

## Лабораторная работа 3 “Wireshark: DNS”

Изучение дополнительных материалов.

### Локальные DNS-сервера

DNS (Domain Name System, система доменных имён) - иерархическая, распределенная в сети система баз данных, предоставляющая пользователям сети Интернет дополнительный сервис по автоматическому преобразованию запросов, оформленных в удобном для человека текстовом формате (например, `www.test.ru`) в цифровой IP-адрес компьютера (например, `192.1.1.1`), где находится искомый ресурс.

Локальный DNS-сервер - это сервер имен Вашей локальной сети или DNS-сервер Вашего интернет-провайдера.

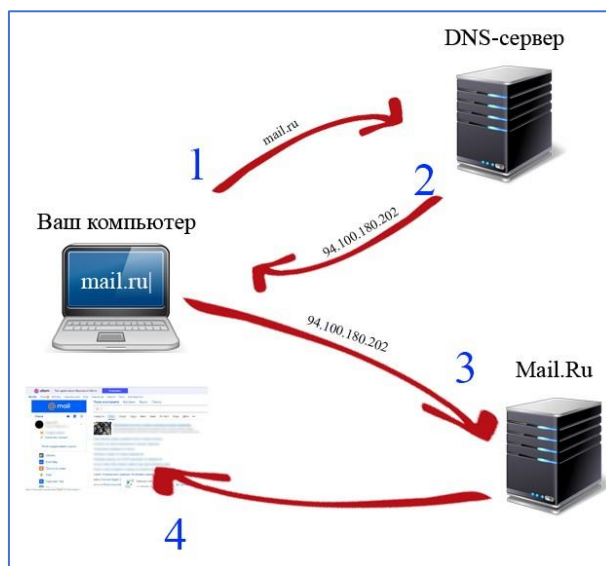


Рисунок 1, Локальные DNS-сервера

### DNS-кэширование

Кэширование DNS включает в себя хранение данных ближе к запрашивающему клиенту, так что разрешение DNS запроса и дополнительных запросов можно избежать, тем самым ускоряя время загрузки и снижения пропускную способность/потребление процессора. Данные DNS могут кэшироваться в различных расположениях, каждое из которых будет хранить записи DNS в течение определенного периода времени.

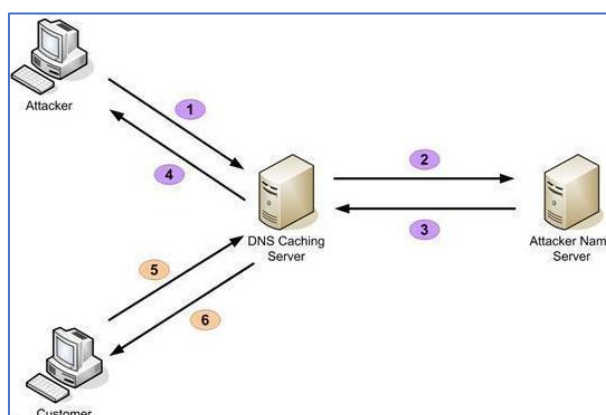


Рисунок 2, DNS-кэширование

## Ресурсные записи DNS

Ресурсные записи DNS — это записи о соответствии имени и служебной информации в системе доменных имен, например, соответствие имени домена и IP-адреса. Редактирование ресурсных записей для доменного имени производится на стороне держателя NS-серверов (например, хостинг-провайдера, на NS-серверы которого делегировано доменное имя).

Имя домена, ресурсы которого описаны в этой записи .....	
Тип	Класс
Время жизни (TTL)	
Длина записи о ресурсах	Информация о ресурсах

Рисунок 3, Ресурсные записи DNS

## Поля ресурсных записей DNS

- **Name / Hostname** (Имя, хост, домен — имеет несколько названий). Определяет домен, к которому относится (привязана) данная ресурсная запись.
- **Type** (Тип). Указывает на тип (назначение) данной ресурсной записи. Наиболее распространенные типы DNS-записей — A, AAAA, MX, CNAME и TXT.
- **Class** (Класс). Здесь указывается тип рабочей сети. Теоретически, система может работать во всех ее типах. Но, TCP/IP сети — самые распространенные. Поэтому, поле редко используется.
- **TTL** (Time To Live) — время жизни (хранения) DNS-записи.
- **RDATA** (Resource Data) — значение данного поля ресурсной записи зависит от ее конкретного типа.
- **Priority** (Приоритет) — задает приоритет (очередность) обработки конкретной DNS-записи.
- **Protocol** (Протокол) — указывает на протокол, используемый TCP, UDP, TLS.
- **Service Name** (Имя сервиса) — его можно посмотреть в файле /etc/services. Например: pop3, telnet.
- **Weight** (Вес) — задает вес хоста. Обработка запросов распределяется по весу хоста.
- **Address** (Адрес) — IP-адрес, который автоматически конвертируется в in-addr.arpa формат.

## Материалы:

- Работа с DNS // HOSTLINE URL: <https://hostline.ru/support/36264281-rabota-s-dns#:~:text=Локальный%20DNS-сервер%20-%20это%20сервер,сети%20или%20DNS-сервер%20Вашего%20интернет-провайдера> (дата обращения: 17.03.2023).
- Кэширование DNS // RECONN URL: <https://reconn.ru/kb/network/keshirovanie-dns#:~:text=Кэширование%20DNS%20включает%20в%20себя,в%20течение%20определенного%20периода%20времени> (дата обращения: 17.03.2023).
- Типы DNS-записей // timeweb URL: <https://timeweb.com/ru/docs/domeny/resursnye-zapisi-domena-dns-zapisi/tipy-dns-zapisej/> (дата обращения: 17.03.2023).
- Что такое DNS-записи и какие типы бывают // eternalhost URL: <https://eternalhost.net/base/domeny/tipy-dns-zapisey> (дата обращения: 17.03.2023).

## Часть 1: nslookup

### 1. Выполните nslookup, чтобы получить IP-адрес веб-сервера petrsu.ru. Какой адрес вы получили?

В выводе утилиты мы можем видеть ip адрес 192.232.254.218, это не адрес сервера, а наш, системный DNS сервер. В следующей строке выводится тот же ip адрес и порт, это адрес DNS сервера вместе с портом. По умолчанию порт - 53. И только после этого находится информация про запрашиваемый сайт. Наш ip адрес 194.85.173.228, это означает, что все пакеты, которые вы будете отправлять на petrsu.ru будут приходить на этот адрес.

```
nikita@nikitagordeev10:~$ nslookup petrsu.ru
Server:      192.168.117.108
Address:     192.168.117.108#53

Non-authoritative answer:
Name:   petrsu.ru
Address: 194.85.173.228
```

Иллюстрация 1, IP-адрес веб-сервера petrsu.ru

### 2. Выполните nslookup, чтобы определить авторитетные DNS-сервера для petrsu.ru. Какие у них адреса?

```
nikita@nikitagordeev10:~$ nslookup -type=NS petrsu.ru
Server:      192.168.117.108
Address:     192.168.117.108#53

Non-authoritative answer:
petrsu.ru    nameserver = ns.petrus.ru.
petrsu.ru    nameserver = ns.karelia.ru.

Authoritative answers can be found from:
ns.petrus.ru internet address = 193.232.254.218
```

Иллюстрация 2, авторитетные DNS-сервера

### 3. Выполните nslookup таким образом, чтобы задействовать конкретный DNS-сервер (не сервер по умолчанию) для получения IP-адрес веб-сервера petrsu.ru. В качестве адреса DNS-сервера можно использовать результат из п.2.

```
nikita@nikitagordeev10:~$ nslookup petrsu.ru ns.petrus.ru
Server:      ns.petrus.ru
Address:     193.232.254.218#53

Name:   petrsu.ru
Address: 194.85.173.228

nikita@nikitagordeev10:~$ nslookup petrsu.ru ns.karelia.ru
Server:      ns.karelia.ru
Address:     194.85.172.133#53

Name:   petrsu.ru
Address: 194.85.173.228
```

Иллюстрация 3, запрос конкретному DNS-серверу

## Часть 2: Ipconfig

### 4. Выполните приведенные выше вариации команды ipconfig, изучите их вывод.

```
Командная строка
C:\Users\nikit>ipconfig -all

Настройка протокола IP для Windows

Имя компьютера . . . . . : nikitagordeev10
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-термутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет

Адаптер Ethernet Ethernet:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek PCIe GbE Family Controller
Физический адрес. . . . . : A8-5E-45-BE-67-C6
DHCP включен. . . . . : Да
Автонастройка включена . . . . . : Да

Неизвестный адаптер ProtonVPN TUN:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : ProtonVPN Tunnel
Физический адрес. . . . . :
DHCP включен. . . . . : Нет
Автонастройка включена . . . . . : Да

Адаптер Ethernet vEthernet (BluestacksNxt):

DNS-суффикс подключения . . . . . :
Описание. . . . . : Hyper-V Virtual Ethernet Adapter
Физический адрес. . . . . : 00-15-5D-E6-58-5C
DHCP включен. . . . . : Нет
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::bad8:7bf:6fe:a212k7(Основной)
IPv4-адрес. . . . . : 172.31.128.1(Основной)
Маска подсети . . . . . : 255.255.240.0
Основной шлюз. . . . . :
IATD DHCPv6 . . . . . : 1023415645
DUID клиента DHCPv6 . . . . . : 00-01-00-01-25-73-9F-F2-A8-5E-45-BE-67-C6
DNS-серверы. . . . . : fec0:0:0:ffff::1k1
                        fec0:0:0:ffff::2k1
                        fec0:0:0:ffff::3k1
NetBios через TCP/IP. . . . . : Включен

Адаптер Ethernet VirtualBox Host-Only Network:

DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес. . . . . : 0A-00-27-00-00-14
```

Иллюстрация 4, ipconfig /all

```
Командная строка
C:\Users\nikit>ipconfig /displaydns

Настройка протокола IP для Windows

array615.prod.do.dsp.mp.microsoft.com
-----
Имя записи. . . . . : array615.prod.do.dsp.mp.microsoft.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 2350
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
A-запись (узла) . . . : 20.54.24.246

push.yandex.ru
-----
Имя записи. . . . . : push.YANDEX.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 385
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
A-запись (узла) . . . : 213.180.204.179

cloud-api.yandex.net
-----
Имя записи. . . . . : cloud-api.yandex.net
Тип записи. . . . . : 5
Срок жизни. . . . . : 135
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : api.disk.yandex.net

Имя записи. . . . . : api.disk.yandex.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 135
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
A-запись (узла) . . . : 213.180.204.127

book.itep.ru
-----
Имя записи. . . . . : book.itep.ru
Тип записи. . . . . : 5
Срок жизни. . . . . : 18632
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : saturn.itep.ru
```

Иллюстрация 5, ipconfig /displaydns

```
C:\Users\nikit>ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
```

Иллюстрация 6, ipconfig /flushdns

## Часть 3: DNS-трассировка с использованием Wireshark

Адаптер беспроводной локальной сети Беспроводная сеть:

```
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . : fe80::696d:aab9:47ca:2ff3%19  
IPv4-адрес . . . . . : 192.168.117.87  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз . . . . . : 192.168.117.108
```

Иллюстрация 7, ipconfig

### Часть 3.1: www.ietf.org

## 5. Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?

No.	Time	Source	Destination	Protocol	Length	Info
22	6.264879	192.168.117.87	192.168.117.108	DNS	72	Standard query 0x87b A www.ietf.org
23	6.271108	192.168.117.87	192.168.117.108	DNS	72	Standard query response 0x5c2b A www.ietf.org
24	6.271630	192.168.117.87	192.168.117.108	DNS	72	Standard query 0xfc9b HTTPS www.ietf.org
25	6.372022	192.168.117.108	192.168.117.87	DNS	149	Standard query response 0x5c2b A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
26	6.372272	192.168.117.108	192.168.117.87	DNS	149	Standard query response 0x87b A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
27	6.372393	192.168.117.108	192.168.117.87	DNS	196	Standard query response 0xfc9b HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS
28	6.374717	192.168.117.87	192.168.117.108	DNS	94	Standard query 0xce36 A nav-edge.smartscreen.microsoft.com
29	6.375066	192.168.117.87	192.168.117.108	DNS	94	Standard query 0xa3bc HTTPS nav-edge.smartscreen.microsoft.com
30	6.376621	192.168.117.87	192.168.117.108	DNS	72	Standard query 0x80e0 A www.ietf.org
31	6.376933	192.168.117.87	192.168.117.108	DNS	72	Standard query 0x3320 HTTPS www.ietf.org
32	6.385371	192.168.117.108	192.168.117.87	DNS	149	Standard query response 0x80e0 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
33	6.435584	192.168.117.108	192.168.117.87	DNS	290	Standard query response 0xa3bc HTTPS nav-edge.smartscreen.microsoft.com CNAME tm-prod-wd-csp-edge.trafficmanager.net C...
34	6.435981	192.168.117.108	192.168.117.87	DNS	229	Standard query response 0xce36 A nav-edge.smartscreen.microsoft.com CNAME tm-prod-wd-csp-edge.trafficmanager.net CNAME...
35	6.436285	192.168.117.108	192.168.117.87	DNS	196	Standard query response 0x3320 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS
38	6.436491	192.168.117.87	192.168.117.108	ICMP	224	Destination unreachable (Port unreachable)
402	7.224534	192.168.117.87	192.168.117.108	DNS	78	Standard query 0xfd45 A analytics.ietf.org
403	7.224893	192.168.117.87	192.168.117.108	DNS	78	Standard query response 0x2f65 HTTPS analytics.ietf.org
441	7.352872	192.168.117.108	192.168.117.87	DNS	161	Standard query response 0xfd45 A analytics.ietf.org CNAME analytics.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.1...
445	7.352872	192.168.117.108	192.168.117.87	DNS	208	Standard query response 0x2f65 HTTPS analytics.ietf.org CNAME analytics.ietf.org.cdn.cloudflare.net HTTPS

Иллюстрация 8, захват пакетов

UDP payload (239 bytes)
> Domain Name System (response)

Иллюстрация 9, тип запроса

- DNS использует UDP port 53, но TCP port 53 также зарезервирован под использование для DNS.
- Большинство DNS-запросов будет обрабатываться с использованием протокола UDP, исключение составляют трансфер зоны (Query type AXFR) и ответы сервера, превышающие 512 байт на одно сообщение.
- Чтобы не использовались для DDoS.

Материалы: DNS использует UDP или TCP? Что говорит RFC // SecurityLab.ru URL:  
<https://www.securitylab.ru/news/536997.php> (дата обращения: 17.03.2023).

## 6. Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?

destination port – порт назначения;

source port – исходящий порт

User Datagram Protocol, Src Port: 62851, Dst Port: 53
Source Port: 62851
Destination Port: 53
Length: 38

Иллюстрация 10, → www.ietf.org

User Datagram Protocol, Src Port: 53, Dst Port: 62851
Source Port: 53
Destination Port: 62851
Length: 115

Иллюстрация 11, ← www.ietf.org

7. На какой IP-адрес отправлен DNS-запрос? Используйте `ipconfig` для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?

```
Адаптер беспроводной локальной сети Беспроводная сеть:  
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . . : fe80::696d:aab9:47ca:2ff3%19  
IPv4-адрес. . . . . : 192.168.117.87  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . : 192.168.117.108
```

Иллюстрация 12, `ipconfig`

No.	Time	Source	Destination	Protocol	Length	Info
14	2.178109	192.168.117.87	192.168.117.108	DNS	72	Standard query 0x9b9d A www.ietf.org
15	2.174704	192.168.117.108	192.168.117.87	DNS	149	Standard query response 0x9b9d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99

Иллюстрация 13, DNS-запрос

8. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

```
▼ Queries  
> www.ietf.org: type A, class IN  
\[Response In: 30\]
```

Иллюстрация 14, тип запроса

Типы dns записей, используемые чаще всего:

- **A (IPv4 Address Record - адресная запись)** - связывает доменное имя с IPv4-адресом хоста
- **AAAA (IPv6 Address Record)** - связывает доменное имя с IPv6-адресом хоста (аналогично A-записи)
- **CNAME (Canonical Name Record - каноническая запись имени)** - используется для перенаправления на другое доменное имя
- **MX (Mail Exchange - почтовый обменник)** - ссылается на почтовый сервер, обслуживающий домен
- **NS (Name Server - сервер имен)** - ссылается на DNS-сервер, ответственный за домен
- **TXT** - текстовое описание домена. Зачастую требуется для выполнения специфических задач (например, подтверждения права собственности на домен при привязке его к почтовому сервису)
- **PTR (Point to Reverse - запись указателя)** - связывает ip-адрес машины с доменом, используется преимущественно для проверки сторонними почтовыми сервисами отправляемых через эту машину электронных писем на отношение к домену, указанному в параметрах почтового сервера. При несоответствии этих параметров письмо проверяется более тщательно по другим критериям.

Материалы:

- Основы работы со службой DNS // 1cloud URL: [https://1cloud.ru/help/dns/dns\\_basics](https://1cloud.ru/help/dns/dns_basics) (дата обращения: 17.03.2023).

9. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

```
Domain Name System (response)
Transaction ID: 0x9b9d
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
< Queries
> www.ietf.org: type A, class IN
< Answers
  < www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1407 (23 minutes, 27 seconds)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  < www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 208 (3 minutes, 28 seconds)
    Data length: 4
    Address: 104.16.45.99
  < www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 208 (3 minutes, 28 seconds)
    Data length: 4
    Address: 104.16.44.99
[Request In: 14]
[Time: 0.004595000 seconds]
```

Иллюстрация 15, ответное сообщение DNS с ресурсными записями DNS

10. Посмотрите на последующий TCP-пакет с флагом SYN, отправленный вашим компьютером. Соответствует ли IP-адрес назначения пакета с SYN одному из адресов, приведенных в ответном сообщении DNS?

Да, содержит

33	6.391251	192.168.117.87	104.16.44.99	TCP	66	61127 → 443 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
----	----------	----------------	--------------	-----	----	-------------------	---

Иллюстрация 16, TCP-пакет с флагом SYN

11. Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

В вашем случае с несколькими изображениями на одной странице Chrome кэширует запись dns и использует ее для всех. Похоже, что chrome будет кэшироваться в течение ~ 30 секунд, а по истечении этого срока он попадет в ваш локальный системный распознаватель, который может кэшировать его дольше в зависимости от вашей конфигурации. Только если это не удастся, он выйдет по сети и сделает дальнейшие DNS-запросы.



## Часть 3.2: nslookup для сервера petrsu.ru

### 12. Сколько пар DNS запрос-ответ появилось в списке?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.117.87	213.180.193.234	TCP	55	60747 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
2	0.100256	213.180.193.234	192.168.117.87	TCP	66	443 → 60747 [ACK] Seq=1 Ack=2 Win=2278 Len=0 SLE=1 SRE=2
3	0.896425	192.168.117.87	149.154.167.41	SSL	399	Continuation Data
4	0.979065	149.154.167.41	192.168.117.87	SSL	1294	Continuation Data
5	0.981876	192.168.117.87	149.154.167.41	SSL	383	Continuation Data
6	0.985738	149.154.167.41	192.168.117.87	SSL	1294	Continuation Data
7	0.985820	192.168.117.87	149.154.167.41	TCP	54	59960 → 443 [ACK] Seq=675 Ack=2481 Win=256 Len=0
8	0.985921	149.154.167.41	192.168.117.87	SSL	548	Continuation Data
9	0.986009	192.168.117.87	149.154.167.41	TCP	54	59960 → 443 [ACK] Seq=675 Ack=2975 Win=254 Len=0
10	1.087862	213.180.204.179	192.168.117.87	TLSv1..	136	Application Data
11	1.100129	149.154.167.41	192.168.117.87	TCP	54	443 → 59960 [ACK] Seq=2975 Ack=675 Win=21177 Len=0
12	1.130475	192.168.117.87	213.180.204.179	TCP	54	60125 → 443 [ACK] Seq=1 Ack=83 Win=260 Len=0
13	1.469595	192.168.117.87	91.105.192.100	SSL	319	Continuation Data
14	1.563074	91.105.192.100	192.168.117.87	TCP	54	443 → 61270 [ACK] Seq=1 Ack=266 Win=2115 Len=0
15	2.912809	192.168.117.87	192.168.117.108	DNS	88	Standard query 0x0001 PTR 108.117.168.192.in-addr.arpa
16	2.916752	192.168.117.108	192.168.117.87	DNS	88	Standard query response 0x0001 No such name PTR 108.117.168.192.in-addr.arpa
17	2.918862	192.168.117.87	192.168.117.108	DNS	69	Standard query 0x0002 A petrsu.ru
18	3.036211	192.168.117.108	192.168.117.87	DNS	85	Standard query response 0x0002 A petrsu.ru A 194.85.173.228
19	3.043423	192.168.117.87	192.168.117.108	DNS	69	Standard query 0x0003 AAAA petrsu.ru
20	3.047547	192.168.117.108	192.168.117.87	DNS	69	Standard query response 0x0003 AAAA petrsu.ru
21	4.834266	192.168.117.87	51.140.202.63	TLSv1..	112	Application Data

Иллюстрация 17, 3 пары DNS запрос-ответ

### 13. Рассмотрите пару с типе A. Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?

destination port – порт назначения;

source port – исходящий порт

User Datagram Protocol, Src Port: 63048, Dst Port: 53
Source Port: 63048
Destination Port: 53

Иллюстрация 18, запрос DNS

User Datagram Protocol, Src Port: 53, Dst Port: 63048
Source Port: 53
Destination Port: 63048

Иллюстрация 19, ответ DNS

### 14. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

```
Адаптер беспроводной локальной сети Беспроводная сеть:
DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . . : fe80::696d:aab9:47ca:2ff3%19
IPv4-адрес . . . . . : 192.168.117.87
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 192.168.117.108
```

Иллюстрация 20, ipconfig

```
C:\Users\nikit>nslookup petrsu.ru
Server: UnKnown
Address: 192.168.117.108

Non-authoritative answer:
Name: petrsu.ru
Address: 194.85.173.228
```

Иллюстрация 21, nslookup

15	2.912809	192.168.117.87	192.168.117.108	DNS	88	Standard query 0x0001 PTR 108.117.168.192.in-addr.arpa
16	2.916752	192.168.117.108	192.168.117.87	DNS	88	Standard query response 0x0001 No such name PTR 108.117.168.192.in-addr.arpa
17	2.918862	192.168.117.87	192.168.117.108	DNS	69	Standard query 0x0002 A petrsu.ru
18	3.036211	192.168.117.108	192.168.117.87	DNS	85	Standard query response 0x0002 A petrsu.ru A 194.85.173.228
19	3.043423	192.168.117.87	192.168.117.108	DNS	69	Standard query 0x0003 AAAA petrsu.ru
20	3.047547	192.168.117.108	192.168.117.87	DNS	69	Standard query response 0x0003 AAAA petrsu.ru

Иллюстрация 22, Wireshark

### 15. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?



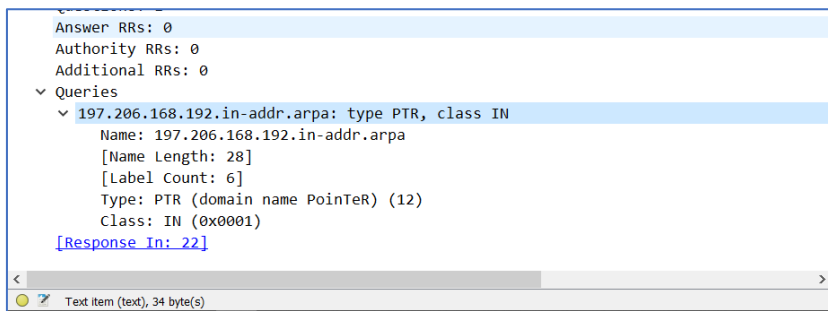


Иллюстрация 23, запрос PTR

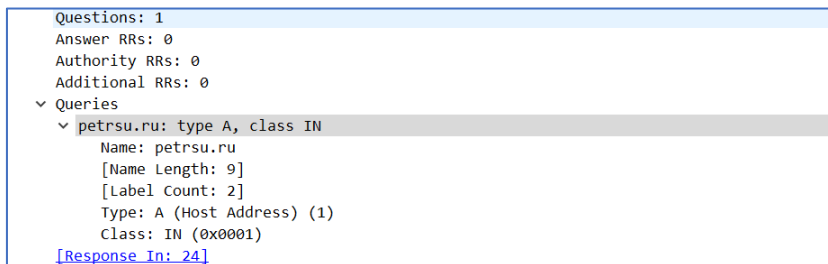


Иллюстрация 24, запрос A

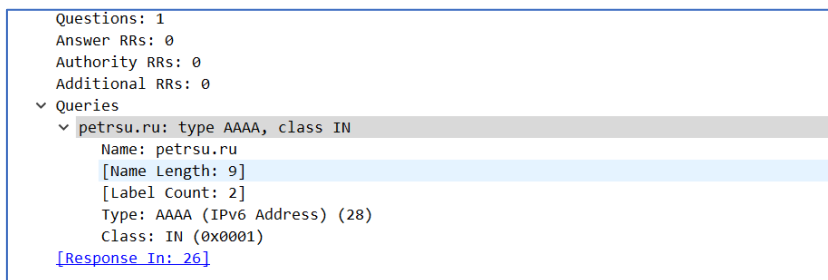


Иллюстрация 25, запрос AAAA

**A (IPv4 Address Record - адресная запись)** - связывает доменное имя с IPv4-адресом хоста

**AAAA (IPv6 Address Record)** - связывает доменное имя с IPv6-адресом хоста (аналогично A-записи)

**PTR (Point to Reverse - запись указателя)** - связывает ip-адрес машины с доменом, используется преимущественно для проверки сторонними почтовыми сервисами отправляемых через эту машину электронных писем на отношение к домену, указанному в параметрах почтового сервера. При несоответствии этих параметров письмо проверяется более тщательно по другим критериям.

**16. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?**

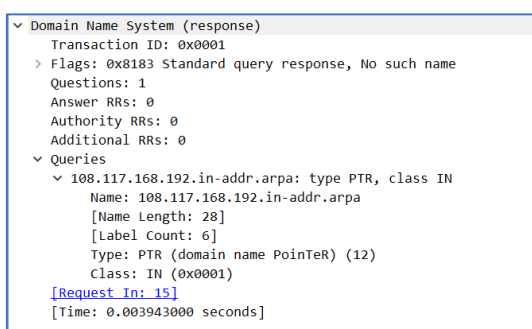


Иллюстрация 26, запрос PTR

```

v Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v petrsu.ru: type A, class IN
      Name: petrsu.ru
      [Name Length: 9]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  v Answers
    v petrsu.ru: type A, class IN, addr 194.85.173.228
      Name: petrsu.ru
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 180 (3 minutes)
      Data length: 4
      Address: 194.85.173.228
      [Request In: 17]
      [Time: 0.117349000 seconds]

```

Иллюстрация 27, запрос A

```

v Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v petrsu.ru: type AAAA, class IN
      Name: petrsu.ru
      [Name Length: 9]
      [Label Count: 2]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      [Request In: 19]
      [Time: 0.004124000 seconds]

```

Иллюстрация 28, запрос AAAA

### Часть 3.3: nslookup -type=NS petrsu.ru

17. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

```
Адаптер беспроводной локальной сети Беспроводная сеть:  
  
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . . : fe80::696d:aab9:47ca:2ff3%19  
IPv4-адрес. . . . . : 192.168.117.87  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . : 192.168.117.108
```

Иллюстрация 29, ipconfig

```
C:\Users\nikit>nslookup -type=NS petrsu.ru  
Server: Unknown  
Address: 192.168.117.108  
  
Non-authoritative answer:  
petrsu.ru nameserver = ns.petrsu.ru  
petrsu.ru nameserver = ns.karelia.ru  
  
ns.petrsu.ru internet address = 193.232.254.218  
ns.karelia.ru internet address = 194.85.172.133
```

Иллюстрация 30, nslookup

6 0.303557	52.149.21.60	192.168.117.87	TCP	54 443 → 60293 [ACK] Seq=362 Ack=3794 Win=2046 Len=0
7 2.766564	192.168.117.87	192.168.117.108	DNS	88 Standard query 0x0001 PTR 108.117.168.192.in-addr.arpa
8 2.800704	192.168.117.108	192.168.117.87	DNS	88 Standard query response 0x0001 No such name PTR 108.117.168.192.in-addr.arpa
9 2.804346	192.168.117.87	192.168.117.108	DNS	69 Standard query 0x0002 NS petrsu.ru
10 2.872214	192.168.117.108	192.168.117.87	DNS	145 Standard query response 0x0002 NS petrsu.ru NS ns.karelia.ru NS ns.petrsu.ru A 193.232.254.218 A 194.85.172.133
11 3.747656	192.168.117.87	213.180.193.234	TCP	55 61544 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
12 3.836448	213.180.193.234	192.168.117.87	TCP	66 443 → 61544 [ACK] Seq=1 Ack=3 Win=356 Len=0 FIN=1

Иллюстрация 31, Wireshark

18. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

```
Domain Name System (query)  
Transaction ID: 0x0001  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
  108.117.168.192.in-addr.arpa: type PTR, class IN  
    Name: 108.117.168.192.in-addr.arpa  
    [Name Length: 28]  
    [Label Count: 6]  
    Type: PTR (domain name Pointer) (12)  
    Class: IN (0x0001)  
[Response In: 8]
```

Иллюстрация 32, запрос PTR

```
Domain Name System (query)  
Transaction ID: 0x0002  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
  petrsu.ru: type NS, class IN  
    Name: petrsu.ru  
    [Name Length: 9]  
    [Label Count: 2]  
    Type: NS (authoritative Name Server) (2)  
    Class: IN (0x0001)  
[Response In: 10]
```

Иллюстрация 33, запрос NS

19. Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов сервера ПетрГУ в нем содержатся? А есть ли их адреса в этом ответе?

```

Domain Name System (response)
Transaction ID: 0x0001
> Flags: 0x0183 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  108.117.168.192.in-addr.arpa: type PTR, class IN
    Name: 108.117.168.192.in-addr.arpa
    [Name Length: 28]
    [Label Count: 6]
    Type: PTR (domain name Pointer) (12)
    Class: IN (0x0001)
[Request In: 7]
[Time: 0.034140000 seconds]

```

Иллюстрация 34, ответ PTR

```

> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 2
Queries
  petsru.ru: type NS, class IN
Answers
  petsru.ru: type NS, class IN, ns ns.karelia.ru
    Name: petsru.ru
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 3480 (58 minutes)
    Data length: 15
    Name Server: ns.karelia.ru
  petsru.ru: type NS, class IN, ns ns.petsru.ru
    Name: petsru.ru
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 3480 (58 minutes)
    Data length: 5
    Name Server: ns.petsru.ru
Additional records
  ns.petsru.ru: type A, class IN, addr 193.232.254.218
    Name: ns.petsru.ru
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 19503 (5 hours, 25 minutes, 3 seconds)
    Data length: 4
    Address: 193.232.254.218
  ns.karelia.ru: type A, class IN, addr 194.85.172.133
    Name: ns.karelia.ru
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 5018 (1 hour, 23 minutes, 38 seconds)
    Data length: 4
    Address: 194.85.172.133
[Request In: 9]
[Time: 0.067868000 seconds]

```

Иллюстрация 35, ответ NS

## Часть 3.4: nslookup petsu.ru 193.232.254.218

20. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?

```
Адаптер беспроводной локальной сети Беспроводная сеть:  
  
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . . : fe80::696d:aab9:47ca:2ff3%19  
IPv4-адрес. . . . . : 192.168.117.87  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . : 192.168.117.108
```

Иллюстрация 36, ipconfig

```
C:\Users\nikit>nslookup -type=NS petsu.ru  
Server: UnKnown  
Address: 192.168.117.108  
  
Non-authoritative answer:  
petsu.ru nameserver = ns.petsu.ru  
petsu.ru nameserver = ns.karelia.ru  
  
ns.petsu.ru internet address = 193.232.254.218  
ns.karelia.ru internet address = 194.85.172.133
```

Иллюстрация 37, nslookup

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.117.87	193.232.254.218	DNS	88	Standard query 0x0001 PTR 218.254.232.193.in-addr.arpa
2	0.229184	193.232.254.218	192.168.117.87	DNS	203	Standard query response 0x0001 PTR 218.254.232.193.in-addr.arpa PTR ns.petsu.ru NS ns.petsu.ru NS ns1.karelia.ru
3	0.234882	192.168.117.87	193.232.254.218	DNS	69	Standard query 0x0002 A petsu.ru
4	0.310314	193.232.254.218	192.168.117.87	DNS	143	Standard query response 0x0002 A petsu.ru A 194.85.173.228 NS ns.karelia.ru NS ns.petsu.ru A 194.85.172.133
5	0.312134	192.168.117.87	193.232.254.218	DNS	69	Standard query 0x0003 AAAA petsu.ru
6	0.381307	193.232.254.218	192.168.117.87	DNS	112	Standard query response 0x0003 AAAA petsu.ru SOA ns.petsu.ru
7	1.224770	192.168.117.87	213.180.193.234	TLSv1...	285	Application Data
8	1.225062	192.168.117.87	213.180.193.234	TLSv1...	100	Application Data
9	1.225279	192.168.117.87	213.180.193.234	TCP	1414	61882 → 443 [ACK] Seq=278 Ack=1 Win=260 Len=1360 [TCP segment of a reassembled PDU]

Иллюстрация 38, Wireshark

21. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

```
Domain Name System (query)  
Transaction ID: 0x0001  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
> 218.254.232.193.in-addr.arpa: type PTR, class IN  
[Response In: 2]
```

Иллюстрация 39, запрос PTR

```
Domain Name System (query)  
Transaction ID: 0x0002  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
> petsu.ru: type A, class IN  
[Response In: 4]
```

Иллюстрация 40, запрос A

```
Domain Name System (query)  
Transaction ID: 0x0003  
> Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
> petsu.ru: type AAAA, class IN  
[Response In: 6]
```

Иллюстрация 41, запрос AAAA

## 22. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

```
Domain Name System (response)
Transaction ID: 0x0001
> Flags: 0x8500 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 2
Queries
> 218.254.232.193.in-addr.arpa: type PTR, class IN
Answers
> 218.254.232.193.in-addr.arpa: type PTR, class IN, ns.petrus.ru
  Name: 218.254.232.193.in-addr.arpa
  Type: PTR (domain name Pointer) (12)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 14
  Domain Name: ns.petrus.ru
Authoritative nameservers
> 254.232.193.in-addr.arpa: type NS, class IN, ns ns.petrus.ru
  Name: 254.232.193.in-addr.arpa
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 2
  Name Server: ns.petrus.ru
> 254.232.193.in-addr.arpa: type NS, class IN, ns ns1.karelia.ru
  Name: 254.232.193.in-addr.arpa
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 14
  Name Server: ns1.karelia.ru
> 254.232.193.in-addr.arpa: type NS, class IN, ns ns.karelia.ru
  Name: 254.232.193.in-addr.arpa
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 5
  Name Server: ns.karelia.ru
Additional records
> ns.karelia.ru: type A, class IN, addr 194.85.172.133
  Name: ns.karelia.ru
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 10800 (3 hours)
  Data length: 4
  Address: 194.85.172.133
> ns1.karelia.ru: type A, class IN, addr 217.77.52.252
  Name: ns1.karelia.ru
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 10800 (3 hours)
  Data length: 4
  Address: 217.77.52.252
[Request In: 1]
[Time: 0.229184000 seconds]
```

Иллюстрация 42, ответ PTR

```
Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 1
Queries
> petrus.ru: type A, class IN
Answers
> petrus.ru: type A, class IN, addr 194.85.173.228
  Name: petrus.ru
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 4
  Address: 194.85.173.228
Authoritative nameservers
> petrus.ru: type NS, class IN, ns ns.karelia.ru
  Name: petrus.ru
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 13
  Name Server: ns.karelia.ru
> petrus.ru: type NS, class IN, ns ns.petrus.ru
  Name: petrus.ru
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 3600 (1 hour)
  Data length: 5
  Name Server: ns.petrus.ru
Additional records
> ns.karelia.ru: type A, class IN, addr 194.85.172.133
  Name: ns.karelia.ru
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 10800 (3 hours)
  Data length: 4
  Address: 194.85.172.133
[Request In: 3]
[Time: 0.075432000 seconds]
```

Иллюстрация 43, ответ A

```
Domain Name System (response)
Transaction ID: 0x0003
> Flags: 0x8500 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
> petrsu.ru: type AAAA, class IN
Authoritative nameservers
  petrsu.ru: type SOA, class IN, mname ns.petrso.ru
    Name: petrsu.ru
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 900 (15 minutes)
    Data length: 31
    Primary name server: ns.petrso.ru
    Responsible authority's mailbox: noc.petrso.ru
    Serial Number: 2023040701
    Refresh Interval: 10800 (3 hours)
    Retry Interval: 1800 (30 minutes)
    Expire limit: 3600000 (41 days, 16 hours)
    Minimum TTL: 900 (15 minutes)
[Request In: 5]
[Time: 0.069173000 seconds]
```

Иллюстрация 44, ответ AAAA