

Система доменных имён DNS

Шулин Егор, 09-331

Что было до DNS?

До изобретения DNS соответствие вида (ip-адрес - имя сервера) хранилось в виде файла на компьютере пользователя

- C:\Windows\System32\drivers\etc\hosts
- Linux/Unix/etc/hosts

Пример файла:

102.54.94.97	server
38.25.63.10	my-client

Что было до DNS?

Минусы файлового подхода:

- Быстрое увеличение размер файла
- Файл был трудноизменяем
- Возможны конфликты имен

Решением этих проблем стало изобретение DNS

Что такое DNS?

- DNS (Domain Name System) – система доменных имен
- DNS позволяет преобразовать имена компьютеров в ip-адреса

Пример:

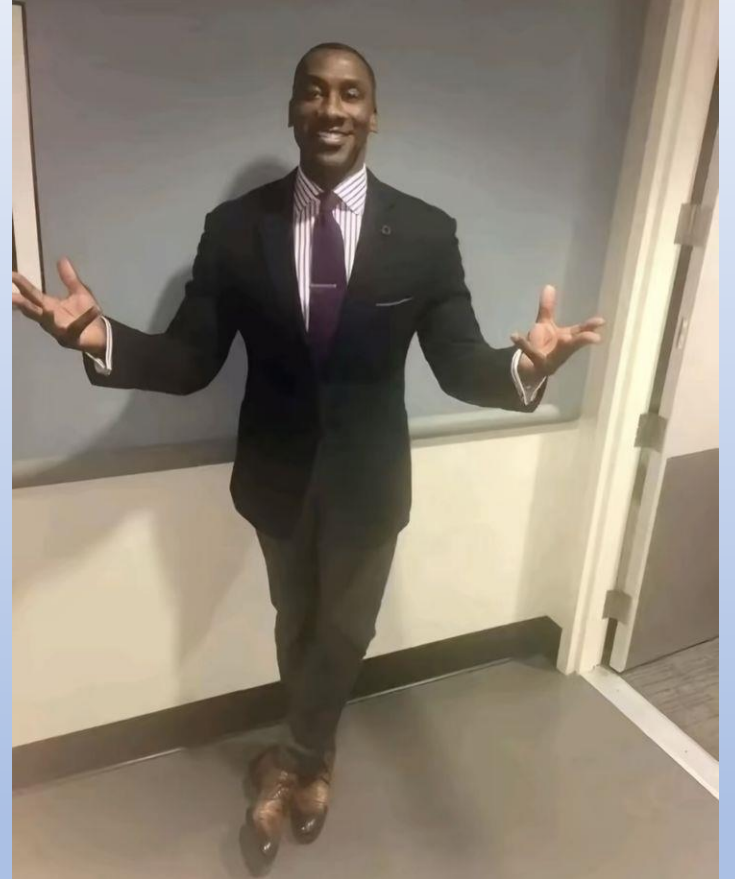
доменное имя – spotify.com

IPv4 - 35.186.224.24



Преимущества DNS

- Понятные человеку имена
- Возможность менять сетевую инфраструктуру
- DNS – распределённая система
- Делегирование обязанностей
- Надёжность
 - Каждую зону обслуживает несколько серверов

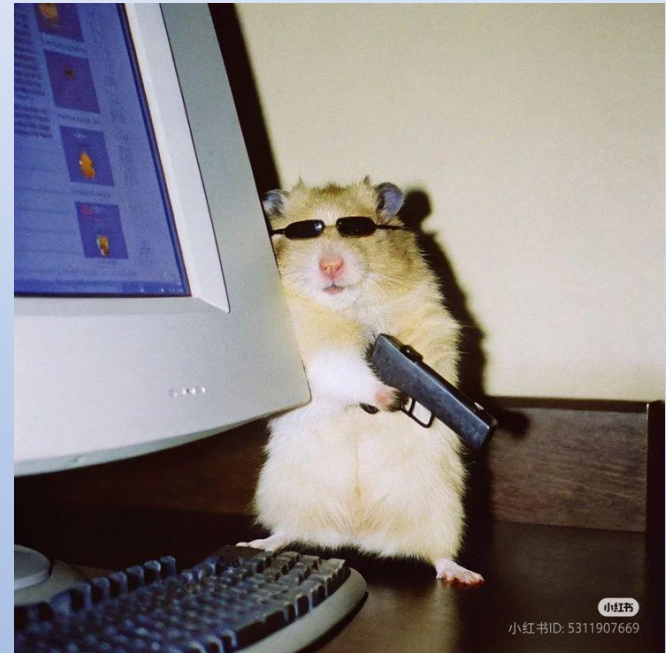


Недостатки DNS (Безопасность)

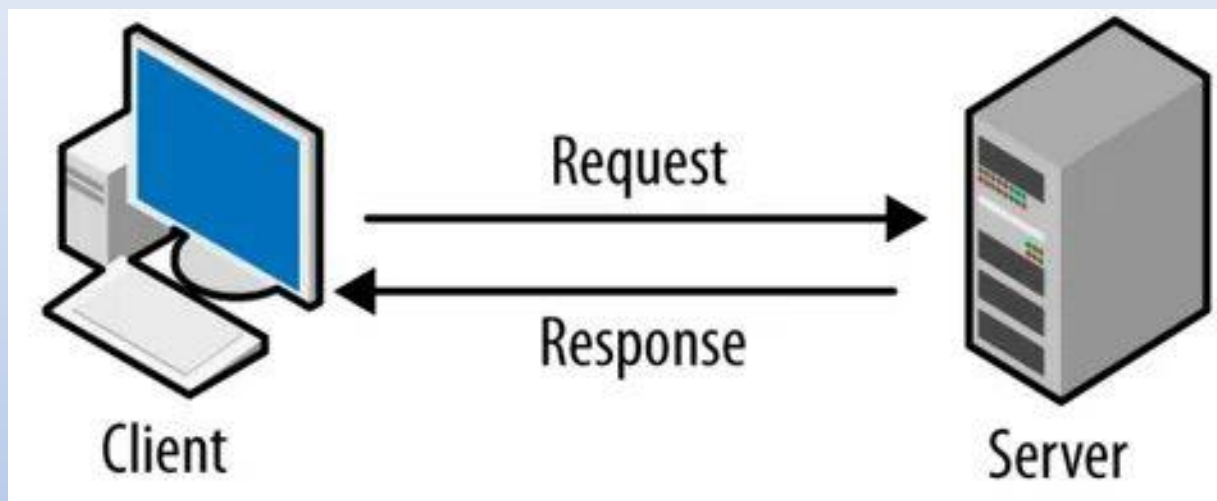
- Данные передаются в открытом виде
 - Можно прочитать и изменить данные
- Ограничение протокола
 - Атаки на DNS, например, отравление кэша

Существуют защищённые протоколы DNS

- Domain Name System Security Extensions (DNSSec)
- DNS over HTTPS (DoH)
- DNS over TLS (DoT)



Протокол DNS



- Работает на основе модели клиент-сервер
- На транспортном уровне использует TCP или UDP (преимущественно)
- Использует 53 порт

Режимы работы DNS сервера

- **Итеративный**

DNS-сервер не ищет ответ сам, а дает указание, куда обратиться далее.

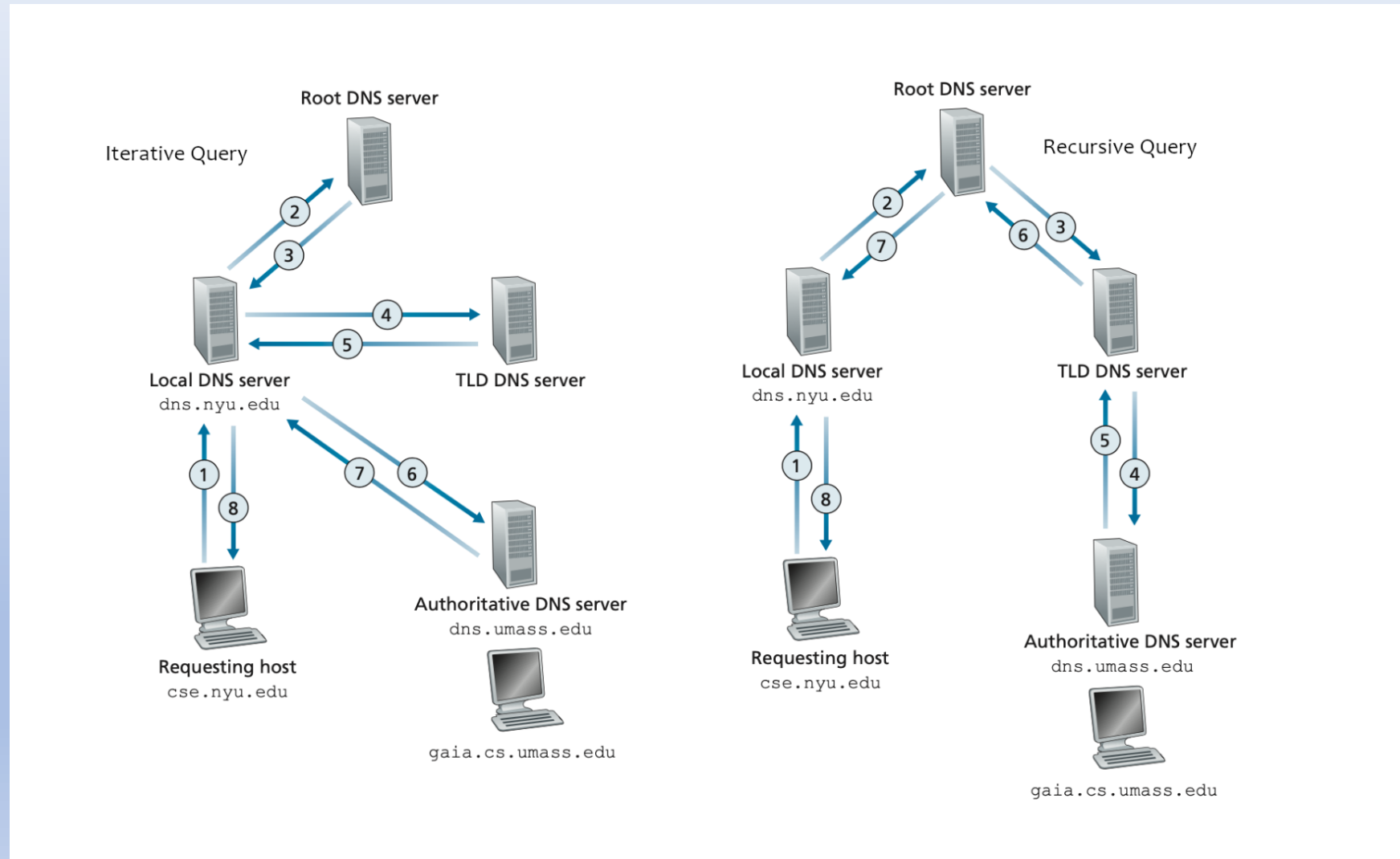
- Если знает ответ – возвращает ip-адрес
- Если не знает – возвращает адрес более “знающего” сервера

- **Рекурсивный**

DNS-сервер берет на себя всю работу по поиску и возвращает клиенту готовый результат.

- Возвращает найденный ip-адрес
- Или отрицательный ответ “Не найдено”

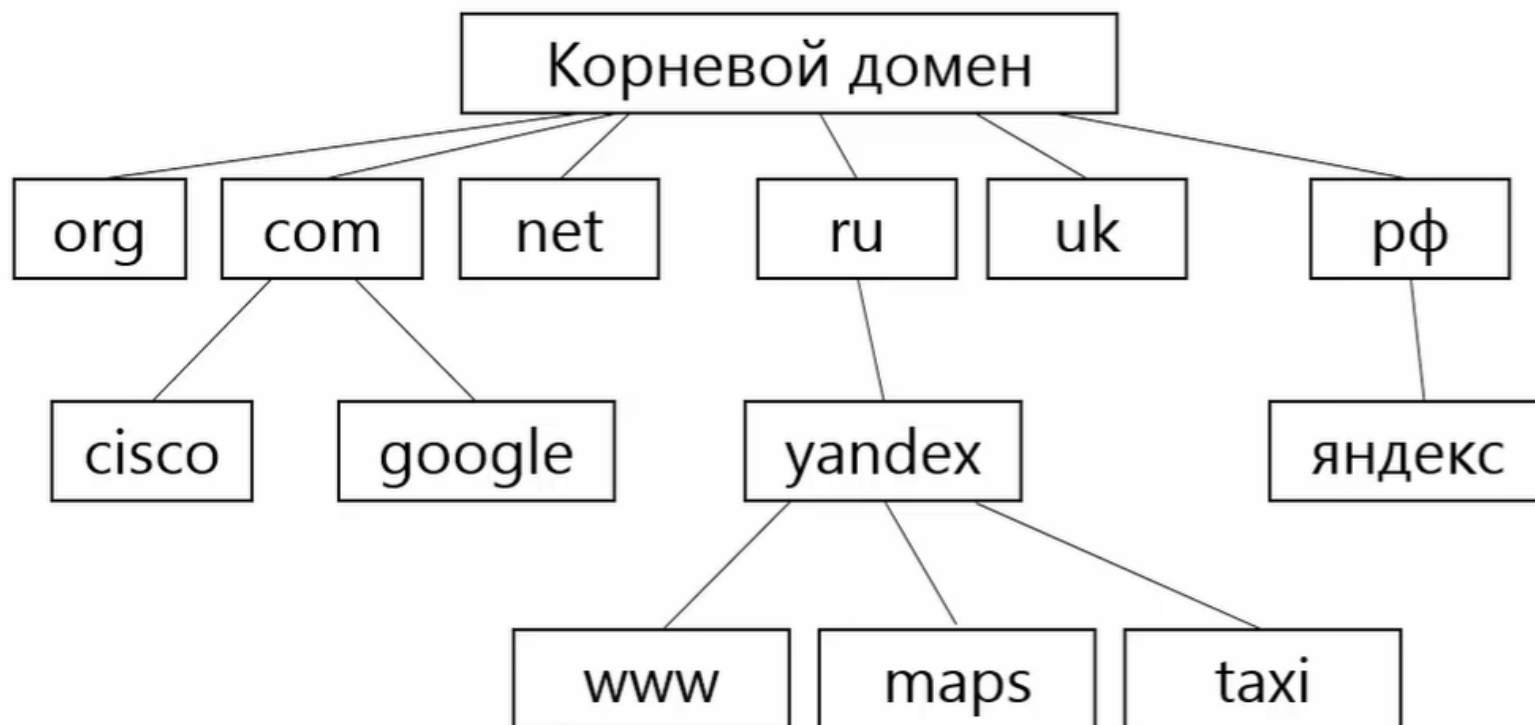
Режимы работы DNS сервера



Структура доменного имени



Дерево доменных имён



Распределение доменных имён

Распределением доменных имён занимаются регистраторы

- Регистратор корневого домена –Internet Corporation for Assigned Names and Numbers (ICANN)
- Регистраторы зон первого уровня
 - Необходима аккредитация ICANN
 - Один или несколько регистраторов для каждой зоны
 - Регистрируют домены второго уровня



Популярные регистраторы доменных имён



name.com



Google Domains

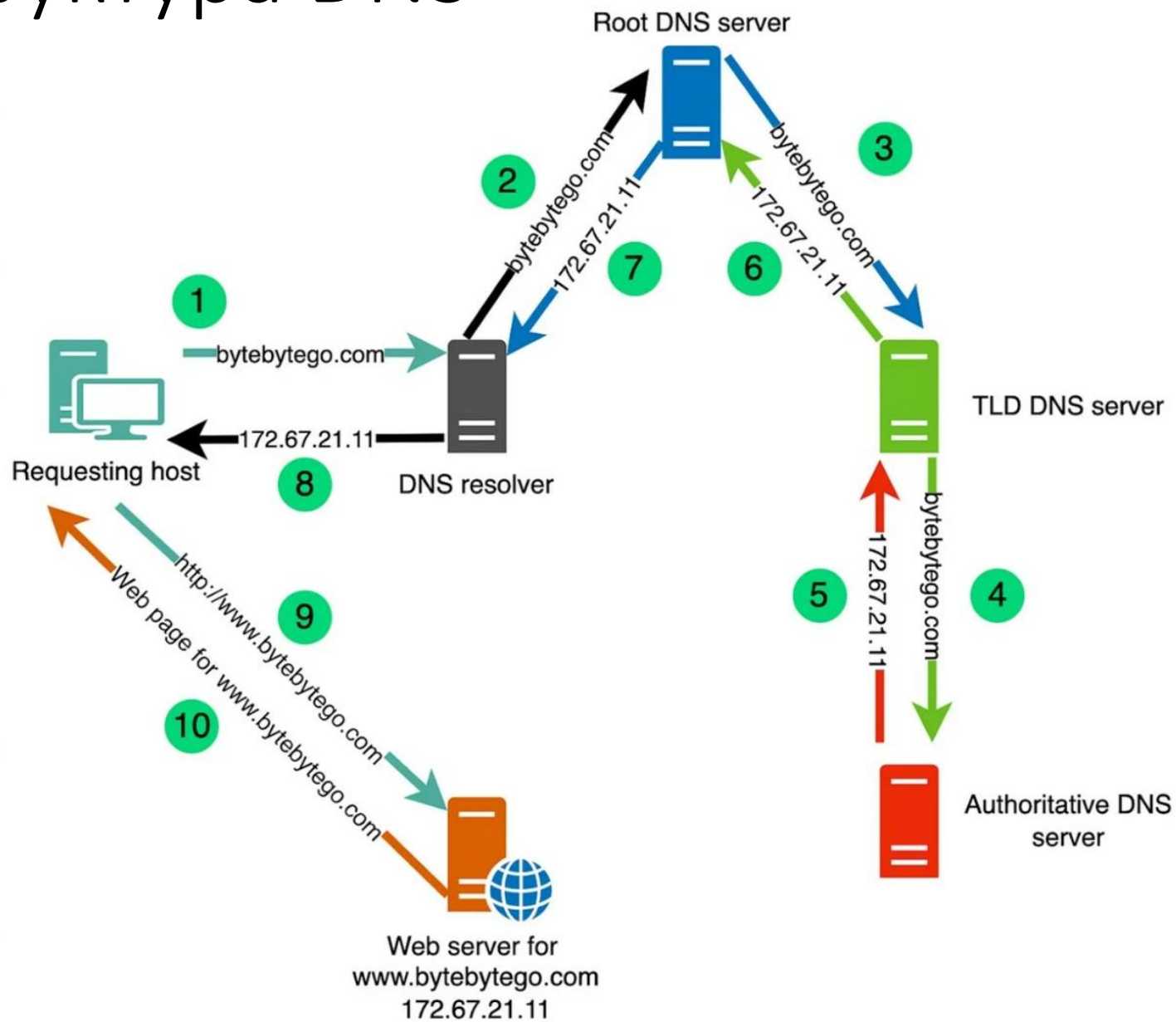


namecheap

Зоны ru и рф

- До 2001 года единственный регистратор
 - Российский НИИ развития общественных сетей (ripn.ru)
- После 2001 года несколько регистраторов, распределенная база данных
- Управление регистраторами
 - Координационный центр национального домена сети Интернет (cctld.ru)

Инфраструктура DNS



Сервер разрешения имён (resolver)

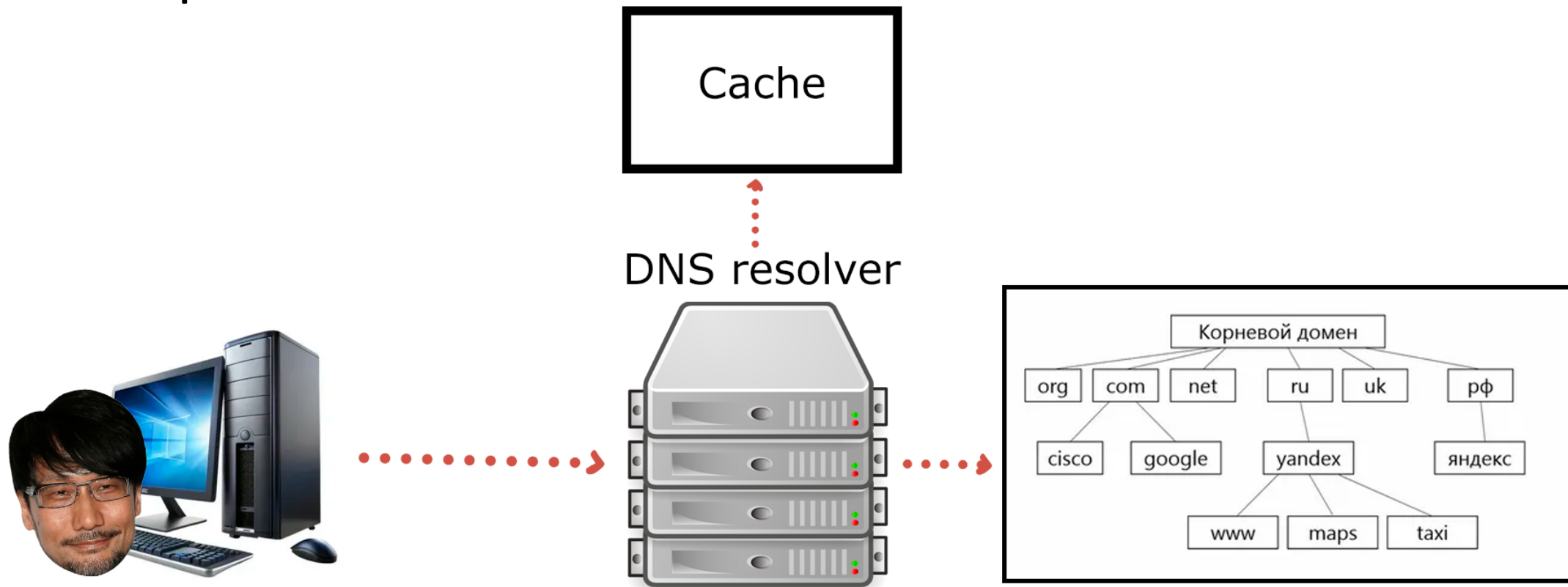
- Предоставляется провайдером/организацией
 - Клиент получает адрес сервера DNS вместе с другими настройками сети по протоколу DHCP
- Открытый сервер
 - Яндекс: 77.88.8.8 и 77.88.8.7 (с блокировкой сайтов для взрослых)
 - Google: 8.8.8.8

Яндекс DNS



Google Public DNS

Кэширование



Типы ответов DNS

- **Авторитетный ответ**

- Получен от сервера, обслуживающего данную доменную зону
- Получен из файлов на диске сервера

- **Неавторитетный ответ**

- Получен от сервера, не обслуживающего данную доменную зону
- Получен из кэша, данные могли устареть

Типы ответов DNS (Windows)

Неавторитетный ответ

```
C:\WINDOWS\system32\cmd.exe
C:\Users\User>nslookup spotify.com
Server: SBT.lan
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Name: spotify.com
Addresses: 2600:1901:1:7c5::
          35.186.224.24
```

Авторитетный ответ

```
C:\WINDOWS\system32\cmd.exe
C:\Users\User>nslookup spotify.com ns-cloud-a3.googledomains.com
Server: UnKnown
Address: 216.239.36.106

Name: spotify.com
Addresses: 2600:1901:1:7c5::
          35.186.224.24
```

Авторитетный сервер
для spotify.com

*Авторитетный сервер – сервер обслуживающий домен

Типы ответов DNS (Linux)

Авторитетный ответ

```
eglay@eglayy:/mnt/c/Users/User$ nslookup spotify.com ns-cloud-a3.googledomains.com
Server:      ns-cloud-a3.googledomains.com
Address:     216.239.36.106#53

Name:   spotify.com
Address: 35.186.224.24
Name:   spotify.com
Address: 2600:1901:1:7c5::
```

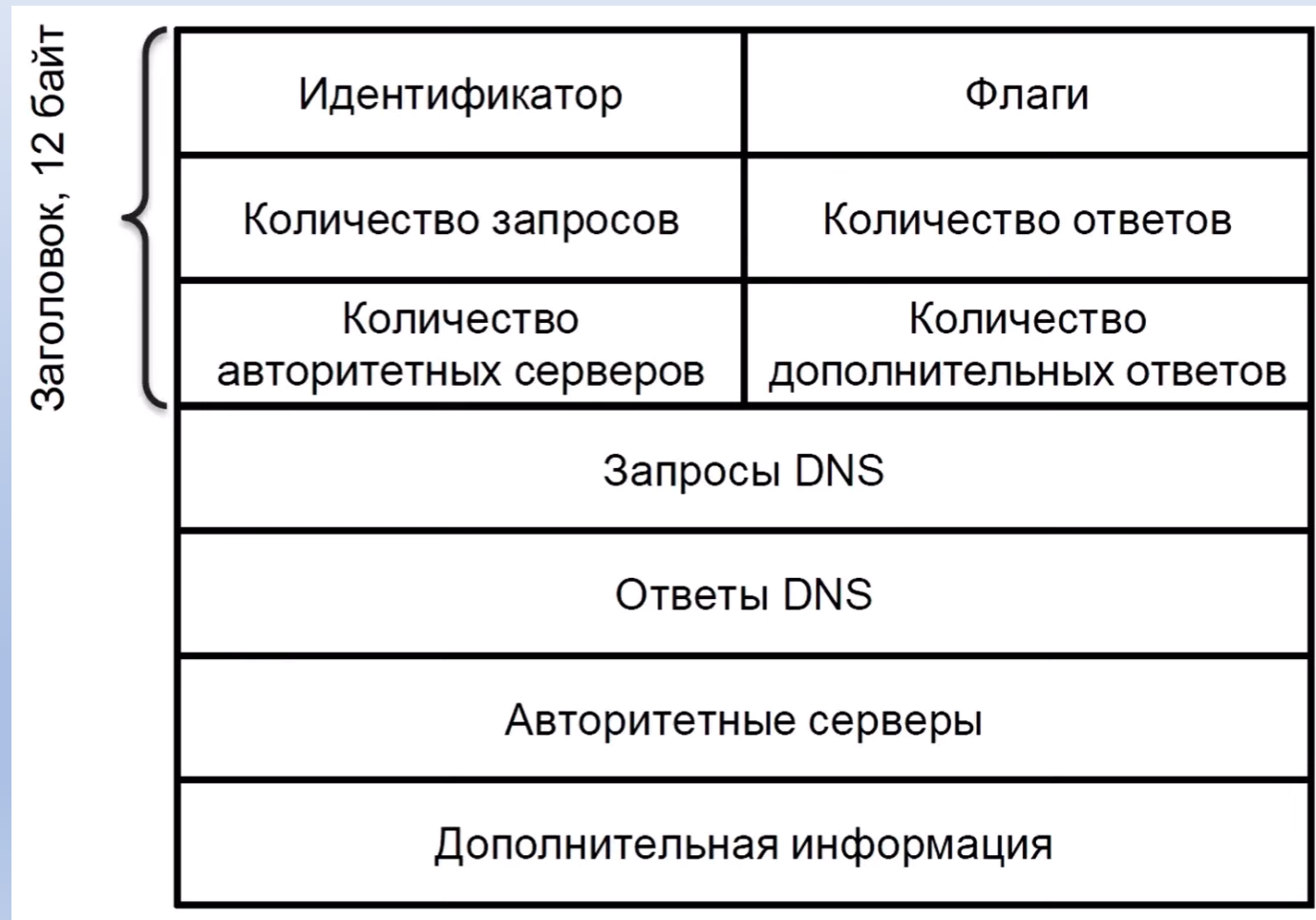
Неавторитетный ответ

```
eglay@eglayy:/mnt/c/Users/User$ nslookup spotify.com
Server:      10.255.255.254
Address:     10.255.255.254#53

Non-authoritative answer:
Name:   spotify.com
Address: 35.186.224.24
Name:   spotify.com
Address: 2600:1901:1:7c5::
```

Формат DNS пакета

*Пакеты передаются в бинарном формате



Формат DNS запроса и DNS ответа

DNS запрос

Имя
Тип записи
Класс записи

DNS ответ

Имя
Тип записи
Класс записи
Время жизни
Длина данных
Данные

Пример DNS запроса (Wireshark)

147 27.722241 192.168.1.231 192.168.1.1 DNS 71 Standard query 0x0004 A spotify.com

```
▶ Frame 147: Packet, 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{100AB252-4142-43C1-9819-04469B22FCF8}
▶ Ethernet II, Src: Intel_03:2a:c3 (c4:d0:e3:03:2a:c3), Dst: Sercomm_5a:00:5c (74:9d:79:5a:00:5c)
▶ Internet Protocol Version 4, Src: 192.168.1.231, Dst: 192.168.1.1
▶ User Datagram Protocol, Src Port: 51001, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0004
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ spotify.com: type A, class IN
      Name: spotify.com
      [Name Length: 11]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
    [Response In: 148]
```

```
0000 74 9d 79 5a 00 5c c4 d0 e3 03 2a c3 08 00 45 00 t.yZ.\. . .*...E.
0010 00 39 c8 69 00 00 80 11 00 00 c0 a8 01 e7 c0 a8 .9.i... ..
0020 01 01 c7 39 00 35 00 25 84 6f 00 04 01 00 00 01 ...9.5.% .o.....
0030 00 00 00 00 00 00 07 73 70 6f 74 69 66 79 03 63 .....s potify.c
0040 6f 6d 00 00 01 00 01 om.....
```

Пример DNS ответа (Wireshark)

148 27.726788 192.168.1.1 192.168.1.231 DNS 87 Standard query response 0x0004 A spotify.com A 35.186.224.24

```

Frame 148: Packet, 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{100AB252-4142-43C1-9819-04469B22FCF8}
Ethernet II, Src: Sercomm_5a:00:5c (74:9d:79:5a:00:5c), Dst: Intel_03:2a:c3 (c4:d0:e3:03:2a:c3)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.231
User Datagram Protocol, Src Port: 53, Dst Port: 51001
Domain Name System (response)
  Transaction ID: 0x0004
  Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
    .... ..0... .. = Truncated: Message is not truncated
    .... ..1... .. = Recursion desired: Do query recursively
    .... ..1... .. = Recursion available: Server can do recursive queries
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... ..0... .. = Non-authenticated data: Unacceptable
    .... ..0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    spotify.com: type A, class IN
      Name: spotify.com
      [Name Length: 11]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  Answers
    spotify.com: type A, class IN, addr 35.186.224.24
      Name: spotify.com
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 59 (59 seconds)
      Data length: 4
      Address: 35.186.224.24
[Request In: 147]
[Time: 4.547000 milliseconds]
```

0000	c4 d0 e3 03 2a c3 74 9d 79 5a 00 5c 08 00 45 00	...*.t.yZ-\..E.
0010	00 49 b0 2f 40 00 40 11 06 3c c0 a8 01 01 c0 a8	.I./@.@.<.....
0020	01 e7 00 35 c7 39 00 35 49 fc 00 04 81 80 00 01	..5.9.5 I.....
0030	00 01 00 00 00 00 07 73 70 6f 74 69 66 79 03 63s potify.c
0040	6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00	om.....
0050	3b 00 04 23 ba e0 18	;...#...

Флаги

- QR - запрос (0) или ответ (1)
- OPCODE (4 бита) - тип запроса,
 - 0 - стандартный запрос
- AA - авторитетный ответ (1) или нет (0)
- TC - пакет был обрезан (1) или не был (0)
- RD - запрос на рекурсивный режим
- RA - рекурсивный режим доступен
- Z - зарезервировано
- RCODE (4 бита) - статус, - успешно, другие коды - ошибка

Что может DNS?

- Определять для доменного имени адреса IPv4 и IPv6
- Задавать несколько доменных имен для одного IP-адреса
- Находить адрес почтового сервера для домена
- Задавать адрес DNS-серверов для доменной зоны
- Определять по IP-адресу доменное имя

Типы записи

- Каждая DNS запись (Resource Record, RR) имеет:
 - Тип записи – для чего предназначена запись
 - Класс записи - в какой сети используется (IN - Интернет)
- A – IPv4 адрес компьютера
- AAAA – IPv6 адрес компьютера

Типы записи A и AAAA (пример)

Тип записи A

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.26100.7171]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\User>nslookup -type=A spotify.com
Server: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Name:    spotify.com
Address: 35.186.224.24
```

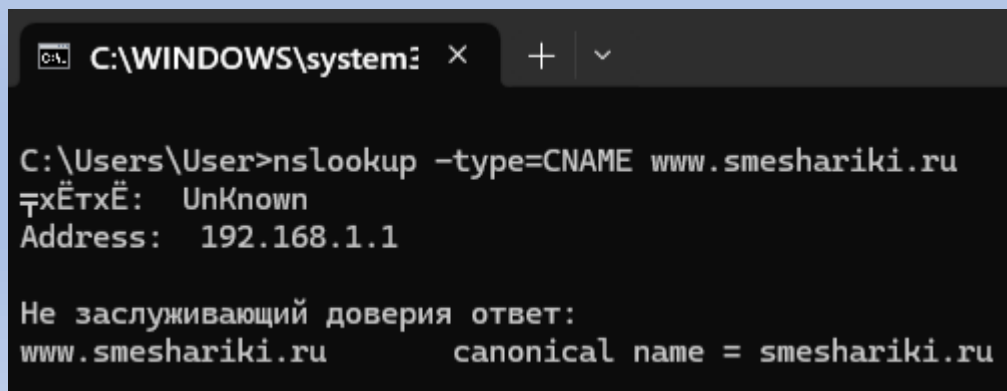
Тип записи AAAA

```
C:\WINDOWS\system32\cmd.exe
C:\Users\User>nslookup -type=AAAA spotify.com
Server: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Name:    spotify.com
Address: 2600:1901:1:7c5::
```

DNS псевдонимы

- Запись типа CNAME (Canonical Name Record/каноническая запись имени)
 - Определяет псевдоним для другого доменного имени
 - `www.smeshariki.ru -> smeshariki.ru`
- Альтернативный способ
 - Задать несколько A записей для одного IP-адреса



```
C:\WINDOWS\system32\cmd.exe
C:\Users\User>nslookup -type=CNAME www.smeshariki.ru
Canonical name for www.smeshariki.ru: smeshariki.ru
Address: 192.168.1.1

Не заслуживающий доверия ответ:
www.smeshariki.ru canonical name = smeshariki.ru
```

Адреса почтовых серверов

- Нужно отправить письмо на banan@gmail.com
 - Как узнать адрес почтового сервера?
- DNS запись типа MX (Mail eXchange)

Адреса почтовых серверов (примеры)

```
C:\WINDOWS\system32\cmd.exe
C:\Users\User>nslookup -type=MX gmail.com
Server: 192.168.1.1
Address: 192.168.1.1

Не заслуживающий доверия ответ:
gmail.com      MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com      MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com      MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com      MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com      MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
```

```
C:\Users\User>nslookup -type=MX yahoo.com
Server: 192.168.1.1
Address: 192.168.1.1

Не заслуживающий доверия ответ:
yahoo.com      MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
```

Адреса серверов DNS



- Предположим, мы хотим узнать адреса обслуживающих серверов зоны taxi.yandex.ru
- Для этого используем DNS запись типа NS (Name Server)

Адреса серверов DNS (Пример)

```
C:\WINDOWS\system32>nslookup -type=NS taxi.yandex.ru
тхѐтхѐ: UnKnown
Address: 192.168.1.1

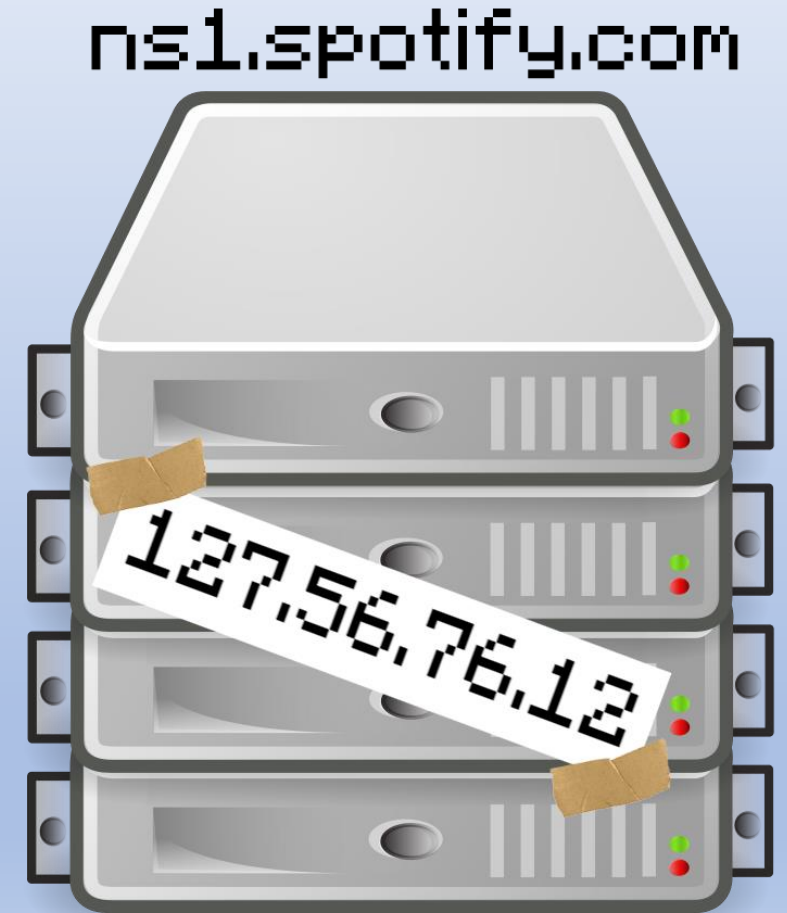
Не заслуживающий доверия ответ:
taxi.yandex.ru nameserver = ns4.yandex.ru
taxi.yandex.ru nameserver = ns3.yandex.ru
```

```
Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
.... ...1 .... = Recursion desired: Do query recursively
.... ....0... = Z: reserved (0)
.... .......0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  taxi.yandex.ru: type NS, class IN
    Name: taxi.yandex.ru
    [Name Length: 14]
    [Label Count: 3]
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
[Response In: 1032789]
```

```
Domain Name System (response)
Transaction ID: 0x0003
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
.... ..0. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
.... ...1 .... = Recursion desired: Do query recursively
.... ....1... = Recursion available: Server can do recursive queries
.... ....0... = Z: reserved (0)
.... ....0... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... .......0 .... = Non-authenticated data: Unacceptable
.... .......0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
  taxi.yandex.ru: type NS, class IN
    Name: taxi.yandex.ru
    [Name Length: 14]
    [Label Count: 3]
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
Answers
  taxi.yandex.ru: type NS, class IN, ns ns4.yandex.ru
    Name: taxi.yandex.ru
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 86400 (1 day)
    Data length: 6
    Name Server: ns4.yandex.ru
  taxi.yandex.ru: type NS, class IN, ns ns3.yandex.ru
    Name: taxi.yandex.ru
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 86400 (1 day)
    Data length: 6
    Name Server: ns3.yandex.ru
[Request In: 1032787]
[Time: 22.455000 milliseconds]
```

Приклеенные A записи (Glue Records)

- Вышестоящий домен использует “приклеенные” A записи, Чтобы определить адреса серверов в NS-записях
- Это нужно, чтобы не возникало логической петли



Определение имени по ip-адресу

- Типы DNS-зон
 - Прямая - определение IP-адреса по доменному имени
 - Обратная (reverse) - определение доменного имени по IP-адресу
- Специальное доменное имя для обратных зон
- in-addr.arpa.
- IP-адрес записывается в обратном порядке
- 77.88.55.88 -> 88.55.88.77.in-addr.arpa.
- 2001:0db8:85a3::8a2e:0370:7334 -> 1.0.0.0...8.b.d.0.1.0.0.2.ip6.arpa.

Определение имени по ip-адресу

- Запись типа PTR(Pointer – указатель)
 - 88.55.88.77.in-addr.arpa. -> yandex

```
C:\WINDOWS\system32 x + v
C:\Users\User>nslookup -type=PTR 88.55.88.77.in-addr.arpa.
тхЕтхЕ: Unknown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
88.55.88.77.in-addr.arpa      name = yandex.ru
```

- Но так бывает не всегда
 - 24.224.186.35.in-addr.arpa. -> 24.224.186.35.bc.googleusercontent.com

```
C:\WINDOWS\system32 x + v
C:\Users\User>nslookup -type=PTR 24.224.186.35.in-addr.arpa.
тхЕтхЕ: Unknown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
24.224.186.35.in-addr.arpa    name = 24.224.186.35.bc.googleusercontent.com
```

Тестирование работы службы DNS

- Консольные утилиты
 - Получение маршрута следования пакетов
 - traceroute (Linux) / tracert (Windows)
 - Проверка доступности хоста
 - ping
 - Запросы
 - nslookup (Windows/Linux)
 - dig (Linux)
 - host (Linux)
- Анализаторы трафика
 - Wireshark (Windows/Linux)



nslookup

nslookup (Windows)

```
C:\Users\User>nslookup youtube.com
Server: 192.168.1.1
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Ль :      youtube.com
Addresses: 2607:f8b0:4008:80e::200e
           142.250.109.190
           142.250.109.91
           142.250.109.136
           142.250.109.93
```

nslookup (Windows) с указанием типа записи

```
C:\Users\User>nslookup -type=MX mail.ru
Server: 192.168.1.1
Address: 192.168.1.1

Не заслуживающий доверия ответ:
mail.ru MX preference = 10, mail exchanger = mxs.mail.ru
```

nslookup (Linux)

```
eglay@eglay: /mnt/c/Users/User$ nslookup youtube.com
Server: 10.255.255.254
Address: 10.255.255.254#53

Non-authoritative answer:
Name:  youtube.com
Address: 142.250.109.190
Name:  youtube.com
Address: 142.250.109.91
Name:  youtube.com
Address: 142.250.109.136
Name:  youtube.com
Address: 142.250.109.93
Name:  youtube.com
Address: 2607:f8b0:4008:80e::200e
```

nslookup (Linux) с указанием типа записи

```
eglay@eglay: /mnt/c/Users/User$ nslookup -type=MX mail.ru
Server: 10.255.255.254
Address: 10.255.255.254#53

Non-authoritative answer:
mail.ru mail exchanger = 10 mxs.mail.ru.

Authoritative answers can be found from:
```

host

host без типа записи

```
eglay@eglayy:/mnt/c/Users/User$ host burgerking.com
burgerking.com has address 3.162.38.89
burgerking.com has address 3.162.38.31
burgerking.com has address 3.162.38.61
burgerking.com has address 3.162.38.124
burgerking.com mail is handled by 10 ASPMX.L.GOOGLE.com.
burgerking.com mail is handled by 30 ASPMX3.GOOGLEMAIL.com.
burgerking.com mail is handled by 30 ASPMX2.GOOGLEMAIL.com.
burgerking.com mail is handled by 20 ALT1.ASPMX.L.GOOGLE.com.
burgerking.com mail is handled by 20 ALT2.ASPMX.L.GOOGLE.com.
```

host без с типом записи

```
eglay@eglayy:/mnt/c/Users/User$ host -t A burgerking.com
burgerking.com has address 3.162.38.89
burgerking.com has address 3.162.38.31
burgerking.com has address 3.162.38.61
burgerking.com has address 3.162.38.124
```

dig

dig без типа записи

```
eglay@eglayy:/mnt/c/Users/User$ dig pogoda.yandex.ru

; <<>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <<>> pogoda.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18470
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;pogoda.yandex.ru.          IN      A

;; ANSWER SECTION:
pogoda.yandex.ru.          535     IN      A      213.180.204.242

;; Query time: 10 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Wed Dec 10 13:56:27 MSK 2025
;; MSG SIZE rcvd: 50
```

dig с типом записи

```
eglay@eglayy:/mnt/c/Users/User$ dig NS pogoda.yandex.ru

; <<>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <<>> NS pogoda.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38326
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 0
;; QUESTION SECTION:
;pogoda.yandex.ru.          IN      NS

;; ANSWER SECTION:
pogoda.yandex.ru.          60      IN      NS      ns3.yandex.ru.
pogoda.yandex.ru.          60      IN      NS      ns4.yandex.ru.

;; Query time: 255 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Wed Dec 10 14:00:05 MSK 2025
;; MSG SIZE rcvd: 81
```


ping

```
C:\Users\User>ping yandex.ru
```

```
Обмен пакетами с yandex.ru [5.255.255.77] с 32 байтами данных:
```

```
Ответ от 5.255.255.77: число байт=32 время=23мс TTL=247
```

```
Ответ от 5.255.255.77: число байт=32 время=22мс TTL=247
```

```
Ответ от 5.255.255.77: число байт=32 время=22мс TTL=247
```

```
Ответ от 5.255.255.77: число байт=32 время=21мс TTL=247
```

```
Статистика Ping для 5.255.255.77:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 21мсек, Максимальное = 23 мсек, Среднее = 22 мсек
```

tracert

```
C:\Users\User>tracert yandex.ru
```

```
Трассировка маршрута к yandex.ru [5.255.255.77]  
с максимальным числом прыжков 30:
```

1	4 ms	1 ms	1 ms	SBT.lan [192.168.1.1]
2	4 ms	2 ms	2 ms	10.16.255.137
3	3 ms	3 ms	3 ms	10.16.248.109
4	19 ms	3 ms	3 ms	10.16.248.170
5	20 ms	2 ms	2 ms	10.16.248.130
6	21 ms	18 ms	18 ms	dante.yndx.net [195.208.208.93]
7	23 ms	23 ms	22 ms	vla-32z8-ae2.yndx.net [93.158.172.39]
8	*	24 ms	22 ms	10.32.87.1
9	24 ms	24 ms	24 ms	10.7.7.1
10	23 ms	22 ms	23 ms	yandex.ru [5.255.255.77]

```
Трассировка завершена.
```

Wireshark (интерфейс программы)

The screenshot displays the Wireshark network protocol analyzer interface. The top pane, titled 'dns', shows a list of captured packets. The selected packet (No. 354) is a DNS query from 192.168.1.231 to 192.168.1.1. The details pane on the right shows the structure of the packet, including the Ethernet II header, the IPv4 header, and the DNS query section. The DNS query is for 'pogoda.yandex.ru'.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
354...	19563.136...	192.168.1.231	192.168.1.1	DNS	101	Standard query 0xf7fc HTTPS nexus-websocket-a.intercom.io
354...	19563.136...	192.168.1.231	192.168.1.1	DNS	101	Standard query 0x66a0 A nexus-websocket-a.intercom.io
354...	19563.149...	192.168.1.1	192.168.1.231	DNS	183	Standard query response 0xf7fc HTTPS nexus-websocket-a.intercom.io SOA ns-97.awsdns-12.com
354...	19563.163...	192.168.1.1	192.168.1.231	DNS	231	Standard query response 0x66a0 A nexus-websocket-a.intercom.io A 18.97.36.44 A 18.97.36.54 A 18.97.36.49 A 18.97.36.57 A 18.97.36.51 A 18.97.36.74 A 18.97.36.73 A 18.97.36.7
354...	19565.138...	192.168.1.231	192.168.1.1	DNS	97	Standard query 0x206c HTTPS gew4-spclient.spotify.com
354...	19565.139...	192.168.1.231	192.168.1.1	DNS	97	Standard query 0xc3f6 A gew4-spclient.spotify.com
354...	19565.149...	192.168.1.1	192.168.1.231	DNS	227	Standard query response 0x206c HTTPS gew4-spclient.spotify.com CNAME edge-web-gew4.dual-gslb.spotify.com SOA ns-cloud-d1.google.com
354...	19565.151...	192.168.1.1	192.168.1.231	DNS	153	Standard query response 0xc3f6 A gew4-spclient.spotify.com CNAME edge-web-gew4.dual-gslb.spotify.com A 35.186.224.28
354...	19567.521...	192.168.1.231	192.168.1.1	DNS	86	Standard query 0xd9cc A s3.eu-west-1.amazonaws.com
354...	19567.529...	192.168.1.1	192.168.1.231	DNS	198	Standard query response 0xd9cc A s3.eu-west-1.amazonaws.com A 52.92.16.184 A 3.5.64.130 A 52.92.36.64 A 3.5.71.255 A 52.92.36.176 A 52.92.0.224 A 3.5.69.24
354...	19567.534...	192.168.1.231	192.168.1.1	DNS	82	Standard query 0x28fe A storage.googleapis.com
354...	19567.540...	192.168.1.1	192.168.1.231	DNS	306	Standard query response 0x28fe A storage.googleapis.com A 173.194.73.207 A 209.85.233.207 A 108.177.14.207 A 74.125.131.207 A 74.125.205.207 A 64.233.164.207 A 142.250.150.207 A 142.251.1.207 A 64.233.162.207 A 64.233.16
354...	19568.559...	192.168.1.231	192.168.1.1	DNS	86	Standard query 0xe187 A s3.eu-west-1.amazonaws.com
354...	19568.566...	192.168.1.1	192.168.1.231	DNS	198	Standard query response 0xe187 A s3.eu-west-1.amazonaws.com A 3.5.69.24 A 52.92.16.184 A 3.5.64.130 A 52.92.36.64 A 3.5.71.255 A 52.92.36.176 A 52.92.0.224
354...	19582.155...	192.168.1.231	192.168.1.1	DNS	88	Standard query 0xa6a3 A ru.pinterest.com
354...	19582.189...	192.168.1.1	192.168.1.231	DNS	270	Standard query response 0xa6a3 A ru.pinterest.com CNAME www.pinterest.com CNAME www.pinterest-com.gslb.pinterest.com CNAME www.gslb.pinterest.net CNAME www.pinterest.com.edgekey.net CNAME e6449.a.akamaiedge.net A 23.32.2
354...	19582.190...	192.168.1.231	192.168.1.1	DNS	88	Standard query 0x22eb HTTPS ru.pinterest.com
354...	19582.204...	192.168.1.1	192.168.1.231	DNS	312	Standard query response 0x22eb HTTPS ru.pinterest.com CNAME www.pinterest.com CNAME www.pinterest-com.gslb.pinterest.com CNAME www.gslb.pinterest.net CNAME www.pinterest.com.edgekey.net CNAME e6449.a.akamaiedge.net SOA n
354...	19583.612...	192.168.1.231	192.168.1.1	DNS	87	Standard query 0x28ab NS pogoda.yandex.ru OPT
354...	19583.637...	192.168.1.1	192.168.1.231	DNS	123	Standard query response 0x28ab NS pogoda.yandex.ru NS ns4.yandex.ru NS ns3.yandex.ru OPT
354...	19595.788...	192.168.1.231	192.168.1.1	DNS	76	Standard query 0x6b6e A sn.splashtop.com
354...	19595.795...	192.168.1.1	192.168.1.231	DNS	157	Standard query response 0x6b6e No such name A sn.splashtop.com SOA ns-744.awsdns-29.net
354...	19599.303...	192.168.1.231	192.168.1.1	DNS	89	Standard query 0x36d4 HTTPS www.recaptcha.net
354...	19599.304...	192.168.1.231	192.168.1.1	DNS	89	Standard query 0x9daf A www.recaptcha.net
354...	19599.313...	192.168.1.1	192.168.1.231	DNS	151	Standard query response 0x36d4 HTTPS www.recaptcha.net SOA ns1.google.com
354...	19599.315...	192.168.1.1	192.168.1.231	DNS	107	Standard query response 0x9daf A www.recaptcha.net A 64.233.164.94
354...	19599.543...	192.168.1.231	192.168.1.1	DNS	89	Standard query 0x98a8 A www.recaptcha.net
354...	19599.543...	192.168.1.231	192.168.1.1	DNS	89	Standard query 0xc9d9 HTTPS www.recaptcha.net
354...	19599.549...	192.168.1.1	192.168.1.231	DNS	107	Standard query response 0x98a8 A www.recaptcha.net A 64.233.164.94
354...	19599.557...	192.168.1.1	192.168.1.231	DNS	151	Standard query response 0xc9d9 HTTPS www.recaptcha.net SOA ns1.google.com
354...	19607.150...	192.168.1.231	77.88.8.1	DNS	81	Standard query 0x12c8 HTTPS yandex.ru
354...	19607.155...	192.168.1.231	77.88.8.1	DNS	81	Standard query 0xbfe3 A yandex.ru
354...	19607.168...	77.88.8.1	192.168.1.231	DNS	144	Standard query response 0x12c8 HTTPS yandex.ru SOA ns1.yandex.ru
354...	19607.177...	77.88.8.1	192.168.1.231	DNS	131	Standard query response 0xbfe3 A yandex.ru A 77.88.44.55 A 5.255.255.77 A 77.88.55.88
354...	19612.835...	192.168.1.231	192.168.1.1	DNS	74	Standard query 0x2e6a A login.live.com
354...	19612.841...	192.168.1.1	192.168.1.231	DNS	359	Standard query response 0x2e6a A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.aadmsa.trafficmanager.net CNAME prdv4a.aadg.msidentity.com CNAME www.tm.v4.a.prd.aadg.akadns.net A 40.126.53.14 A 40.126
354...	19614.238...	192.168.1.231	192.168.1.1	DNS	79	Standard query 0xfe34 A graph.microsoft.com
354...	19614.245...	192.168.1.1	192.168.1.231	DNS	207	Standard query response 0xfe34 A graph.microsoft.com CNAME ags.privatelink.msidentity.com CNAME www.tm.prd.ags.akadns.net A 20.231.130.224 A 20.20.34.96 A 20.20.34.160
354...	19615.782...	192.168.1.231	192.168.1.1	DNS	74	Standard query 0xecee A assets.msn.com
354...	19615.788...	192.168.1.1	192.168.1.231	DNS	342	Standard query response 0xecee A assets.msn.com CNAME assets.msn-com-world-atm-default.trafficmanager.net CNAME assets.msn-com-ion.edgesuite.net CNAME a1666.dscr.akamai.net A 23.35.104.169 A 23.35.104.163 A 23.35.104.192

Packet Details:

- Frame 3548946: Packet, 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{100AB252-4142-43C1-9819-04469B22F...}
- Ethernet II, Src: Intel_03:2a:c3 (c4:d0:e3:03:2a:c3), Dst: Sercomm_5a:00:5c (74:9d:79:5a:00:5c)
 - Destination: Sercomm_5a:00:5c (74:9d:79:5a:00:5c)
 - ...0... = LG bit: Globally unique address (factory default)
 - ...0... = IG bit: Individual address (unicast)
 - Source: Intel_03:2a:c3 (c4:d0:e3:03:2a:c3)
 - Type: IPv4 (0x0800)
 - [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.1.231, Dst: 192.168.1.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 73
 - Identification: 0x5ee4 (24292)
 - 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 128
 - Protocol: UDP (17)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.231
 - Destination Address: 192.168.1.1
 - [Stream index: 57]

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 1 bit(s)

Пакеты: 3549611 - Отображено: 9479 (0.3%)

Профиль: Default

Wireshark (разбор запроса)

```
Frame 3548946: Packet, 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{100AB252-4142-43C1-9819-04469B22FC}
Ethernet II, Src: Intel_03:2a:c3 (c4:d0:e3:03:2a:c3), Dst: Sercomm_5a:00:5c (74:9d:79:5a:00:5c)
Internet Protocol Version 4, Src: 192.168.1.231, Dst: 192.168.1.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 73
  Identification: 0x5ee4 (24292)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.231
  Destination Address: 192.168.1.1
  [Stream index: 57]
User Datagram Protocol, Src Port: 59095, Dst Port: 53
  Source Port: 59095
  Destination Port: 53
  Length: 53
  Checksum: 0x847f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2848]
  [Stream Packet Number: 7]
  [Timestamps]
  UDP payload (45 bytes)
```

```
Domain Name System (query)
  Transaction ID: 0x28ab
  Flags: 0x0120 Standard query
    0... .... = Response: Message is a query
    .000 0... .... = Opcode: Standard query (0)
    .... 0. .... = Truncated: Message is not truncated
    .... 1. .... = Recursion desired: Do query recursively
    .... 0.. .... = Z: reserved (0)
    .... 1. .... = AD bit: Set
    .... 0..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    pogoda.yandex.ru: type NS, class IN
      Name: pogoda.yandex.ru
      [Name Length: 16]
      [Label Count: 3]
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
  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
  [Response In: 3548947]
```

Wireshark (запрос в бинарном виде)

0000	74 9d 79	5a 00 5c c4 d0	e3 03 2a c3 08 00 45 00	t·yZ·\· · · · · *
0010	00 49 5e e4 00 00 80 11	00 00 c0 a8 01 e7 c0 a8	· I ^ · · · · ·	
0020	01 01 e6 d7 00 35 00 35	84 7f 28 ab 01 20 00 01	· · · · · 5 · 5 · · (· · ·	
0030	00 00 00 00 00 01 06 70	6f 67 6f 64 61 06 79 61	· · · · · · p o g o d a · y a	
0040	6e 64 65 78 02 72 75 00	00 02 00 01 00 00 29 04	n d e x · r u · · · · ·) ·	
0050	d0 00 00 00 00 00 00		· · · · · ·	

Пример рекурсивного режима работы DNS

Запрос:

```
C:\Users\User>nslookup -type=AAAA yandex.ru
ТхТхТхТх: SBT.lan
Address: 192.168.1.1
```

```
Не заслуживающий доверия ответ:
Ль : yandex.ru
Address: 2a02:6b8:a::a
```

```
▼ Domain Name System (query)
Transaction ID: 0xdc67
▼ Flags: 0x0100 Standard query
  0... .. = Response: Message is a query
  .000 0... .. = Opcode: Standard query (0)
  .... ..0. .... = Truncated: Message is not truncated
  .... ..1 .... = Recursion desired: Do query recursively
  .... ..0.. .... = Z: reserved (0)
  .... ....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ yandex.ru: type AAAA, class IN
    Name: yandex.ru
    [Name Length: 9]
    [Label Count: 2]
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
[Response In: 275780]
```

Ответ:

```
▼ Domain Name System (response)
Transaction ID: 0xdc67
▼ Flags: 0x8180 Standard query response, No error
  1... .. = Response: Message is a response
  .000 0... .. = Opcode: Standard query (0)
  .... ..0.. .... = Authoritative: Server is not an authority for domain
  .... ..0. .... = Truncated: Message is not truncated
  .... ..1 .... = Recursion desired: Do query recursively
  .... ..1... .... = Recursion available: Server can do recursive queries
  .... ....0.. .... = Z: reserved (0)
  .... ....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
  .... ....0 .... = Non-authenticated data: Unacceptable
  .... ....0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ yandex.ru: type AAAA, class IN
    Name: yandex.ru
    [Name Length: 9]
    [Label Count: 2]
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
▼ Answers
  ▼ yandex.ru: type AAAA, class IN, addr 2a02:6b8:a::a
    Name: yandex.ru
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 164 (2 minutes, 44 seconds)
    Data length: 16
    AAAA Address: 2a02:6b8:a::a
[Request In: 275779]
[Time: 3.734000 milliseconds]
```

Пример итеративного режима работы DNS

1) Получаем сервера, обслуживающие корневую зону

```
C:\Users\User>nslookup -type=NS .  
ᐅxĖtxĖ: SBT.lan  
Address: 192.168.1.1
```

Не заслуживающий доверия ответ:

```
(root) nameserver = g.root-servers.net  
(root) nameserver = h.root-servers.net  
(root) nameserver = i.root-servers.net  
(root) nameserver = j.root-servers.net  
(root) nameserver = k.root-servers.net  
(root) nameserver = l.root-servers.net  
(root) nameserver = m.root-servers.net  
(root) nameserver = a.root-servers.net  
(root) nameserver = b.root-servers.net  
(root) nameserver = c.root-servers.net  
(root) nameserver = d.root-servers.net  
(root) nameserver = e.root-servers.net  
(root) nameserver = f.root-servers.net
```

2) Получаем ip-адреса tld серверов домена .ru

```
C:\Users\User>nslookup yandex.ru a.root-servers.net  
in-addr.arpa nameserver = f.in-addr-servers.arpa  
in-addr.arpa nameserver = b.in-addr-servers.arpa  
in-addr.arpa nameserver = d.in-addr-servers.arpa  
in-addr.arpa nameserver = a.in-addr-servers.arpa  
in-addr.arpa nameserver = c.in-addr-servers.arpa  
in-addr.arpa nameserver = e.in-addr-servers.arpa  
f.in-addr-servers.arpa internet address = 193.0.9.1  
f.in-addr-servers.arpa AAAA IPv6 address = 2a13:27c0:30::1  
b.in-addr-servers.arpa internet address = 199.253.183.183  
b.in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87  
d.in-addr-servers.arpa internet address = 200.10.60.53  
d.in-addr-servers.arpa AAAA IPv6 address = 2001:13c7:7010::53  
a.in-addr-servers.arpa internet address = 199.180.182.53  
a.in-addr-servers.arpa AAAA IPv6 address = 2620:37:e000::53  
c.in-addr-servers.arpa internet address = 196.216.169.10  
c.in-addr-servers.arpa AAAA IPv6 address = 2001:43f8:110::10  
e.in-addr-servers.arpa internet address = 203.119.86.101  
e.in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::101  
ᐅxĖtxĖ: UnKnown  
Address: 198.41.0.4  
  
ᐅᐅ : yandex.ru  
Served by:  
- a.dns.ripn.net  
193.232.128.6  
2001:678:17:0:193:232:128:6  
ru  
- d.dns.ripn.net  
194.190.124.17  
2001:678:18:0:194:190:124:17  
ru  
- f.dns.ripn.net  
193.232.156.17  
2001:678:14:0:193:232:156:17  
ru  
- b.dns.ripn.net  
194.85.252.62  
2001:678:16:0:194:85:252:62  
ru  
- e.dns.ripn.net  
193.232.142.17  
2001:678:15:0:193:232:142:17  
ru
```

Пример итеративного режима работы DNS

3) Отправляем запрос к серверу a.dns.ripn.net (193.232.128.6)

```
C:\Users\User>nslookup yandex.ru 193.232.128.6
ᐅxЁtxЁ: UnKnown
Address: 193.232.128.6

ᐅᐅ : yandex.ru
Served by:
- ns2.yandex.RU
    93.158.134.1
    2a02:6b8:0:1::1
    YANDEX.RU
- ns1.yandex.RU
    213.180.193.1
    2a02:6b8::1
    YANDEX.RU
```

4) Отправляем запрос ns2.yandex.RU (93.158.134.1)

```
C:\Users\User>nslookup yandex.ru 93.158.134.1
ᐅxЁtxЁ: UnKnown
Address: 93.158.134.1

ᐅᐅ : yandex.ru
Addresses: 2a02:6b8:a::a
    77.88.55.88
    5.255.255.77
    77.88.44.55
```

В результате получаем ip-адреса серверов, обслуживающий yandex.ru

2a02:6b8:a::a
77.88.55.88
5.255.255.77
77.88.44.55

Тест

- **1. Что означает аббревиатура DNS?**
 - a) Digital Naming Service
 - b) Domain Name System
 - c) Data Network Switch
 - d) Domain Navigation System
- **2. Какой тип DNS-записи связывает доменное имя с IPv4-адресом?**
 - a) AAAA
 - b) CNAME
 - c) MX
 - d) A
- **3. Какой порт используется по умолчанию для DNS-запросов?**
 - a) 25
 - b) 53
 - c) 80
 - d) 443

Тест

- **4. В зоне in-addr.arpa хранятся записи какого типа?**
 - a) A
 - b) AAAA
 - c) PTR
 - d) CNAME
- **5. Что такое TTL в контексте DNS?**
 - a) Time To Leave — время покинуть сеть
 - b) Total Traffic Limit — общий лимит трафика
 - c) Time To Live — время жизни записи в кэше
 - d) Transmission Time Limit — лимит времени передачи
- **6. Какой тип DNS-сервера НЕ является авторитативным для зоны, но кэширует ответы для ускорения работы?**
 - a) Корневой сервер
 - b) Рекурсивный резолвер
 - c) TLD-сервер
 - d) Авторитативный сервер домена

Тест

- **7. Вы ввели в браузере "example.com", но сайт не открывается. Какая из этих команд поможет диагностировать проблему с DNS?**
 - a) ping example.com
 - b) nslookup example.com
 - c) tracert example.com
 - d) Все вышеперечисленные
- **8. Какой стандарт позволяет шифровать DNS-трафик между клиентом и резолвером?**
 - a) DNSSEC
 - b) DoH (DNS over HTTPS)
 - c) EDNS
 - d) IPv6
- **9. Что такое "доменная зона" (DNS zone)?**
 - a) Географический регион, обслуживаемый DNS-сервером
 - b) Административная единица делегирования в DNS
 - c) Часть доменного имени после точки
 - d) Группа DNS-серверов одного провайдера

Тест

- **10. Что такое ICANN и какова её основная роль в работе DNS?**
 - a) Это компания, которая продаёт домены в зоне .com через сайт GoDaddy.
 - b) Это международный регулятор, который координирует уникальность ключевых параметров интернета: имён доменов и IP-адресов.
 - c) Это организация, которая определяет, какие сайты можно открывать в каждой стране.
 - d) Это провайдер интернет-услуг, который обслуживает корневые DNS-серверы.

