

**Московский государственный технический
университет им. Н.Э. Баумана**

**Факультет «Информатика и системы управления»
Кафедра ИУ5 «Системы обработки информации и управления»**

Курс «Сети и телекоммуникации»

**Отчет по лабораторной работе №8
«Ознакомление с системой и протоколом dns»
Вариант №3**

Выполнил:

студент группы ИУ5-51Б

Бирюкова Екатерина

Подпись и дата:

Проверил:

Подпись и дата:

Цель работы

Лабораторная работа ставит цели закрепления теоретического материала по протоколам и программному обеспечению системы доменных имен. Ознакомиться с работой утилит host, nslookup, dig. Научиться делать обратный DNS запрос.

Задание:

1. Разрешение адресов в системе DNS с использованием различных утилит системы Linux
 - 1.1. Запустить анализатор протоколов Wireshark и указать фильтр для перехвата трафика DNS.
 - 1.2. В терминале последовательно выполнить разрешение доменных имен согласно варианту из ЛР1 с использованием трех утилит:
 - а) host
 - б) nslookup
 - в) dig
 - 1.3. Остановить захват пакетов в анализаторе протоколов Wireshark.
 - 1.4. Проанализировать вывод команд и перехваченные пакеты.
 - 1.5. В отчете привести последовательно вывод каждой команды, сопроводив его соответствующими перехваченными пакетами и выводами по работе программ.
2. Получение ресурсных записей различных типов с использованием утилиты nslookup
 - 2.1. Запустить анализатор протоколов Wireshark и указать фильтр для перехвата трафика DNS.
 - 2.2. Последовательно получить от сервера DNS следующие ресурсные записи для доменного имени согласно варианту:
 - а) адреса IPv4
 - б) адреса IPv6
 - в) почтовые серверы

г) серверы DNS

д) авторитетный сервер для доменного имени

2.3. Остановить захват пакетов в анализаторе протоколов Wireshark.

2.4. Проанализировать вывод команд и перехваченные пакеты. В отчете привести последовательно вывод каждой команды, сопроводив его соответствующими перехваченными пакетами и выводами по работе программ.

3. Проведение обратного запроса DNS с использованием утилиты host

3.1. Запустить анализатор протоколов Wireshark и указать фильтр для перехвата трафика DNS.

3.2. Провести обратный запрос DNS для IPv4-адреса из предыдущего пункта.

3.3. Провести обратный запрос DNS для IPv6-адреса из предыдущего пункта. При формировании команды запроса руководствоваться примером ресурсной записи:

3.4. Остановить захват пакетов в анализаторе протоколов Wireshark.

5. Проанализировать вывод команд и перехваченные пакеты.

3.5. В отчете привести последовательно вывод каждой команды, сопроводив его соответствующими перехваченными пакетами и выводами по работе программ.

4. Получение всех ресурсных записей для определенного доменного имени с использованием утилиты host

4.1. Запустить анализатор протоколов Wireshark и указать фильтр для перехвата трафика: IP-адреса ПК и сервера DNS, протоколы (TCP или UDP).

4.2. Выполнить запрос «ресурсной записи» ANY для доменного имени согласно варианту.

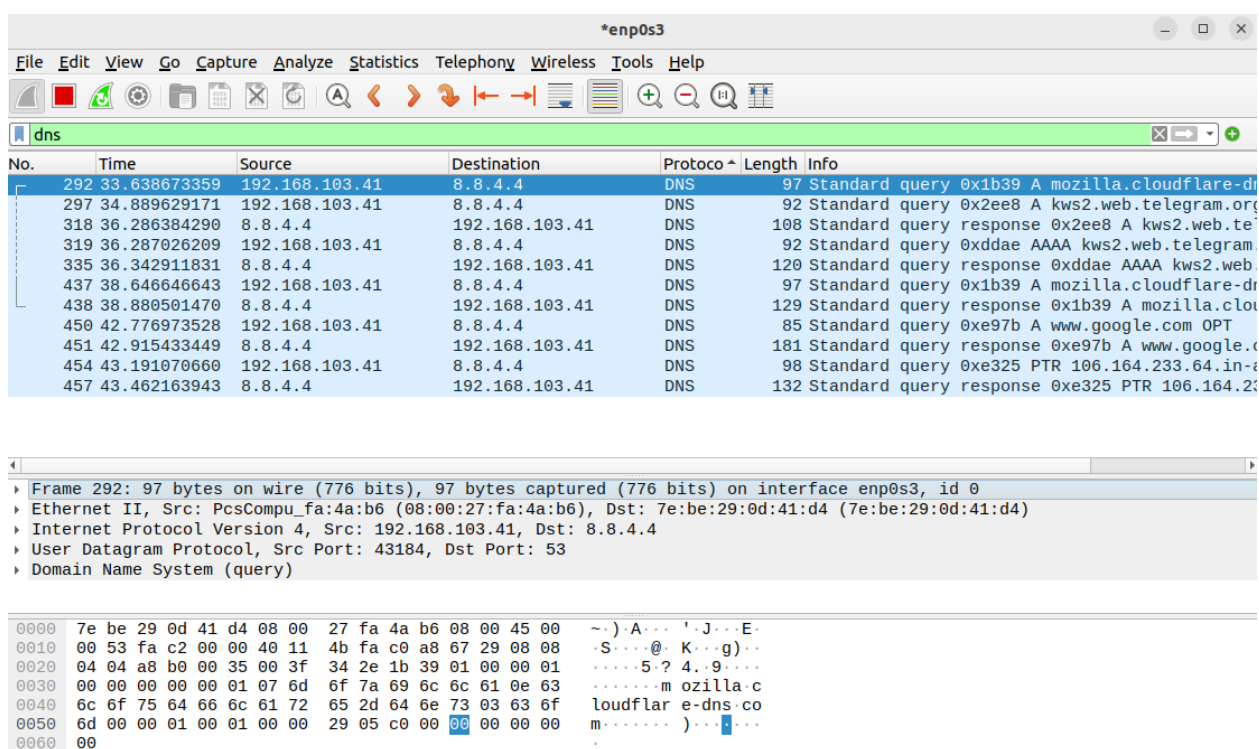
4.3. Остановить захват пакетов в анализаторе протоколов Wireshark. Проанализировать вывод команд и перехваченные пакеты.

4.4. В отчете привести вывод команды, сопроводив его соответствующими перехваченными пакетами и выводами по процедуре получения записи.

Ход лабораторной работы:

1. Разрешение адресов в системе DNS с использованием различных утилит системы Linux

1.1. Запустить анализатор протоколов Wireshark и указать фильтр для перехвата трафика DNS.



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows a list of captured packets, with the filter 'dns' applied. The selected packet (No. 292) is a DNS Standard query from 192.168.103.41 to 8.8.4.4. The packet details pane shows the structure of the DNS query, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data of the packet in hexadecimal and ASCII.

1.2. В терминале последовательно выполнить разрешение доменных имен согласно варианту из ЛР1 (www.industry.su, www.yandex.ru, www.oracle.com) с использованием трех утилит:

а) host

| | | | | | | |
|------|---------------|----------------|----------------|-----|-----|---|
| 6677 | 733.822109013 | 192.168.103.41 | 8.8.4.4 | DNS | 84 | Standard query 0x9b1b A www.yandex.ru OPT |
| 6678 | 733.928858072 | 8.8.4.4 | 192.168.103.41 | DNS | 132 | Standard query response 0x9b1b A www.yandex.ru OPT |
| 6679 | 733.930819357 | 192.168.103.41 | 8.8.4.4 | DNS | 84 | Standard query 0x9730 AAAA www.yandex.ru OPT |
| 6681 | 733.995513246 | 8.8.4.4 | 192.168.103.41 | DNS | 112 | Standard query response 0x9730 AAAA www.yandex.ru OPT |
| 6682 | 733.996122931 | 192.168.103.41 | 8.8.4.4 | DNS | 84 | Standard query 0xc31 MX www.yandex.ru OPT |
| 6685 | 734.252674730 | 8.8.4.4 | 192.168.103.41 | DNS | 103 | Standard query response 0xc31 MX www.yandex.ru OPT |

б) nslookup

| | | | | | | |
|------|---------------|----------------|----------------|-----|-----|---|
| 7232 | 799.434936745 | 192.168.103.41 | 8.8.4.4 | DNS | 84 | Standard query 0x0494 A www.yandex.ru OPT |
| 7235 | 799.546891097 | 8.8.4.4 | 192.168.103.41 | DNS | 132 | Standard query response 0x0494 A www.yandex.ru OPT |
| 7236 | 799.549492533 | 192.168.103.41 | 8.8.4.4 | DNS | 84 | Standard query 0x8f72 AAAA www.yandex.ru OPT |
| 7238 | 800.027685776 | 8.8.4.4 | 192.168.103.41 | DNS | 112 | Standard query response 0x8f72 AAAA www.yandex.ru OPT |

В) dig

| | | | | | |
|------|---------------|----------------|----------------|-----|--|
| 8388 | 932.630958644 | 192.168.103.41 | 8.8.4.4 | DNS | 84 Standard query 0x86da A www.yandex.ru OPT |
| 8392 | 932.704900895 | 8.8.4.4 | 192.168.103.41 | DNS | 132 Standard query response 0x86da A www.yandex.ru |

```
stud51@ubuntu18:~$ host www.yandex.ru; nslookup www.industry.su; dig www.oracle.com
www.yandex.ru has address 77.88.44.55
www.yandex.ru has address 5.255.255.77
www.yandex.ru has address 77.88.55.88
www.yandex.ru has IPv6 address 2a02:6b8:a::a
www.yandex.ru mail is handled by 10 mx.yandex.ru.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.industry.su
Address: 31.31.205.163

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.oracle.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5116
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.oracle.com.                IN      A

;; ANSWER SECTION:
www.oracle.com.                197     IN      CNAME   ds-www.oracle.com.edgekey.net.
ds-www.oracle.com.edgekey.net. 19485   IN      CNAME   e2581.dscx.akamaiedge.net.
e2581.dscx.akamaiedge.net.     20      IN      A       92.122.109.102

;; Query time: 98 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 18 15:24:27 MSK 2024
;; MSG SIZE rcvd: 138
```

1.3. Остановить захват пакетов в анализаторе протоколов Wireshark.

Остановить с помощью кнопки сверху



| | | | | | |
|-------|-----------------|----------------|----------------|-----|---|
| 10506 | 1692.9823769... | 192.168.103.41 | 8.8.4.4 | DNS | 84 Standard query 0x37d6 A www.yandex.ru OPT |
| 10507 | 1693.3174715... | 8.8.4.4 | 192.168.103.41 | DNS | 132 Standard query response 0x37d6 A www.yan |
| 10508 | 1693.3217951... | 192.168.103.41 | 8.8.4.4 | DNS | 84 Standard query 0xc6da AAAA www.yandex.ru |
| 10509 | 1693.3847644... | 8.8.4.4 | 192.168.103.41 | DNS | 112 Standard query response 0xc6da AAAA www.y |
| 10510 | 1693.3864520... | 192.168.103.41 | 8.8.4.4 | DNS | 84 Standard query 0xf6ca MX www.yandex.ru OI |
| 10512 | 1693.5500646... | 8.8.4.4 | 192.168.103.41 | DNS | 103 Standard query response 0xf6ca MX www.ya |
| 10513 | 1693.6073611... | 192.168.103.41 | 8.8.4.4 | DNS | 86 Standard query 0xe361 AAAA www.industry.s |
| 10516 | 1693.6753436... | 8.8.4.4 | 192.168.103.41 | DNS | 143 Standard query response 0xe361 AAAA www. |
| 10517 | 1693.7033621... | 192.168.103.41 | 8.8.4.4 | DNS | 85 Standard query 0x203e A www.oracle.com OI |
| 10518 | 1693.7708360... | 8.8.4.4 | 192.168.103.41 | DNS | 180 Standard query response 0x203e A www.ora |

1.4. Проанализировать вывод команд и перехваченные пакеты.

Мы видим, что были перехвачены пакеты протокола DNS. Используются два адреса: 192.168.103.41 — адрес ПК в локальной сети и 8.8.4.4 — адрес маршрутизатора.

Для `www.yandex.ru` запрашивается запись типа `A` и `AAAA` для получения `IPv4` и `IPv6`. Также запрашивается `MX` запись, которая используется для почтовых серверов.

Для `www.industry.su` используется `AAAA`, для `www.oracle.com` – `A`.

Для домена `www.yandex.ru` возвращена запись типа `A` (`IPv4`-адрес), `AAAA` (`IPv6`-адрес) и `MX`-запись.

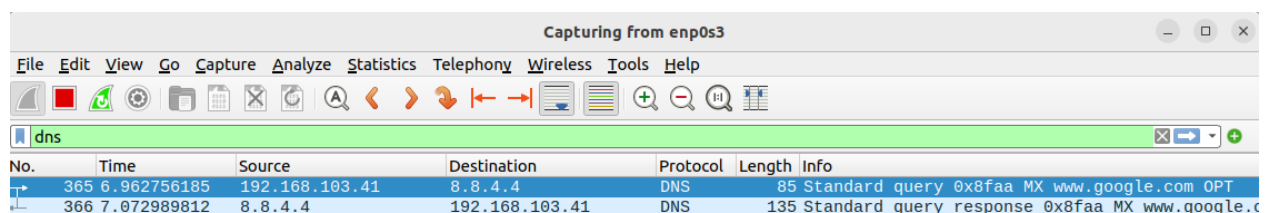
Для домена `www.industry.su` был использован локальный `DNS`-сервер для разрешения и возвращен `IPv4` адрес.

Для домена `www.oracle.com` была возвращена запись типа `A` (`IPv4`-адрес), а также `CNAME`-запись, указывающая на основной домен.

1.5.В отчете привести последовательно вывод каждой команды, сопроводив его соответствующими перехваченными пакетами и выводами по работе программ.

2. Получение ресурсных записей различных типов с использованием утилиты `nslookup`

2.1.Запустить анализатор протоколов `Wireshark` и указать фильтр для перехвата трафика `DNS`.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|--|
| 365 | 6.962756185 | 192.168.103.41 | 8.8.4.4 | DNS | 85 | Standard query 0x8faa MX www.google.com OPT |
| 366 | 7.072989812 | 8.8.4.4 | 192.168.103.41 | DNS | 135 | Standard query response 0x8faa MX www.google.c |

2.2.Последовательно получить от сервера `DNS` следующие ресурсные записи для доменного имени:

в) почтовые серверы

```

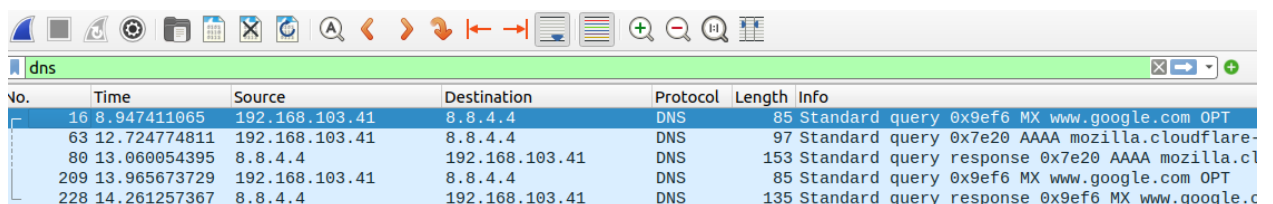
> set type=MX
> www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
*** Can't find www.google.com: No answer

Authoritative answers can be found from:
google.com
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 707023159
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60
>

```

2.3. Остановить захват пакетов в анализаторе протоколов Wireshark.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------------|----------------|----------|--------|--|
| 16 | 8.947411065 | 192.168.103.41 | 8.8.4.4 | DNS | 85 | Standard query 0x9ef6 MX www.google.com OPT |
| 63 | 12.724774811 | 192.168.103.41 | 8.8.4.4 | DNS | 97 | Standard query 0x7e20 AAAA mozilla.cloudflare- |
| 80 | 13.060054395 | 8.8.4.4 | 192.168.103.41 | DNS | 153 | Standard query response 0x7e20 AAAA mozilla.cl |
| 209 | 13.965673729 | 192.168.103.41 | 8.8.4.4 | DNS | 85 | Standard query 0x9ef6 MX www.google.com OPT |
| 228 | 14.261257367 | 8.8.4.4 | 192.168.103.41 | DNS | 135 | Standard query response 0x9ef6 MX www.google.c |

2.4. Проанализировать вывод команд и перехваченные пакеты. В отчете привести последовательно вывод каждой команды, сопроводив его соответствующими перехваченными пакетами и выводами по работе программ.

```

stud51@ubuntu18:~$ dig www.yandex.ru MX

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.yandex.ru MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 25856
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      MX

;; ANSWER SECTION:
www.yandex.ru.                300     IN      MX      10 mx.yandex.ru.

;; Query time: 311 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 18 16:00:18 MSK 2024
;; MSG SIZE rcvd: 61

stud51@ubuntu18:~$ dig www.yandex.ru AAAA

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.yandex.ru AAAA
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 34480
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      AAAA

;; ANSWER SECTION:
www.yandex.ru.                300     IN      AAAA     2a02:6b8:a::a

```

```

stud51@ubuntu18:~$ dig www.yandex.ru A
; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.yandex.ru A
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 52352
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                393     IN      A      77.88.55.88
www.yandex.ru.                393     IN      A      77.88.44.55
www.yandex.ru.                393     IN      A      5.255.255.77

;; Query time: 267 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 18 16:02:18 MSK 2024
;; MSG SIZE rcvd: 90

stud51@ubuntu18:~$ dig www.yandex.ru NS
; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.yandex.ru NS
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 28925
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      NS

```

```

; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      NS

;; AUTHORITY SECTION:
yandex.ru.                    900     IN      SOA     ns1.yandex.ru. sysadmin.yandex-team.ru. 20230
34128 600 300 2592000 900

;; Query time: 118 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 18 16:02:22 MSK 2024
;; MSG SIZE rcvd: 103

stud51@ubuntu18:~$ dig www.yandex.ru SOA
; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.yandex.ru SOA
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 41072
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      SOA

;; AUTHORITY SECTION:
yandex.ru.                    900     IN      SOA     ns1.yandex.ru. sysadmin.yandex-team.ru. 20230
34128 600 300 2592000 900

;; Query time: 109 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 18 16:02:26 MSK 2024
;; MSG SIZE rcvd: 103

```

Команда dig для домена www.yandex.ru была выполнена по запросам пяти типов ресурсных записей: A, AAAA, MX, NS и SOA. Результаты показывают следующее:

Для запроса A был получен IPv4-адрес домена www.yandex.ru: это 77.88.55.88. Запись была найдена в секции ANSWER, что указывает на успешное разрешение имени.

Запрос на получение записи AAAA, которая отвечает за IPv6-адреса, вернул данных. В секции ANSWER присутствуют результаты, поэтому статус

запроса NOERROR показывает, что сервер обработал запрос корректно. Это означает, что у домена `www.yandex.ru` IPv6-адрес это `2a02:6b8:a::a`.

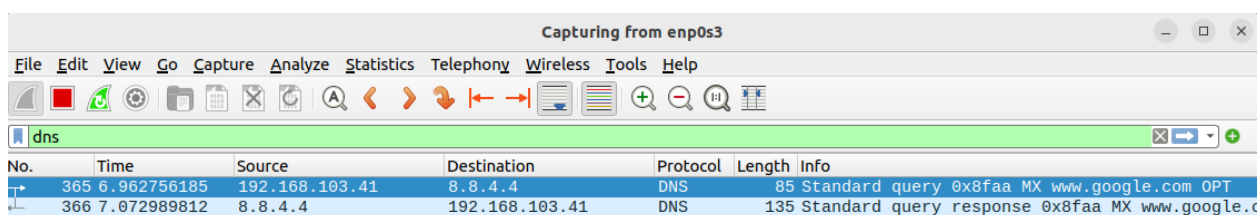
При запросе MX, который отвечает за почтовые серверы, данные также присутствуют. Сервер вернул информацию из секции ANSWER с записью, где указано, что авторитетным сервером является `mx.yandex.ru`.

Для запроса NS, который отвечает за список DNS-серверов, в секции ANSWER данные не представлены, а в секции AUTHORITY содержится запись SOA, где указан авторитетный сервер `ns1.yandex.ru`, а ответственным лицом – `sysadmin.yandex-team.ru`.

Запрос SOA вернул информацию о том, что для домена `www.yandex.ru` авторитетным сервером является `ns1.yandex.ru`. Дополнительно указано, что ответственным лицом является `sysadmin.yandex.ru`, а также представлены параметры зоны, такие как серийный номер зоны и тайм-ауты для обновлений.

3. Проведение обратного запроса DNS с использованием утилиты host

3.1. Запустить анализатор протоколов Wireshark и указать фильтр для перехвата трафика DNS.



The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates 'Capturing from enp0s3'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows two captured packets, both of type DNS. The first packet is a standard query for the MX record of www.google.com. The second packet is the corresponding standard query response.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|--|
| 365 | 6.962756185 | 192.168.103.41 | 8.8.4.4 | DNS | 85 | Standard query 0x8faa MX www.google.com OPT |
| 366 | 7.072989812 | 8.8.4.4 | 192.168.103.41 | DNS | 135 | Standard query response 0x8faa MX www.google.c |

3.2. Провести обратный запрос DNS для IPv4-адреса из предыдущего пункта.

```

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53899
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                46      IN      A      5.255.255.77
www.yandex.ru.                46      IN      A      77.88.55.88
www.yandex.ru.                46      IN      A      77.88.44.55

;; Query time: 191 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 23 09:10:52 MSK 2024
;; MSG SIZE rcvd: 90

stud51@ubuntu18:~$ dig -x 77.88.55.88

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> -x 77.88.55.88
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4076
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;88.55.88.77.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
88.55.88.77.in-addr.arpa. 141     IN      PTR      yandex.ru.

;; Query time: 80 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 23 09:11:16 MSK 2024
;; MSG SIZE rcvd: 76

stud51@ubuntu18:~$

```

3.3. Провести обратный запрос DNS для IPv6-адреса из предыдущего пункта. При формировании команды запроса руководствоваться примером ресурсной записи:

```

stud51@ubuntu18:~$ dig -x 2a02:6b8:a::a

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> -x 2a02:6b8:a::a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60649
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.0.0.0.8.b.6.0.2.0.a.2.ip6.arpa.
. IN PTR

;; ANSWER SECTION:
a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.0.0.0.8.b.6.0.2.0.a.2.ip6.arpa.
257 IN PTR yandex.ru.

;; Query time: 824 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Dec 23 09:16:28 MSK 2024
;; MSG SIZE rcvd: 124

```



```

stud51@ubuntu18:~$ dig www.yandex.ru ANY

; <<> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<> www.yandex.ru ANY
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 24263
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.yandex.ru.                IN      ANY

;; ANSWER SECTION:
www.yandex.ru.                300     IN      MX      10 mx.yandex.ru.
www.yandex.ru.                600     IN      A       77.88.44.55
www.yandex.ru.                600     IN      A       5.255.255.77
www.yandex.ru.                600     IN      A       77.88.55.88
www.yandex.ru.                300     IN      AAAA    2a02:6b8:a::a

;; Query time: 86 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Wed Dec 25 14:16:35 MSK 2024
;; MSG SIZE rcvd: 137

```

4.3. Остановить захват пакетов в анализаторе протоколов Wireshark.

Проанализировать вывод команд и перехваченные пакеты.

Запрос dig www.yandex.ru ANY вернул записи типов A, AAAA и MX.

| | | | | | | | | | |
|-----|---------------|---------------|---------------|-----|-----|-------------------------|--------|------|---------------|
| 400 | 269.540743613 | 192.168.43.41 | 8.8.4.4 | DNS | 85 | Standard query | 0xd6f3 | AAAA | ntp.ubuntu.co |
| 401 | 269.611688960 | 8.8.4.4 | 192.168.43.41 | DNS | 149 | Standard query response | 0xa714 | A | ntp.ubu |
| 402 | 269.611689133 | 8.8.4.4 | 192.168.43.41 | DNS | 169 | Standard query response | 0xd6f3 | AAAA | ntp. |
| 410 | 276.662541945 | 192.168.43.41 | 8.8.4.4 | DNS | 100 | Standard query | 0x318a | AAAA | connectivity- |
| 411 | 276.757825040 | 8.8.4.4 | 192.168.43.41 | DNS | 436 | Standard query response | 0x318a | AAAA | conn |
| 425 | 333.359686664 | 192.168.43.41 | 8.8.4.4 | DNS | 84 | Standard query | 0xa6ed | ANY | www.yandex.ru |
| 426 | 333.444457191 | 8.8.4.4 | 192.168.43.41 | DNS | 179 | Standard query response | 0xa6ed | ANY | www.y |
| 432 | 340.536103001 | 192.168.43.41 | 8.8.4.4 | DNS | 100 | Standard query | 0x14e4 | AAAA | connectivity- |
| 433 | 340.705717908 | 8.8.4.4 | 192.168.43.41 | DNS | 436 | Standard query response | 0x14e4 | AAAA | conn |
| 440 | 424.125168735 | 192.168.43.41 | 8.8.4.4 | DNS | 84 | Standard query | 0x3f6b | ANY | www.yandex.ru |
| 441 | 424.227756761 | 8.8.4.4 | 192.168.43.41 | DNS | 179 | Standard query response | 0x3f6b | ANY | www.y |
| 448 | 464.979987496 | 192.168.43.41 | 8.8.4.4 | DNS | 84 | Standard query | 0xa86d | ANY | www.yandex.ru |
| 449 | 465.084260825 | 8.8.4.4 | 192.168.43.41 | DNS | 179 | Standard query response | 0xa86d | ANY | www.y |
| 450 | 468.443393688 | 192.168.43.41 | 8.8.4.4 | DNS | 100 | Standard query | 0xf656 | AAAA | connectivity- |
| 451 | 468.523834182 | 8.8.4.4 | 192.168.43.41 | DNS | 436 | Standard query response | 0xf656 | AAAA | conn |

4.4. В отчете привести вывод команды, сопроводив его соответствующими перехваченными пакетами и выводами по процедуре получения записи.

Контрольные вопросы:

1. Что такое система доменных имён (DNS)?

DNS (Domain Name System) - это иерархическая и децентрализованная система именования для компьютеров, сервисов и других ресурсов, подключенных к Интернету или частным сетям. Она преобразует человекопонятные доменные имена (например, google.com) в IP-адреса (например, 172.217.160.142), которые используются компьютерами для связи друг с другом. DNS работает как телефонная книга для Интернета, позволяя пользователям получать доступ к ресурсам, не запоминая сложные цифровые адреса.

2. Для чего используется файл hosts?

Файл hosts — это простой текстовый файл, который используется операционной системой для сопоставления доменных имен с IP-адресами. Когда компьютер делает запрос на подключение к домену, он сначала проверяет файл hosts. Если запись для этого домена найдена, компьютер использует указанный в файле IP-адрес и не обращается к DNS-серверу. Файл hosts часто используется для:

Локального перенаправления: Для перенаправления доменных имен на локальный компьютер (например, для тестирования веб-сайтов).

Блокировки доменов: Для блокировки доступа к определенным сайтам, перенаправляя их на 127.0.0.1 (localhost).

Временного переопределения DNS: Для временного использования других IP-адресов для определенных доменов.

3. Каковы ключевые характеристики DNS?

Иерархическая структура: DNS имеет иерархическую структуру, которая отражает организацию Интернета, с корневым доменом, доменами верхнего уровня (TLD), доменами второго уровня и т. д.

Децентрализованная: DNS — это децентрализованная система, где ответственность за отдельные зоны и домены распределяется между различными серверами. Это повышает надежность и отказоустойчивость.

Кэширование: DNS использует кэширование для ускорения процесса разрешения имен. DNS-серверы могут временно сохранять результаты запросов, чтобы не повторять один и тот же запрос постоянно.

Масштабируемость: DNS разработана с учетом масштабируемости, что позволяет поддерживать огромное количество доменных имен и пользователей в Интернете.

Протокол UDP/TCP: DNS использует UDP (User Datagram Protocol) для большинства запросов, но может использовать TCP (Transmission Control Protocol) для передачи более крупных ответов (например, при использовании DNSSEC) или запросов.

Разрешение имен: Основная функция DNS — это разрешение доменных имен в IP-адреса.

Типы записей: DNS поддерживает различные типы записей (A, AAAA, CNAME, MX, TXT и т. д.) для различных целей (например, A и AAAA для IP-адресов, MX для почтовых серверов).

4. Что такое домен и поддомен?

Домен: Домен — это адрес в интернете, который обычно представляет собой веб-сайт или другой интернет-ресурс. Домены состоят из двух или более частей, разделенных точками (например, example.com, google.ru).

Поддомен: Поддомен — это часть домена, расположенная слева от основного домена, также разделенная точкой (например, www.example.com, blog.example.com). Поддомены обычно используются для организации контента на сайте, таких как блоги, магазины или различные сервисы.

5. Что такое корневой домен?

Корневой домен — это вершина иерархии DNS. Он представлен точкой (.) и обычно не отображается явно в доменных именах. Корневые DNS-серверы содержат информацию о DNS-серверах верхнего уровня (например, .com, .org, .ru). Существуют 13 корневых серверов по всему миру.

6. Что такое рекурсия в DNS?

Рекурсия в DNS — это метод обработки запроса, при котором DNS-сервер, получив запрос, сам выполняет все необходимые шаги для нахождения ответа, обращаясь к другим серверам, пока не получит IP-адрес для запрошенного домена. При рекурсивном запросе клиент делает запрос на рекурсивный DNS-сервер, и тот берёт на себя ответственность за выполнение всех промежуточных запросов до получения нужного IP-адреса.

7. Как выполняется DNS-запрос?

DNS-запрос обычно выполняется в несколько этапов:

Проверка локального кэша: Операционная система сначала проверяет локальный кэш DNS, чтобы узнать, есть ли там нужный IP-адрес.

Запрос к DNS-серверу, настроенному на компьютере: Если в кэше нет нужного адреса, компьютер делает запрос к DNS-серверу, настроенному в его сетевых настройках (обычно это DNS-сервер провайдера).

Рекурсивный или итеративный запрос: DNS-сервер может обрабатывать запрос рекурсивно (сам обращается к другим серверам) или итеративно (отправляет клиенту ссылку на другой сервер).

Обращение к корневому серверу: Если DNS-сервер не знает IP-адрес, он обращается к одному из корневых DNS-серверов.

Обращение к TLD-серверу: Корневой сервер направляет к серверу домена верхнего уровня (например, .com).

Обращение к серверу домена: Сервер TLD направляет к серверу домена (например, example.com).

Получение IP-адреса: Сервер домена возвращает IP-адрес запрашиваемого имени.

Отправка ответа клиенту: DNS-сервер отправляет IP-адрес клиенту, а клиент сохраняет его в кэше.

8. *Что такое обратный DNS-запрос (Reverse DNS Lookup)?*

Обратный DNS-запрос — это процесс поиска доменного имени по IP-адресу. В отличие от обычного запроса, который преобразует имя в IP-адрес, обратный запрос позволяет узнать имя хоста, связанное с определенным IP-адресом. Обратные запросы используются для проверки подлинности отправителей электронной почты, для анализа трафика и в других случаях, где требуется узнать имя хоста по его IP-адресу. Для таких запросов используются PTR записи в DNS.

host, nslookup, и dig — это три утилиты командной строки, используемые для получения информации о хостах и доменных именах. Они выполняют похожие задачи, но имеют ключевые различия в функциональности, гибкости и детальности выдаваемой информации.

| Утилита | Простота использования | Гибкость | Детализация информации |
|----------|------------------------|----------|------------------------|
| host | Высокая | Низкая | Низкая |
| nslookup | Средняя | Средняя | Средняя |
| dig | Низкая | Высокая | Высокая |

| Характеристика | TCP | UDP |
|-------------------|-------------------------------|-----------------------------|
| Соединение | Ориентированный на соединение | Без установления соединения |
| Гарантия доставки | Гарантированная | Не гарантированная |
| Порядок пакетов | Гарантирован | Не гарантирован |

| Характеристика | TCP | UDP |
|--------------------|----------------------------------|---------------------------------|
| Управление потоком | Есть | Нет |
| Накладные расходы | Высокие | Низкие |
| Скорость передачи | Медленнее | Быстрее |
| Применение | Веб, почта, передача файлов, SSH | Стриминг, игры, VoIP, DNS, DHCP |

Это основные типы записей DNS (Domain Name System), используемые для разрешения доменных имен в соответствующие IP-адреса и другие связанные данные.