

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**

**Лабораторная работа № 4**

**по теме «Анализ трафика компьютерных сетей с помощью утилиты  
Wireshark»**

Выполнил:

Гурьянов Кирилл Алексеевич

Группа: Р33302

Преподаватель:

Алиев Тауфик Измайлович

Санкт-Петербург

2024

<b>Цель работы</b>	<b>3</b>
<b>Вариант</b>	<b>3</b>
<b>Анализ трафика утилиты ping</b>	<b>3</b>
Ответы на вопросы	3
<b>Анализ трафика утилиты traceroute</b>	<b>6</b>
Ответы на вопросы	6
<b>Анализ DNS-трафика</b>	<b>8</b>
Ответы на вопросы	9
<b>Анализ трафика утилиты nslookup</b>	<b>10</b>
Ответы на вопросы	11
<b>Вывод</b>	<b>12</b>

# Цель работы

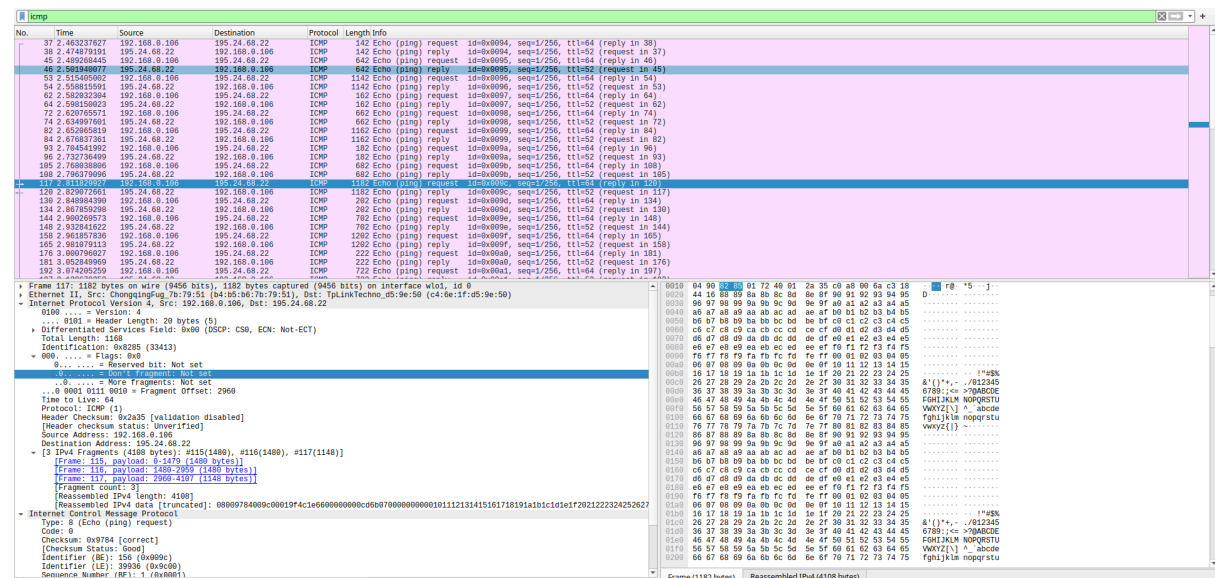
Изучение структуры протокольных блоков данных, анализ реального трафика на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark.

## Вариант

<http://guryanov-plasticsurgeon.ru/>

## Анализ трафика утилиты ping

for i in {100..10100..500}; do ping -c 1 -s \$i guryanov-plasticsurgeon.ru; done



## Ответы на вопросы

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

Фрагментизация исходного пакета имеет место быть, в случае, если суммарный размер фрейма, переданный канальному уровню, превышает 1514 байт (максимальный размер кадра на канальном уровне). В кадре 14 байт отведено под заголовок. Таким образом 1500 байт составляет максимальный размер пакета на сетевой уровне или максимальному передаваемому блоку данных MTU, который является настраиваемым, однако по умолчанию для большинства сетевых устройств составляет 1500

байт. Пакет IP имеет заголовок 20 байт, ICMP пакет имеет заголовок 8 байт, отчего максимальный размер данных пакета может быть только 1472 байта. Анализ трафика показал, что еще 16 байт занимает Timestamp, отчего на сами данные остается только 1456 байт.

Таким образом, если мы пытаемся передать пакет размером большим, чем 1472 байта, то имеет место быть фрагментация пакетов. На это указывается поле MF, которое в случае установки его в единицу, показывает, что пакет был фрагментирован.

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

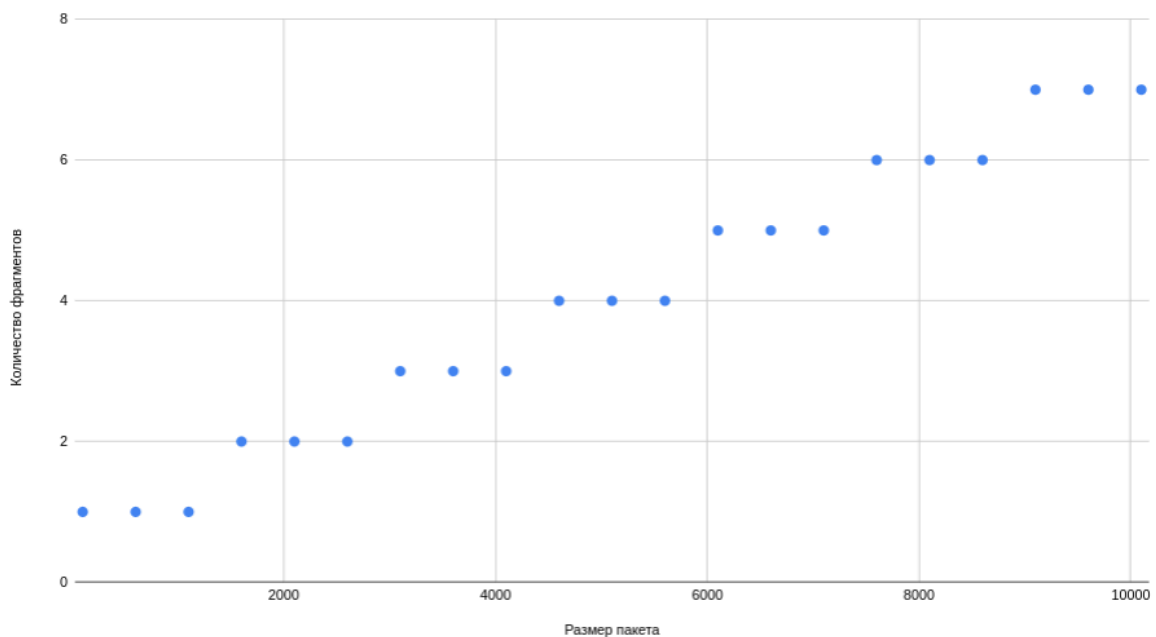
Данная информация указывается в флаге MF, если MF установлен в 1, то это означает, что ожидаются еще пакеты, т.к. данный пакет не последний. Если же MF установлен в 0, то новые пакеты не ожидаются.

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

Количество пакетов зависит от размера самого пакета. Если размер данных пакета превышает 1472 байт, то пакет фрагментируется. Стоит учитывать, что к первому пакету добавляется 8 байтовых заголовков (в отличие от последующих пакетов). Таким образом, количество фрагментов, необходимых для передачи ping-пакета размером N, равно отношению N к 1480 байт.

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

График зависимости количества фрагментов от размера пакета



### 5. Как изменить поле TTL с помощью утилиты ping?

Для изменения поля TTL необходимо указать флаг `-t` при использовании `ping`.

```

~ / Docs / VT / 6sem / cn ping -c 1 -s 1474 -t 12 guryanov-plasticsurgeon.ru
PING guryanov-plasticsurgeon.ru (195.24.68.22) 1474(1502) bytes of data.

--- guryanov-plasticsurgeon.ru ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
    
```

### 6. Что содержится в поле данных ping-пакета?

0000	c4 6e 1f d5 9e 50 b4 b5 b6 7b 79 51 08 00 45 00	· n · · · P · · · { y Q · · E ·
0010	00 80 82 58 40 00 40 01 ef e3 c0 a8 00 6a c3 18	· · · X @ · @ · · · · · j · ·
0020	44 16 08 00 af 10 00 94 00 01 9f 4c 1e 66 00 00	D · · · · · · · · · · L · f · ·
0030	00 00 25 1a 02 00 00 00 00 00 10 11 12 13 14 15	· · % · · · · · · · · · · ·
0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25	· · · · · · · · · · ! " # \$ %
0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	& ' ( ) * + , - . / 0 1 2 3 4 5
0060	36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45	6 7 8 9 ; : < = > ? @ A B C D E
0070	46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55	F G H I J K L M N O P Q R S T U
0080	56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63	V W X Y Z [ \ ] ^ _ ` a b c

Поле данных ping-пакета имеет набор символов английского алфавита.

# Анализ трафика утилиты traceroute

```
tracert -n guryanov-plasticsurgeon.ru
Traceroute to guryanov-plasticsurgeon.ru (195.24.68.22), 30 hops max, 60 byte packets
 1 192.168.0.1 2.534 ms 9.279 ms 9.218 ms
 2 93.100.176.1 9.303 ms 12.478 ms 12.441 ms
 3 93.100.0.81 12.405 ms 12.371 ms 12.334 ms
 4 93.100.0.147 12.297 ms 18.920 ms 21.982 ms
 5 * * *
 6 185.37.128.0 8.744 ms 10.010 ms 19.306 ms
 7 194.226.100.82 25.438 ms 25.402 ms 25.313 ms
 8 31.131.196.94 22.110 ms 22.027 ms 21.992 ms
 9 31.131.196.95 21.946 ms 22.020 ms 21.875 ms
10 * * *
11 * * *
12 * * *
13 195.24.68.22 67.692 ms 67.663 ms 67.636 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
516	23.039243316	192.168.0.1	192.168.0.106	DNS	158	Standard query response 0x8eb AAAA guryanov-plasticsurgeon.ru 50A ns3.nic.ru
517	23.039836327	192.168.0.106	195.24.68.22	UDP	74	44539 - 33434 Len=32
518	23.039845599	192.168.0.106	195.24.68.22	UDP	74	57763 - 33435 Len=32
519	23.039861346	192.168.0.106	195.24.68.22	UDP	74	59593 - 33436 Len=32
520	23.039755094	192.168.0.106	195.24.68.22	UDP	74	53455 - 33437 Len=32
521	23.039793726	192.168.0.106	195.24.68.22	UDP	74	36545 - 33438 Len=32
522	23.039829744	192.168.0.106	195.24.68.22	UDP	74	55490 - 33439 Len=32
523	23.039865701	192.168.0.106	195.24.68.22	UDP	74	53262 - 33440 Len=32
524	23.039904942	192.168.0.106	195.24.68.22	UDP	74	52196 - 33441 Len=32
525	23.039939639	192.168.0.106	195.24.68.22	UDP	74	56568 - 33442 Len=32
526	23.039975256	192.168.0.106	195.24.68.22	UDP	74	53288 - 33443 Len=32
527	23.040011123	192.168.0.106	195.24.68.22	UDP	74	53332 - 33444 Len=32
528	23.040046709	192.168.0.106	195.24.68.22	UDP	74	55659 - 33445 Len=32
529	23.040082106	192.168.0.106	195.24.68.22	UDP	74	47474 - 33446 Len=32
530	23.040117252	192.168.0.106	195.24.68.22	UDP	74	38964 - 33447 Len=32
531	23.040153399	192.168.0.106	195.24.68.22	UDP	74	46388 - 33448 Len=32
532	23.040191408	192.168.0.106	195.24.68.22	UDP	74	48263 - 33449 Len=32
533	23.040216122	192.168.0.106	195.24.68.22	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
534	23.040252732	192.168.0.106	195.24.68.22	UDP	74	59562 - 33450 Len=32
535	23.040282926	192.168.0.1	192.168.0.106	ICMP	102	Time to live exceeded (Time to live exceeded in transit)
536	23.040320287	192.168.0.1	192.168.0.106	ICMP	102	Time to live exceeded (Time to live exceeded in transit)
537	23.040342707	192.168.0.1	192.168.0.106	ICMP	102	Time to live exceeded (Time to live exceeded in transit)
538	23.040364266	192.168.0.106	195.24.68.22	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
539	23.040381128	93.100.176.1	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
540	23.040423288	93.100.176.1	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
541	23.040434358	93.100.0.81	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
542	23.040434629	93.100.0.81	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
543	23.040411493	93.100.0.81	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
544	23.040411793	93.100.0.147	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
545	23.040418174	93.100.0.147	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
546	23.040412034	93.100.0.147	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
547	23.040432254	192.168.0.106	195.24.68.22	ICMP	74	47161 - 33451 Len=32
548	23.040431033	192.168.0.106	195.24.68.22	UDP	74	44211 - 33452 Len=32
549	23.040761445	192.168.0.106	195.24.68.22	UDP	74	54119 - 33453 Len=32
550	23.040819615	192.168.0.106	195.24.68.22	UDP	74	47527 - 33454 Len=32
551	23.040854582	192.168.0.106	195.24.68.22	UDP	74	48404 - 33455 Len=32
552	23.040892854	192.168.0.106	195.24.68.22	UDP	74	34713 - 33456 Len=32
553	23.040928761	192.168.0.106	195.24.68.22	UDP	74	56385 - 33457 Len=32
554	23.040950179	192.168.0.106	195.24.68.22	UDP	74	47967 - 33458 Len=32
555	23.050091666	192.168.0.106	195.24.68.22	UDP	74	49588 - 33459 Len=32
556	23.050117953	192.168.0.106	195.24.68.22	UDP	74	51855 - 33460 Len=32
557	23.050154533	192.168.0.106	195.24.68.22	UDP	74	47540 - 33461 Len=32
558	23.050191252	192.168.0.106	195.24.68.22	UDP	74	45484 - 33462 Len=32
559	23.050227279	192.168.0.106	195.24.68.22	UDP	74	36561 - 33463 Len=32
560	23.050263768	192.168.0.106	195.24.68.22	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
561	23.050307723	194.226.100.82	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
562	23.050347853	194.226.100.82	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
563	23.050388863	194.226.100.82	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
564	23.050430914	31.131.196.94	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
565	23.050488284	31.131.196.94	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
566	23.050538294	31.131.196.94	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
567	23.050488594	31.131.196.95	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
568	23.050488594	31.131.196.95	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
569	23.050509455	31.131.196.95	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
570	23.050509455	31.131.196.95	192.168.0.106	ICMP	70	Time to live exceeded (Time to live exceeded in transit)
571	23.050535317	195.24.68.22	195.24.68.22	UDP	74	47122 - 33464 Len=32
572	23.050593188	192.168.0.106	195.24.68.22	UDP	74	55829 - 33465 Len=32
573	23.050504038	192.168.0.106	195.24.68.22	UDP	74	33328 - 33466 Len=32
574	23.050575738	192.168.0.106	195.24.68.22	UDP	74	48552 - 33467 Len=32
575	23.050612684	192.168.0.106	195.24.68.22	UDP	74	32997 - 33468 Len=32
576	23.050647731	192.168.0.106	195.24.68.22	UDP	74	45183 - 33469 Len=32

## Ответы на вопросы

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

Заголовок IP пакета имеет размер 20 байт.

```
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 195.24.68.22
 0100 .... = Version: 4
 .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb376 (45942)
  ▶ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 6
    Protocol: UDP (17)
    Header Checksum: 0x38fa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.106
    Destination Address: 195.24.68.22
  ▶ User Datagram Protocol, Src Port: 37661, Dst Port: 33451
  ▶ Data (32 bytes)
    Data: 4041424344445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f
    [Length: 32]
```

Поле данных содержит 32 байта, в которых передаются символы английского алфавита.

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.

Поле TTL в заголовке ICMP пакета используется для предотвращения заикливания пакетов в сети. При отправке пакета его TTL устанавливается на определенное начальное значение (обычно 64), и каждый маршрутизатор, через который проходит пакет, уменьшает значение TTL на 1. Если значение TTL достигает нуля, пакет отбрасывается, и маршрутизатор отправляет обратно ICMP сообщение о превышении TTL (Time Exceeded).

При выполнении команды traceroute каждый отправляемый пакет имеет начальное значение TTL, которое постепенно уменьшается по мере прохождения через маршрутизаторы по пути к целевому узлу. Таким образом, каждый маршрутизатор, через который проходит пакет, уменьшает значение TTL перед его передачей дальше.

Сначала утилита отправляет три пакета с TTL равным 1, благодаря чему получает ICMP-ответы от первого маршрутизатора в пути. Затем еще три пакета с TTL равным 2, получая ICMP-ответы от второго маршрутизатора и т.д. По итогу, при определенном TTL, сообщение достигает адреса получателя.

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

При использовании утилиты traceroute вместо ICMP-пакетов с пустым полем данных, отправляются UDP датаграммы, содержащие содержащие символы английского алфавита. Кроме этого, ICMP-пакеты, генерируемые утилитой ping, содержат TTL = 64, а пакеты, генерируемые traceroute последовательно увеличивают TTL, пока не достигнут пункта назначения.

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

ICMP reply пакеты используются для обеспечения подтверждения успешной доставки пакетов. Примеры ICMP ответов включают Echo Reply,

который используется в командах `ring` для проверки доступности узлов в сети.

ICMP эггот пакеты используются для сообщения об ошибках, возникших в процессе обработки пакетов в сети. Примеры ICMP ошибок включают `Time Exceeded`, который сообщает отправителю о том, что TTL пакета истек, и `Destination Unreachable`, который указывает на то, что пункт назначения недоступен или что пакет не может быть доставлен. ICMP ошибки помогают обнаруживать и реагировать на проблемы в сети, такие как недоступность узлов, сетевые перегрузки и неправильно настроенные маршрутизаторы.

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

Если мы уберем ключ `d` (или ключ `n` в `tracert.exe`), то в выводе появятся имена хостов, через которые проходят пакеты. Из-за этого появятся DNS запросы, в которых мы запрашиваем имя хоста по его IP-адресу.

No.	Time	Source	Destination	Protocol	Length	Info
89	5.102334859	192.168.0.106	192.168.0.1	DNS	86	Standard query 0xa21 A guryanov-plasticurgeon.ru
90	5.10247912	192.168.0.106	192.168.0.1	DNS	86	Standard query 0xb27 AAAA guryanov-plasticurgeon.ru
91	5.105973886	192.168.0.1	192.168.0.106	DNS	120	Standard query response 0xa21 A guryanov-plasticurgeon.ru A 195.24.68.22
92	5.117524860	192.168.0.1	192.168.0.106	DNS	138	Standard query response 0xb27 AAAA guryanov-plasticurgeon.ru SOA ns3.nic.ru
120	5.121384654	192.168.0.106	192.168.0.1	DNS	85	Standard query 0x5a5 PTR 1.176.180.83.in-addr.arpa
123	5.130681773	192.168.0.106	192.168.0.1	DNS	115	Standard query response 0x5a5 PTR 81.0.180.93.in-addr.arpa PTR 93.180.176.1.pool.snt.ru
124	5.131245014	192.168.0.106	192.168.0.1	DNS	84	Standard query 0x29ae PTR 81.0.180.93.in-addr.arpa
125	5.13709457	192.168.0.1	192.168.0.106	DNS	115	Standard query response 0x29ae PTR 81.0.180.93.in-addr.arpa PTR 80-0.02.snt.ru
134	5.138182526	192.168.0.106	192.168.0.1	DNS	85	Standard query 0x5f17 PTR 147.0.180.93.in-addr.arpa
140	5.14382725	192.168.0.1	192.168.0.106	DNS	137	Standard query response 0x5f17 PTR 147.0.180.93.in-addr.arpa PTR K12-CORE
147	5.14896334	192.168.0.106	192.168.0.1	DNS	85	Standard query 0xd1c1 PTR 0.128.37.185.in-addr.arpa
148	5.152155859	192.168.0.1	192.168.0.106	DNS	149	Standard query response 0xd1c1 No such name PTR 0.128.37.185.in-addr.arpa SOA ns.snt.ru
149	5.152745893	192.168.0.106	192.168.0.1	DNS	87	Standard query 0x1a4d PTR 82.180.226.194.in-addr.arpa
170	5.159531938	192.168.0.1	192.168.0.106	DNS	123	Standard query response 0x1a4d PTR 82.180.226.194.in-addr.arpa PTR 0b03.spb.ertelecom.ru
171	5.160601486	192.168.0.106	192.168.0.1	DNS	86	Standard query 0x27b7 PTR 94.186.131.31.in-addr.arpa
172	5.168485693	192.168.0.1	192.168.0.106	DNS	133	Standard query response 0x27b7 PTR 94.186.131.31.in-addr.arpa PTR 31x131x106x95.static.ertelecom.ru
173	5.169061230	192.168.0.106	192.168.0.1	DNS	86	Standard query 0x27b7 PTR 94.186.131.31.in-addr.arpa
174	5.169184265	192.168.0.1	192.168.0.106	DNS	133	Standard query response 0x50d4 PTR 95.196.131.31.in-addr.arpa PTR 31x131x106x95.static.ertelecom.ru
175	5.169206698	192.168.0.106	192.168.0.1	DNS	70	Standard query 0x425 AAAA github.com
176	5.169726874	192.168.0.1	192.168.0.106	DNS	119	Standard query response 0x3683 PTR 22.68.24.195.in-addr.arpa PTR wcap.hosting.nic.ru
224	12.118327070	192.168.0.106	192.168.0.1	DNS	70	Standard query 0x5426 A github.com
225	12.118349933	192.168.0.106	192.168.0.1	DNS	70	Standard query 0x425 AAAA github.com
226	12.121725759	192.168.0.1	192.168.0.106	DNS	86	Standard query response 0x5426 A github.com A 140.82.121.4
227	12.121726389	192.168.0.1	192.168.0.106	DNS	137	Standard query response 0x5426 AAAA github.com SOA ns-1707.madns-21.co.uk

# Анализ DNS-трафика

No.	Time	Source	Destination	Protocol	Length	Info
609	8.814224473	192.168.0.1	192.168.0.106	DNS	102	Standard query response 0x1294 A ssl.gstatic.com A 74.125.131.94 OPT
647	8.851314513	192.168.0.106	192.168.0.1	DNS	88	Standard query 0xb53c AAAA fonts.gstatic.com OPT
648	8.851348927	192.168.0.106	192.168.0.1	DNS	88	Standard query 0xa592 A fonts.gstatic.com OPT
649	8.851361351	192.168.0.106	192.168.0.1	DNS	88	Standard query 0xb548 A fonts.gstatic.com OPT
650	8.851412676	192.168.0.106	192.168.0.1	DNS	88	Standard query 0x7770 AAAA fonts.gstatic.com OPT
658	8.853875545	192.168.0.106	192.168.0.106	DNS	116	Standard query response 0xb555 AAAA fonts.gstatic.com AAAA 2a00:1450:4010:c08::5e OPT
659	8.853875915	192.168.0.1	192.168.0.106	DNS	104	Standard query response 0xa592 A fonts.gstatic.com A 173.184.73.84 OPT
660	8.853875976	192.168.0.1	192.168.0.106	DNS	104	Standard query response 0xb548 A fonts.gstatic.com A 173.184.73.84 OPT
661	8.853876026	192.168.0.1	192.168.0.106	DNS	116	Standard query 0x7770 AAAA fonts.gstatic.com AAAA 2a00:1450:4010:c08::5e OPT
1032	19.134807089	192.168.0.106	192.168.0.1	DNS	106	Standard query 0xb5a7 AAAA optimizationid-pa.googleapis.com OPT
1033	19.134809123	192.168.0.106	192.168.0.1	DNS	106	Standard query 0x7341 A optimizationid-pa.googleapis.com OPT
1034	19.134956759	192.168.0.106	192.168.0.1	DNS	106	Standard query 0x1318 A optimizationid-pa.googleapis.com OPT
1035	19.135019116	192.168.0.106	192.168.0.1	DNS	106	Standard query 0x2981 AAAA optimizationid-pa.googleapis.com OPT
1036	19.137711374	192.168.0.106	192.168.0.1	DNS	87	Standard query 0x7b70 A guryanov-plasticurgeon.ru OPT
1037	19.137711616	192.168.0.106	192.168.0.1	DNS	87	Standard query 0xb557 AAAA guryanov-plasticurgeon.ru OPT
1038	19.137892314	192.168.0.106	192.168.0.1	DNS	97	Standard query 0x4a25 A guryanov-plasticurgeon.ru OPT
1039	19.137891847	192.168.0.106	192.168.0.1	DNS	97	Standard query 0x4a25 A guryanov-plasticurgeon.ru OPT
1040	19.141476819	192.168.0.1	192.168.0.106	DNS	218	Standard query response 0xb5a7 AAAA optimizationid-pa.googleapis.com AAAA 2a00:1450:4010:c08::5f AAAA 2a00:1450:4010:c0f::5f AAAA 2a00:1450:4010:c03::5f AAAA 2a00:1450:4010:c07::5f
1041	19.141477180	192.168.0.1	192.168.0.106	DNS	206	Standard query response 0x7341 A optimizationid-pa.googleapis.com A 64.233.161.95 A 173.184.73.95 A 64.233.164.95 A 209.85.233.95 A 74.125.131.95 A 142.251.1.95
1042	19.141477259	192.168.0.1	192.168.0.106	DNS	206	Standard query response 0x1318 A optimizationid-pa.googleapis.com A 74.125.131.95 A 142.251.1.95 A 64.233.164.95 A 64.233.162.95 A 209.85.233.95 A 64.233.165.95
1043	19.141477398	192.168.0.1	192.168.0.106	DNS	218	Standard query response 0x2981 AAAA optimizationid-pa.googleapis.com AAAA 2a00:1450:4010:c03::5f AAAA 2a00:1450:4010:c08::5f AAAA 2a00:1450:4010:c0f::5f AAAA 2a00:1450:4010:c07::5f
1044	19.141477398	192.168.0.1	192.168.0.106	DNS	137	Standard query response 0xb570 A guryanov-plasticurgeon.ru A 195.24.68.22 OPT
1045	19.141477429	192.168.0.1	192.168.0.106	DNS	127	Standard query response 0xf425 A guryanov-plasticurgeon.ru A 195.24.68.22 OPT
1047	19.144584804	192.168.0.106	192.168.0.1	DNS	84	Standard query 0xb518 A safebrowsing.google.com OPT
1048	19.144581623	192.168.0.106	192.168.0.1	DNS	94	Standard query 0xf83c A safebrowsing.google.com OPT
1049	19.144587061	192.168.0.106	192.168.0.1	DNS	94	Standard query 0xb518 A safebrowsing.google.com OPT
1050	19.144602563	192.168.0.106	192.168.0.1	DNS	94	Standard query 0x914a AAAA safebrowsing.google.com OPT
1051	19.151362107	192.168.0.1	192.168.0.106	DNS	235	Standard query response 0xb5c1 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2607:fb80:4001:c1b::50 AAAA 2607:fb80:4001:c1b::88 AAAA 2607:fb80:4001:c1b::5d AAAA 2607:fb80:4001:c1b::88 AAAA 2607:fb80:4001:c1b::5d
1052	19.151362768	192.168.0.1	192.168.0.106	DNS	139	Standard query response 0xf83c A safebrowsing.google.com CNAME sb.l.google.com A 142.250.183.46 OPT
1053	19.151362818	192.168.0.1	192.168.0.106	DNS	139	Standard query response 0xb5c1 A safebrowsing.google.com CNAME sb.l.google.com A 142.250.183.46 OPT
1054	19.151362868	192.168.0.1	192.168.0.106	DNS	235	Standard query response 0xb5c1 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2607:fb80:4001:c1b::50 AAAA 2607:fb80:4001:c1b::88 AAAA 2607:fb80:4001:c1b::5d AAAA 2607:fb80:4001:c1b::88
1063	19.164402653	192.168.0.1	192.168.0.106	DNS	149	Standard query response 0xb5a2 AAAA safebrowsing.google.com SOA ns3.nic.ru OPT
1064	19.164403014	192.168.0.1	192.168.0.106	DNS	149	Standard query response 0xb557 AAAA guryanov-plasticurgeon.ru SOA ns3.nic.ru OPT
1228	20.564439933	192.168.0.106	192.168.0.1	DNS	91	Standard query 0x7726 A fonts.googleapis.com OPT
1229	20.564503815	192.168.0.106	192.168.0.1	DNS	91	Standard query 0xb5a7 AAAA fonts.googleapis.com OPT
1230	20.564558545	192.168.0.106	192.168.0.1	DNS	91	Standard query 0xf8f1 A fonts.googleapis.com OPT
1231	20.564605152	192.168.0.106	192.168.0.1	DNS	91	Standard query 0x732a AAAA platform.twitter.com OPT
1232	20.567171372	192.168.0.106	192.168.0.1	DNS	91	Standard query 0x770f A platform.twitter.com OPT
1236	20.567513172	192.168.0.106	192.168.0.1	DNS	91	Standard query 0x732a AAAA platform.twitter.com OPT
1237	20.567626885	192.168.0.106	192.168.0.1	DNS	91	Standard query 0x484e A platform.twitter.com OPT
1238	20.567614465	192.168.0.106	192.168.0.1	DNS	91	Standard query 0x4847 AAAA platform.twitter.com OPT
1239	20.567615379	192.168.0.106	192.168.0.1	DNS	78	Standard query 0x1e63 A s.w.org OPT
1240	20.567699427	192.168.0.106	192.168.0.1	DNS	78	Standard query 0x1e63 AAAA s.w.org OPT
1241	20.568019711	192.168.0.106	192.168.0.1	DNS	78	Standard query 0x1e63 AAAA s.w.org OPT
1242	20.568078857	192.168.0.106	192.168.0.1	DNS	78	Standard query 0xb061 A s.w.org OPT
1243	20.568082005	192.168.0.1	192.168.0.106	DNS	119	Standard query response 0xb5a7 AAAA fonts.googleapis.com AAAA 2a00:1450:4010:c02::5f OPT
1244	20.568083945	192.168.0.1	192.168.0.106	DNS	107	Standard query response 0x7726 A fonts.googleapis.com A 74.125.285.95 OPT
1245	20.568083915	192.168.0.1	192.168.0.106	DNS	119	Standard query response 0x1e63 AAAA fonts.googleapis.com AAAA 2a00:1450:4010:c02::5f OPT
1246	20.568083975	192.168.0.1	192.168.0.106	DNS	107	Standard query response 0xf8f1 A fonts.googleapis.com A 74.125.285.95 OPT
1248	20.571223599	192.168.0.1	192.168.0.106	DNS	285	Standard query response 0xc99a AAAA platform.twitter.com CNAME cs472.wac.ebocastcdn.net CNAME cs1-spr-8315.wac.ebocastcdn.net CNAME wac-spr-8315.ebocastcdn.net CNAME cs1-lb-ru...



## Ответы на вопросы

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

Мною был очищен кэш DNS, из-за чего мой компьютер не знал IP-адрес сайта, к которому шло обращение. Для того, чтобы его узнать, был отправлен DNS запрос типа A на рекурсивный сервер, чтобы узнать IP-адрес ресурса версии 4. Кроме этого был отправлен запрос типа AAAA, чтобы получить адрес IPv6. В свою очередь рекурсивный сервер вернул адрес запрашиваемого ресурса.

```
Domain Name System (query)
Transaction ID: 0x7b70
Flags: 0x0100 Standard query
  0... .. = Response: Message is a query
  .000 0... .. = Opcode: Standard query (0)
  ... .. = Truncated: Message is not truncated
  ...1... .. = Recursion desired: Do query recursively
  ... .. = Z: reserved (0)
  ... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
  guryanov-plasticsurgeon.ru: type A, class IN
    Name: guryanov-plasticsurgeon.ru
    [Name Length: 26]
    [Label Count: 2]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Additional records
  <Root>: type OPT
    Name: <Root>
    Type: OPT (41)
    UDP payload size: 1472
    Higher bits in extended RCODE: 0x00
    EDNS0 version: 0
    Z: 0x0000
      0... .. = DO bit: Cannot handle DNSSEC security RRs
      .000 0000 0000 0000 = Reserved: 0x0000
    Data length: 0
[Response To: 10441]

Domain Name System (response)
Transaction ID: 0x7b70
Flags: 0x8100 Standard query response, No error
  1... .. = Response: Message is a response
  .000 0... .. = Opcode: Standard query (0)
  ... .. = Authoritative: Server is not an authority for domain
  ... .. = Truncated: Message is not truncated
  ...1... .. = Recursion desired: Do query recursively
  ... .. = Recursion available: Server can do recursive queries
  ... .. = Z: reserved (0)
  ... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
  ... .. = Non-authenticated data: Unacceptable
  ... .. = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
  guryanov-plasticsurgeon.ru: type A, class IN
    Name: guryanov-plasticsurgeon.ru
    [Name Length: 26]
    [Label Count: 2]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Answers
  GURYANOV-PLASTICSURGEON.ru: type A, class IN, addr 195.24.68.22
    Name: GURYANOV-PLASTICSURGEON.ru
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 3246 (54 minutes, 6 seconds)
    Data length: 4
    Address: 195.24.68.22
Additional records
  <Root>: type OPT
    Name: <Root>
    Type: OPT (41)
    UDP payload size: 1232
    Higher bits in extended RCODE: 0x00
    EDNS0 version: 0
    Z: 0x0000
      0... .. = DO bit: Cannot handle DNSSEC security RRs
      000 0000 0000 0000 = Reserved: 0x0000
    Data length: 0
[Request In: 1036]
[Time: 0.002765608 seconds]
```

### 2. Какие бывают типы DNS-запросов?

Итеративный (он же *прямой*, он же *нерекурсивный*) запрос посылает доменное имя DNS серверу и просит вернуть либо IP адрес этого домена,

либо имя DNS сервера, авторитативного для этого домена. При этом, сервер DNS не опрашивает другие серверы для получения ответа. Так работают корневые и TLD серверы.

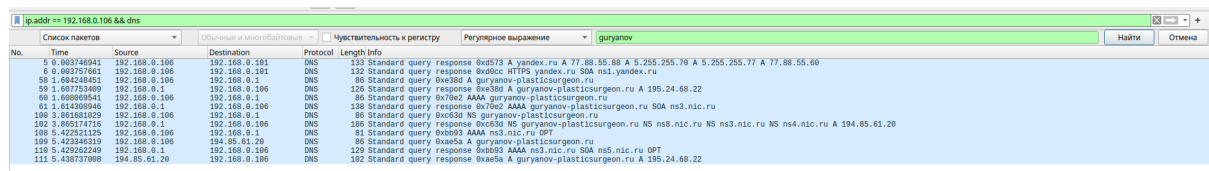
Рекурсивный запрос посылает DNS серверу доменное имя и просит возвратить IP адрес запрошенного домена. При этом сервер может обращаться к другим DNS серверам.

Обратный запрос посылает IP и просит вернуть доменное имя.

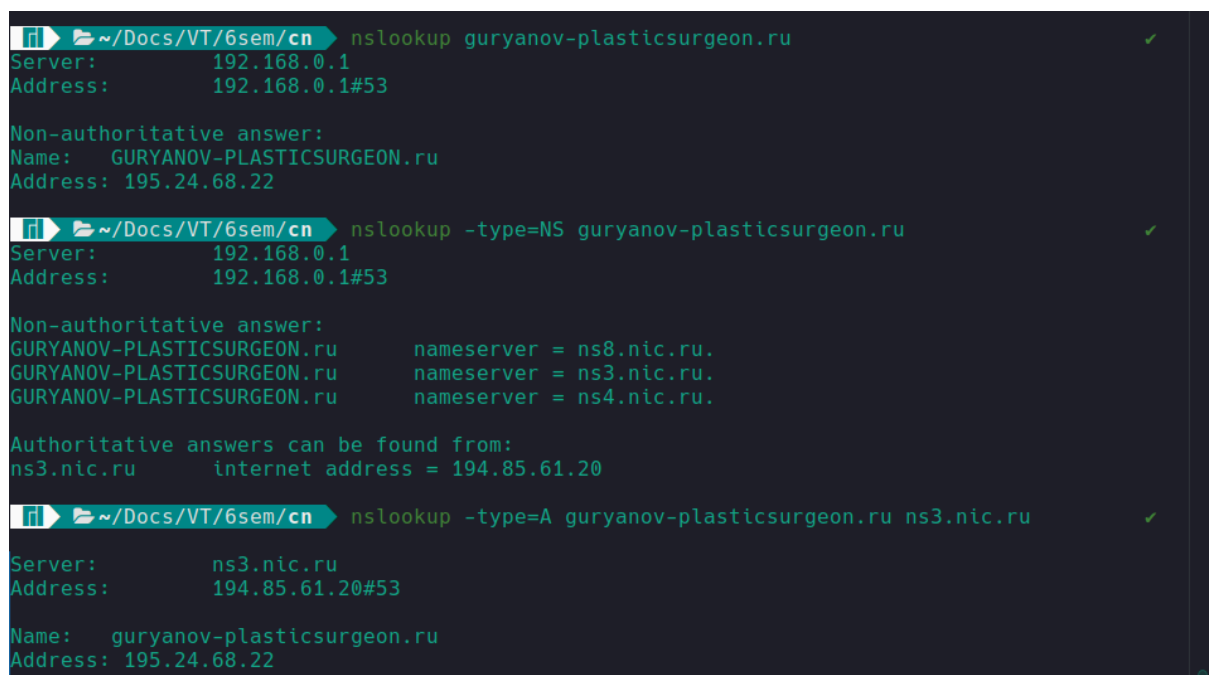
### 3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Выполнение дополнительных DNS-запросов необходимо, если изображения, содержащиеся на сайте, находятся на другом доменном имени. Также такая ситуация возможна в случае, если сайт использует CDN (Content Delivery Network) для ускорения загрузки сайта. С его помощью данные передаются быстро, независимо от местонахождения хоста. Это возможно благодаря распределенным по всему миру кэширующим серверам.

## Анализ трафика утилиты nslookup



No.	Time	Source	Destination	Protocol	Length	Info
5	0.003746041	192.168.0.106	192.168.0.181	DNS	133	Standard query response 0x5713 A yandex.ru A 77.88.55.88 A 5.255.255.70 A 5.255.255.77 A 77.88.55.60
6	0.003757651	192.168.0.106	192.168.0.181	DNS	132	Standard query response 0x5b0c HTTPS yandex.ru SOA ns1.yandex.ru
58	1.004248451	192.168.0.106	192.168.0.1	DNS	86	Standard query 0x638d A guryanov-plasticsurgeon.ru
59	1.007753400	192.168.0.1	192.168.0.106	DNS	126	Standard query response 0x638d A guryanov-plasticsurgeon.ru A 195.24.68.22
60	1.008069541	192.168.0.106	192.168.0.1	DNS	86	Standard query 0x70e2 AAAA guryanov-plasticsurgeon.ru
61	1.014300940	192.168.0.1	192.168.0.106	DNS	138	Standard query response 0x70e2 AAAA guryanov-plasticsurgeon.ru SOA ns3.nic.ru
100	3.881681029	192.168.0.106	192.168.0.1	DNS	86	Standard query 0xc63d NS guryanov-plasticsurgeon.ru
102	3.893174710	192.168.0.1	192.168.0.106	DNS	186	Standard query response 0xc63d NS guryanov-plasticsurgeon.ru NS ns8.nic.ru NS ns3.nic.ru NS ns4.nic.ru A 194.85.61.20
108	5.422521120	192.168.0.106	192.168.0.1	DNS	81	Standard query 0xb093 AAAA ns3.nic.ru OPT
109	5.423440310	192.168.0.106	194.85.61.20	DNS	86	Standard query 0xae5a A guryanov-plasticsurgeon.ru
110	5.426262240	192.168.0.1	192.168.0.106	DNS	129	Standard query response 0xb093 AAAA ns3.nic.ru SOA ns5.nic.ru OPT
111	5.438737008	194.85.61.20	192.168.0.106	DNS	182	Standard query response 0xae5a A guryanov-plasticsurgeon.ru A 195.24.68.22



```
~/Docs/VT/6sem/cn nslookup guryanov-plasticsurgeon.ru ✓
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   GURYANOV-PLASTICSURGEON.ru
Address: 195.24.68.22

~/Docs/VT/6sem/cn nslookup -type=NS guryanov-plasticsurgeon.ru ✓
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
GURYANOV-PLASTICSURGEON.ru      nameserver = ns8.nic.ru.
GURYANOV-PLASTICSURGEON.ru      nameserver = ns3.nic.ru.
GURYANOV-PLASTICSURGEON.ru      nameserver = ns4.nic.ru.

Authoritative answers can be found from:
ns3.nic.ru      internet address = 194.85.61.20

~/Docs/VT/6sem/cn nslookup -type=A guryanov-plasticsurgeon.ru ns3.nic.ru ✓
Server:      ns3.nic.ru
Address:     194.85.61.20#53

Name:   guryanov-plasticsurgeon.ru
Address: 195.24.68.22
```

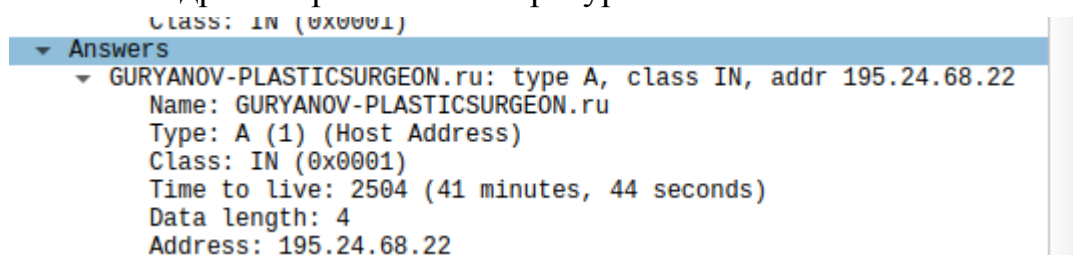
## Ответы на вопросы

### 1. Чем различается трасса трафика в п.2 и п.4, указанных выше?

Сначала nslookup посылает запрос на рекурсивный DNS-сервер с типом запроса A, чтобы узнать IP-адрес сервера по его url. DNS-сервер в своем ответе присылает IP-адрес узла. После этого мы посылаем DNS-запрос с type=NS, чтобы получить IP-адрес авторитарного сервера, на котором хранится информация о всех IP-адресах нашей зоны. В отчет получает IP-адрес авторитативного сервера. После этого посылаем DNS-запрос уже на авторитарный сервер по адресу 194.85.61.20 и получаем IP-адрес сайта.

### 2. Что содержится в поле «Answers» DNS-ответа?

Поле Answer содержит имя хоста, тип и класс записи, TTL, длину поля и IP-адрес запрашиваемого ресурса.



### 3. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?

С помощью утилиты nslookup было определено, что авторитативный ответ может вернуть сервер ns3.nic.ru

## **Вывод**

В ходе выполнения лабораторной работы был проведен анализ сетевого трафика с использованием программы Wireshark. Было проведено исследование пакетов, передаваемых при выполнении утилит `ping` и `tracert`, изучено их содержимое и информация, которую они несут. Также был проанализирован трафик DNS запросов и ответов, генерируемых утилитой `nslookup`. Оказалось, что кэширование также влияет на работу DNS, и в процессе работы нам пришлось очистить кэш и изучить работу DNS-запросов.