

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего
образования

Санкт-Петербургский национальный исследовательский университет ИТМО
Мегафакультет трансляционных информационных технологий

Факультет информационных технологий и программирования

Практическая работа №7. DNS

По дисциплине «Телекоммуникационные системы и технологии»

Выполнили:

студенты группы №М3306

Тимофеев Вячеслав

Проверил:

Самигуллин



УНИВЕРСИТЕТ ИТМО

Цель работы: закрепить понимание принципов работы DNS, получить практические навыки использования утилит работы с серверами системы DNS и конфигурирования DNS сервера на платформе Linux

Артефакты выполнения:

Часть 2

1) dig www.itmo.ru

```
[root@c7-1 ~]# dig www.itmo.ru

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3670
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.itmo.ru.                IN      A

;; ANSWER SECTION:
www.itmo.ru.                7200    IN      A      51.250.54.78

;; AUTHORITY SECTION:
itmo.ru.                    7200    IN      NS      ns5.itmo.ru.
itmo.ru.                    7200    IN      NS      ns3.itmo.ru.
itmo.ru.                    7200    IN      NS      ns.itmo.ru.
itmo.ru.                    7200    IN      NS      ns2.itmo.ru.

;; ADDITIONAL SECTION:
ns5.itmo.ru.                7200    IN      A      51.250.74.203
ns3.itmo.ru.                7200    IN      A      77.234.216.2
ns.itmo.ru.                 7200    IN      A      77.234.194.2
ns2.itmo.ru.                7200    IN      A      77.234.221.75

;; Query time: 30 msec
;; SERVER: 172.28.16.1#53(172.28.16.1)
```

2)

а) Вывести только результат разрешения www.itmo.ru (только IP-адрес)

```
[root@c7-1 ~]# dig www.itmo.ru +short
51.250.54.78
```

б) Вывести на экран подробную информацию о разрешении имени с выводом всех промежуточных серверов, определить какой именно DNS сервер вернул адрес IP хоста

```
[root@c7-1 ~]# dig www.itmo.ru +trace
; <<> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<> www.itmo.ru +trace
;; global options: +cmd
.      439839 IN      NS      m.root-servers.net.
.      439839 IN      NS      b.root-servers.net.
.      439839 IN      NS      g.root-servers.net.
.      439839 IN      NS      l.root-servers.net.
.      439839 IN      NS      k.root-servers.net.
.      439839 IN      NS      d.root-servers.net.
.      439839 IN      NS      a.root-servers.net.
.      439839 IN      NS      e.root-servers.net.
.      439839 IN      NS      c.root-servers.net.
.      439839 IN      NS      i.root-servers.net.
.      439839 IN      NS      j.root-servers.net.
.      439839 IN      NS      h.root-servers.net.
.      439839 IN      NS      f.root-servers.net.
.      439839 IN      NS      b.root-servers.net.
.      439839 IN      NS      g.root-servers.net.
.      439839 IN      NS      l.root-servers.net.
.      439839 IN      NS      k.root-servers.net.
.      439839 IN      NS      d.root-servers.net.
.      439839 IN      NS      a.root-servers.net.
.      439839 IN      NS      e.root-servers.net.
.      439839 IN      NS      c.root-servers.net.
.      439839 IN      NS      i.root-servers.net.
.      439839 IN      NS      j.root-servers.net.
.      439839 IN      NS      h.root-servers.net.
.      439839 IN      NS      f.root-servers.net.
.      439839 IN      NS      m.root-servers.net.
;; Received 813 bytes from 172.28.16.1#53(172.28.16.1) in 7 ms
ru.    172800 IN      NS      a.dns.ripn.net.
ru.    172800 IN      NS      e.dns.ripn.net.
ru.    172800 IN      NS      f.dns.ripn.net.
ru.    172800 IN      NS      d.dns.ripn.net.
ru.    172800 IN      NS      b.dns.ripn.net.
ru.    86480  IN      DS      43786 8 2 3C597475449908C74419D5F69E32D8C9B18EA48CBDA433C09A356191 28CED431
ru.    86480  IN      RRSIG   DS 8 1 86480 2024041908000 2024040808000 5513 . P1501bb74KL1HY5a5t13E3at0AUBE10B9yf4ZvwhHfE1KB0s15Wj zDyGci:WVQ5pLr8B1f61YqKL26vHhQcJfIzuAg08tB1fccN848L6/ IZfhQKABHdHWP0omKa/GeerHWit1Ne1ySTDzGtSwj
LM4f1pJ4tSEy3j kN1hSe7UJ3vMH06iHhCnqla+gt1Ctj+3jLRf5q9kKcudr8t9A/d RaH+Puy23k1set753D96210pLQ1VXwV68GfDhxcPp0H+rvQo77K0z Q1o8pw5Enrp77d46mEahwJcuH+P2H6SLKvF+Ew08835AVoc93va8B8 WvZExm=
;; Received 687 bytes from 198.41.0.4#53(a.root-servers.net) in 35 ms
itmo.ru. 345600 IN      NS      ns.itmo.ru.
itmo.ru. 345600 IN      NS      ns3.itmo.ru.
itmo.ru. 345600 IN      NS      ns5.itmo.ru.
j20c8qkdhua3umk8t289ff60u2q01.ru. 3600 IN NS0C 1 1 0 - 221C11SHOOTMDEKPRW1D8AQL4884M6 NS SOA RRSIG DNSKEY NS0C3PARAM
j20c8qkdhua3umk8t289ff60u2q01.ru. 3600 IN NS0C 8 2 3600 202405086135509 20240408042095 52263 ru. K4F+ry47pVRU76v6iXZ/kt9vXRvXb1tFQ4bn1koLpLvtpyQq2dtV03Y 9hc8NxxKdeJ0j1LHITnPNBQfbbBuk0pvn7Af7eY15cJo0828xikAxtVH dorD2tt88dVHF582TtTCLAZNB2U11/K6b
tn/E4s/1ZGds3Qkce/9yy8 CpM=
4qj9cuih1prlB1srnvev8a49g4s04.ru. 3600 IN NS0C 1 1 0 - 4055GUB220P82AUVPLR3J0IKAREULV8Z NS DS RRSIG
4qj9cuih1prlB1srnvev8a49g4s04.ru. 3600 IN RRSIG NS0C 8 2 3600 20240421140308 20240316001932 52263 ru. 8mQ60xJ8yUucqf1lgPbeCH12unppq6k1tPiQrtcb98ICXREnB0oxpn Rohd8UCPtUoPsp60G32Yzz1iCV8CnB7J0oTP9KABBMuJStYeyOyIxpI Ee67wiknJzFHT0iYjut46y+uuf0wuK6zy
bFk59twk7jF611c1D8ULc1 Z6M=
;; Received 624 bytes from 193.232.156.17#53(f.dns.ripn.net) in 126 ms
www.itmo.ru. 7200 IN      A      51.250.54.78
itmo.ru. 7200 IN      NS      ns5.itmo.ru.
itmo.ru. 7200 IN      NS      ns.itmo.ru.
itmo.ru. 7200 IN      NS      ns2.itmo.ru.
itmo.ru. 7200 IN      NS      ns3.itmo.ru.
;; Received 191 bytes from 51.250.74.203#53(ns5.itmo.ru) in 19 ms
```

с) Вывести конфигурационную запись (SOA) домена itmo.ru, определить, значения каждого из числовых параметров записи

```
itmo.ru. 35972 IN      SOA      ns.itmo.ru. hostmaster.itmo.ru. 2024012202 3600 3600 1800 86400 3600
[root@c7-1 ~]# dig itmo.ru SOA +noall +answer +multiline
; <<> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<> itmo.ru SOA +noall +answer +multiline
;; global options: +cmd
itmo.ru. 3599 IN SOA ns.itmo.ru. hostmaster.itmo.ru. (
    2024012262 ; serial
    3600       ; refresh (1 hour)
    1800       ; retry (30 minutes)
    86400      ; expire (1 day)
    3600       ; minimum (1 hour)
)
```

serial – серийный номер зоны

refresh – время обновления реплики

retry – время до повторной попытки

expire – время работы реплики без обновления

minimum – минимальный TTL

д) Определить, какие сервера обрабатывают почту домена itmo.ru

```
[root@c7-1 ~]# dig itmo.ru MX +short
10 emx.mail.ru.
```

e) Определить, какие DNS сервера обслуживают зону itmo.ru и их IP-адреса

```
[[root@c7-1 ~]# dig itmo.ru NS

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> itmo.ru NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36426
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 8

;; QUESTION SECTION:
;itmo.ru.                IN      NS

;; ANSWER SECTION:
itmo.ru.                 7200    IN      NS      ns5.itmo.ru.
itmo.ru.                 7200    IN      NS      ns.itmo.ru.
itmo.ru.                 7200    IN      NS      ns2.itmo.ru.
itmo.ru.                 7200    IN      NS      ns3.itmo.ru.

;; AUTHORITY SECTION:
itmo.ru.                 7200    IN      NS      ns.itmo.ru.
itmo.ru.                 7200    IN      NS      ns2.itmo.ru.
itmo.ru.                 7200    IN      NS      ns3.itmo.ru.
itmo.ru.                 7200    IN      NS      ns5.itmo.ru.

;; ADDITIONAL SECTION:
ns5.itmo.ru.             7200    IN      A       51.250.74.203
ns.itmo.ru.              7200    IN      A       77.234.194.2
ns2.itmo.ru.             7200    IN      A       77.234.221.75
ns3.itmo.ru.             7200    IN      A       77.234.216.2
ns.itmo.ru.              7200    IN      A       77.234.194.2
ns2.itmo.ru.             7200    IN      A       77.234.221.75
ns3.itmo.ru.             7200    IN      A       77.234.216.2
ns5.itmo.ru.             7200    IN      A       51.250.74.203

;; Query time: 11 msec
;; SERVER: 172.28.16.1#53(172.28.16.1)
```

f) Значение записи в зоне обратного просмотра

```
[[root@c7-1 ~]# dig -x 77.88.55.242

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> -x 77.88.55.242
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47516
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;242.55.88.77.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
242.55.88.77.in-addr.arpa. 296    IN      PTR      ya.ru.

;; AUTHORITY SECTION:
55.88.77.in-addr.arpa.    13306   IN      NS      ns4.yandex.ru.
55.88.77.in-addr.arpa.    13306   IN      NS      ns3.yandex.ru.

;; ADDITIONAL SECTION:
ns4.yandex.ru.            264959  IN      A       77.88.21.1
ns3.yandex.ru.            264959  IN      A       87.250.250.1

;; Query time: 4 msec
;; SERVER: 172.28.16.1#53(172.28.16.1)
```

g) Определить количество серверов, поддерживающих корневую зону

```
[root@c7-1 ~]# dig NS . +short
f.root-servers.net.
m.root-servers.net.
b.root-servers.net.
g.root-servers.net.
l.root-servers.net.
k.root-servers.net.
d.root-servers.net.
a.root-servers.net.
e.root-servers.net.
c.root-servers.net.
i.root-servers.net.
j.root-servers.net.
h.root-servers.net.
[root@c7-1 ~]# dig NS . +short | wc -l
13
```

Часть 3

```
[[root@c7-1 ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
    listen-on port 53 { 127.0.0.1; 10.0.0.1; };
    // listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    recursing-file "/var/named/data/named.recursing";
    secroots-file "/var/named/data/named.secroots";
    allow-query { localhost; 10.0.0.0/24; };
    allow-recursion { localhost; 10.0.0.0/24; };

    /*
     - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
     - If you are building a RECURSIVE (caching) DNS server, you need to enable
       recursion.
     - If your recursive DNS server has a public IP address, you MUST enable access
       control to limit queries to your legitimate users. Failing to do so will
       cause your server to become part of large scale DNS amplification
       attacks. Implementing BCP38 within your network would greatly
       reduce such attack surface
    */
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.root.key";

    managed-keys-directory "/var/named/dynamic";

    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";

    version "My Own DNS Server";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Проверим разрешение имён на хосте c7-2

```
[root@c7-2 ~]# dig www.itmo.ru

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38761
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
;; QUESTION SECTION:
;www.itmo.ru.                IN      A

;; ANSWER SECTION:
www.ITMO.ru.                7069    IN      A      51.250.54.78

;; AUTHORITY SECTION:
ITMO.ru.                    345469  IN      NS      ns.itmo.RU.
ITMO.ru.                    345469  IN      NS      ns5.itmo.RU.
ITMO.ru.                    345469  IN      NS      ns3.itmo.RU.

;; ADDITIONAL SECTION:
ns3.ITMO.ru.                345469  IN      A      77.234.216.2
ns5.ITMO.ru.                345469  IN      A      51.250.74.203
ns.ITMO.ru.                 345469  IN      A      77.234.194.2

;; Query time: 1 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)
```

```
[root@c7-2 ~]# dig @10.0.0.1 ch txt version.bind +short
"My Own DNS Server"
```

Часть 4

```
zone "KEG.local" IN {
    type master;
    file "/var/named/KEG.local.db";
    allow-transfer { none; };
    allow-update { any; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

[[root@c7-1 ~]# named-checkconf
[[root@c7-1 ~]#
```

```
[[root@c7-1 ~]# cat /var/named/KEG.local.db
$TTL 300
@      IN      SOA ns1.KEG.local. hostmaster.KEG.local. (
                                2024040618 ; serial
                                43200      ; refresh
                                3600       ; retry
                                3600000    ; expire
                                300       ; minimum

@      IN      NS ns1.KEG.local.
ns1    IN      A  10.0.0.1
gate   IN      A  10.0.0.1
www    IN      CNAME gate.KEG.local.

[[root@c7-1 ~]# named-checkzone KEG.local /var/named/KEG.local.db
zone KEG.local/IN: loaded serial 2024040618
OK
```

Проверим, что всё работает

```
[root@c7-2 ~]# dig KEG.local

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> KEG.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61793
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;KEG.local.                IN      A

;; AUTHORITY SECTION:
KEG.local.                300     IN      SOA     ns1.KEG.local. hostmaster.KEG.local. 2024040618 43200
0 3600 3600000 300

;; Query time: 1 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)
```

```
[root@c7-2 ~]# dig NS KEG.local

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> NS KEG.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48541
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;KEG.local.                IN      NS

;; ANSWER SECTION:
KEG.local.                300     IN      NS      ns1.KEG.local.

;; ADDITIONAL SECTION:
ns1.KEG.local.            300     IN      A       10.0.0.1

;; Query time: 1 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)
```

```
[root@c7-2 ~]# dig ns1.KEG.local

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> ns1.KEG.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12992
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns1.KEG.local.            IN      A

;; ANSWER SECTION:
ns1.KEG.local.            300     IN      A       10.0.0.1

;; AUTHORITY SECTION:
KEG.local.                300     IN      NS      ns1.KEG.local.

;; Query time: 1 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)
```

```
[root@c7-2 ~]# dig NS KEG.local SOA +noall +answer +multiline
;; Warning, extra type option

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> NS KEG.local SOA +noall +answer +multiline
;; global options: +cmd
KEG.local.                300 IN SOA ns1.KEG.local. hostmaster.KEG.local. (
                                2024040618 ; serial
                                43200      ; refresh (12 hours)
                                3600      ; retry (1 hour)
                                3600000   ; expire (5 weeks 6 days 16 hours)
                                300       ; minimum (5 minutes)
                                )
```

```

[root@c7-2 ~]# dig gate.KEG.local

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> gate.KEG.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51032
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gate.KEG.local.                IN      A

;; ANSWER SECTION:
gate.KEG.local.                300     IN      A      10.0.0.1

;; AUTHORITY SECTION:
KEG.local.                     300     IN      NS      ns1.KEG.local.

;; ADDITIONAL SECTION:
ns1.KEG.local.                 300     IN      A      10.0.0.1

;; Query time: 1 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)

```

```

[root@c7-2 ~]# dig www.KEG.local

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> www.KEG.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22730
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.KEG.local.                 IN      A

;; ANSWER SECTION:
www.KEG.local.                 300     IN      CNAME   gate.KEG.local.
gate.KEG.local.                 300     IN      A      10.0.0.1

;; AUTHORITY SECTION:
KEG.local.                     300     IN      NS      ns1.KEG.local.

;; ADDITIONAL SECTION:
ns1.KEG.local.                 300     IN      A      10.0.0.1

;; Query time: 1 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)

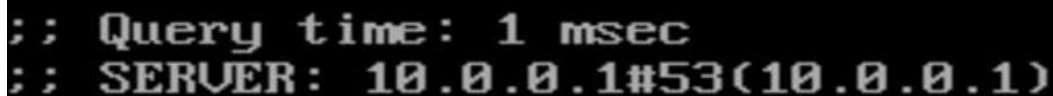
```


Вопросы и задания:

1) Опишите, как в выводе команды **dig** соотносятся секции **HEADER**, **QUESTION SECTION**, **ANSWER SECTION**, **AUTHORITY SECTION**, **SERVER**, **WHEN** и **MSG SIZE** с полями секции **HEADER**. Опишите назначение каждой секции

- **HEADER** – секция, отображающая информацию о версии утилиты, ID запроса, полученных ошибках, использованных флагах вывода и количестве записей в других секциях
- **QUESTION SECTION** – секция, которая отображает текущий запрос
- **ANSWER SECTION** – секция, в которой отображается результат обработки созданного запроса
- **AUTHORITY SECTION** – показывает имена DNS-адресов, обработавших запрос
- **ADDITIONAL SECTION** – показывает IP-адреса этих серверов
- **SERVER** – IP-адрес и порт отвечающего DNS-сервера
- **WHEN** – время запуска команды
- **MSG SIZE** - размер ответа от DNS-сервера

2) Как по ответу утилиты **dig** в Части 3 можно понять, что ответ получен именно от вашего кэширующего DNS сервера?



```
:: Query time: 1 msec  
:: SERVER: 10.0.0.1#53(10.0.0.1)
```

Вывод: закрепили понимание принципов работы DNS, получили практические навыки использования утилит работы с серверами системы DNS и конфигурирования DNS сервера на платформе Linux (dig)