 ms
2108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=22.350 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.693/23.333/27.868/2.949 ms
-----
```

Pinging discord.com with packet size 3100 bytes
PING discord.com (162.159.138.232): 3100 data bytes
3108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=17.532 ms
3108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=19.800 ms
3108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=22.445 ms
3108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=18.167 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 17.532/19.486/22.445/1.898 ms

Pinging discord.com with packet size 4100 bytes
PING discord.com (162.159.138.232): 4100 data bytes
4108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=16.034 ms
4108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=22.341 ms
4108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=16.561 ms
4108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=19.673 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.034/18.652/22.341/2.543 ms

Pinging discord.com with packet size 5100 bytes
PING discord.com (162.159.138.232): 5100 data bytes
5108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=151.171 ms
5108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=34.703 ms
Request timeout for icmp_seq 2
--- discord.com ping statistics ---
4 packets transmitted, 2 packets received, 50.0% packet loss
round-trip min/avg/max/stddev = 34.703/92.937/151.171/58.234 ms

Pinging discord.com with packet size 6100 bytes
PING discord.com (162.159.138.232): 6100 data bytes
6108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=23.969 ms
6108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=21.578 ms
6108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=35.747 ms
6108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=26.077 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.578/26.843/35.747/5.382 ms

Pinging discord.com with packet size 7100 bytes
PING discord.com (162.159.138.232): 7100 data bytes
7108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=177.752 ms
7108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=21.012 ms
7108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=25.265 ms
7108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=31.289 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.012/63.829/177.752/65.874 ms

Pinging discord.com with packet size 8100 bytes

```

PING discord.com (162.159.138.232): 8100 data bytes
8108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=24.060 ms
8108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=19.181 ms
Request timeout for icmp_seq 2
8108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=1031.885 ms
8108 bytes from 162.159.138.232: icmp_seq=3 ttl=55 time=32.150 ms
--- discord.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.181/276.819/1031.885/435.962 ms
-----

```

```

Pinging discord.com with packet size 9100 bytes
PING discord.com (162.159.138.232): 9100 data bytes
9108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=19.118 ms
9108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=24.894 ms
9108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=57.159 ms
--- discord.com ping statistics ---
4 packets transmitted, 3 packets received, 25.0% packet loss
round-trip min/avg/max/stddev = 19.118/33.724/57.159/16.738 ms
-----

```

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

Да. При больших пакетах как раз используется. Флаг More fragments

The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows several fragmented IP packets (protocol 1514) from source 162.159.138.232 to destination 192.168.0.103. The packet details pane for packet 764 (a reassembled packet) shows the IP header with the 'More fragments' flag (MF) set, indicated by the '001' flag field. The packet bytes pane shows the raw data of the packet.

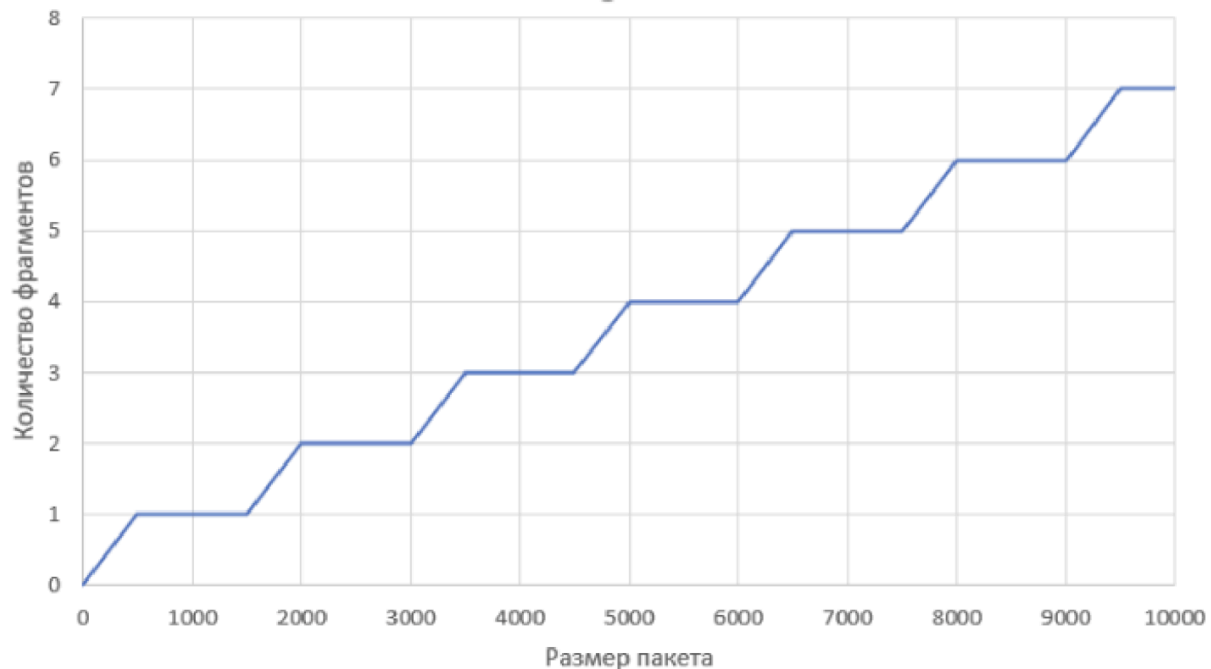
2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?

При флаге More fragments значит, что пакет не последний. Если флага нет, то значит последний.

3. Чему равно количество фрагментов при передаче ping-пакетов?

Зависит от величины пакета и MTU (до 1500 байт обычно).

4. Построить график, в котором на оси абсцисс находится размер_пакета, а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет.



5. Как изменить поле TTL с помощью утилиты ping?

флаг -i

6. Что содержится в поле данных ping-пакета?

(набор символов)

```

... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3368 (13160)
001. .... = Flags: 0x1, More fragments
0... .... = Reserved bit: Not set
0... .... = Don't fragment: Not set
1... .... = More fragments: Set
...0 0010 0010 1011 = Fragment Offset: 4440
Time to Live: 55
Protocol: ICMP (1)
Header Checksum: 0x39e7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 162.159.135.232
Destination Address: 192.168.0.103
[Reassembled IPv4 in frame: 796]
▼ Data (1480 bytes)
Data [truncated]: 505152535455565758595a5b5c5d5e5f006162636465666768696a6b6c6d6e6f7071
[Length: 1480]
0020 00 67 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d .gPQRSTU VWXYZ[\
0030 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d ^_abcde fghijklm
0040 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d nopqrstu vwxyz{ }
0050 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d ~.
0060 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d
0070 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad
0080 ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd
0090 be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd
00a0 ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd
00b0 de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed
00c0 ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd
00d0 fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d
00e0 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
00f0 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d .. !"#%&'()*+,-
0100 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789;<=
0110 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d >?@ABCDE FGHIJKLM
0120 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VWXYZ[\
0130 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d ^_abcde fghijklm
0140 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d nopqrstu vwxyz{ }
0150 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d ~.
0160 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d
0170 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad
0180 ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd

```

Этап 2 (traceroute)

traceroute -d discord.com

traceroute: Warning: discord.com has multiple addresses; using 162.159.135.232

traceroute to discord.com (162.159.135.232), 64 hops max, 40 byte packets

```

1  192.168.0.1 (192.168.0.1)  4.191 ms  9.618 ms  3.754 ms
2  188.243.46.1.pool.sknt.ru (188.243.46.1)  3.866 ms  4.141 ms  4.426 ms
3  router.sknt.ru (93.100.0.20)  7.358 ms  6.477 ms  8.479 ms
4  linux-mx (185.37.128.84)  3.856 ms  8.843 ms  3.802 ms
5  filter-tspu-id-1779 (185.37.128.22)  4.401 ms  4.799 ms  51.899 ms
6  185.37.128.0 (185.37.128.0)  10.307 ms  4.078 ms  4.093 ms

```

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?

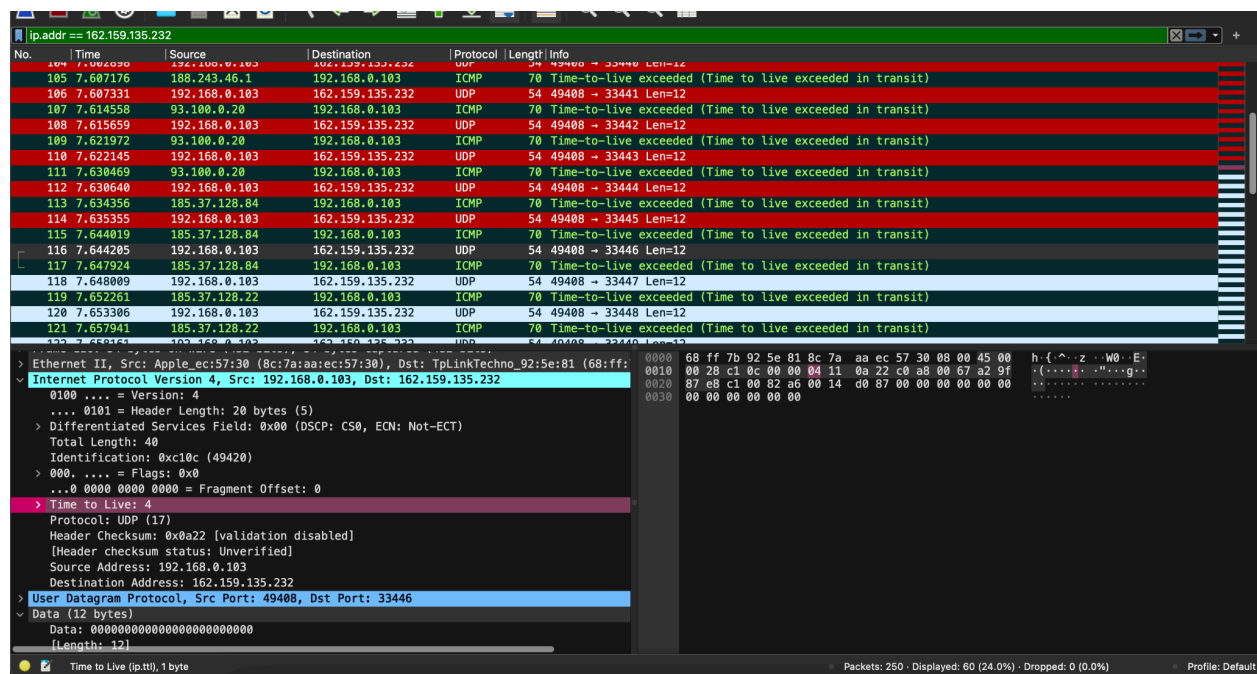
2. Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracer? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

No.	Time	Source	Destination	Protocol	Length	Info
104	7.606230	192.168.0.103	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
105	7.607176	188.243.46.1	192.168.0.103	ICMP	54	49408 + 33447 Len=12
106	7.607331	192.168.0.103	162.159.135.232	UDP	54	49408 + 33441 Len=12
107	7.614558	93.100.0.20	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
108	7.615659	192.168.0.103	162.159.135.232	UDP	54	49408 + 33442 Len=12
109	7.619172	93.100.0.20	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
110	7.622145	192.168.0.103	162.159.135.232	UDP	54	49408 + 33443 Len=12
111	7.630469	93.100.0.20	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
112	7.630640	192.168.0.103	162.159.135.232	UDP	54	49408 + 33444 Len=12
113	7.634356	185.37.128.84	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
114	7.635355	192.168.0.103	162.159.135.232	UDP	54	49408 + 33445 Len=12
115	7.640819	185.37.128.84	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
116	7.644205	192.168.0.103	162.159.135.232	UDP	54	49408 + 33446 Len=12
117	7.647924	185.37.128.84	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
118	7.648009	192.168.0.103	162.159.135.232	UDP	54	49408 + 33447 Len=12
119	7.652261	185.37.128.22	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
120	7.653306	192.168.0.103	162.159.135.232	UDP	54	49408 + 33448 Len=12
121	7.657941	185.37.128.22	192.168.0.103	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
122	7.658151	103.160.0.102	162.159.135.232	UDP	54	49408 + 33449 Len=12


```

> Ethernet II, Src: Apple AC:57:30 (8c:7a:a6:e5:7f:30), Dst: TpLinkTech_92:5e:81 (68:ff:fe:00:00:00)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 162.159.135.232
    0100 .... = Version: 4
      ... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xc10e (49422)
> 0000 .... = Flags: 0x0
      ... 0000 0000 0000 = Fragment Offset: 0
Time to Live: 5
    Protocol: UDP (17)
    Header checksum: 0x0920 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.103
    Destination Address: 162.159.135.232
> User Datagram Protocol, Src Port: 49408, Dst Port: 33448
Data (12 bytes)
  Data: 00000000000000000000000000000000
[Length: 12]
  
```

Packets: 250 / Displayed: 60 (24.0%) - Dropped: 0 (0.0%) Profile: Default



3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracer, от ICMP пакетов, генерируемых утилитой ping (см. предыдущее задание).

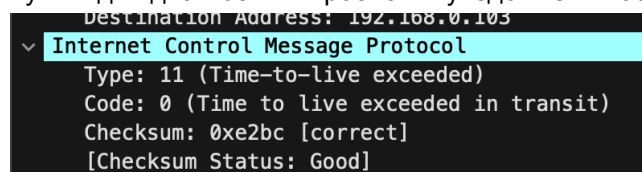
В traceroute маленький пакет с нулями

4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

reply: тип ответа указывает на успешную доставку пакета

error: Если в процессе маршрутизации пакета возникают проблемы или ошибки, такие как недоступный узел, превышение времени жизни пакета (TTL), неправильный адрес и т. д., то узел, столкнувшийся с этой проблемой, может отправить обратно "ICMP error" сообщение

Нужны для диагностики проблем и уведомлений об успешной доставке.



5. Что изменится в работе tracer, если убрать ключ «-d»? Какой дополнительный трафик при этом будет генерироваться?

Будут добавлены имена хостов. Соответственно выполняться будет дольше.

Этап 3 (анализ http)

Wireshark не загружает трафик http, так как идёт по tcp с динамической подгрузкой контента.

Но должны увидеть вот такую картину:


```
[-] Hypertext Transfer Protocol
[-] GET / HTTP/1.1\r\n
[-] [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Cache-Control: max-age = 3600\r\n
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    If-Modified-Since: Mon, 26 Jul 2021 16:20:55 GMT\r\n
    If-None-Match: "60fee0e7-2cd"\r\n
    User-Agent: Microsoft-CryptoAPI/10.0\r\n
    Host: xl.c.lencr.org\r\n
    \r\n
```

```
[-] Internet Protocol, Src: 184.51.233.240 (184.51.233.240), Dst: 192.168.1.102 (192.168.1.102)
[-] Transmission Control Protocol, Src Port: http (80), Dst Port: 57927 (57927), Seq: 1, Ack: 228, L
[-] Hypertext Transfer Protocol
[-] HTTP/1.1 304 Not Modified\r\n
[-] [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    [Message: HTTP/1.1 304 Not Modified\r\n]
    [Severity level: chat]
    [Group: Sequence]
    Request Version: HTTP/1.1
    Response Code: 304
    Content-Type: application/pkix-crl\r\n
    Last-Modified: Mon, 26 Jul 2021 16:20:55 GMT\r\n
    ETag: "60fee0e7-2cd"\r\n
    Cache-Control: max-age=3600\r\n
    Expires: Thu, 05 May 2022 15:45:44 GMT\r\n
    Date: Thu, 05 May 2022 14:45:44 GMT\r\n
    Connection: keep-alive\r\n
    \r\n
```

По заголовку 304 Not Modified определяется, что не нужно отправлять тело вместе с ответом. В первом запросе в поле Cache-Control установлено значение 3600 секунд для кэширования, чтобы при обновлении страницы не тащилась лишняя информация, если изменений не поступало

Этап 4 (анализ dns)

```
sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder
```

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?

После очистки кэша будет отправлен запрос на dns сервер для нахождения соответствия домену айпи адреса.

7737	59.544192	2a05:3580:0:d1::	2a05:3580:de24:1e0...	DNS	117	Standard que
7738	59.544192	2a05:3580:0:d1::	2a05:3580:de24:1e0...	DNS	105	Standard que
7739	59.544193	2a05:3580:0:d1::	2a05:3580:de24:1e0...	DNS	287	Standard que
7740	59.544194	2a05:3580:0:d1::	2a05:3580:de24:1e0...	DNS	323	Standard que
7741	59.544195	2a05:3580:0:d1::	2a05:3580:de24:1e0...	DNS	323	Standard que

```
> Frame 7738: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface en0
> Ethernet II, Src: TpLinkTechno_92:5e:81 (68:ff:7b:92:5e:81), Dst: Apple_ec:57:30 (8c:7a:
> Internet Protocol Version 6, Src: 2a05:3580:0:d1::, Dst: 2a05:3580:de24:1e01:c170:81d5:f
> User Datagram Protocol, Src Port: 53, Dst Port: 49675
v Domain Name System (response)
  Transaction ID: 0x3e18
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v apple.com: type A, class IN
      Name: apple.com
      [Name Length: 9]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  > Answers
    [Request ID: 7738]
```

2. Какие бывают типы DNS-запросов?

Прямой(домен в адрес), обратный(адрес в домен), рекурсивный(выполняется dns сервером пока не будет найден целевой домен (или сообщение об отсутствии)), интерактивный(поиск рекурсивный клиентом)

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Если они закешированы на cdn серверах (находятся на других серверах).

Ссылка на файлы

https://github.com/Ja1rman/computer_networks_labs/tree/main/lab4

Вывод

В процессе выполнения лабораторной работы познакомился с программой WireShark и поработал с некоторыми командами (ping, traceroute) в unix системе.