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.

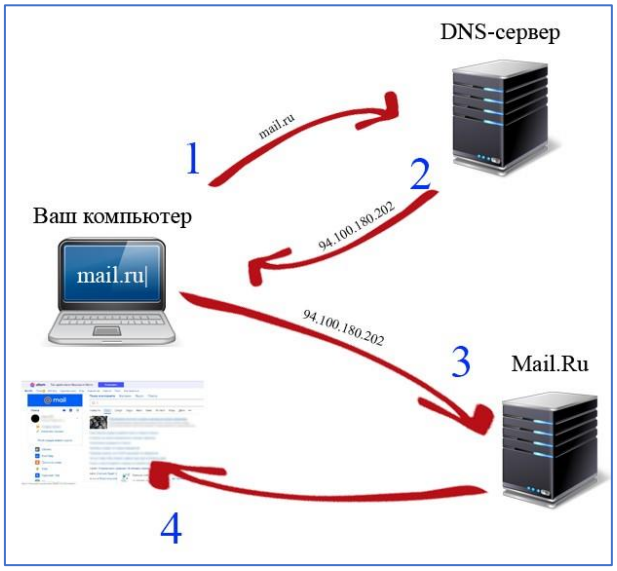


Рисунок 1, Локальные DNS-сервера

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.

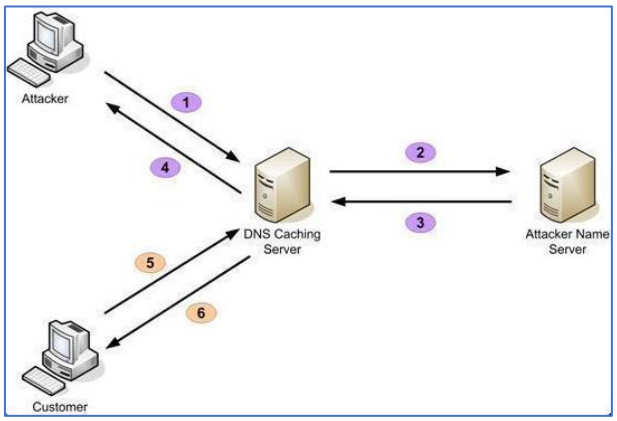


Рисунок 2, DNS-кэширование

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).

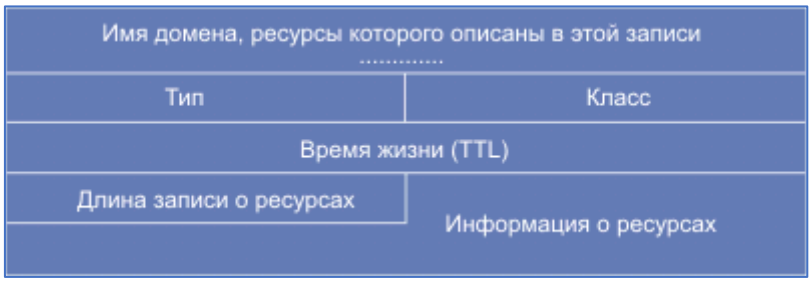


Рисунок 3, Ресурсные записи DNS

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.petrsu.ru.
petrsu.ru       nameserver = ns.karelia.ru.

Authoritative answers can be found from:
ns.petrsu.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.petrsu.ru
Server:         ns.petrsu.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.

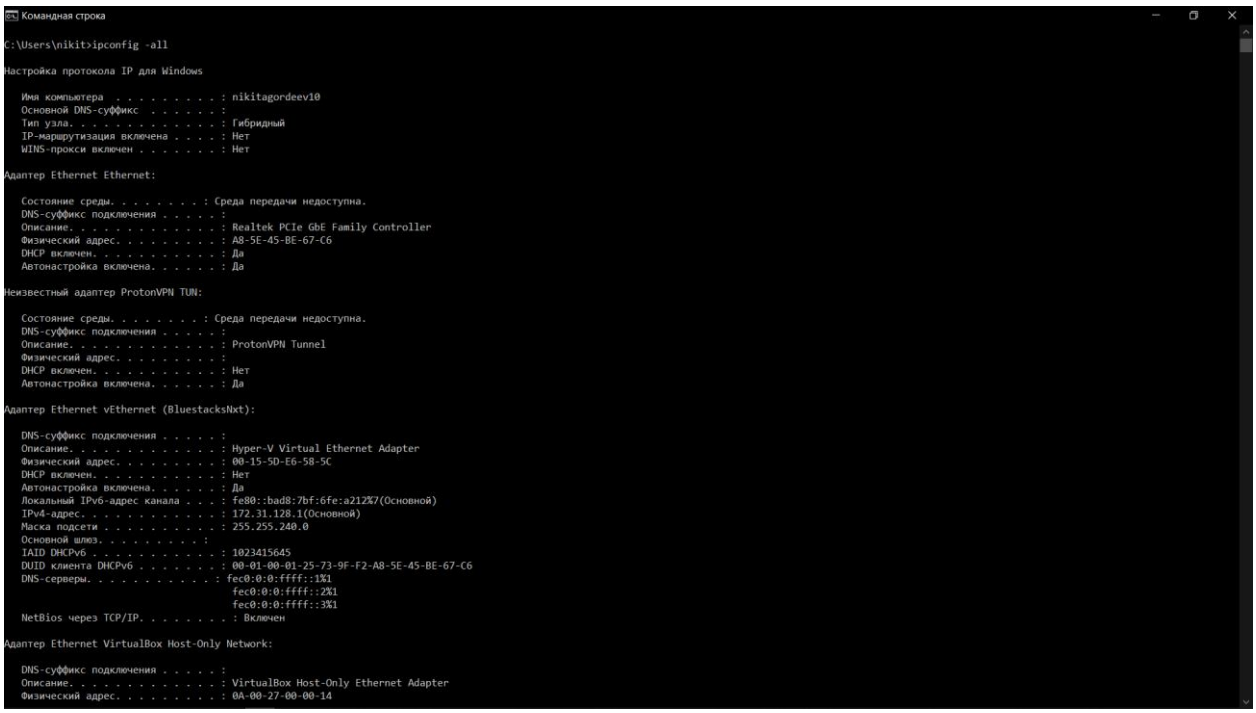


Иллюстрация 4, ipconfig /all

Иллюстрация 5, ipconfig /displaydns

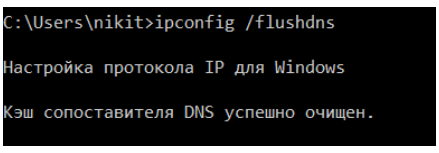


Иллюстрация 6, ipconfig /flushdns

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?

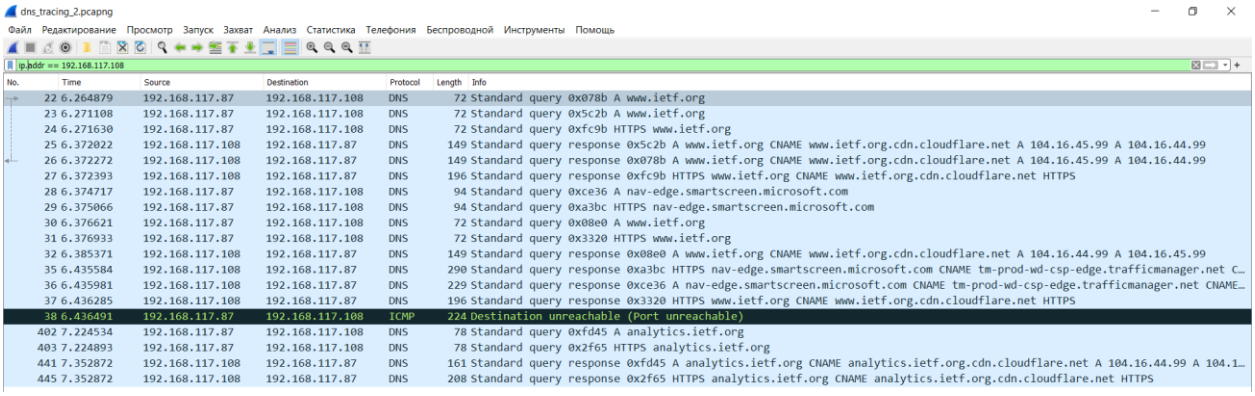


Иллюстрация 8, захват пакетов

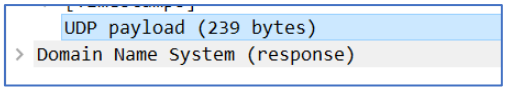


Иллюстрация 9, тип запроса

- 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

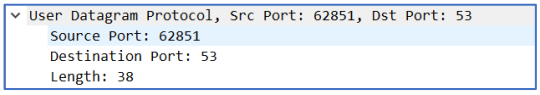


Иллюстрация 10, → www.ietf.org

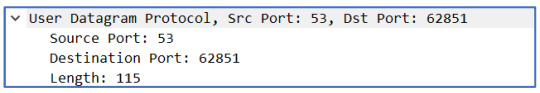


Иллюстрация 11, ← www.ietf.org

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

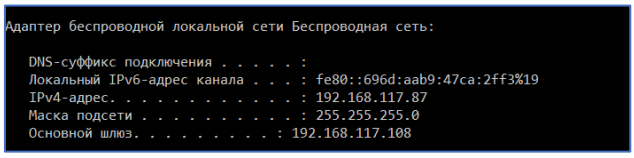


Иллюстрация 12, ipconfig

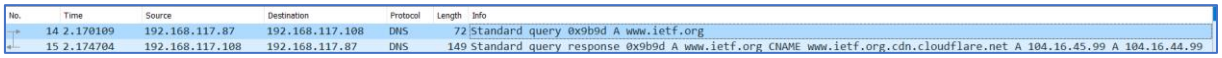


Иллюстрация 13, DNS-запрос

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

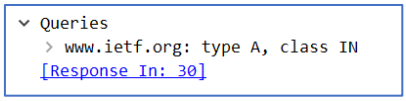


Иллюстрация 14, тип запроса

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 (дата обращения: 17.03.2023).

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

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

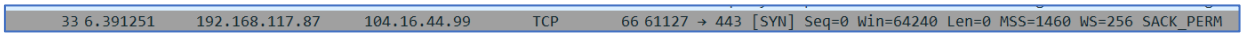


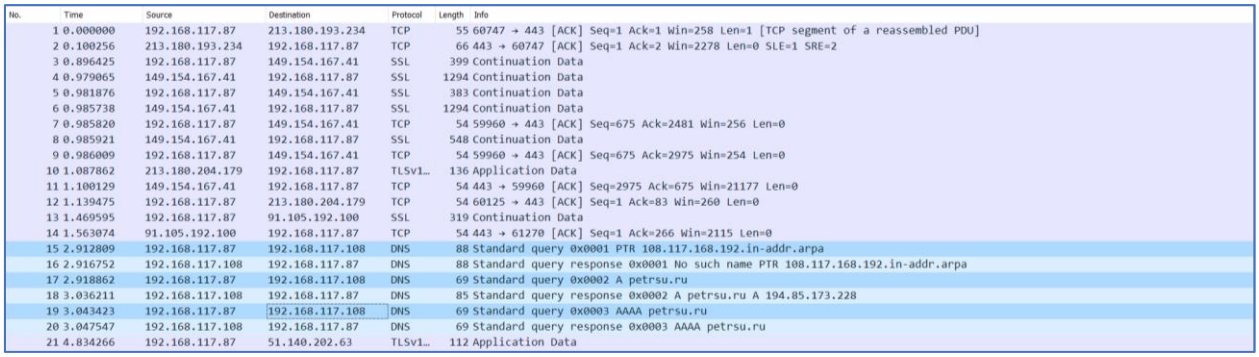
Иллюстрация 16, TCP-пакет с флагом SYN

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?

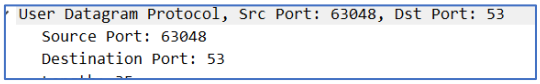


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.117.87	213.180.193.234	TCP	55	60747 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
2	0.100256	213.180.193.234	192.168.117.87	TCP	66	443 → 60747 [ACK] Seq=1 Ack=2 Win=2278 Len=0 SLE=1 SRE=2
3	0.896425	192.168.117.87	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	1.139475	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

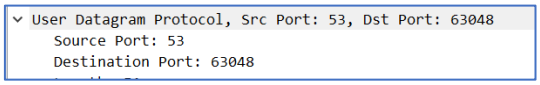
13. Рассмотрите пару с type A. Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?

destination port – порт назначения;
source port – исходящий порт



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

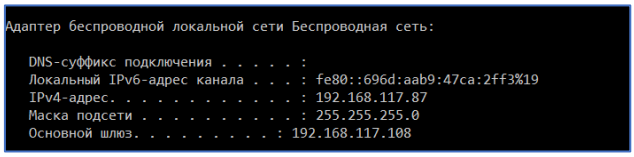
Иллюстрация 18, запрос DNS



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

Иллюстрация 19, ответ DNS

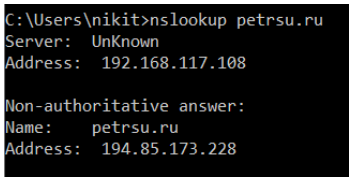
14. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?



```
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
```

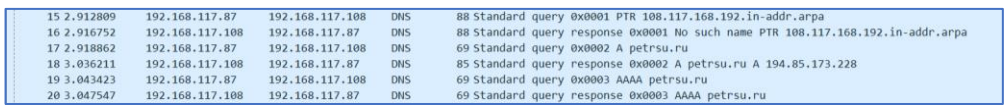
Иллюстрация 20, ipconfig



```
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»?

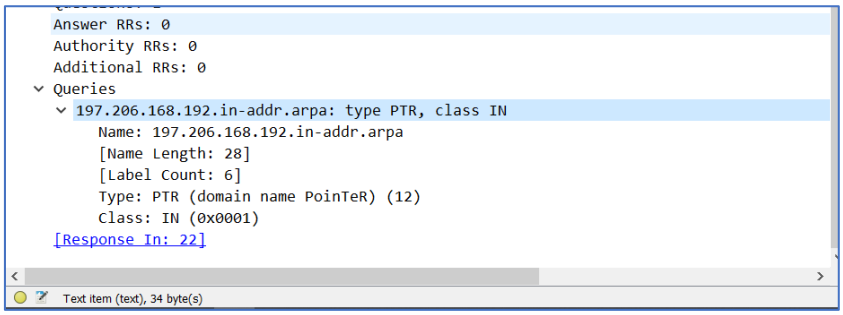


Иллюстрация 23, запрос PTR

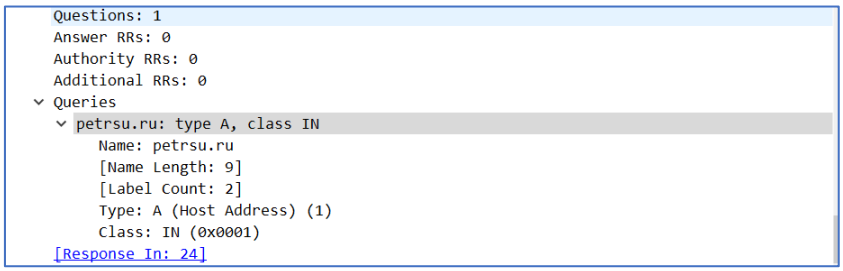


Иллюстрация 24, запрос A

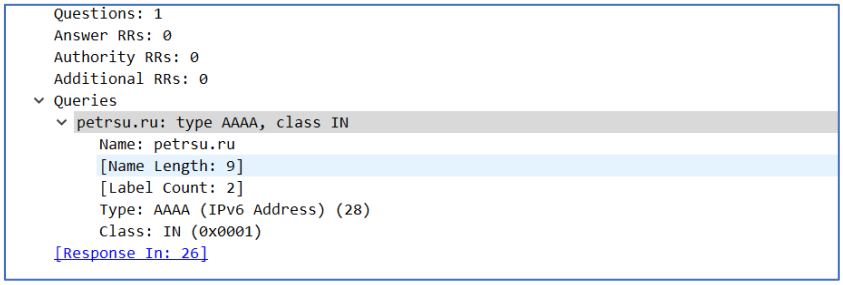


Иллюстрация 25, запрос AAAA

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?

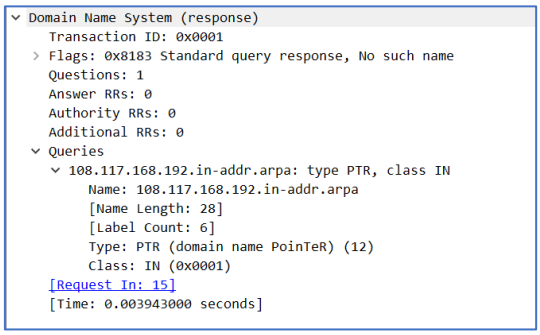


Иллюстрация 26, запрос PTR

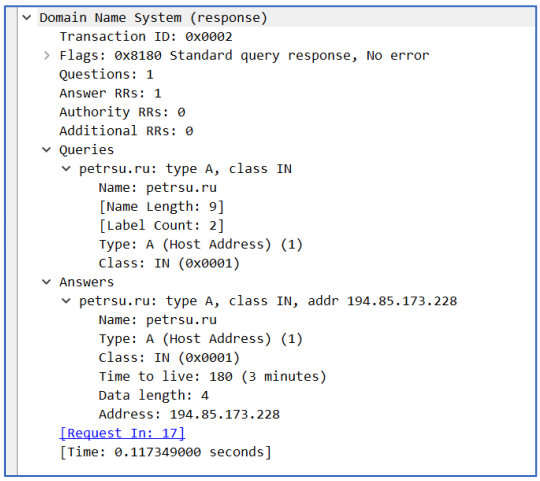


Иллюстрация 27, запрос A

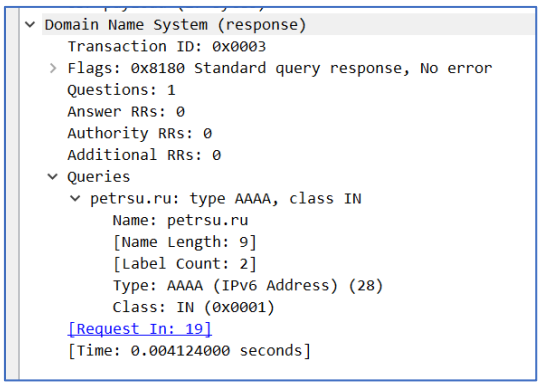


Иллюстрация 28, запрос AAAA

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	3.826148	213.180.193.234	192.168.117.87	TCP	66	443 → 61544 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2

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
  v Queries
    v 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
  v Queries
    v 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?

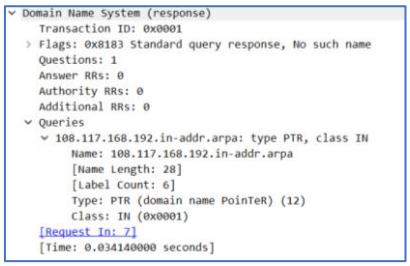


Иллюстрация 34, ответ PTR

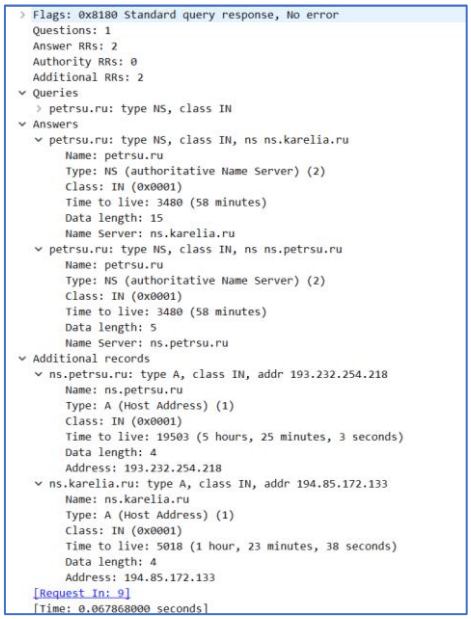


Иллюстрация 35, ответ NS

Часть 3.4: nslookup petrsu.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 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 37, nslookup

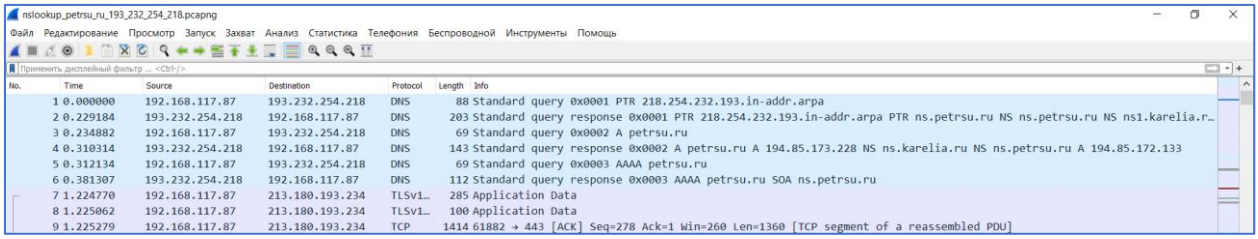


Иллюстрация 38, Wireshark

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
  v 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
  v Queries
    > petrsu.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
  v Queries
    > petrsu.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?

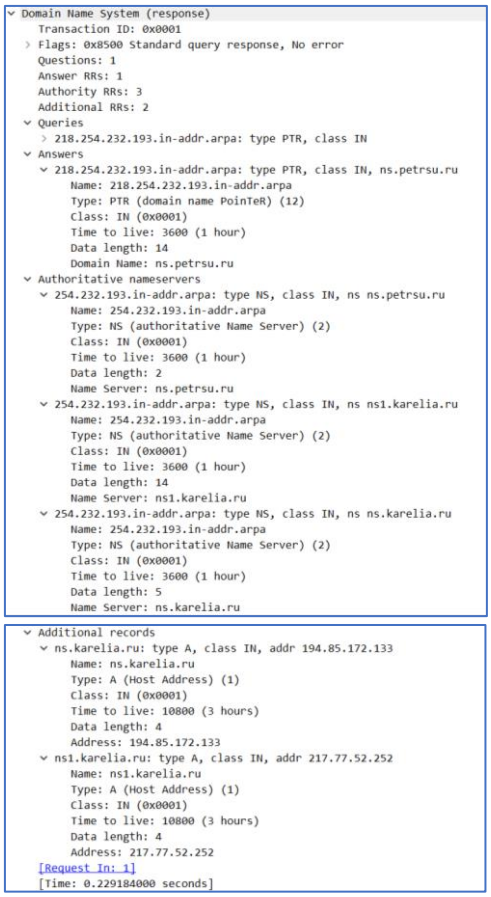


Иллюстрация 42, ответ PTR

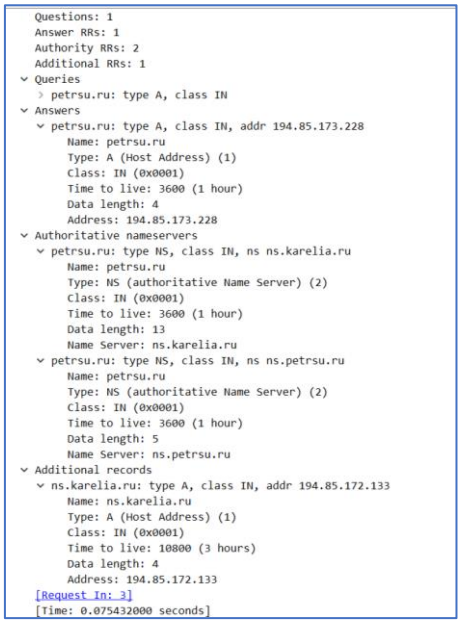


Иллюстрация 43, ответ A

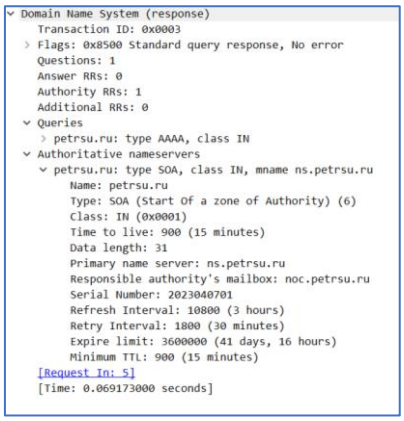


Иллюстрация 44, ответ AAAA