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. P33131

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 "
```

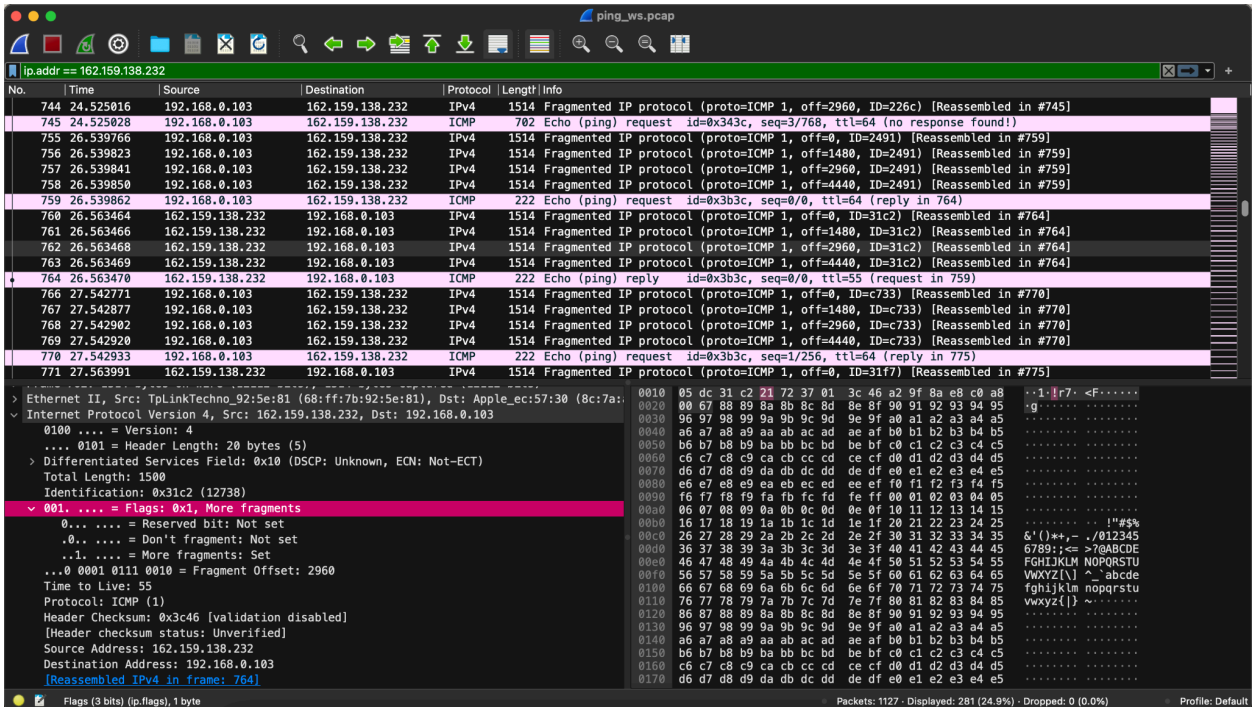
» sudo bash ping.sh

```
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
```

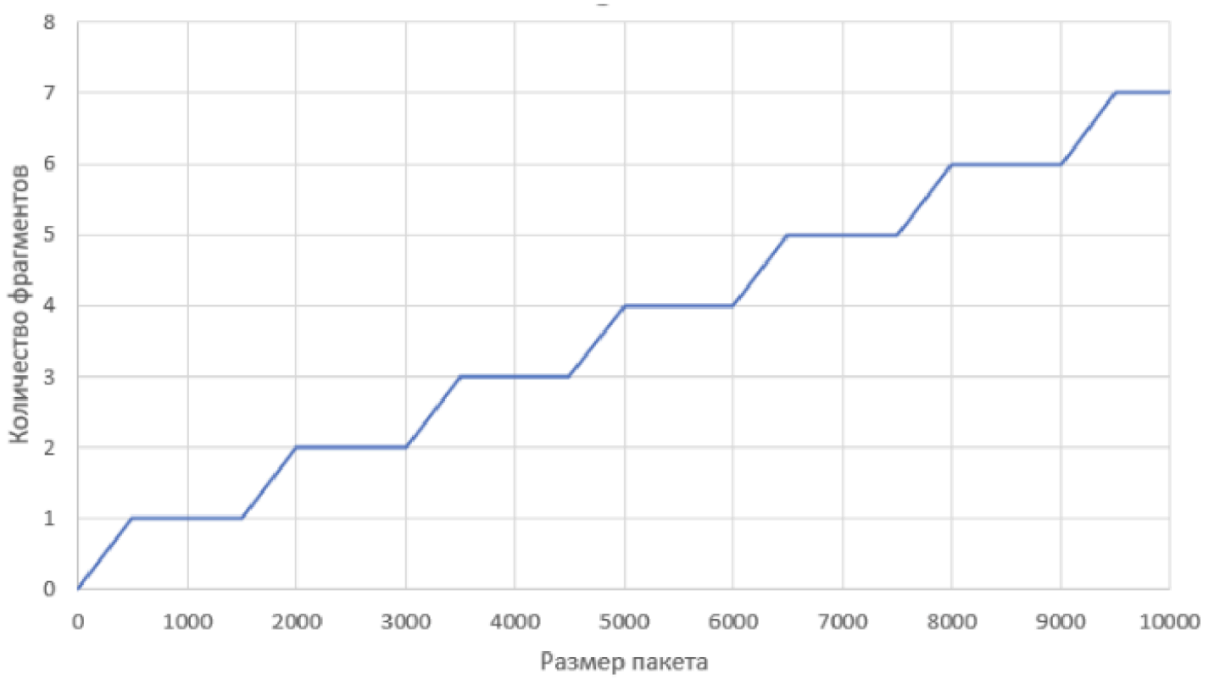
```
PING discord.com (162.159.138.232): 8100 data bytes
8108 bytes from 162.159.138.232: icmp_seq=0 ttl=55 time=24.060 ms
8108 bytes from 162.159.138.232: icmp_seq=1 ttl=55 time=19.181 ms
Request timeout for icmp_seq 2
8108 bytes from 162.159.138.232: icmp_seq=2 ttl=55 time=1031.885 ms
8108 bytes from 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

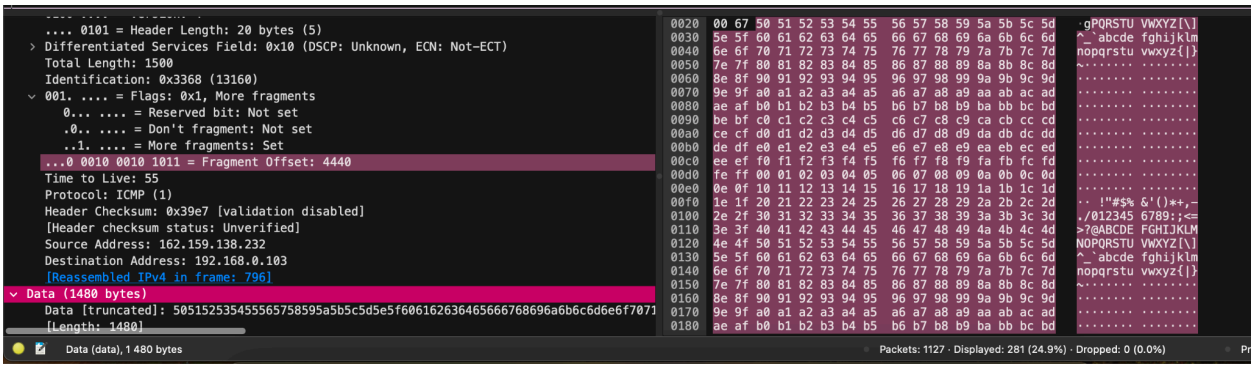


2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?
При флаге More fragments значит, что пакет не последний. Если флага нет, то значит последний.
3. Чему равно количество фрагментов при передаче ping-пакетов?
Зависит от величины пакета и MTU (до 1500 байт обычно).

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)



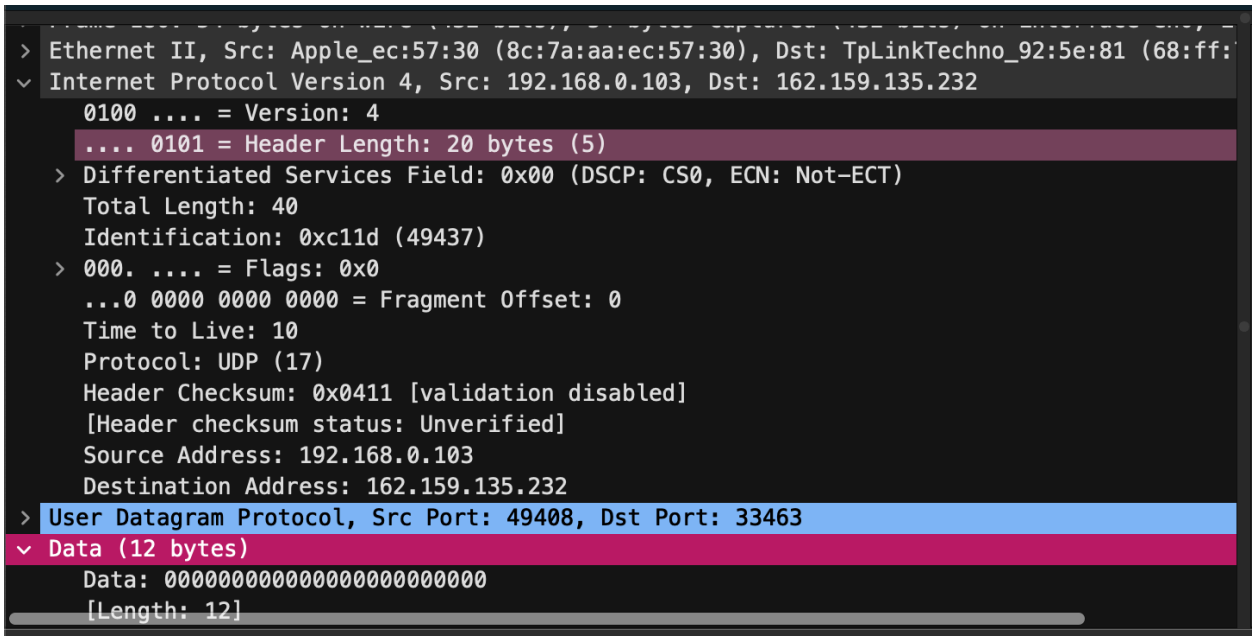
Этап 2 (traceroute)

```
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  linx-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
```

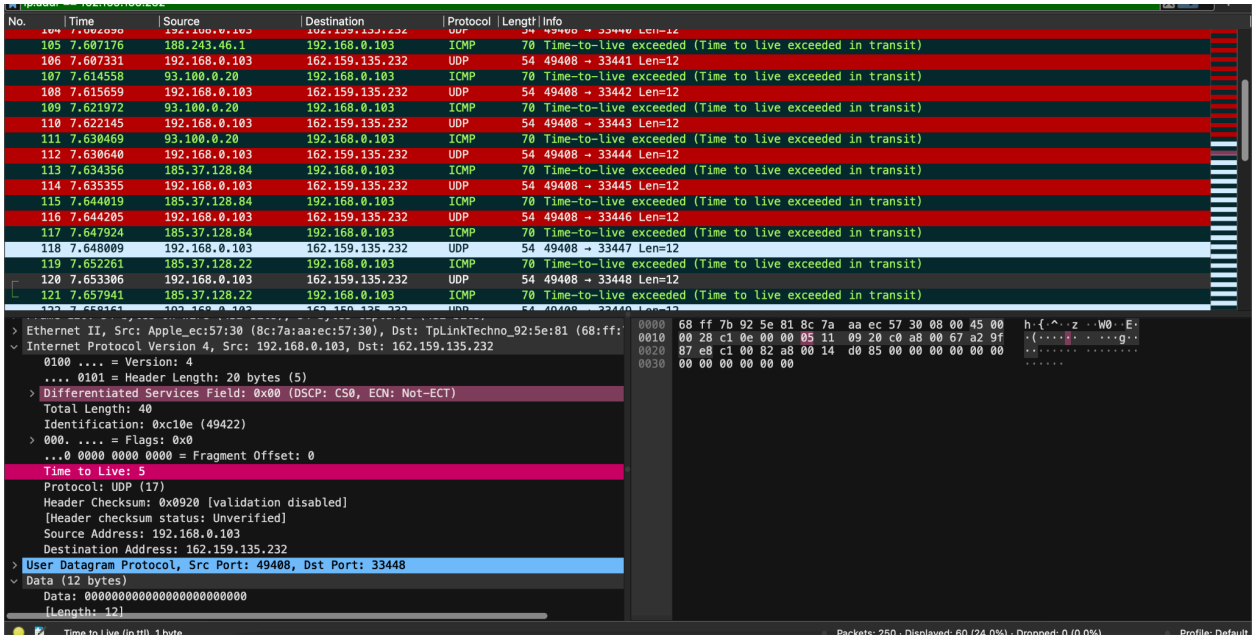
```
 7  139.45.232.193 (139.45.232.193)  3.706 ms  5.957 ms  4.109 ms
 8  ae4-9.rt.tc1.sto.se.retn.net (87.245.233.73)  16.140 ms  14.870 ms  15.932 ms
 9  gw-as13335.retn.net (87.245.242.217)  16.602 ms  35.375 ms  14.445 ms
10  162.159.135.232 (162.159.135.232)  13.612 ms  36.573 ms  14.717 ms
```

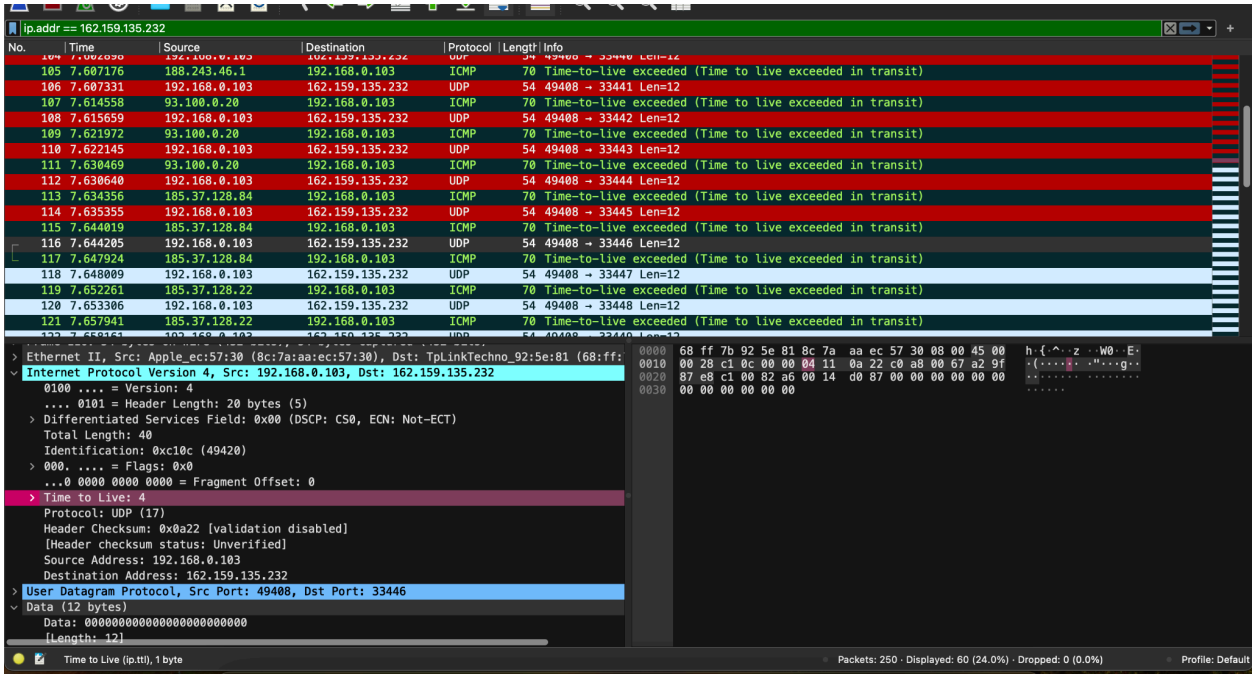
1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?



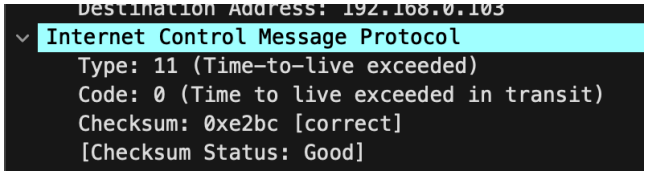
2. Как и почему изменяется поле TTL в следующих друг за другом ICMPпакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

При каждом новом пакете ttl увеличивается на 1. Так утилита понимает, сколько переходов было сделано





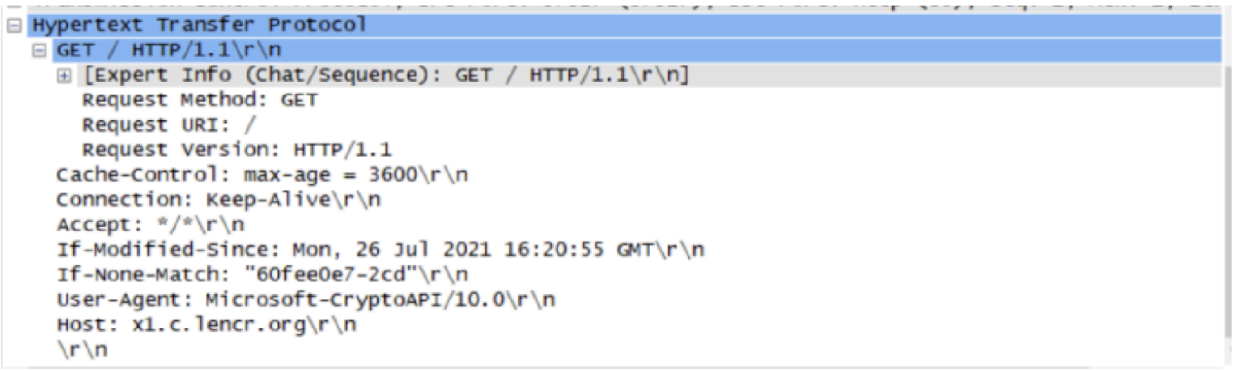
3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMPпакетов, генерируемых утилитой ping (см. предыдущее задание).
В traceroute маленький пакет с нулями
4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?
reply: тип ответа указывает на 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.

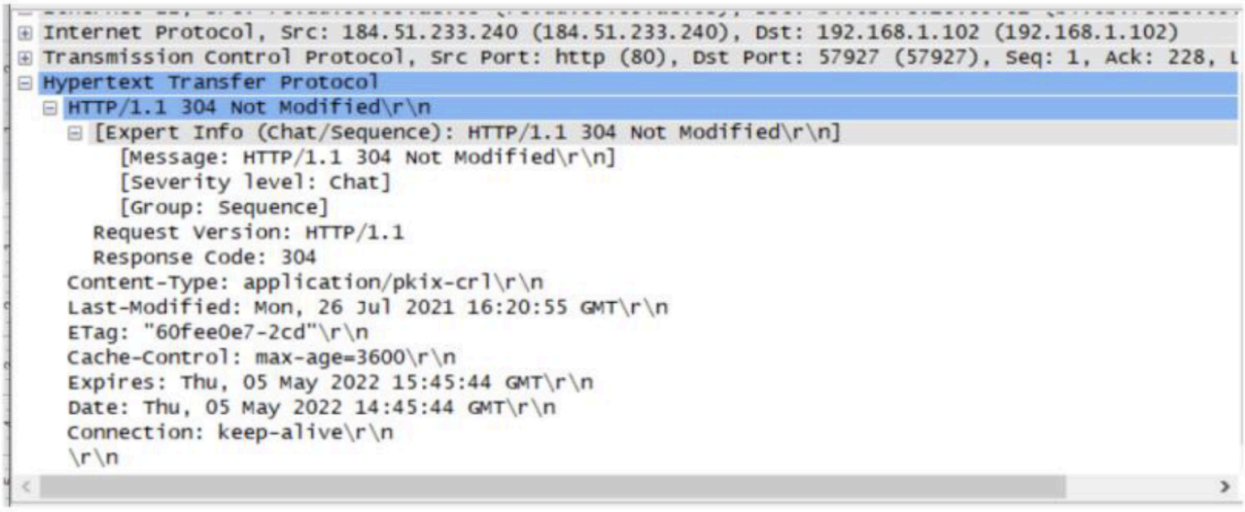


5. Что изменится в работе tracert, если убрать ключ «-d»? Какой дополнительный трафик при этом будет генерироваться?
Будут добавлены имена хостов. Соответственно выполняться будет дольше.

Этап 3 (анализ http)

WireShark не загружает трафик http, так как идёт по tcp с динамической подгрузкой контента.
Но должны увидеть вот такую картину:





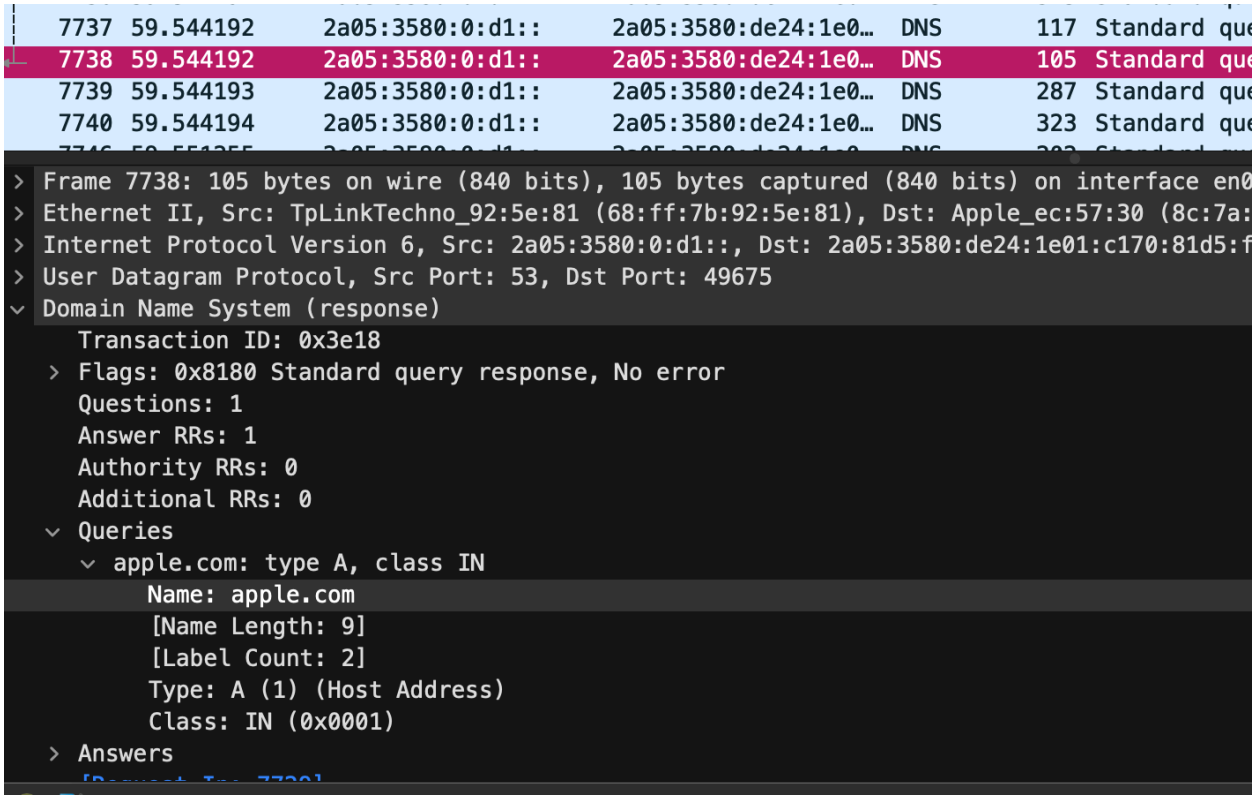
По заголовку 304 Not Modified определяется, что не нужно отправлять тело вместе с ответом. В первом запросе в поле Cache-Control установлено значение 3600 секунд для кэширования, чтобы при обновлении страницы не тащилась лишняя информация, если изменений не поступало

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.



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.